MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA
CURSO DE GRADUAÇÃO EM CIBERSEGURANÇA

Projeto Pedagógico

Graduação em Cibersegurança

Versão Curricular: 2025-v01

FACULDADE DE ENGENHARIA ELÉTRICA (FEELT)
Campus Santa Mônica, Uberlândia/MG, Brasil 2025
http://www.feelt.ufu.br

PROJETO PEDAGÓGICO DO CURSO DE GRADUAÇÃO EM CIBERSEGURANÇA

REITOR
Prof. Dr. Carlos Henrique de Carvalho

VICE-REITORA
Profa. Dra. Catarina Azeredo

PRÓ-REITOR DE GRADUAÇÃO
Prof. Dr. Waldenor Barros Moraes Filho

PRÓ-REITOR DE PESQUISA E PÓS-GRADUAÇÃO
Prof. Dr. Thiago Gonçalves Paluma Rocha

PRÓ-REITOR DE EXTENSÃO E CULTURA
Prof. Dr. Florisvaldo Paulo Ribeiro Júnior

PRÓ-REITOR DE ADMINISTRAÇÃO E PLANEJAMENTO
Prof. Dr. Vinicius Vieira Favaro

PRÓ-REITORA DE ASSISTÊNCIA ESTUDANTIL
Profa. Dra. Luciana Saraiva da Silva

PRÓ-REITOR DE GESTÃO DE PESSOAS
Prof. Dr. Sebastião Elias da Silveira

DIRETOR DA FACULDADE DE ENGENHARIA ELÉTRICA
Prof. Dr. Lorenço Santos Vasconcelos

PRESIDENTE DA COMISSÃO PROPONENTE
Prof. Dr. Marcelo Rodrigues de Sousa

Comissão de elaboração deste Projeto Pedagógico:

- Prof. Dr. Marcelo Rodrigues de Sousa – Presidente;
- Prof. Dr. Igor Sousa Peretta;
- Prof. Dr. Kil Jin Brandini Park;
- Prof. Dr. Márcio José da Cunha.

Uberlândia/MG, Brasil 2025

Sumário

1 Identificação do Curso

DENOMINAÇÃO
Cibersegurança

GRAU
Bacharelado

MODALIDADE
Presencial

TURNO DE OFERTA
Noturno

REGIME ACADÊMICO
Semestral

TITULAÇÃO
Bacharel em Cibersegurança

CARGA HORÁRIA
3.200 horas

DURAÇÃO
8 semestres (4 anos)

TEMPO MÁXIMO DE INTEGRALIZAÇÃO CURRICULAR
12 semestres (6 anos)

INGRESSO
Semestral

NÚMERO DE VAGAS OFERTADAS
30 vagas semestrais;
(total de 60 vagas anuais)

Logomarca do Curso

Logomarca criada em outubro de 2025 pelo docente Igor Santos Peretta. Disponibilizado para o uso do curso de Cibersegurança nos termos da licença **CC-BY-ND 4.0**. A logomarca está disponível para download em:

http://www.feelt.ufu.br/Ciberseguranca/logotipo

2 Endereços

Universidade Federal de Uberlândia
Av. João Naves de Ávila, 2121 Campus Santa Mônica
Bloco 3P - Reitoria, CEP 38400-902, Uberlândia/MG
Telefone: (34) 3239 2911
http://www.ufu.br

Faculdade de Engenharia Elétrica
Av. João Naves de Ávila, 2121 Campus Santa Mônica
Bloco 3N - Sala 3N101, CEP 38400-902, Uberlândia/MG
Telefone: (34) 3239 4701
http://www.feelt.ufu.br

Coordenação do Curso de Cibersegurança
Av. João Naves de Ávila, 2121 Campus Santa Mônica
Bloco 3N - Sala 3N103, CEP 38400-902, Uberlândia/MG
Telefone: (34) 3239 4776
http://www.feelt.ufu.br/graduacao/ciberseguranca
E-mail: cocia@eletrica.ufu.br

3 Apresentação

O presente Projeto Pedagógico do Curso (PPC) de Bacharelado em *Cibersegurança* propõe uma formação contemporânea, interdisciplinar e orientada a problemas reais, apta a responder a desafios estratégicos do país nas frentes de proteção de dados, resiliência cibernética, automação inteligente e inovação responsável. O curso articula sólidos fundamentos científicos com competências profissionais e sociais, integrando ensino, pesquisa e extensão em diálogo permanente com o setor produtivo e com as demandas do serviço público.

A proposta pedagógica parte de três eixos complementares: (i) **fundamentos** em computação, matemática, sistemas, redes e ciência de dados; (ii) **competências de cibersegurança** que percorrem o ciclo de prevenção, detecção, resposta e recuperação (governança, risco e conformidade; arquitetura segura; criptografia aplicada; segurança de redes, aplicações e dados; *threat intelligence*; engenharia de privacidade); e (iii) **inteligência artificial** em toda a sua cadeia (modelagem, aprendizado de máquina, aprendizado profundo, MLOps, IA confiável), enfatizando aspectos éticos, jurídicos e sociotécnicos.

Metodologicamente, o curso adota um modelo centrado no estudante e orientado a projetos, com *sprints* e entregas incrementais, que favorecem a aprendizagem ativa, o pensamento crítico e a comunicação técnica. As atividades curriculares são organizadas para promover integração horizontal (entre disciplinas do mesmo período) e vertical (ao longo dos períodos), culminando em desafios integradores que simulam contextos de alta complexidade e colaboração multidisciplinar. A avaliação privilegia evidências de aprendizagem por meio de artefatos técnicos, relatórios, demonstrações e portfólios, com *feedback* formativo contínuo.

O perfil do egresso almejado é o de um profissional capaz de:

- conceber, analisar e implementar soluções seguras de software, dados e infraestrutura, com base em princípios de *security-by-design* e *privacy-by-default*;

- empregar métodos de IA para apoiar decisões, automatizar processos e aprimorar a defesa cibernética, garantindo rastreabilidade, robustez e conformidade;
- atuar de forma ética e responsável, considerando marcos regulatórios, direitos fundamentais e impactos sociais, ambientais e econômicos da tecnologia;
- comunicar-se com clareza com públicos técnicos e não técnicos, trabalhar em equipes diversas e liderar iniciativas de inovação.

A estrutura curricular prevê integração sistemática com pesquisa e extensão, uso de laboratórios especializados, participação em comunidades técnicas e iniciativas de empreendedorismo tecnológico. Parcerias institucionais e convênios com organizações públicas e privadas potencializam cenários reais de aprendizagem, estágios e projetos *capstone*. Com isso, o curso se compromete a formar profissionais preparados para um ecossistema digital em rápida transformação, sem abrir mão de rigor acadêmico, compromisso ético e responsabilidade social.

Curso Inovador

O curso **Cibersegurança**, modalidade bacharelado, propõe uma **quebra de paradigma** na oferta de cursos com carga horária igual ou superior a 3.200 horas. A matriz concentra-se em 9 módulos distribuídos ao longo de 4 anos, favorecendo profundidade, integração entre conteúdos e foco em competências. Graças à curadoria estruturada de conhecimentos disponíveis na *WEB* e ao emprego de sistemas de *inteligência artificial* como tutores de aprendizagem e apoio à docência, o curso pode ser ministrado plenamente por um corpo de apenas 13 (treze) professores 40h[1], em regime de 40h semanais, preservando qualidade acadêmica, acompanhamento formativo e aderência a boas práticas pedagógicas ativas (projetos, *sprints*, avaliação contínua).

[1] Considerando os cursos atuais de tecnologia da Universidade Federal de Uberlândia — Ciência da Computação, Sistemas de Informação e Engenharia de Computação —, que apresentam, respectivamente, 50, 45 e 54 disciplinas. Em regra, um docente ministra 3 disciplinas de graduação por semestre; assim, inferem-se mínimos de 17, 15 e 18 docentes para implementar, em cada caso, sem considerar as diversas áreas de conhecimento das disciplinas, a coordenação, o coordenador de estágio supervisionado e a extensão universitária. Na realidade, esses números de professores necessários aos cursos, no padrão atual, são bem maiores. Por exemplo, quando o curso de Sistemas de Informação foi criado, foram contratados pelo REUNI 26 (vinte e seis) professores para sua efetivação.

Oferta Noturna e Impacto Social

A decisão de ofertar o curso no **período noturno** é estratégica e inclusiva. Em primeiro lugar, amplia o *acesso* e a *equidade*, permitindo que estudantes que trabalham em horário comercial — especialmente de camadas sociais historicamente sub-representadas — ingressem e permaneçam na universidade. Em segundo lugar, a oferta noturna favorece a *aprendizagem situada*: muitos discentes atuam em *service desks*, *NOCs*, equipes de desenvolvimento ou áreas administrativas durante o dia e trazem, à noite, problemas reais para os laboratórios, acelerando o ciclo *aprender–aplicar–refletir*. Em terceiro lugar, a modalidade noturna *aproxima universidade e setor produtivo*: estágios e projetos *in-company* podem ocorrer em horário comercial, enquanto as *sprints* de integração, os *code reviews* e as defesas técnicas se realizam no turno da noite, com participação remota de mentores da indústria.

Do ponto de vista **pedagógico**, o desenho noturno incentiva a adoção sistemática de recursos assíncronos (repositórios, *labs*, trilhas em vídeo, *notebooks* reprodutíveis, *rubrics* claras) e de *IA tutora* para apoio integral (dentro e fora de sala), promovendo *feedback* imediato e eficiente para o estudante. Do ponto de vista **logístico**, o planejamento contempla janelas ampliadas de laboratório, biblioteca e suporte de TI, além de protocolos de segurança e mobilidade no campus. Por fim, há um **ganho formativo** específico em cibersegurança: operações, monitoração e resposta a incidentes são atividades continuamente demandadas fora do horário comercial; treinar equipes no período noturno aproxima o curso das rotinas reais de *SOC*, *blue/purple teams* e plantões de infraestrutura, fortalecendo empregabilidade e prontidão profissional.

Agradecimentos e Inspirações

Reconhecemos, com gratidão, a inspiração pedagógica da **Escola da Ponte** (Portugal) e do seu professor emérito **José Pacheco**[2], cuja defesa da autonomia discente, da aprendizagem por projetos e da corresponsabilidade na construção do conhecimento influenciou decisivamente este desenho curricular.

Agradecemos, igualmente, ao exemplo da ***Alpha School*** (EUA) e do Instituto de Tecnologia e Liderança (INTELI), cuja integração competente entre tecnologia educacional, personalização do percurso e métricas de aprendizagem orientadas a resultados reforça nossa proposta de ensino inovador, inclusivo e conectado a desafios reais.

Registramos também nosso agradecimento ao físico **Richard P. Feynman** e às suas reflexões sobre o ensino no Brasil — especialmente relatadas em *"O Senhor Está Brincando, Sr. Feynman!"*[1] —, que denunciaram práticas de me-

morização desvinculadas da compreensão. Sua defesa de uma aprendizagem baseada em curiosidade, experimentação e entendimento conceitual inspira-nos a cultivar competências profundas, transferíveis e eticamente orientadas à solução de problemas reais.

4 Justificativa e Histórico

4.1 Justificativa

O curso *Cibersegurança*, modalidade bacharelado, justifica-se pela convergência de três vetores: (i) a centralidade estratégica dos sistemas digitais para a economia, a administração pública e os direitos fundamentais; (ii) a expansão contínua da superfície de ataque decorrente da transformação digital (nuvem, mobilidade, internet das coisas, 5G, automação industrial e finanças digitais); e (iii) a maturação de métodos de Inteligência Artificial (IA) capazes de ampliar, acelerar e qualificar a defesa cibernética, do planejamento à resposta a incidentes, preservando privacidade, conformidade regulatória e valores éticos.

Do ponto de vista formativo, o curso responde a lacunas recorrentes observadas por organizações públicas e privadas: dificuldade em encontrar profissionais que dominem simultaneamente *fundamentos rigorosos de computação*, *engenharia segura de software e dados* e *aplicação responsável de IA*. A proposta integra esses eixos em um currículo orientado a competências, com aprendizagem baseada em projetos e avaliação por evidências (portfólios, artefatos técnicos e relatórios), promovendo autonomia intelectual, pensamento crítico e comunicação técnica eficaz para públicos diversos.

A opção por ofertá-lo no **período noturno** reforça sua relevância social e aderência às práticas do setor. Em termos de *acesso* e *equidade*, amplia a participação de estudantes que trabalham em horário comercial — historicamente sub-representados na educação superior — e viabiliza trajetórias formativas sem ruptura de vínculos laborais. Em termos **profissionais**, aproxima a formação das rotinas reais da cibersegurança: *monitoramento*, resposta a incidentes, plantões de infraestrutura e operações de *SOC*/*blue team* ocorrem, com frequência, fora do horário comercial. Treinar no turno da noite, com laboratórios estendidos, simulações e *tabletops* nesse mesmo período, melhora a prontidão operacional do egresso. Em termos **pedagógicos**, o desenho noturno estimula o uso estruturado de recursos assíncronos (trilhas, *notebooks* reprodutíveis, repositórios de

labs) e de *tutores de IA*, garantindo feedback frequente e flexibilização responsável; ao mesmo tempo, facilita parcerias *in-company* durante o dia e mentoria da indústria nas sessões noturnas.

No plano social e regulatório, a formação dialoga com marcos legais e boas práticas de proteção de dados, segurança da informação e governança digital, difundindo a cultura de *privacy-by-default* e *security-by-design*. Ao articular ciência, tecnologia e impacto público, o curso contribui para reduzir assimetrias de segurança, sustentar a continuidade de serviços essenciais, preservar a integridade de cadeias produtivas e promover ecossistemas digitais confiáveis, inclusivos e sustentáveis.

Em síntese, a relevância do curso decorre (a) da demanda consistente por profissionais com visão sistêmica de risco, (b) da necessidade de incorporar IA de forma auditável e ética aos processos de defesa cibernética, e (c) do compromisso universitário com pesquisa, inovação e extensão voltadas a problemas reais de alta complexidade — agora potencializado por uma **oferta noturna** que amplia o acesso, eleva a aderência ao mundo do trabalho e intensifica o realismo dos cenários de aprendizagem.

4.2 Histórico

A criação do curso *Cibersegurança*, modalidade bacharelado, resulta da trajetória consolidada de ensino, pesquisa e extensão da Faculdade de Engenharia Elétrica (FEELT) da Universidade Federal de Uberlândia (UFU), reconhecida nacionalmente pela excelência nas áreas de Computação e Engenharia. Em particular, o Departamento de Engenharia de Computação e Inovação em Engenharia acumula cerca de quatro décadas de experiência na formação de profissionais de tecnologia, integrando de modo consistente fundamentos teóricos, prática laboratorial, inovação e empreendedorismo.

Nesse contexto, o novo curso constitui uma evolução natural do projeto acadêmico da FEELT, alinhando-se às transformações do ecossistema digital e à demanda crescente por especialistas capazes de atuar de forma integrada em segurança cibernética, inteligência artificial e governança tecnológica. Sua concepção pedagógica combina o legado de rigor acadêmico da UFU com arranjos curriculares contemporâneos — modulares, interdisciplinares, orientados por competências e conectados a problemas reais — de modo a favorecer a aprendizagem ativa e a inserção qualificada dos egressos.

A presente proposta decorre dessa trajetória institucional de excelência em Computação e Engenharia, lastreada na integração ensino–pesquisa–extensão, na formação baseada em projetos e em parcerias com órgãos públicos, empresas e organizações da sociedade civil. O desenho curricular foi estruturado para refletir:

- a atualização contínua do estado da arte em segurança de software, redes, dados e infraestrutura, articulada a práticas de laboratório e ambientes de simulação;
- a incorporação transversal de IA (aprendizado de máquina, aprendizado profundo, MLOps e IA confiável/responsável) aos processos de engenharia segura e ao ciclo de vida de soluções digitais;
- a ênfase em governança, risco e conformidade (GRC), incluindo gestão do ciclo de vida de vulnerabilidades, observabilidade, resposta a incidentes, proteção de dados e privacidade;
- a adoção de metodologias ativas (projetos integradores, *sprints*, estudos de caso) e avaliação formativa baseada em evidências (artefatos, relatórios, demonstrações e portfólios);
- o fortalecimento de laboratórios, *cyber ranges* e ambientes de experimentação com acesso a cenários realistas e desafios alinhados ao ecossistema de inovação.

Esse movimento consolida práticas pedagógicas já validadas pela FEELT e as alinha às competências profissionais emergentes, às Diretrizes Curriculares vigentes e às necessidades estratégicas do país em soberania digital, confiabilidade e transformação tecnológica.

O curso *Cibersegurança* estará vinculado à Faculdade de Engenharia Elétrica (FEELT) da UFU, unidade responsável por sua gestão acadêmica, pedagógica e administrativa. A FEELT abriga atualmente seis cursos presenciais de graduação — cinco no campus Santa Mônica, em Uberlândia/MG (Engenharia Elétrica; Engenharia Biomédica; Engenharia de Computação; Engenharia Eletrônica e de Telecomunicações; Engenharia de Controle e Automação) e um no campus Patos de Minas/MG (Engenharia Eletrônica e de Telecomunicações) — além de dois programas de pós-graduação *stricto sensu*: o Programa de Pós-Graduação em Engenharia Elétrica e o Programa de Pós-Graduação em Engenharia Biomédica.

Com a aprovação do novo Regimento Interno da FEELT (dezembro de 2023), a estrutura organizacional da unidade foi reorganizada em Departamentos Acadêmicos, que substituíram os antigos núcleos temáticos. Cada departamento é responsável por atividades de ensino, pesquisa e extensão em áreas específicas do conhecimento, organizando a atuação docente e a oferta de disciplinas para os diversos cursos de graduação e pós-graduação.

Os departamentos atualmente constituídos na FEELT são:

- Departamento de Sistemas de Potência e Energia (DSPE)
- Departamento de Engenharia Biomédica (DEB)
- Departamento de Computação e Inovação em Engenharia (DCIE)

- Departamento de Sistemas de Controle e Automação (DSCA)
- Departamento de Eletrônica e Telecomunicações (DETEL)
- Departamento de Máquinas Elétricas e Materiais (DMEM)

O curso *Cibersegurança* terá sua base acadêmica integrada ao Departamento de Computação e Inovação em Engenharia (DCIE), embora conte com a contribuição voluntária de docentes de outros departamentos da FEELT, bem como de unidades acadêmicas externas, como o Instituto de Matemática, o Instituto de Física e a Faculdade de Computação (FACOM).

A estrutura da FEELT também favorece a participação dos(as) discentes em programas de formação complementar, como mobilidade acadêmica nacional e internacional, Empresa Júnior, Programa de Educação Tutorial (PET), monitoria, iniciação científica (PIBIC, PIVIC/UFU), projetos de extensão e programas de cooperação acadêmica (ex: Capes/Brafitec). No âmbito da pós-graduação, os(as) docentes da FEELT atuam em linhas de pesquisa avançadas nas áreas de inteligência artificial, sistemas embarcados, processamento de sinais, realidade virtual, bioengenharia, fontes alternativas de energia, entre outras.

Essa estrutura acadêmica consolidada e integrada garante ao Bacharelado em *Cibersegurança* uma base sólida para o sucesso de seus futuros egressos.

4.3 Relação entre Sociedade e o Curso

O curso está intrinsecamente conectado às demandas regionais e nacionais por infraestrutura digital segura, serviços confiáveis e inovação orientada por dados. Sua pertinência social se expressa em quatro dimensões complementares:

1. **Desenvolvimento econômico e produtividade:** sustentação da continuidade de negócios, proteção de cadeias de suprimento e aumento da competitividade em setores intensivos em software e dados, com impactos diretos em eficiência operacional, qualidade de serviços e atração de investimentos.

2. **Interesse público e cidadania digital:** preservação de dados pessoais e sensíveis, fortalecimento da resiliência de serviços críticos (saúde, energia, finanças, educação, administração pública) e promoção de ambientes digitais acessíveis, confiáveis e inclusivos, alinhados à legislação vigente e a padrões internacionais.

3. **Inovação e empreendedorismo:** estímulo à criação de soluções e *startups* em cibersegurança e IA aplicada (detecção de anomalias, *threat intelligence*, automação de respostas, *privacy engineering*), em sinergia com

parques tecnológicos, órgãos governamentais, setor produtivo e terceiro setor.

4. **Formação de capital humano especializado:** qualificação de egressos aptos a liderar projetos, elaborar políticas de segurança, traduzir requisitos legais em arquitetura técnica e comunicar riscos de forma clara a diferentes audiências, promovendo uma cultura de *security-by-design* e *privacy-by-default*.

A oferta **no período noturno** é estratégica para ampliar o acesso, a permanência e a relevância social da formação. Em termos de *equidade*, viabiliza o ingresso de estudantes que trabalham em horário comercial, permitindo mobilidade social sem ruptura de vínculos laborais.

Parcerias institucionais, convênios e projetos de pesquisa e extensão reforçam a inserção do curso em redes de cooperação, potencializando estágios, desafios tecnológicos, programas de inovação e *capstones*[1] orientados a problemas reais. Assim, a universidade cumpre seu papel na produção de conhecimento, na transferência de tecnologia e na formação de profissionais capazes de enfrentar os desafios contemporâneos de cibersegurança e IA com rigor científico, responsabilidade ética e compromisso social — agora com o diferencial de uma **oferta noturna** que amplia o acesso, aproxima-se do cotidiano das operações de segurança e potencializa a empregabilidade.

[1] Um projeto *capstone* é um trabalho final que consolida os conhecimentos e habilidades adquiridos durante a formação acadêmica, geralmente realizado no final do curso. Ele pode ter formatos variados — projeto prático, pesquisa aplicada, protótipo ou produto — e serve para aplicar o aprendizado em um contexto do mundo real, demonstrando competências para o mercado de trabalho.

5 Princípios e Fundamentos

O curso *Cibersegurança*, modalidade bacharelado, estrutura-se sobre fundamentos científicos, tecnológicos e sociotécnicos que orientam a formação integral do estudante e a contribuição do curso para a sociedade. Tais fundamentos articulam-se com a missão institucional, com políticas públicas educacionais e com as melhores práticas internacionais em educação em Computação, Segurança da Informação e IA responsável.

5.1 Fundamentos Formativos

- **Base científica sólida:** ênfase em fundamentos de computação, matemática, estatística, arquitetura de computadores, sistemas operacionais, redes, engenharia de software e ciência de dados como alicerce para competências avançadas em cibersegurança e IA.
- **Integração sistêmica hardware–software–dados:** visão de sistema de ponta a ponta, abrangendo camadas de hardware, firmware, sistemas, aplicações, dados e nuvem, com atenção a dependências, superfícies de ataque e requisitos não funcionais (segurança, privacidade, desempenho, disponibilidade).
- **Ciclo completo de segurança:** prevenção, detecção, resposta e recuperação, incluindo governança, risco e conformidade (GRC), *threat modeling*, criptografia aplicada, segurança de redes e aplicações, engenharia de privacidade (*privacy engineering*) e resiliência operacional.
- **IA aplicada e confiável:** modelagem, aprendizado de máquina e profundo, MLOps e avaliação de *trustworthiness* (robustez, explicabilidade, auditabilidade, segurança, segurança de *model supply chain*), com atenção a vieses, impacto social e marcos regulatórios.

- **Formação humanística e ética:** compreensão crítica dos impactos da tecnologia, desenvolvimento de pensamento sistêmico, comunicação técnica, trabalho colaborativo e responsabilidade social.

5.2 Princípios Pedagógicos

1. **Aprendizagem ativa e orientada a projetos:** uso de projetos integradores, *sprints* e desafios com problemas autênticos e avaliação por evidências (artefatos, relatórios, demonstrações e portfólios).
2. **Aprendizagem aberta e mediada por IA generativa:** uso pedagógico de recursos da Web (*OER commons*, repositórios científicos, dados públicos e conteúdos multimodais) e de LLMs como co-tutores para personalização do estudo, feedback imediato e prática guiada; desenvolvimento de literacia digital e "engenharia de prompts" para pesquisa eficaz; verificação crítica e triangulação de fontes (com registro de referências), mitigando vieses e "alucinações"; respeito à ética, à LGPD e à segurança dos dados; e promoção da autonomia, metacognição e inclusão por meio de trilhas adaptativas.
3. **Integração horizontal e vertical do currículo:** articulação entre componentes de um mesmo período (integração horizontal) e encadeamento progressivo de competências ao longo dos períodos (integração vertical), culminando em experiências *capstone*.
4. **Formação por competências (CBL):** construção de competências técnicas, analíticas, comunicacionais e éticas, com rubricas claras de desempenho e feedback formativo contínuo.
5. **Flexibilidade e atualização contínua:** conteúdos e práticas ajustados à evolução do estado da arte, às demandas do ecossistema produtivo e às políticas públicas, preservando o rigor acadêmico.
6. **Pesquisa, extensão e empreendedorismo:** indissociabilidade entre ensino, pesquisa e extensão; promoção de cultura de inovação, transferência tecnológica e interação com organizações públicas e privadas.

5.3 Princípios Éticos e Sociotécnicos

- **Segurança e privacidade por concepção:** adoção de *security-by-design* e *privacy-by-default* como princípios estruturantes de arquitetura, engenharia e operação de sistemas.

- **Conformidade e responsabilidade:** atenção a marcos legais e normativos aplicáveis (proteção de dados, segurança da informação, propriedade intelectual, acesso à informação), traduzindo requisitos em controles técnicos e processos verificáveis.
- **Transparência, explicabilidade e equidade:** desenvolvimento e uso responsável de IA, com registro de decisões, rastreabilidade de dados e modelos, mitigação de vieses e avaliação de impacto.
- **Inclusão e diversidade:** promoção de ambientes de aprendizagem acessíveis, plurais e antidiscriminatórios, valorizando diferentes trajetórias e perspectivas.
- **Sustentabilidade e bem público:** compromisso com soluções tecnológicas que respeitem recursos, favoreçam serviços essenciais, ampliem a confiança digital e reduzam assimetrias de segurança.

5.4 Coerência com a Missão e Visão da Universidade Federal de Uberlândia

O curso alinha-se à missão institucional de desenvolver ensino, pesquisa e extensão de forma integrada, socialmente referenciada e comprometida com valores democráticos e direitos fundamentais. A visão de ser referência regional, nacional e internacional em qualidade acadêmica e impacto social é materializada por meio de:

- **excelência científica e tecnológica** em cibersegurança e IA;
- **formação ética e cidadã** para atuação responsável em setores público e privado;
- **inserção qualificada** em redes de cooperação, laboratórios e ecossistemas de inovação.

5.5 Diretrizes Curriculares

- **Estrutura modular e iterativa:** unidades curriculares com objetivos claros, resultados de aprendizagem mensuráveis e progressão de complexidade.
- **Ambientes e laboratórios especializados:** infraestrutura para experimentação realista (redes, nuvem, *sandbox* de segurança, observabilidade, *MLOps*), fortalecendo a prática baseada em evidências.

- **Acompanhamento e melhoria contínua:** avaliação sistemática do currículo por meio de indicadores (aprendizagem, inserção profissional, impacto de projetos), com revisão periódica e participação de colegiados, NDE e partes interessadas externas.
- **Ética e conformidade transversais:** tratamento transversal de LGPD/privacidade, segurança, confiabilidade de IA e aspectos jurídico-regulatórios em disciplinas e projetos.

Esses princípios e diretrizes asseguram a coerência entre organização curricular, metodologias de ensino e avaliação, garantindo formação de excelência alinhada às demandas contemporâneas de Cibersegurança.

6 Perfil Profissional do Egresso

O Bacharel em *Cibersegurança* é um profissional com base científica sólida em Computação, Matemática e Engenharia, capaz de projetar, implementar, auditar e governar soluções digitais **seguras, confiáveis e inteligentes** ao longo de todo o ciclo de vida de sistemas e dados. Com **visão sistêmica** e **formação ética**, o egresso integra cibersegurança (prevenção, detecção, resposta e recuperação) e IA confiável (modelagem, avaliação, operação e governança), atuando de forma colaborativa em contextos interdisciplinares, regulatórios e de **alta complexidade sociotécnica**.

A formação articula fundamentos e prática em **software security**, **hardware/-security of systems** (incluindo *side-channels*, Meltdown/Spectre), **segurança Web**, **segurança de redes** (TCP/IP, DNS, firewalls, VPNs), **criptografia e PKI/-TLS**, **blockchain/Bitcoin**, **IA/ML/DL** aplicadas à defesa (deteção de intrusões, anomalias, classificação de malware, *threat intel*), **Adversarial ML**, **privacidade diferencial** e **aprendizado federado**, além de **DevSecOps**, **MLOps/LLMOps** e **GRC** (governança, risco e conformidade). Projetos integradores, *cyber ranges* e extensão universitária (mínimo de 405h) consolidam competências técnicas, comunicacionais e de liderança, culminando em TCC, estágio ou *startup* com MVP funcional.

6.1 Competências e Resultados de Aprendizagem

Ao concluir o curso, o egresso será capaz de:

1. **Engenharia segura e por evidências**: conceber e avaliar arquiteturas seguras (aplicação, dados, redes e infraestrutura), dominando *secure SDLC*, *threat modeling*, revisão de código, testes de segurança (BOF, ROP, XSS, CSRF, SQLi, *race conditions*), endurecimento de sistemas e resposta a incidentes.

2. **Criptografia aplicada e confiança**: selecionar e operar primitivas (AES/GCM, HMAC, RSA/DH/EC), **PKI/TLS**, gestão de chaves e certificados, e **blockchain** (transações, scripts, árvore de Merkle, consenso) em casos de uso reais.

3. **IA para cibersegurança**: planejar *pipelines* de dados de segurança; treinar e validar modelos (clássicos e profundos) para detecção, correlação e priorização de alertas; empregar **explainability** e métricas robustas (ROC/PR, *calibration*).

4. **Segurança de IA**: analisar e mitigar **ataques adversariais** (evasão, *poisoning/backdoor*, *model stealing*, *membership inference*), aplicar **privacidade diferencial** e **aprendizado federado** com agregação segura, e operar **LLMs/RAG** com **guardrails** (proteção contra *prompt injection*, *data exfiltration* e *jailbreaks*).

5. **Operação e governança**: implementar **DevSecOps/MLOps/LLMOps**, observabilidade, gestão do ciclo de vulnerabilidades, continuidade de negócios e **conformidade** (ISO 27001/27701, LGPD, NIST CSF, boas práticas MITRE ATT&CK), articulando requisitos técnicos, legais e de risco.

6. **Comunicação e liderança**: produzir relatórios executivos e técnicos, *runbooks* e políticas; conduzir *blue/red/purple teaming*; liderar equipes multidisciplinares com ética, diversidade e responsabilidade socioambiental.

7. **Inovação e empreendedorismo**: transformar problemas reais em produtos/serviços (MVP), com análise de viabilidade, propriedade intelectual, *go-to-market* e indicadores de impacto.

6.2 Áreas de Atuação

- Engenharia de Segurança (aplicações, dados, redes e nuvem), Arquitetura e GRC; Operações de Segurança (SOC, *threat hunting*, resposta a incidentes).
- Ciência de Dados e *Machine Learning* aplicados à segurança; **Adversarial ML** e **Segurança de LLMs**.
- Criptografia aplicada, gestão de chaves e **PKI/TLS**; soluções **blockchain**.
- Desenvolvimento seguro (*secure coding*, *DevSecOps*); MLOps/LLMOps.
- Pesquisa acadêmica e P&D; consultoria e auditoria técnica; empreendedorismo em cibersegurança/IA.

6.3 Postura Ética e Compromissos

O egresso atua com **integridade**, **responsabilidade** e **respeito aos direitos fundamentais**, observando a LGPD e normas setoriais, adotando práticas de ciência aberta responsável, reprodutibilidade e inclusão. Cultiva **aprendizagem contínua**, pensamento crítico e engajamento cidadão, orientando decisões por evidências, risco e impacto social/ambiental.

6.4 Diferenciais do Egresso

- Sólida experiência prática em **laboratórios e *cyber ranges***, com **portfólio de evidências** (artefatos, relatórios, demos) e vivência em extensão (carga horária igual ou superior a 405h).
- Domínio integrado de **cibersegurança** e **IA** do ponto de vista **técnico**, **operacional** e **regulatório**, com capacidade de **tradução** entre áreas técnicas e de negócio.
- Capacidade de **liderar** iniciativas de alto impacto, inovar e sustentar soluções **seguras e confiáveis** em escala.

6.5 Ética, Cidadania Digital e Valores Profissionais

O egresso deverá:

- Respeitar direitos fundamentais e a legislação aplicável, zelando pela proteção de dados, pela transparência, pela responsabilização e pela explicabilidade das soluções.
- Promover diversidade, equidade e inclusão em ambientes de estudo e trabalho; cultivar colaboração, empatia e escuta ativa.
- Comprometer-se com o bem público, a redução de assimetrias de segurança e a sustentabilidade dos ecossistemas digitais.

6.6 Trajetórias Profissionais e Continuidade Acadêmica

O curso prepara para inserção qualificada em setores público e privado, com progressão de carreira em engenharia/arquitetura de segurança, operações, GRC, ciência de dados/IA aplicada à segurança e liderança técnica. O egresso também estará apto a prosseguir estudos em programas de pós-graduação (lato e stricto sensu) nas áreas de Computação, Engenharia Elétrica, Ciência de Dados, Direito e Políticas Públicas com foco em segurança, privacidade e IA.

6.7 Avaliação de Competências e Evidências

As competências são validadas por meio de:

- projetos integradores e *capstones* com problemas autênticos;
- artefatos técnicos (código, modelos, pipelines, infra como código, documentação);
- relatórios, demonstrações públicas e portfólios individuais;
- rubricas claras de desempenho e feedback formativo contínuo;
- participação em atividades de pesquisa, extensão, desafios técnicos e estágios.

6.8 Síntese: Mapa de Competências (Eixo $\times$ Resultado)

Eixos e **resultados de aprendizagem (síntese):**

1. Fundamentos — Modelar problemas; projetar *software* e dados com requisitos não funcionais explícitos; comprovar propriedades e analisar desempenho;
2. Cibersegurança — Aplicar *security-by-design*; conduzir GRC; executar *DevSecOps*, DFIR e resposta a incidentes; operar SOC com evidências e métricas;

3. IA Confiável — Treinar/operar modelos; garantir rastreabilidade e governança; avaliar robustez, privacidade, explicabilidade e equidade;
4. Ética e Sociedade — Atuar conforme marcos legais; produzir relatórios claros; avaliar impactos sociotécnicos e promover acessibilidade e inclusão;
5. Gestão e Colaboração — Liderar equipes; gerir projetos e riscos; comunicar-se com clareza em português e inglês; empreender e inovar.

Em conjunto, esses elementos definem um perfil de egresso apto a criar valor público e privado com alto padrão técnico, responsabilidade ética e visão sistêmica, contribuindo para a confiança digital e para o desenvolvimento sustentável da sociedade.

7 Objetivos do Curso

7.1 Objetivo Geral

Formar bacharéis em *Cibersegurança* com sólida base científica e capacidade de atuar ao longo de todo o ciclo de vida de sistemas e dados — da concepção à operação — aplicando *security-by-design*, *privacy-by-default* e princípios de IA confiável, de modo ético, responsável e orientado a resultados, contribuindo para a confiança digital, a inovação e o desenvolvimento sustentável.

7.2 Objetivos Específicos

1. **Base científica e de engenharia:** consolidar fundamentos de computação, matemática, estatística, redes, sistemas e engenharia de *software* que sustentem a prática avançada em cibersegurança e IA.
2. **Engenharia segura:** capacitar o estudante a especificar, projetar, implementar, testar e auditar soluções com requisitos não funcionais explícitos (segurança, privacidade, desempenho, disponibilidade, observabilidade).
3. **Ciclo de segurança de ponta a ponta:** desenvolver competências para prevenção, detecção, resposta e recuperação, abrangendo GRC, *threat modeling*, *DevSecOps*, DFIR e resiliência operacional.
4. **IA confiável na prática:** habilitar a modelagem, avaliação e operação de ML/DL, com MLOps/LLMOps, rastreabilidade de dados e de modelos, mitigação de vieses, robustez, explicabilidade e segurança da cadeia de IA.
5. **Segurança de dados e privacidade:** formar para a engenharia de privacidade (*privacy engineering*), proteção de dados em todo o ciclo de vida, anonimização, governança e aderência regulatória (p. ex., LGPD).

6. **Integração sociotécnica e ética:** promover visão crítica sobre impactos sociais, legais, ambientais e econômicos das tecnologias, com postura ética, cidadã e compromisso com o bem público.
7. **Gestão, comunicação e colaboração:** desenvolver competências para liderança técnica, trabalho em equipes multidisciplinares, comunicação técnica com públicos diversos e gestão de projetos, riscos e qualidade.
8. **Inovação e empreendedorismo:** estimular a criação e validação de soluções, produtos e serviços em ecossistemas de P&D, setor público, empresas e *startups*, com foco em problemas reais de alta complexidade.
9. **Aprendizagem ao longo da vida:** cultivar autonomia intelectual, pensamento crítico e atualização contínua frente à evolução do estado da arte e das demandas da sociedade.

7.3 Objetivos Educacionais do Programa (OEP)

Os Objetivos Educacionais do Programa descrevem desempenhos esperados dos egressos após **3 a 5 anos** de formados. Eles orientam a melhoria contínua do curso e sua inserção social.

OEP 1: **Liderança técnica e impacto:** egressos atuam como engenheiros(as) ou arquitetos(as) de soluções seguras e inteligentes, liderando iniciativas que elevam a maturidade de segurança, a eficiência operacional e a confiabilidade de serviços digitais.

OEP 2: **Excelência em segurança e IA:** egressos concebem, implementam e operam soluções com *security-by-design* e IA confiável, evidenciando conformidade, rastreabilidade e resultados mensuráveis de risco e desempenho.

OEP 3: **Responsabilidade ética e regulatória:** egressos traduzem marcos legais e normativos em controles técnicos e processos auditáveis, promovendo proteção de dados, direitos fundamentais e ambientes digitais inclusivos.

OEP 4: **Inovação e empreendedorismo:** egressos criam, escalam ou sustentam produtos e serviços inovadores em cibersegurança e IA, interagindo com ecossistemas de P&D, setor público e privado, e contribuindo para o desenvolvimento socioeconômico.

OEP 5: **Desenvolvimento profissional contínuo:** egressos mantêm trajetória de atualização técnica e acadêmica (certificações, pós-graduação, publicações), ampliando escopo de atuação e responsabilidade.

7.4 Resultados de Aprendizagem Associados

Para garantir o alinhamento entre o que se ensina e o que se espera do egresso, os OEP conectam-se a resultados de aprendizagem do curso (ver capítulos *Perfil do Egresso* e *Princípios*), sintetizados a seguir:

1. Projetar e implementar sistemas com requisitos de segurança e privacidade explícitos, sustentados por evidências técnicas e documentação.
2. Modelar, avaliar e operar soluções de IA confiável, com governança de dados e modelos e monitoramento em produção.
3. Conduzir GRC, análise e tratamento de riscos, resposta a incidentes e melhoria contínua baseada em métricas.
4. Comunicar riscos, decisões e resultados a públicos técnicos e não técnicos, liderando equipes e projetos multidisciplinares.
5. Avaliar impactos sociotécnicos, mitigar vieses e promover inclusão, acessibilidade e sustentabilidade nos ambientes digitais.

7.5 Indicadores e Monitoramento dos Objetivos

Os objetivos serão monitorados por indicadores quantitativos e qualitativos, analisados periodicamente pelo Núcleo Docente Estruturante (NDE) e Colegiado, incluindo:

- **Inserção e progressão profissional:** taxa e tempo de inserção no mercado; evolução de responsabilidades (ex.: arquitetura, liderança, GRC, SOC, MLOps/LLMOps).
- **Evidências de prática:** portfólios de egressos, relatórios de *capstones*, participação em DFIR/SOC, contribuições para *open-source*/comunidades técnicas.
- **Conformidade e impacto:** relatos de implementação de auditorias, de certificações, de ganhos de maturidade (ex.: melhoria de MTTR/MTTD, redução de exposição) e de *security-by-design*/*privacy-by-default*, .
- **Inovação e formação continuada:** participação em P&D, *startups*, patentes, publicações, certificações e pós-graduação.

- **Satisfação e relevância social:** pesquisas com egressos/empregadores, aderência dos projetos às demandas regionais e nacionais e contribuição a políticas públicas/serviços essenciais.

Em conjunto, esses objetivos orientam a organização curricular, as metodologias de ensino, a avaliação por evidências e as parcerias institucionais, assegurando a formação de profissionais capazes de elevar a confiança digital e impulsionar a inovação baseada em dados com rigor técnico, responsabilidade ética e visão sistêmica.

8 Estrutura Curricular

8.1 Premissas e Organização Geral

A matriz do curso *Cibersegurança*, modalidade bacharelado, adota organização por projetos, integração horizontal (entre componentes do período) e vertical (progressão de competências), com prática intensiva em laboratórios e desafios autênticos junto a empresas e comunidade. A avaliação é formativa, baseada em evidências (projetos reais, artefatos técnicos, relatórios, demonstrações públicas e portfólios) e rubricas por competência. Há uma única disciplina de 60h a ser cursada como optativa no período 7 do curso.

Janelas de oferta e cargas por período

- **Períodos 1 a 6:** 20 horas-aula no turno noturno, distribuídas uniformemente de segunda a sexta, em 15 semanas ⇒ **300h** por período;
- **Períodos 7 e 8:** 10 horas-aula no turno noturno, de segunda a sexta, em 15 semanas ⇒ **150h** por período;
- Os sábados são dias letivos onde é possível desenvolver atividades normais do curso.

8.2 Regime e Tempo de Integralização

O Curso de Cibersegurança é oferecido em **regime semestral** e **período noturno**. O estudante tem um prazo mínimo de oito semestres e um prazo máximo de doze semestres para a integralização regulamentar do curso. O Quadro 8.1, a seguir, mostra a carga horária semanal dos módulos, além das cargas horárias dos componentes de Atividades Curriculares de Extensão (ACE), Atividade de Conclusão do Curso (ACC) e Atividades Acadêmicas Complementares (AAC).

Quadro 8.1: Carga Horária Semanal por Período

Período	CH Semanal (horas)	Total (horas)
1º	24	360
2º	24	360
3º	24	360
4º	24	360
5º	24	360
6º	24	360
7º	14	210
8º	13	195
Estágio Supervisionado	—	440
Atividades Acadêmicas Complementares	—	195
TOTAL		**3200**

8.3 Arquitetura Curricular por Período

O currículo do curso Cibersegurança da UFU contempla as indicações e sugestões realizadas pela ACM (Association for Computing Machinery) , pelo IEEE (Institute of Electrical and Electronics Engineer) nos currículos de referência criados em conjunto por ambas, pela SBC (Sociedade Brasileira de Computação), e fundamentalmente, pela Resolução CNE/CES nº 5 de 16 de novembro de 2016 do MEC que institui as Diretrizes Curriculares Nacionais específicas para os cursos da área de computação.

O currículo do Curso está organizado em oito (8) períodos (ou semestres) sendo que os componentes curriculares do curso estão divididos em: Disciplinas Obrigatórias, Disciplina Optativa, Atividade de Conclusão de curso (Estágio Supervisionado e Projeto de Graduação), Atividades Complementares e Atividades de Extensão.

As disciplinas obrigatórias e optativa, por sua vez, possuem atividades classificadas nas modalidades: Prática, Teórica. A estrutura curricular apresenta um total de 3200 horas.

Quadro 8.2: Fluxo Curricular

PEF	Componente Curricular	Natureza	Carga Horária			Requisitos		UA Oferta
			CHT	CHP	TOT	PREQ	CREQ	
1º	Módulo 1 — Programação e Matemática Aplicada	Obrigatória	0	150	150	Livre	Livre	FEELT
	Módulo 2 — Aplicação para ambiente WEB	Obrigatória	0	150	150	Livre	Livre	FEELT
	ACE I — Atividades Curriculares de Extensão I[1]	Obrigatória	0	60	60	Livre	Livre	FEELT
	ENADE (Ingressante)[2]	Obrigatória	–	0	0	Livre	Livre	–
2º	Módulo 3 — Segurança WEB	Obrigatória	0	300	300	Módulo 1; Módulo2	Livre	FEELT
	ACE II — Atividades Curriculares de Extensão II[1]	Obrigatória	0	60	60	Livre	Livre	FEELT
3º	Módulo 4 — Hardware e Segurança de Sistemas	Obrigatória	0	300	300	Módulo 3	Livre	FEELT
	ACE III — Atividades Curriculares de Extensão III[1]	Obrigatória	0	60	60	Livre	Livre	FEELT
4º	Módulo 5 — Segurança de Redes	Obrigatória	0	300	300	Módulo 4	Livre	FEELT
	ACE IV — Atividades Curriculares de Extensão IV[1]	Obrigatória	0	60	60	Livre	Livre	FEELT
5º	Módulo 6 — Criptografia e Segurança Blockchain	Obrigatória	0	300	300	Módulo 5	Livre	FEELT
	ACE V — Atividades Curriculares de Extensão V[1]	Obrigatória	0	60	60	Livre	Livre	FEELT
6º	Módulo 7 — Inteligência Artificial em Cibersegurança	Obrigatória	0	300	300	Módulo 6	Livre	FEELT
	Disciplina Optativa[3]	Optativa	–	0	60	Livre	Livre	FEELT

Continua na próxima página

Quadro 8.2: Fluxo Curricular (Continuação)

PER	Componente Curricular	Natureza	Carga Horária			Requisitos		UA Oferta
			CHT	CHP	TOT	PREQ	CREQ	
7º	Módulo 8 — Projeto de Graduação I	Obrigatória	0	150	150	Módulo 7	Livre	FEELT
	ACE VI — Atividades Curriculares de Extensão VI[1]	Obrigatória	0	60	60	Livre	Livre	FEELT
8º	Módulo 9 — Projeto de Graduação II	Obrigatória	0	150	150	Módulo 8	Livre	FEELT
	ACE VII — Atividades Curriculares de Extensão VII[1]	Obrigatória	0	45	45	Livre	Livre	FEELT
	ENADE (Concluinte)[2]	Obrigatória	–	0	0	Livre	Livre	–
Atividades Acadêmicas Complementares (AAC)[4]		Obrigatória	–	0	195	Livre	Livre	–
Estágio Supervisionado[5]		Obrigatória	–	0	440	1.440h vencidas	Livre	–
Opt.	Língua Brasileira de Sinais - Libras I	Optativa	30	30	60	Livre	Livre	FACED
	Tópicos Especiais em Cibersegurança	Optativa	30	30	60	Livre	Livre	FEELT

[1] Os discentes deverão integralizar **405 horas** de atividades extensionistas (ACE) ao longo do curso.

[2] O Exame Nacional de Desempenho dos Estudantes (ENADE) integra o Sistema Nacional de Avaliação da Educação Superior (Sinaes) e é componente curricular obrigatório, conforme Lei nº 10.861, de 14 de abril de 2004.

[3] O estudante deverá cumprir uma carga horária mínima de 60 horas em disciplinas optativas.

[4] Para integralização curricular, o discente deverá realizar **195 horas** horas de atividades acadêmicas complementares (AAC) ao longo do curso.

[5] O estudante necessita cumprir uma carga horária mínima de **440 horas** no Estágio Supervisionado em sua área de formação.

Requisitos Legais e Normativos

Com base na legislação, estão elencados a seguir conteúdos requeridos e seu respectivo componente curricular.

Quadro 8.3: Requisitos legais e normativos

Temática	Legislação	Módulos/Disciplina	Períodos	Natureza
Educação Ambiental	Lei nº9.795, de 27/04/1999; Decreto nº4.281, de 25/06/2002 Resolução nº26/2012, de 30/11/2012, do Conselho Universitário, que estabelece a Política Ambiental da UFU	1 e 2	1 e 2	Obrigatória
Educação em Direitos Humanos	Resolução CNE/CP nº1/2012, de 30/05/2012, que estabelece as Diretrizes Nacionais para a Educação em Direitos Humanos.	1 e 2	1 e 2	Obrigatória
Educação para as relações étnico-raciais e o Ensino de História e Cultura afro-brasileira, africana e indígena	Lei nº10.639, de 09/01/2003; Resolução nº1/2004, de 17/06/2004; Resolução nº4/2014, CONGRAD.	1 e 2	1 e 2	Obrigatória
LIBRAS	Decreto nº5.626/2005, de 22/12/2005, que regulamenta a Lei nº10.436, de 24/04/2002; Decreto nº4.281, de 25/06/2002	Língua Brasileira de Sinais - Libras I	Livre	Optativa

Disciplina Optativa - carga horária mínima 60h

Há três possibilidades para o discente cursar uma ou mais disciplinas optativas:

1. Será oferecida, conforme a demanda e a disponibilidade de docentes a disciplina presencial “Língua Brasileira de Sinais - Libras I”, cujo código é LIBRAS01, com carga horária total de 60 horas, sendo 30h teóricas e 30h práticas, oferecida pela unidade Faculdade de Educação (FACED).

2. Será oferecida, conforme a demanda e a disponibilidade de docentes a disciplina presencial “Tópicos Especiais de Cibersegurança”, cujo código é TECCIB, com carga horárias total de 60 horas, sendo 30h teóricas e 30h práticas, oferecida pela unidade Faculdade de Engenharia Elétrica (FEELT).

3. Cursar qualquer disciplina em qualquer curso superior da Universidade Federal de Uberlândia (UFU), mediante requerimento e aprovação no conselho do curso.

A carga horária mínima que o estudante deve integralizar por meio de uma ou mais disciplinas optativas é de 60 horas.

8.4 Ementas Resumidas e Diretrizes

As ementas seguem o padrão conciso e orientado a competências: objetivos de aprendizagem claros, conteúdos nucleares e práticas guiadas por projetos e *sprint*. Abaixo, a síntese por família (ementas completas estão apresentadas no Anexo **Ementas**):

Módulo 01: Programação e Matemática Aplicada *Período/Semestre:* 1º
Carga horária: 150h
Objetivos: Formar a base algorítmica e matemática para todo o curso; treinar raciocínio lógico e trabalho em equipe via projetos.
Conteúdos: Lógica e estruturas de programação, estruturas de dados básicas, álgebra linear, cálculo numérico, lógica matemática, noções de arquitetura/sistemas digitais, design e prototipação. Os usos sociais da tecnologia à luz de específicas questões tais como gênero, desigualdade de renda, direitos humanos e dos desafios contemporâneos da diversidade e da inclusão.

Módulo 02: Aplicação para ambiente WEB *Período/Semestre:* 1º
Carga horária: 150h
Objetivos: Capacitar na construção de aplicações Web seguras e testáveis, preparando o terreno para segurança Web.
Conteúdos: HTML/CSS/JS, MVC/MVVM, APIs, Banco de Dados (relacional/não relacional), requisitos, testes, usabilidade, CSP (noções). Os usos da tecnologia à luz de específicas questões tais como aspectos ambientais e econômicos, educação ambiental.

Módulo 03: Segurança WEB *Período/Semestre:* 2º
Carga horária: 300h
Objetivos: Proteger camadas de interface/servidor contra ataques de entrada e sessão. Endurecer o backend e a integração rede–aplicação–dados.
Conteúdos: CSRF (GET/POST, *same-site*, tokens), XSS (refletido/persistente/DOM, worms), CSP e *encoding*,**SQL Injection** (PoC e *prepared statements*), serviços Web, políticas de acesso e *logging*; noções de sistemas distribuídos aplicados à Web.

Módulo 04: Hardware e Segurança de Sistemas *Período/Semestre:* 3º
Carga horária: 300h
Objetivos: Entender superfícies de ataque em baixo nível e explorar/mitigar vulnerabilidades clássicas. Avançar em exploração/defesa e consolidar segurança de CPU moderna.
Conteúdos: Set-UID/Set-GID, variáveis de ambiente, *dynamic linker*, *buffer overflow* (I), Shellshock, *format string* (I), *race conditions* (I), *reverse shell*, *side-channels* via cache e **Meltdown**, *return-to-libc*, ROP, *format string*/*race* (II), Dirty COW, **Spectre**, mitigação e limites.

Módulo 05: Segurança de Redes *Período/Semestre:* 4º

Carga horária: 300h

Objetivos: Instrumentar e compreender tráfego para defesa e teste. Projetar perímetro/serviços seguros e mitigar ataques de infraestrutura.

Conteúdos: NIC/BPF, *pcap*/Scapy, *sniffing/spoofing*, checksums, SYN flood, TCP (handshake), TCP reset, *session hijacking*, Firewalls (packet/stateful/-proxy, Netfilter/iptables), evasão (SSH/VPN), DNS (cache poisoning, Kaminsky, rebinding, DNSSEC), VPN TLS/SSL, Heartbleed.

Módulo 06: Criptografia e Segurança Blockchain *Período/Semestre:* 5º

Carga horária: 300h

Objetivos: Aplicar primitivas criptográficas com uso correto de APIs. Operar criptografia de chave pública e infraestrutura de confiança; compreender blockchain em produção.

Conteúdos: DES/AES e modos (ECB/CBC/CTR/AEAD–GCM), IV/padding, hash (MD/SHA), HMAC, integridade/senhas, *hash chain*, endereços e scripts (P2PKH/P2SH), DH, RSA (OAEP/assinaturas), PKI/TLS, cadeia de confiança e MITM; transações, propagação, mineração, Merkle, consenso e duplo gasto.

Módulo 07: Inteligência Artificial em Cibersegurança *Período/Semestre:* 6º

Carga horária: 300h

Objetivos: Empregar ML/DL básico para detecção e triagem de incidentes. Elevar a defesa com DL avançado e segurança de IA.

Conteúdos: Supervisionado/não supervisionado, anomalia (Isolation Forest/autoencoder), RNNs para *logs*, embeddings e RAG (básico), métricas ROC/PR e explainability, Transformers, GANs/difusão (dados sintéticos), ataques adversariais (FGSM/PGD/C&W), *poisoning/backdoor*, DP-SGD, FL seguro, segurança de LLMs/RAG e LLMOps.

Módulo 08: Projeto de Graduação I *Período/Semestre:* 7º

Carga horária: 150h

Objetivos: Integrar conhecimentos em problema real com trilhas Acadêmica, Corporativa ou Empreendedora; entregar MVP/estudo completo e defesa pública.

Conteúdos: Scoping, estado da arte/prática, plano (backlog, riscos), MVP, validação e transferência; PI/relatório/artigo.

Módulo 09: Projeto de Graduação II *Período/Semestre:* 8º

Carga horária: 150h

Objetivos: Integrar conhecimentos em problema real com trilhas Acadêmica, Corporativa ou Empreendedora; entregar MVP/estudo completo e defesa pública.

Conteúdos: Scoping, estado da arte/prática, plano (backlog, riscos), MVP, validação e transferência; PI/relatório/artigo; confecção e apresentação de **Memorial de Extensão** comprovando carga horária igual ou superior a 405h.

Integração com SEED Security Labs

Os *labs* do SEED são distribuídos ao longo dos Projetos e componentes:

Software BOF, ROP, Format String, Dirty COW;

Networking Sniffing/Spoofing, ARP/ICMP, Firewall, VPN, BGP;

Web XSS, CSRF, SQLi, Clickjacking;

Crypto Secret-Key, PRNG, Hash Length Extension, MD5 Collision, TLS/PKI;

System/Hardware Blockchain e Mobile.

Blockchain e Mobile — sempre em ambientes controlados, com segurança operacional e documentação reprodutível.

8.5 Coerência com Perfil do Egresso

A nova arquitetura curricular garante: (i) fundamentos sólidos; (ii) ciclo completo de segurança (prevenção–detecção–resposta–recuperação); (iii) IA confiável aplicada à defesa; (iv) ética, LGPD e governança; (v) gestão e comunicação. As cargas por período, as 405h de extensão, as 300h de projeto de graduação, as 440h de estágio supervisionado e as 195h de complementares compõem um percurso formativo robusto, de alto impacto acadêmico e social.

Evidencia-se que a **extensão** está no DNA do curso e é desenvolvida em todos os períodos em atividades com a comunidade externa, nos projetos semestrais que devem ser inscritos no Sistema de Extensão da UFU, de forma a serem referendados e avaliados na sua forma e intenção.

8.6 Atividades de Conclusão do Curso (ACC)

O componente curricular **ACC** consiste em duas atividades: o Projeto de Graduação e o Estágio Supervisionado (440h).

Projeto de Graduação

O Projeto de Graduação será desenvolvido no último ano (períodos 7 e 8), com carga horária total de **300h**, correspondendo a 2 módulos: **Projeto de Graduação I**, no período 7, e **Projeto de Graduação II**, no período 8.

O projeto de graduação constitui uma etapa relevante no processo de formação dos estudantes, na qual os conhecimentos adquiridos ao longo dos módulos anteriores são aplicados, considerando oportunidades em três trilhas de desenvolvimento: empreendedora (destinada aos alunos que desejam estabelecer o seu próprio negócio), corporativa (voltada para os que almejam uma carreira em uma empresa) e acadêmica (para os que anseiam pelo magistério e/ou pela pesquisa). Essas trilhas são meticulosamente desenvolvidas para proporcionar uma experiência de aprendizado personalizada, permitindo que os estudantes adaptem sua formação acadêmica aos seus objetivos profissionais.

“A trilha acadêmica” destina-se a indivíduos que almejam prosseguir estudos em níveis mais avançados, como mestrado e doutorado, ou que anseiam por carreiras em pesquisa e ensino. A relevância desta trilha reside na ênfase atribuída à pesquisa original, ao pensamento crítico e à capacidade de contribuir para o corpo de conhecimento existente em sua área de estudo. Ademais, os discentes são incentivados a participar de projetos de pesquisa, conferências acadêmicas e outras atividades que possam aprimorar sua compreensão e experiência no campo escolhido. A seguir, são apresentadas as atividades oferecidas na Trilha Acadêmica:

- aprofundamento em metodologia da pesquisa científica;
- escrita e apresentação de artigos científicos;
- elaboração de projetos de pesquisa;
- prospecção de programas de pós-graduação no Brasil e no exterior;
- preparação para o Exame Nacional para Ingresso na Pós-Graduação em Computação (POSCOMP);
- preparação para processos seletivos em diversos programas no Brasil e no exterior.

A formação profissional, por outro lado, é ideal para estudantes que visam carreiras em grandes empresas ou organizações internacionais. Esta formação acadêmica foca-se no desenvolvimento de competências práticas e conhecimentos especializados no domínio empresarial, incluindo a gestão de projetos, liderança, estratégia de negócios e análise de dados. Ademais, proporciona aos discentes a possibilidade de compreender a dinâmica organizacional e desenvolver competências.

A “trilha corporativa”, por sua vez, é ideal para estudantes que visam carreiras em grandes empresas ou organizações internacionais. A referida trilha concentra-se

em habilidades práticas e conhecimentos específicos do setor, tais como gestão de projetos, liderança, estratégia de negócios e análise de dados. Ademais, proporciona aos discentes a oportunidade de compreender a dinâmica organizacional e desenvolver competências fundamentais para o sucesso em ambientes corporativos. Dentre as atividades oferecidas no programa de desenvolvimento profissional, denominado “Trilha Corporativa”, destacam-se: aprofundamento técnico nos assuntos do projeto; criação de patentes, registros de software e propriedade intelectual; condução de carreira corporativa, mercado de trabalho e suas oportunidades; preparação para processos seletivos específicos; e preparação para certificações.

A “trilha Empreendedora” propicia aos discentes um espírito empreendedor, por intermédio de uma formação integrada em negócios e inovação. A presente trilha é destinada a indivíduos que tenham interesse em criar suas próprias *startups*, desenvolver novos produtos ou serviços, ou ainda, compreender o ecossistema empreendedor. O programa de formação abrange desde os fundamentos do empreendedorismo até aspectos mais complexos, como o financiamento de *startups*, o marketing digital e a gestão de inovação, preparando os estudantes para os desafios do mundo dos negócios. Dentre as atividades oferecidas no programa “trilha Empreendedora”, destacam-se: orientação sobre o processo de abertura e gestão de pequenas empresas ou startups no Brasil; busca de financiamento; criação de patentes, registros de software e propriedade intelectual; concepção e gestão de produtos; papel do empreendedor; e responsabilidade social. A formação profissional, por outro lado, é ideal para estudantes que visam carreiras em grandes empresas ou organizações internacionais. Esta formação acadêmica foca-se no desenvolvimento de competências práticas e conhecimentos especializados no domínio empresarial, incluindo a gestão de projetos, liderança, estratégia de negócios e análise de dados. Ademais, proporciona aos discentes a possibilidade de compreender a dinâmica organizacional e desenvolver competências.

Cada um dos módulos referentes ao Projeto de Graduação apresenta uma carga horária total de 150 horas, distribuídas ao longo de 15 semanas. Desse total, semanalmente, 4 horas são destinadas a encontros com os professores supervisores, enquanto as 6 horas restantes são dedicadas ao desenvolvimento dos projetos. Os artefatos a serem entregues incluem o plano de projeto, as entregas do plano por *sprint* e o relatório e/ou artigo final. Em encontros com os professores supervisores, são realizadas orientações e atividades pertinentes a cada trilha. Para o autoestudo, são disponibilizados conteúdos básicos de cada trilha. A elaboração de planos de projetos por parte dos discentes deve ser realizada seguindo diferentes modelos, de acordo com a trilha escolhida (incluindo *backlog*, cronograma, riscos, entre outros). Os projetos de graduação são uma oportunidade para os discentes consolidarem seus conhecimentos e aprimorarem suas habilidades de trabalho em equipe, comunicação, liderança e resolução de problemas. A responsabilidade pela entrega final do projeto é superior em comparação aos módulos anteriores, o que resulta em maior engajamento e motivação dos alunos em relação ao alcance de seus objetivos.

Estágio Supervisionado

O Estágio Supervisionado é uma das atividades necessárias para a conclusão do curso de Cibersegurança quando da sua validação como Atividade de Conclusão de Curso. O estudante necessita, obrigatoriamente, cumprir uma carga horária mínima estipulada de 440 horas de estágio na sua área de formação. O Estágio Supervisionado poderá ser iniciado após o estudante ter vencido 1.440h de atividades do curso, correspondentes aos 4 primeiros períodos do curso.

São necessários o acompanhamento de um supervisor – um profissional da mesma área de formação (ou área afim) que faça parte do quadro de empregados da parte cedente do estágio – e a realização de horas supervisionadas por um professor do curso. Ao final do estágio, o estudante deve apresentar um relatório para o registro final das atividades realizadas.

Para realizar essa atividade, o discente deve estar matriculado nos períodos 5, 6, 7 ou 8, ou seja, a partir do terceiro ano do curso. Um certificado de conclusão de estágio deverá ser emitido pela Coordenação de Estágio do Curso. O detalhamento dos procedimentos relativos ao Estágio Supervisionado consta nas Normas Complementares de Estágio do Cibersegurança, aprovada nos âmbitos do Colegiado do Curso e da Unidade Acadêmica com anuência do NDE.

Estágio Não Obrigatório

Embora não seja uma modalidade aceita para a quitação da Atividade de Conclusão de Curso, de acordo com o anexo da Resolução CONGRAD nº 24/2012, o estudante é autorizado a desenvolver um estágio não obrigatório. Essa modalidade de estágio é desenvolvida como atividade opcional e complementar, acrescida à carga horária regular e obrigatória de acordo com as normas complementares de estágio e as normas de Atividades Acadêmicas Complementares do curso. São necessários o acompanhamento de um supervisor – um profissional da mesma área de formação (ou área afim) que faça parte do quadro de empregados da parte cedente do estágio – e a realização de horas supervisionadas por um professor do curso.

Para realizar essa atividade, o discente tem o pré-requisito mínimo de 600 horas integralizadas do currículo com a necessidade de aprovação em todos os Corrigir a Norma componentes curriculares dos 1º e 2º períodos do curso. O detalhamento do Estágio Não Obrigatório consta nas Normas Complementares de Estágio do Curso Cibersegurança, aprovada nos âmbitos do Colegiado do Curso e da Unidade Acadêmica com anuência do NDE.

8.7 Atividades Acadêmicas Complementares

Total de **195h**, incluindo monitorias, iniciação científica, organização/participação em eventos, cursos livres, desafios técnicos e ações de extensão extra-projeto, registradas e validadas conforme normas específicas.

De acordo com o Parecer do CNE/CES nº 136/2012, as Atividades Acadêmicas Complementares são componentes curriculares que têm como objetivo principal enriquecer e expandir o perfil do egresso com atividades que privilegiem aspectos diversos da sua formação, incluindo atividades desenvolvidas fora do ambiente acadêmico. Tais atividades constituem instrumental importante para o desenvolvimento pleno do aluno, servindo de estímulo a uma formação prática independente e interdisciplinar, sobretudo nas relações com o mundo do trabalho.

Ainda, as atividades podem ser cumpridas em diversos ambientes, como a instituição a que o estudante está vinculado, outras instituições e variados ambientes sociais, técnico-científicos ou profissionais, em modalidades tais como: formação profissional (cursos de formação profissional, experiências de trabalho ou estágios não obrigatórios), de pesquisa e publicação (iniciação científica e participação em eventos técnico-científicos, publicações científicas), de ensino (programas de monitoria e tutoria), de gestão e política (representação discente em comissões e comitês), de empreendedorismo e inovação (participação em incubadoras, *startups* ou outros mecanismos), de qualificação e experiência internacional entre outras. Essas atividades devem ser permanentemente incentivadas no cotidiano acadêmico, permitindo a diversificação das atividades complementares desenvolvidas pelos estudantes.

No Quadro 8.4, temos a relação de Atividades Acadêmicas Complementares (AAC) propostas neste projeto, com carga horária máxima a ser integralizada por tipo de atividade. A carga horária mínima a ser integralizada com essas atividades é de 195 horas, sem necessidade de pré-requisito. São consideradas atividades válidas para a quitação desse componente as que **foram realizadas durante o período de vínculo do estudante ao curso**.

Quadro 8.4: Carga Horária Máxima das AAC

Código	Descrição	CH/un.	CH Máx.
	Formação Profissional		
ATCO1181	Realização e conclusão de Curso Online Aberto e Massivo (MOOC) aprovado pelo Colegiado do Curso	15	90
ATCO1188	Aprovação em disciplina de quaisquer cursos de graduação da Universidade Federal de Uberlândia	-	180

Continua na próxima página

Quadro 8.4: Carga Horária Máxima das AAC (Continuação)

Código	Descrição	CH/un.	CH Máx.
ATCO1135	Participação em oficinas, cursos ou mini-cursos relacionados ao aprendizado de técnicas úteis à profissão	15	45
ATCO1182	Obtenção de certificações técnicas na área de Computação, Engenharia de Computação, Cibersegurança ou Inteligência Artificial	30	60
ATCO0725	Participação em visitas técnicas orientadas	5	10
ATCO0254	Estágio não obrigatório	2	36
	Pesquisa		
ATCO1104	Participação em Iniciação Científica com bolsa (PIBIC ou PIBITI)	45	90
ATCO1105	Participação em Iniciação Científica sem bolsa (PIVIC)	45	90
ATCO0044	Apresentação de trabalhos em eventos científicos na forma oral ou pôster	10|15	45
ATCO0964	Publicação de trabalhos científicos - resumo e/ou pôster	5|10	20
ATCO0965	Publicação de Trabalhos completos em anais de eventos	5|15|30	45
ATCO0993	Publicações em periódicos especializados (revistas indexadas da área)	30|45	90
ATCO0994	Publicações em periódicos não especializados (revistas de outras áreas, jornais e revistas não indexadas)	5|10	15
ATCO1184	Publicação de livro ou capítulo de livro especializado com código ISBN e corpo editorial técnico-científico	30|45	90
ATCO1185	Publicação de livro ou capítulo de livro, especializado ou não, sem código ISBN ou corpo editorial técnico-científico	5	15
	Ensino		
ATCO0354	Monitoria em disciplina ministrada na UFU, fora do escopo do curso	5	15
ATCO1919	Monitoria em módulo de graduação relativas aos 1º e 2º semestres do curso	10	30
ATCO2020	Monitoria em módulo de graduação relativas ao 3º semestre em diante do curso	15	45
ATCO0753	Participação no Programa de Educação Tutorial – PET	15	60
ATCO0599	Participação em grupo de estudos de temas específicos registrado e certificado pela Instituição	10	30
ATCO1186	Participação orientada por docente no desenvolvimento de material informacional ou didático para uso interno à UFU	info	30
ATCO1187	Ministrante de palestras, minicursos, seminários e oficinas para comunidade interna da UFU	info	30
	Gestão e Representação Estudantil		
ATCO0319	Membro de Diretório Acadêmico	10	30

Continua na próxima página

Quadro 8.4: Carga Horária Máxima das AAC (Continuação)

Código	Descrição	CH/un.	CH Máx.
ATCO0327	Membro do Diretório Central dos Estudantes	10	30
ATCO1019	Representante Discente no Conselho de Unidade ou Colegiado de Curso	15	45
ATCO0315	Membro de Conselho Superior da UFU	15	45
	Empreendorismo e Inovação		
ATCO1188	Participação ou desenvolvimento de projetos junto a incubadoras de empresas	5|15	45
ATCO1189	Fundador ou membro de empresa do tipo *startup* de tecnologia	15|30	90
ATCO2121	Patente ou Registro de Software	45	90
	Qualificação e Experiência Internacional		
ATCO1099	Curso de língua estrangeira ou aprovação em exame de proficiência em língua estrangeira	5|10|15	30
ATCO0344	Mobilidade Internacional oficializada pela DRII/UFU	10	60
ATCO1190	Realização de intercâmbio internacional para estágio ou pesquisa na área de formação	4	60
	Outras		
ATCO0750	Participação no Exame Nacional do Desempenho de Estudante (ENADE)	15	15
ATCO0345	Mobilidade Nacional	10|15	45
ATCO0285	Frequência e aprovação em disciplinas facultativas (outras Unidades Acadêmicas da UFU ou outra IES)	info	45
ATCO0706	Participação em projetos institucionais (PIBEG, PGB, PIBID, PROGRAD), sem registro no SIEX	15	30
ATCO0492	Participação em Competições Técnicas	5|10|20|30	90
ATCO0491	Participação em Competições Culturais, Artísticas, ou Esportivas	5|10|20	35
ATCO1191	Participação como ouvinte em eventos técnicos e/ou científicos (congressos, simpósios, seminários, mesa-redonda, workshops)	5|10	30
ATCO1192	Organização ou participação na organização de eventos institucionais, técnicos ou científicos para comunidade interna da UFU	10	30

A requisição para a quitação desse componente curricular é de responsabilidade do estudante que deverá apresentar requerimento com esse objetivo. O detalhamento das Atividades Acadêmicas Complementares consta em normas específicas[2] aprovadas nos âmbitos do Colegiado do Curso com anuência do NDE e da Unidade Acadêmica. Os casos omissos deverão ser tratados pelo Colegiado do Curso.

[2] https://www.feelt.ufu.br/graduacao/cibersegurançã/saiba-mais/atividades-complementares

8.8 Atividades Curriculares de Extensão

O curso é desenvolvido em 9 módulos, sendo que nos primeiros 7 módulos será desenvolvido pelo menos 1 (um) Projeto. No último ano, períodos 7 e 8, em 2 módulos será implementado um **Capstone**. No fluxo curricular, há um grupo de 7 disciplinas que regem a extensão no curso. São as disciplinas Atividades Curriculares de Extensão I a VII, com carga horária total de 405h.

As disciplinas de "Atividades Curriculares de Extensão" são distribuídas no curso na forma:

- Período 1 - "Atividades Curriculares de Extensão I", 60h;
- Período 2 - "Atividades Curriculares de Extensão II", 60h;
- Período 3 - "Atividades Curriculares de Extensão III", 60h;
- Período 4 - "Atividades Curriculares de Extensão IV", 60h;
- Período 5 - "Atividades Curriculares de Extensão V", 60h;
- Período 7 - "Atividades Curriculares de Extensão VI", 60h;
- Período 8 - "Atividades Curriculares de Extensão VII", 45h.

As atividades de extensão, que devem ser desenvolvidas em pelo menos 405h, são *integradas* a esses projetos, com problemas reais de empresas e comunidade, pactuados em planos de trabalho, indicadores e relatórios de impacto social/tecnológico. A validação de horas de extensão decorre das entregas dos projetos (sem ampliar a janela diária de aulas), conforme as regras institucionais. Ao final, no módulo 9, Projeto de Graduação II, o discente deve apresentar um **memorial de extensão** onde são apresentadas todas as atividades de extensão desenvolvidas por ele em todo curso.

A extensão universitária se destina a conectar a universidade à comunidade em que está inserida, compartilhando com o público externo o conhecimento obtido por meio do ensino e da pesquisa realizados internamente. Essa abordagem busca atuar na transformação da realidade social, intervindo para suprir deficiências identificadas, indo além da formação dos alunos regulares da instituição.

Sobre extensão universitária, este projeto pedagógico atende às seguintes legislações e diretrizes:

- Lei nº 13.005 de 25 de junho de 2014, que aprova o Plano Nacional de Educação – PNE, em especial sua Meta 12.7;
- Resolução CNE/CES nº 07/2018 de 18 de dezembro de 2018, estabelecendo as Diretrizes para a Extensão na Educação Superior Brasileira;

- Resolução nº 25/2019 do Conselho Universitário, definindo a Política de Extensão da Universidade Federal de Uberlândia;
- Resolução nº 05/2020 do Conselho de Extensão, Cultura e Assuntos Estudantis, relacionada ao Plano de Extensão da Unidade (PEX);
- Resolução nº 13/2019 do Conselho de Graduação, regulamentando a inserção de atividades de extensão nos Currículos dos Cursos de Graduação da Universidade Federal de Uberlândia.

No presente projeto, as atividades de extensão universitária junto à comunidade foram destacadas das Atividades Acadêmicas Complementares, para possibilitar o controle e o registro independente das ações extensionistas de cada discente visando ao atendimento da meta 12.7 da Lei nº 13.005/2014[3].

Este projeto propõe o controle e registro das atividades de extensão universitária de cada discente junto à comunidade, em conformidade com a legislação vigente, por meio de um Memorial de Atividades Curriculares de Extensão a ser apresentado no módulo “Projeto de Graduação II”.

No primeiro semestre, em “Atividade Curriculares de Extensão I”, serão apresentadas as práticas e normativas específicas relacionadas à extensão universitária, com o objetivo de preparar os(as) estudantes para jornadas acadêmicas extensionistas e explorar possibilidades de envolvimento em projetos.

As atividades de extensão desenvolvidas pelo discente nos 8 períodos do curso devem ser devidamente registradas na plataforma SIEX[4] da PROEXC/UFU. São exemplos de projetos extensionistas reconhecidos nos termos destas atividades:

- Projetos desenvolvidos em parceria ativa com a comunidade externa por docentes e/ou técnico-administrativos do curso ou da FEELT, registrados na plataforma SIEX;
- Projetos desenvolvidos em parceria ativa com a comunidade externa por docentes e/ou técnico-administrativos de outras unidades acadêmicas da UFU, registrados no SIEX;
- Projetos desenvolvidos em parceria ativa pelo(a) próprio(a) estudante com a comunidade externa, representada por empresas (inclusive o local de estágio externo), instituições, organizações públicas ou da sociedade civil, ou outras iniciativas com relevância social, desde que orientados por docentes ou técnico-administrativos da UFU e registrados no SIEX;
- Participação em projetos ou na administração da CONSELT[5], empresa júnior vinculada à FEELT, ou em outras empresas juniores da UFU, em razão de sua natureza extensionista e do vínculo institucional estabelecido por

[3] Meta de 10% dos créditos curriculares destinados à extensão universitária
[4] Sistema de Informação de Extensão da UFU - http://www.siex.proex.ufu.br/
[5] https://conselt.com.br/

meio de docentes ou técnico-administrativos da UFU que atuam como tutores;

- Contribuições efetivas — compreendidas como participações registradas, validadas por orientador(a) da UFU e preferencialmente aceitas nos repositórios principais — em projetos FOSS[6], OSHW[7], OSAI[8] ou outras iniciativas assim reconhecidas, com documentação técnica e códigos-fonte publicados em repositórios públicos amplamente reconhecidos, desde que a participação seja orientada por docentes ou técnico-administrativos da UFU e registrada no SIEX;
- Ações de comunicação pública do conhecimento, tais como podcasts, blogs, vlogs, vídeos ou outras mídias digitais, desde que fundamentadas na interação dialógica entre a universidade e a comunidade externa e resultem em produção conjunta ou retroalimentada de saberes, sob orientação de docentes ou técnico-administrativos da UFU e com registro no SIEX;
- Casos omissos deverão ser avaliados e aprovados pelo Colegiado do Curso com anuência do Núcleo Docente Estruturante (NDE) e da Coordenação de Extensão da Unidade Acadêmica.

A atividade “Memorial de Atividades Curriculares de Extensão” a ser desenvolvida no último período do curso tem como objetivo proporcionar um espaço coletivo de reflexão sobre o extensão e seu papel transformador. A aprovação no módulo “Projeto de Graduação II” está condicionada à entrega do memorial e à comprovação, por meio de certificados emitidos via plataforma SIEX, da carga horária mínima exigida de atividades de extensão (**405 horas**). O registro dos projetos de extensão no SIEX, necessário para a emissão dos certificados, é de responsabilidade dos respectivos coordenadores vinculados à UFU. Os estudantes têm liberdade para participar de quantos projetos desejarem, desde que cumpram integralmente a carga horária mínima prevista pelas diretrizes curriculares.

8.9 Metodologia

O curso utiliza uma metodologia onde a aprendizagem é baseada em projetos, ou “project-based learning” (PBL). A sua implementação é fundamentada nos

[6] *Free and Open Source Software*, software de código aberto e livre, conforme os princípios da *Open Source Initiative* disponíveis em https://opensource.org/osd, com tutoriais de colaboração e sites para encontrar projetos em https://www.firsttimersonly.com/

[7] *Open Source Hardware*, hardware livre e aberto, conforme os princípios da *Open Source Hardware Association*, disponíveis em https://oshwa.org/resources/open-source-hardware-definition/

[8] *Open Source Artificial Intelligence*, inteligência artificial aberta, conforme os princípios disponíveis em https://opensource.org/ai/open-source-ai-definition

seguintes pontos:

1. O curso está dividido em módulos semestrais e em cada semestre deve realizado um projeto, a partir de uma demanda real de um cliente, denominado de “parceiro de negócio”. Os parceiros de negócios são empresas (públicas e privadas), ONGs e outras organizações. Objetiva-se estimular a ação discente na relação teoria-prática.

2. Os parceiros de negócios submetem propostas em um modelo de fluxo contínuo por meio de um sítio que implementa o “Escritório de Projetos” (EP). Nesse ambiente, são apresentados os tipos de projeto que podem ser submetidos, em função dos módulos que serão cursados pelos alunos. As propostas mais alinhadas com os objetivos de aprendizagem dos módulos são selecionadas pela coordenação de Projetos. A coordenação de Projetos faz o trabalho de definição de escopo de um projeto selecionado, anteriormente ao seu início. Para cada módulo há um tipo de projeto que pode ser realizado.

3. Os projetos visam sempre o desenvolvimento de protótipos ou definição processos e procedimentos, ou seja, comportam-se como extensão e projetos de pesquisa científica e tecnológica. Além disso, tornam nativo no curso o conceito de curricularização da extensão. Em outras palavras, na prática, cada módulo do curso tem um projeto de extensão e de pesquisa. As atividades de extensão são registradas e gerenciadas na ACE’s (Atividades Curriculares de Extensão I a VIII).

4. Ao longo do projeto, os alunos desenvolvem competências em três eixos: negócios (ligadas a temas como administração, economia e empreendedorismo), socioemocionais (autoconhecimento, comunicação, colaboração, pensamento crítico e cidadania global) e conhecimento (cibersegurança, inteligência artificial e computação, conforme detalhado no Perfil do Egresso.

5. As competências socioemocionais são abordadas não somente de forma curricular, ao longo dos projetos, mas também de forma transversal em atividades realizadas internamentes na Faculdade de Engenharia Elétrica e demais unidades da UFU.

6. No padrão ideal, os alunos são alocados em turmas de 30 alunos, divididos em 6 grupos de 5 alunos cada. As salas de aula, denominadas “ateliês”, estão ajustadas para esse modelo, com 6 mesas cada,o devidamente equipadas e aparelhadas. Em cada turma é alocado um parceiro de negócio, ou seja, ao final o parceiro recebe 6 protótipos desenvolvidos por cada um dos 6 grupos de alunos. Para turmas de tamanhos distintos de 30 alunos, deve-se seguir uma distribuição aproximada da ideal.

7. Em cada turma há um professor exclusivo, chamado de “professor-orientador”, que se reúne com os alunos usualmente às segundas e sextas. Os professores-orientadores desempenham papel semelhante aos orientadores de pós-

graduação, qual seja, acompanhar e apoiar o desenvolvimento dos projetos pelos alunos, sendo contratados em regime integral para essa finalidade.

8. 8. Além desses, há os “professores-instrutores”, que se reúnem com os alunos usualmente às terças, quartas e quintas. Os professores-instrutores conduzem atividades relacionadas com suas áreas de especialidade, de forma que os respectivos conteúdos curriculares possam subsidiar o desenvolvimento do projeto em desenvolvimento e pesquisa.

9. Os módulos de 15 semanas são divididos em 7 *sprints* e 2 semanas cada e, em cada *sprint*, os alunos desenvolvem 3 tipos de atividades: encontros, autoestudo e desenvolvimento de projeto. Os encontros são atividades realizadas com os professores nos ateliês, conforme mencionado anteriormente. O autoestudo pode ser a leitura de textos previamente selecionados, assistir ou estudar conteúdos disponíveis na WEB (vídeos, cursos e canais de ensino), ou o uso da inteligência artificial para aprendizagem guiada. O desenvolvimento do projeto usa a metodologia SCRUM para seu gerenciamento. O sucesso do módulo é a realização do projeto propriamente dito, somadas às atividades de estudo realizadas.

10. O conjunto dessas atividades está previamente definido e compõe o chamado “Learning Backlog” (LBL), que é uma lista de atividades cadastrada em uma plataforma, que permite fazer em tempo real o acompanhamento dos alunos, por meio de detalhados painéis de controle.

9 Diretrizes Metodológicas do Ensino

O curso Cibersegurança, modalidade bacharelado, da Universidade Federal de Uberlândia adota uma concepção pedagógica centrada na formação integral do(a) estudante, combinando o desenvolvimento de conhecimentos técnico-científicos com habilidades práticas, atitudes éticas e capacidades reflexivas. As diretrizes metodológicas são pautadas por uma abordagem orientada por competências (Competency-Based Learning), que valoriza o protagonismo discente, a interdisciplinaridade e a articulação entre teoria e prática.

9.1 Princípios Metodológicos

As práticas de ensino-aprendizagem são orientadas pelos seguintes princípios:

- Integração entre teoria e prática, por meio de projetos, estudos de caso, práticas laboratoriais, desafios de engenharia e atividades extensionistas;
- Interdisciplinaridade, promovendo conexões entre áreas da ciência da computação, engenharia elétrica, eletrônica, controle e automação, ciências humanas e sociais aplicadas;
- Flexibilidade curricular, com espaço para percursos formativos personalizados, opcionais e reconhecimento de saberes adquiridos em experiências acadêmicas e profissionais;
- Aprendizagem ativa, com incentivo ao uso de metodologias como sala de aula invertida[1], aprendizagem baseada em projetos (PBL), resolução de problemas (ABP), estudos dirigidos e simulações computacionais;

[1] *Flipped Classroom*, modelo pedagógico em que a lição de casa tradicional se torna o aprendizado em casa, e as atividades em sala de aula são focadas em exercícios e discussões mais aprofundadas.

- Tecnologias digitais na educação, uso da inteligência artificial como tutoria, aproveitando plataformas virtuais, ambientes de codificação online, ferramentas colaborativas e sistemas de avaliação digital;
- Educação híbrida, integrando atividades presenciais e remotas de forma planejada, conforme a natureza dos componentes curriculares e as necessidades dos(as) estudantes;
- Formação continuada, com incentivo à aprendizagem ao longo da vida, à autonomia intelectual e à curiosidade investigativa.

9.2 Educação a Distância (EaD)

O curso Cibersegurança da UFU não adota a Educação a Distância (EaD) como uma ferramenta de ensino. Todavia, conforme o curso seja implantado e a metodologia de ensino proposta estiver madura, o uso da e EaD no curso será objeto de estudo.

9.3 Integração com Pesquisa, Extensão e Vivência Profissional

A metodologia do curso articula ensino, pesquisa e extensão como dimensões indissociáveis da formação universitária. Os(as) estudantes são incentivados(as) a participar de projetos de iniciação científica, programas de extensão, atividades em laboratórios especializados, empresas juniores, PET, hackathons, maratonas de programação, estágios e cooperação internacional.

Além disso, o curso valoriza as aprendizagens desenvolvidas em contextos extracurriculares, por meio de mecanismos formais de aproveitamento de estudos e competências adquiridas fora da sala de aula, conforme normativas internas da UFU.

9.4 Avaliação do Processo de Ensino-Aprendizagem

A avaliação no curso é formativa, diagnóstica e contínua, buscando não apenas aferir resultados, mas orientar o desenvolvimento progressivo das competências previstas. As estratégias de avaliação são variadas e contextualizadas, incluindo:

1. provas escritas e orais;
2. projetos e trabalhos em grupo;
3. atividades práticas e laboratoriais;
4. autoavaliações e coavaliações;
5. apresentações técnicas e relatórios;
6. portfólios e produções técnicas autorais.

A coerência entre métodos de ensino, objetivos da disciplina, competências visadas e formas de avaliação é elemento fundamental da qualidade do processo formativo.

10 Atenção ao Estudante

O curso Cibersegurança da UFU compreende que a excelência acadêmica exige um ambiente de aprendizagem acolhedor, saudável, diverso e acessível. Por isso, desenvolve e apoia ações de atenção estudantil em articulação com a FEELT e os órgãos centrais da universidade.

10.1 Acompanhamento Acadêmico e Pedagógico

A Coordenação do Curso e a Direção da FEELT acompanham ativamente o percurso dos(as) estudantes, prestando orientação individual, apoio à matrícula, aconselhamento pedagógico e mediação de conflitos acadêmicos. Também são promovidas ações de recepção de calouros e oficinas de ambientação universitária.

10.2 Assistência Estudantil e Políticas de Permanência

A Pró-Reitoria de Assistência Estudantil (PROAE) oferece suporte amplo aos(às) estudantes, com ações conduzidas por diretorias especializadas como a DIPAE (Diretoria de Inclusão, Promoção e Assistência Estudantil). Entre os programas e serviços, destacam-se:

- Auxílios financeiros para moradia, alimentação, transporte e creche;
- Bolsas acadêmicas (monitoria, PIBIC, extensão, PET);
- Apoio à acessibilidade e à inclusão de pessoas com deficiência;

- Acompanhamento psicopedagógico e social individualizado;
- Incentivo à inclusão digital e ao acesso universal ao conhecimento;
- Reconhecimento da diversidade étnico-racial, cultural e de gênero.

10.3 Saúde Mental e Bem-Estar Psicológico

A UFU mantém serviços de orientação em saúde mental por meio da Divisão de Saúde do Estudante, que atua em parceria com o Sistema de Saúde Universitário (SIS-UFU) e projetos de promoção de bem-estar. O atendimento contempla:

- Apoio psicológico individual e escuta qualificada;
- Encaminhamento para rede SUS quando necessário;
- Campanhas educativas e preventivas (ex: ansiedade, depressão, suicídio);
- Oficinas temáticas e grupos de apoio organizados pelo setor especializado.

Mais informações: https://proae.ufu.br/servicos/orientacao-em-saude-mental.

10.4 Promoção da Diversidade, Inclusão e Direitos Humanos

A UFU reafirma seu compromisso com o combate a todas as formas de preconceito, discriminação e exclusão. Campanhas institucionais e programas permanentes promovem o respeito às diferenças e a construção de um ambiente universitário mais justo, seguro e plural.

Ações voltadas ao combate à LGBTfobia, ao racismo, ao capacitismo e à xenofobia são desenvolvidas em articulação com o Comitê de Diversidade da UFU, os coletivos estudantis e os programas institucionais da PROAE.

Observação: A UFU também conta com comissões permanentes, grupos estudantis, projetos de extensão e programas de mentoria voluntária que fortalecem a escuta e o acolhimento à comunidade discente.

10.5 Canais de Apoio ao Estudante

A Universidade Federal de Uberlândia disponibiliza uma ampla rede de apoio aos(às) estudantes, com foco na permanência qualificada, saúde, inclusão e bem-estar. Para informações detalhadas, editais atualizados e inscrições, recomenda-se acompanhar regularmente:

- O site da Pró-Reitoria de Assistência Estudantil (PROAE):

  https://proae.ufu.br/tags/auxilios-estudantis.

- Editais PROAE publicados periodicamente e que contêm informações sobre auxílios diversos:

  https://proae.ufu.br/tags/auxilios-estudantis

- Fórum de Assuntos Estudantis, um espaço permanente de debate, proposição, negociação, reivindicação e encaminhamento de demandas referentes a política de assistência estudantil da universidade:

  https://proae.ufu.br/servicos/forum-de-assuntos-estudantis-fae

11 Avaliação

O processo de avaliação é fundamental para assegurar a qualidade da formação acadêmica, orientar o aperfeiçoamento das práticas pedagógicas e garantir que os objetivos do curso sejam atingidos de forma coerente e efetiva. A avaliação ocorre em dois níveis complementares: o da aprendizagem discente e o do curso como um todo.

11.1 Avaliação da Aprendizagem

A avaliação da aprendizagem no curso Cibersegurança é formativa, contínua, diagnóstica e somativa, conforme previsto no Regimento Geral da UFU e nas diretrizes pedagógicas da FEELT. Seu principal objetivo é acompanhar o desenvolvimento progressivo das competências cognitivas, técnicas e atitudinais previstas no perfil do egresso.

As principais características desse processo são:

- Caráter processual, com instrumentos variados aplicados ao longo do semestre letivo;
- Foco em competências, privilegiando a capacidade do(a) estudante em aplicar conhecimentos em situações reais ou simuladas;
- Diversidade de métodos, incluindo provas escritas e orais, relatórios técnicos, projetos, atividades práticas, autoavaliações, apresentações, seminários, experimentações e resolução de problemas;
- Critérios transparentes, previamente definidos nos planos de ensino, permitindo que o(a) estudante conheça os objetivos e os parâmetros de avaliação desde o início do componente curricular;

- Oportunidade de recuperação, assegurada conforme o Regulamento da Graduação da UFU, para estudantes que não alcançarem o rendimento mínimo satisfatório;
- Registro sistemático, realizado por meio de sistema de gestão acadêmica, com acesso garantido ao(à) discente.

A avaliação não se limita à aferição de resultados, mas constitui um instrumento de acompanhamento, *feedback* e reorientação pedagógica, em consonância com os princípios da aprendizagem significativa, da interdisciplinaridade e do ensino centrado no estudante.

11.2 Avaliação do Curso

A avaliação do curso Cibersegurança da UFU ocorre de forma permanente, participativa e orientada para a melhoria contínua, envolvendo docentes, discentes, técnico-administrativos e coordenação.

Esse processo se dá por meio de:

- Autoavaliação institucional coordenada pela CPA (Comissão Própria de Avaliação), com aplicação de instrumentos periódicos junto à comunidade acadêmica;
- Relatórios semestrais de acompanhamento da coordenação do curso, com base em indicadores de rendimento, evasão, trancamentos, participação em programas acadêmicos e empregabilidade dos egressos;
- Revisão e atualização do Projeto Pedagógico do Curso, realizada periodicamente com base nos dados da autoavaliação, demandas da sociedade e atualizações das diretrizes nacionais;
- Participação ativa do NDE (Núcleo Docente Estruturante), responsável por analisar o desenvolvimento do currículo e propor ajustes em componentes curriculares, metodologias e estratégias avaliativas;
- Mecanismos de escuta ativa e representação discente, por meio do colegiado do curso e da participação dos estudantes em comissões internas;
- Instrumentos externos de avaliação, como o ENADE, cujos resultados são analisados e utilizados na formulação de ações de melhoria do desempenho coletivo e da formação.

A Avaliação do Curso é parte integrante do processo de gestão acadêmica participativa e visa promover uma cultura institucional de autocrítica, inovação e excelência na formação de profissionais da segurança da informação.

11.3 Procedimentos de acompanhamento e avaliação do ensino-aprendizagem

A metodologia empregada na avaliação está fundamentada no conceito de "Learning Backlog (LBL)", que consiste em um conjunto de atividades previamente definidas para cada módulo, correlacionando as competências do perfil do egresso com os conteúdos curriculares. As atividades são organizadas em três tipos: encontros com os professores, autoestudos de materiais selecionados e desenvolvimento do protótipo/solução do projeto.

Em geral, um LBL apresenta de 150 a 200 atividades por módulo de 15 (ou 18) semanas, ou seja, de 10 a 14 atividades por semana. As atividades não devem ser necessariamente executadas em datas pré-estabelecidas, admitindo-se apenas uma exceção. A recomendação semanal visa garantir a autonomia discente no que diz respeito à gestão do seu próprio aprendizado. O planejamento é realizado com o apoio e a supervisão de seus professores orientadores.

Ademais, a própria natureza das atividades, sobretudo os autoestudos e o desenvolvimento, tem como cerne a aprendizagem ativa, ou seja, o aluno é o protagonista de seu próprio aprendizado, gerenciando sua própria autonomia. É importante mencionar, todavia, que, como se trata de um curso presencial, mesmo nessas atividades em que há mais autonomia, a presença dos alunos é verificada e sempre há supervisão docente.

O aluno será considerado aprovado se obtiver, no mínimo, 60 pontos ao final do módulo e apresentar, no mínimo, 75% de presença. A avaliação em questão abarca o conjunto de atividades do LBL no módulo em sua totalidade. Isso significa que todas as disciplinas e seus respectivos conteúdos curriculares estão integrados e consolidados de forma transdisciplinar. A avaliação é organizada por módulos, não por disciplina. Os discentes que obtiverem reprovação devem realizar o módulo novamente de forma integral, incluindo todas as disciplinas correlatas.

12 Acompanhamento de Egressos

O curso Cibersegurança da Universidade Federal de Uberlândia reconhece a importância do acompanhamento sistemático de seus egressos como ferramenta para:

- Avaliar a efetividade da formação oferecida;
- Identificar demandas do mercado de trabalho e tendências tecnológicas;
- Promover a atualização do Projeto Pedagógico do Curso (PPC);
- Fortalecer o vínculo institucional com os profissionais formados;
- Incentivar a participação de ex-alunos(as) em projetos, eventos e processos formativos.

12.1 Instrumentos e Estratégias de Acompanhamento

Atualmente, o acompanhamento dos egressos ocorre por meio de:

- Aplicação periódica de questionários de egresso, organizados pela Coordenação do Curso, com apoio do Núcleo Docente Estruturante (NDE) do curso e da Comissão Própria de Avaliação (CPA) da UFU, a fim de mapear trajetórias profissionais, empregabilidade, continuidade de estudos e percepção sobre a formação recebida;
- Participação de egressos em eventos acadêmicos, como semanas de curso, seminários, bancas de TCC, oficinas de carreira, rodas de conversa e eventos de boas-vindas;
- Contato com egressos por meio de redes sociais, grupos de ex-alunos e mailing institucional, com apoio da Direção da FEELT e do setor de comunicação da UFU;

- Levantamento de indicadores institucionais (tais como tempo até o primeiro emprego, faixa salarial, área de atuação, envolvimento com pesquisa e inovação) a partir de dados coletados localmente e em parceria com a CPA.

12.2 Objetivos do acompanhamento de egressos

As informações obtidas por esses mecanismos subsidiam:

- A revisão da matriz curricular e o ajuste de conteúdos e metodologias;
- A validação do perfil profissional do egresso, conforme as necessidades da sociedade e dos setores produtivos;
- O fortalecimento da articulação com o mercado de trabalho e com ex-alunos(as) em posições estratégicas;
- O desenvolvimento de políticas institucionais de educação continuada, pós-graduação e formação permanente.

A UFU, por meio da CPA e dos colegiados de curso, estimula a construção de políticas institucionais permanentes para o acompanhamento de egressos, integrando bases de dados, experiências bem-sucedidas e iniciativas dos cursos de graduação.

13 Considerações Finais

O Projeto Pedagógico do curso Cibersegurança, modalidade bacharelado, da Universidade Federal de Uberlândia reflete o compromisso da instituição com a formação de profissionais éticos, tecnicamente qualificados, inovadores e socialmente responsáveis. Estruturado em consonância com a Resolução CNE/CES nº 5/2016, com as diretrizes do Computing Curricula for 2025 e com o Projeto Institucional da UFU, este PPC apresenta uma proposta formativa fundamentada em competências, interdisciplinaridade, integração teoria-prática e valorização da diversidade humana e cultural.

A matriz curricular, os objetivos do curso, o perfil do egresso, as estratégias de ensino e os mecanismos de avaliação foram cuidadosamente definidos para garantir uma formação alinhada aos desafios tecnológicos contemporâneos e às demandas da sociedade. O curso busca oferecer ao(à) estudante um percurso formativo flexível, crítico, inovador e capaz de dialogar com a complexidade do mundo do trabalho, da ciência e da vida em sociedade.

Este documento expressa também a valorização do diálogo entre discentes, docentes, técnicos(as) e gestores(as), bem como o papel estratégico da universidade pública no desenvolvimento regional e nacional. O bacharelado em Cibersegurança da FEELT/UFU reafirma, assim, sua missão de formar profissionais comprometidos com a excelência acadêmica, a justiça social e a construção de um futuro sustentável.

14 Anexo
Ementas dos Módulos

Módulo 01 — Programação e Matemática Aplicada

Carga horária: 150 horas

Ementa

O módulo inaugura a formação em programação e matemática articulada à metodologia de projetos do curso Cibersegurança. Destina-se a discentes sem experiência prévia em desenvolvimento de *software* e enfatiza competências essenciais à prática profissional: trabalho em equipe, comunicação, pensamento crítico, resolução de problemas e resiliência. Por meio de problemas autênticos, os estudantes exploram lógica e estruturas de programação, fundamentos de álgebra linear, cálculo numérico, lógica matemática, além de tópicos introdutórios de arquitetura de computadores e sistemas digitais. O percurso integra *design thinking*, modelagem, prototipação e gestão ágil de projetos (*SCRUM*), conectando análise setorial e posicionamento estratégico ao ciclo de vida de produtos de software. Ao final, espera-se a entrega de um protótipo funcional que demonstre domínio conceitual e técnico, alinhado a necessidades pactuadas com um “cliente” da turma e a valores de diversidade, inclusão, acessibilidade e impacto social.

Objetivos de Aprendizagem

Ao término do módulo, o discente deverá ser capaz de:

1. Modelar problemas e conceber soluções computacionais utilizando lógica algorítmica, estruturas de controle e modularização.
2. Aplicar conhecimentos de álgebra linear, cálculo numérico e lógica matemática ao raciocínio e à validação de soluções.

3. Empregar boas práticas de programação (padrões de codificação, depuração, testes iniciais) em artefatos de baixa complexidade.
4. Planejar e executar projetos com métodos ágeis (*SCRUM*), documentando requisitos (histórias de usuário) e critérios de qualidade.
5. Utilizar princípios de *design thinking*, HCI e visualização para prototipar interfaces e comunicar soluções.
6. Analisar cenários, posicionamento e riscos (SWOT) para fundamentar decisões de produto e estratégia de entrega.
7. Produzir e apresentar um protótipo funcional (por exemplo, um jogo ou aplicação educacional) com documentação técnica e narrativa do projeto.
8. Apresentar e analisar os usos sociais da tecnologia à luz de específicas questões tais como gênero, desigualdade de renda e dos desafios contemporâneos da diversidade e da inclusão.

Conteúdos Programáticos

1. Fundamentos de Programação

- Lógica algorítmica; entrada e saída de dados; estruturas de controle e repetição; funções e modularização; depuração.
- Técnicas de programação para problemas de baixa complexidade; padrões de codificação; projeto de algoritmos; paradigmas (procedural, OO, funcional).
- Estruturas de dados: TAD Lista e Pilha; análise elementar de complexidade; algoritmos de busca e ordenação.

2. Matemática Aplicada

- Álgebra linear aplicada a redes, criptografia e aprendizagem de máquina: vetores, matrizes, transformações lineares, auto-valores e auto-vetores.
- Cálculo numérico: resolução numérica de sistemas lineares; noções de estabilidade e erro; otimização básica.
- Lógica matemática: cálculo proposicional e cálculo de predicados de primeira ordem.

3. Arquitetura e Sistemas Digitais (noções)

- Arquitetura de computadores; álgebra booleana; máquinas de estado; história e fundamentos da computação (visão).
- Teoria da computação (introdução): modelos e limites computacionais (visão histórica e conceitual).

4. Engenharia de Software e Projetos

- Conceitos de produto, processos e modelos de desenvolvimento; elicitação e engenharia de requisitos; requisitos funcionais e não funcionais; histórias de usuário.
- Qualidade de *software* e testes: casos de teste, planejamento de testes, abordagens de testes, *testability* inicial. Empregar Git + testes automatizados mínimos (build/test) e relatório de qualidade (lint/coverage) em projeto curto;
- Gestão ágil: *SCRUM* (papéis, eventos, artefatos); execução e monitoramento de projetos; ciclo de vida de projetos; ferramentas de gestão de tempo (ex.: Pomodoro) e priorização.

5. Interação Humano–Computador, Design e Visualização

- Design de interação, *design thinking*, design universal; personas, prototipação e usabilidade; experiência do usuário (UX).
- Visualização e *storytelling* de dados aplicados à comunicação do projeto e de resultados.
- Computação gráfica (noções): modelagem e transformações geométricas; animação de imagens (aplicado a jogos/protótipos).

6. Estratégia, Negócios e Sociedade

- Análise de cenário; diferenciação, posicionamento e segmentação; frameworks (Oceano Azul, 5 Forças, 4Ps, 6D *disruption*); matriz SWOT e riscos; Product Box e *Canvas Value Proposition*; *startup pitches*.
- Fundamentos de sistemas de informação e teoria geral de sistemas; paradigmas e linguagens de programação (visão geral); POO (introdução).
- Aprendizagem pessoal e organizacional; organização do tempo e aprendizagem; comunicação não violenta, escuta ativa e empatia; liderança e propósito individual.
- Diversidade, inclusão e acessibilidade; história e cultura afro-brasileira, africana e indígena; relações étnico-raciais; direitos humanos; ética na computação e impacto social da informática.
- Noções de finanças aplicadas a produtos (fluxo de caixa, juros simples e compostos, NPV/IRR/PV/FV) para embasar decisões de prototipagem e entrega.

Metodologia

Aprendizagem baseada em projetos (*project-based learning*) com *sprints* quinzenais e rituais *SCRUM*; oficinas de modelagem e prototipação; laboratórios de programação; estudos de caso; *code review* e demonstrações incrementais; aprendizagem guiada por inteligência artificial e atividades de reflexão ética e de inclusão.

Avaliação

A avaliação do estudante se dá através de dois caminhos:

50% Avaliação das atividades de autoestudo e atividades definidas no *backlog* de cada estudante;

50% Avaliação formativa e somativa do projeto, considerando: (i) entregas incrementais (código, protótipos, documentação); (ii) testes e demonstrações funcionais; (iii) relatórios de requisitos, arquitetura inicial e estratégia de produto; (iv) apresentação pública do protótipo; (v) participação e colaboração em equipe.

Competências Desenvolvidas (síntese)

Raciocínio algorítmico e matemático; fundamentos de programação e estruturas de dados; noções de arquitetura e sistemas digitais; engenharia de requisitos e qualidade; gestão ágil de projetos; design e usabilidade; comunicação técnica, liderança e trabalho em equipe; consciência ética, diversidade e impacto social, uso da inteligência artificial no processo de aprendizagem e desenvolvimento de projetos.

Bibliografia Básica

CORMEN, T. H.; LEISERSON, C. E.; RIVEST, R. L.; STEIN, C. *Algoritmos: teoria e prática*. 4. ed. Rio de Janeiro: Grupo GEN, 2022.

GOODRICH, M. T.; TAMASSIA, R.; GOLDWASSER, M. H. *Data Structures and Algorithms in Python*. Hoboken: Wiley, 2013.

MENEZES, N. N. C. *Introdução à Programação com Python*. 4. ed. São Paulo: Novatec, 2024.

SOMMERVILLE, I. *Engenharia de Software*. 10. ed. São Paulo: Pearson, 2019.

PRESSMAN, R. S.; MAXIM, B. R. *Engenharia de Software: uma abordagem profissional*. 9. ed. Porto Alegre: AMGH, 2021.

SUTHERLAND, J. *SCRUM: a arte de fazer o dobro do trabalho na metade do tempo*. Rio de Janeiro: Leya, 2016.

PATTERSON, D. A.; HENNESSY, J. L. *Organização e Projeto de Computadores*. 5. ed. Rio de Janeiro: Elsevier, 2014.

MANO, M. M.; CILETTI, M. D. *Projeto de Sistemas Digitais*. 5. ed. São Paulo: Pearson, 2015.

SIPSER, M. *Introduction to the Theory of Computation*. 3rd ed. Boston: Cengage Learning, 2012.

LAY, D. C.; LAY, S. R.; McDONALD, J. J. *Álgebra Linear e Suas Aplicações*. 5. ed. Rio de Janeiro: LTC, 2016.

BURDEN, R. L.; FAIRES, J. D. *Análise Numérica*. 9. ed. São Paulo: Cengage Learning, 2015.

HUTH, M.; RYAN, M. *Logic in Computer Science: Modelling and Reasoning about Systems*. 2nd ed. Cambridge: Cambridge University Press, 2004.

ROGERS, Y.; SHARP, H.; PREECE, J. *Design de Interação: além do humano-computador*. 4. ed. Porto Alegre: Bookman, 2013.

KNAFLIC, C. N. *Storytelling com Dados*. Rio de Janeiro: Alta Books, 2017.

Bibliografia Complementar

MARTIN, R. C. *Código Limpo: habilidades práticas do Agile Software*. Rio de Janeiro: Alta Books, 2009.

MARTIN, R. C. *Arquitetura Limpa*. Rio de Janeiro: Alta Books, 2019.

KLEINBERG, J.; TARDOS, É. *Algorithm Design*. Boston: Pearson, 2005.

SEDGEWICK, R.; WAYNE, K. *Algorithms*. 4th ed. Boston: Addison-Wesley, 2011.

MILLER, B. N.; RANUM, D. L. *Problem Solving with Algorithms and Data Structures Using Python*. 3rd ed. Open Book Project, 2013.

DELAMARO, M. E.; MALDONADO, J. C.; JINO, M. *Introdução ao Teste de Software*. 2. ed. Rio de Janeiro: Elsevier, 2014.

AMMANN, P.; OFFUTT, J. *Introduction to Software Testing*. 2nd ed. Cambridge: Cambridge University Press, 2016.

KNAPP, J.; ZERATSKY, J.; KOWITZ, B. *Sprint*. Rio de Janeiro: Intrínseca, 2017.

BROWN, T. *Design Thinking*. Rio de Janeiro: Alta Books, 2020.

KELLEY, T.; KELLEY, D. *Confiança Criativa*. São Paulo: HSM, 2014.

OSTERWALDER, A.; PIGNEUR, Y. *Business Model Generation*. Rio de Janeiro: Alta Books, 2011.

OSTERWALDER, A. et al. *Value Proposition Design*. Rio de Janeiro: Alta Books, 2015.

KIM, W. C.; MAUBORGNE, R. *A Estratégia do Oceano Azul*. Rio de Janeiro: Elsevier/Campus, 2015.

RIES, E. *A Startup Enxuta*. São Paulo: Leya, 2012.

CAGAN, M.; JONES, C. *INSPIRED*. São Paulo: Alta Books, 2018.

KRUG, S. *Não me faça pensar!*. 3. ed. Porto Alegre: Bookman, 2014.

NORMAN, D. A. *O Design do Dia-a-Dia*. 2. ed. Rio de Janeiro: Rocco, 2018.

TUFTE, E. R. *The Visual Display of Quantitative Information*. 2nd ed. Cheshire: Graphics Press, 2001.

MUNZNER, T. *Visualization Analysis and Design*. Boca Raton: CRC Press, 2014.

HEARN, D.; BAKER, M. P. *Computação Gráfica com OpenGL*. 4. ed. São Paulo: Pearson, 2011.

FOLEY, J.; VAN DAM, A.; FEINER, S.; HUGHES, J. *Computer Graphics: Principles and Practice*. 3rd ed. Boston: Addison-Wesley, 2013.

TOCCI, R. J.; WIDMER, N. S.; MOSS, G. L. *Sistemas Digitais: princípios e aplicações*. 11. ed. São Paulo: Pearson, 2011.

HOPCROFT, J. E.; MOTWANI, R.; ULLMAN, J. D. *Introdução à Teoria de Autômatos, Linguagens e Computação*. 3. ed. São Paulo: Pearson, 2008.

VAN LOAN, C. F. *Introduction to Scientific Computing*. 2nd ed. Upper Saddle River: Prentice Hall, 1997.

ENDERTHON, H. B. *A Mathematical Introduction to Logic*. 2nd ed. San Diego: Academic Press, 2001.

BENYON, D. *Interação Humano-Computador*. 3. ed. São Paulo: Pearson, 2011.

QUINN, M. J. *Ethics for the Information Age*. 8th ed. Boston: Pearson, 2020.

COSTANZA-CHOCK, S. *Design Justice*. Cambridge: MIT Press, 2020.

O'NEIL, C. *Algoritmos de Destruição em Massa*. São Paulo: Rua do Sabão, 2017.

SWEIGART, A. *Automate the Boring Stuff with Python*. 2nd ed. San Francisco: No Starch Press, 2019.

Módulo 2 — Aplicação para ambiente WEB

Carga horária: 150 horas

Ementa

O módulo introduz o desenvolvimento de aplicações WEB como suporte a processos organizacionais intensivos em Internet, articulando fundamentos de computação, engenharia de *software* e gestão de projetos. Por meio de abordagem prática, os discentes planejam, concebem, implementam e validam soluções cliente–servidor, exercitando rituais ágeis (*SCRUM*), versionamento e colaboração (Git), prototipação guiada por *design thinking* e princípios de usabilidade/experiência do usuário. A construção de *front-end* (HTML, CSS, JavaScript) e *back-end* (arquitetura de serviços, APIs, camadas de aplicação) é integrada a modelagem de dados (relacional, documentos e grafos), protocolos e arquitetura da Web, redes TCP/IP e fundamentos de segurança e privacidade (LGPD). São incorporados tópicos de algoritmos (busca, ordenação, grafos), estruturas de dados, matemática discreta, probabilidade e estatística aplicadas. Os usos da tecnologia à luz de específicas questões tais como aspectos ambientais e econômicos, educação ambiental. O módulo ancora-se em problemas reais de organizações, conectando estratégia, inovação e viabilidade de negócio, e promovendo competências transversais de comunicação, trabalho em equipe e liderança.

Objetivos de Aprendizagem

Ao final do módulo, o discente deverá ser capaz de:

1. Contextualizar requisitos de negócio e traduzi-los em especificações funcionais e não funcionais para aplicações Web.
2. Planejar e executar projetos ágeis, conduzindo rituais *SCRUM*, uso de Git e integração contínua básica.
3. Projetar e implementar *front-end* (HTML, CSS, JavaScript) com padrões de interação, acessibilidade e usabilidade.
4. Projetar e implementar *back-end* com camadas de aplicação, padrões arquiteturais (MVC/MVP/MVVM) e integração com bancos de dados.
5. Modelar dados (conceitual e lógica) em paradigmas relacional, documentos e grafos; empregar SQL básico e operações de manipulação.
6. Compreender a arquitetura da Web e os protocolos de comunicação (TCP e UDP, HTTP e HTTPS), relacionando-os ao funcionamento da solução.
7. Aplicar princípios de segurança da informação, privacidade e conformidade (LGPD) no ciclo de vida do software.

8. Utilizar fundamentos de algoritmos, estruturas de dados, matemática discreta, probabilidade e estatística no raciocínio e tomada de decisão do projeto.
9. Apresentar e analisar os usos da tecnologia à luz de específicas questões tais como aspectos ambientais e econômicos.
10. Apresentar, documentar e defender soluções com clareza, colaborando em equipes multidisciplinares.

Conteúdos Programáticos

1. Engenharia de Software e Gestão de Projetos

- Elicitação e engenharia de requisitos; requisitos funcionais e não funcionais; histórias de usuário; métricas de software.
- Processos e métodos: PMI/PMBOK (visão), metodologias ágeis, *SCRUM* (papéis, eventos, artefatos), ferramentas de gestão.
- Planejamento e controle de testes: testes unitários, de interface (robôs), critérios de aceitação e qualidade de software.
- Versionamento e colaboração com Git; fluxos de *branches*; *pull requests*; revisão por pares.

2. Front-end e Interação Humano–Computador

- Arquitetura da Web no cliente; HTML semântico; CSS (layout e responsividade); JavaScript e APIs de navegador.
- Padrões de projeto (MVC/MVP/MVVM) no cliente; eventos; componentes; XMLHttpRequest/*fetch*.
- Design de interação e *design thinking*; personas, jornadas, prototipação; usabilidade e UX; acessibilidade.

3. Back-end, Dados e Integração

- Camada de aplicação; servidores de páginas e de aplicação; APIs REST; integração cliente–servidor.
- Modelagem conceitual e lógica; bancos relacionais (SQL básico, DDL/DML); bancos de documentos e de grafos.
- Arquiteturas de dados *on-premises* e em nuvem; fundamentos de desempenho e escalabilidade.

4. Redes e Arquitetura da Internet

- Arquitetura TCP/IP; endereçamento; TCP e UDP; redes sem fio e IP móvel; programação de *sockets* (noções).
- Protocolo HTTP/HTTPS; camadas de aplicação e transporte; diagnóstico básico de rede para aplicações Web.
- Virtualização e containers; Kubernetes básicos; serviços em nuvem (IaaS/-PaaS).

5. Segurança, Privacidade e Conformidade

- Princípios de segurança da informação; políticas (ISO/IEC 27001); controle de acesso; auditoria.
- Criptografia (noções): chaves, confidencialidade, integridade; uso seguro de HTTPS; boas práticas em aplicações Web e móveis.
- LGPD: privacidade e direitos dos titulares; *privacy-by-design* aplicado à solução desenvolvida.

6. Fundamentos Analíticos e de Computação

- Algoritmos de busca e ordenação; análise de complexidade (noções).
- Estruturas de dados e TADs (vetores, árvores, grafos).
- Matemática discreta: relações e funções; recorrência/recursão; teoria dos grafos (grafos, subgrafos, caminhos, ciclos).
- Probabilidade e estatística: variáveis aleatórias, estatística descritiva, distribuições (noções), aplicação a decisões de projeto.

7. Estratégia, Negócios e Aspectos Ambientais e Sociais

- Estratégia e inovação: *frameworks* (Oceano Azul, 5 Forças, 4Ps, 6D *disruption*); mentalidade empreendedora; planos de negócio.
- Comunicação, linguagem e *pitch*; escuta ativa, comunicação não violenta, empatia e trabalho em equipe.
- Ética na computação; educação ambiental; impacto ambiental da informática; futuro da computação.
- Noções de finanças: fluxo de caixa; juros simples e compostos; NPV/IR-R/PV/FV (visão aplicada à viabilidade de produtos Web).
- Os usos da tecnologia à luz de específicas questões tais como aspectos ambientais e econômicos.

Metodologia

Aprendizagem baseada em projetos (*project-based learning*) com *sprints* quinzenais e rituais *SCRUM*; oficinas de modelagem e prototipação; laboratórios de programação; estudos de caso; laboratórios práticos de *front-end*/*back-end*; exercícios guiados de modelagem de dados; *code review* e integração contínua básica; aprendizagem guiada por inteligência artificial e atividades de reflexão ética e de comunicação técnica.

Avaliação

A avaliação do estudante se dá através de dois caminhos:

50% Avaliação das atividades de autoestudo e atividades definidas no *backlog* de cada estudante;

50% Avaliação formativa e somativa do projeto baseada em: (i) entregas incrementais do projeto (código, protótipos e documentação); (ii) testes e demonstrações funcionais; (iii) relatórios técnicos e de reflexão (UX, segurança/privacidade e viabilidade); (iv) apresentação pública do produto; e (v) participação e colaboração em equipe.

Competências Desenvolvidas (síntese)

Trabalho em equipe e liderança; comunicação técnica e *pitch*; pensamento crítico e resolução de problemas; raciocínio algorítmico e modelagem; *secure coding* e privacidade; concepção e entrega de aplicações Web cliente–servidor orientadas a requisitos de negócio, uso da inteligência artificial no processo de aprendizagem e desenvolvimento de projetos.

Bibliografia Básica

CHACON, S.; STRAUB, B. *Pro Git*. 2. ed. Berkeley: Apress, 2014.

DUCKETT, J. *HTML e CSS: projete e construa websites*. Rio de Janeiro: Alta Books, 2014.

FLANAGAN, D. *JavaScript: The Definitive Guide*. 7th ed. Sebastopol: O'Reilly, 2020.

HAVERBEKE, M. *Eloquent JavaScript*. 3rd ed. San Francisco: No Starch Press, 2018.

SIMPSON, K. *You Don't Know JS Yet: Get Started*. Sebastopol: O'Reilly, 2020.

ROGERS, Y.; SHARP, H.; PREECE, J. *Design de Interação: além do humano-computador*. 4. ed. Porto Alegre: Bookman, 2013.

HORTON, S.; QUESENBERY, W. *A Web for Everyone: Designing Accessible User Experiences*. Brooklyn: Rosenfeld Media, 2014.

RICHARDSON, L.; AMUNDSEN, M.; RUBY, S. *RESTful Web APIs*. Sebastopol: O'Reilly, 2013.

AMUNDSEN, M. *Designing Web APIs*. Sebastopol: O'Reilly, 2020.

KLEPPMANN, M. *Designing Data-Intensive Applications*. Sebastopol: O'Reilly, 2017.

SILBERSCHATZ, A.; KORTH, H. F.; SUDARSHAN, S. *Sistemas de Banco de Dados*. 7. ed. Rio de Janeiro: LTC, 2020.

BEAULIEU, A. *Learning SQL*. 3rd ed. Sebastopol: O'Reilly, 2020.

ROBINSON, I.; WEBBER, J.; EIFREM, E. *Graph Databases*. 2nd ed. Sebastopol: O'Reilly, 2015.

GOURLEY, D. et al. *HTTP: The Definitive Guide*. Sebastopol: O'Reilly, 2002.

GRIGORIK, I. *High Performance Browser Networking*. Sebastopol: O'Reilly, 2013.

ZALEWSKI, M. *The Tangled Web: A Guide to Securing Modern Web Applications*. San Francisco: No Starch Press, 2012.

BIONI, B. R. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2021.

ROSEN, K. H. *Matemática Discreta e suas Aplicações*. 7. ed. Porto Alegre: AMGH, 2011.

Bibliografia Complementar

KRUG, S. *Não me faça pensar!*. 3. ed. Porto Alegre: Bookman, 2014.

COOPER, A. et al. *About Face: The Essentials of Interaction Design*. 4th ed. Indianapolis: Wiley, 2014.

VEROU, L. *CSS Secrets*. São Paulo: Novatec, 2017.

STEFANOV, S. *JavaScript Patterns*. Sebastopol: O'Reilly, 2010.

COSTA, L. *Testing JavaScript Applications*. Shelter Island: Manning, 2021.

FOWLER, M. *Patterns of Enterprise Application Architecture*. Boston: Addison-Wesley, 2003.

NEWMAN, S. *Building Microservices*. 2nd ed. Sebastopol: O'Reilly, 2021.

RICHARDSON, C. *Microservices Patterns*. Shelter Island: Manning, 2018.

MASSE, M. *REST API Design Rulebook*. Sebastopol: O'Reilly, 2011.

AGARWAL, R.; ANDERSON, B.; GUPTA, V. *OAuth 2 in Action*. Shelter Island: Manning, 2017.

PETROV, A. *Database Internals*. Sebastopol: O'Reilly, 2019.

KARWIN, B. *SQL Antipatterns: Avoiding the Pitfalls of Database Programming*. Dallas: Pragmatic Bookshelf, 2010.

CHODOROW, K. *MongoDB: The Definitive Guide*. 3rd ed. Sebastopol: O'Reilly, 2019.

KUROSE, J. F.; ROSS, K. W. *Redes de Computadores e a Internet: uma abordagem top-down*. 6. ed. São Paulo: Pearson, 2013.

TANENBAUM, A. S.; WETHERALL, D. *Redes de Computadores*. 5. ed. São Paulo: Pearson, 2011.

STUTTARD, D.; PINTO, M. *The Web Application Hacker's Handbook*. 2nd ed. Indianapolis: Wiley, 2011.

HOFFMAN, A. *Web Application Security*. Sebastopol: O'Reilly, 2020 (ou 2024, ed. atualizada).

HUMBLE, J.; FARLEY, D. *Continuous Delivery*. Boston: Addison-Wesley, 2010.

DELAMARO, M. E.; MALDONADO, J. C.; JINO, M. *Introdução ao Teste de Software*. 2. ed. Rio de Janeiro: Elsevier, 2014.

AMMANN, P.; OFFUTT, J. *Introduction to Software Testing*. 2nd ed. Cambridge: Cambridge Univ. Press, 2016.

QUINN, M. J. *Ethics for the Information Age*. 8th ed. Boston: Pearson, 2020.

Módulo 3 — Segurança WEB

Carga horária: 300h

Ementa

Introdução prática e fundamentada à *Web Security*, com ênfase nos vetores **CSRF** (Cross-Site Request Forgery) e **XSS** (Cross-Site Scripting) e em bases de dados para aplicações Web. O módulo explora o ciclo completo de concepção–implementação–validação de controles (tokens secretos, *same-site cookies*, política de conteúdo – *Content Security Policy*) em cenários de *GET*/*POST*, além de refletido, persistente e *DOM-based XSS* e sua autoprogação (*worms*). Integra fundamentos de **bancos de dados** (relacional, não relacional e arquitetura *cloud*), comunicação e colaboração (ferramentas, bloqueios e intencionalidade comunicacional), diversidade social no Brasil e estratégia/inovação (análise de cenário, transformação digital e inovação aberta), conectando decisões técnicas a impactos organizacionais e sociais. **SQL e injeção** (causas e *prepared statements*), **SQL Injection** em aplicações cliente–servidor, integração com rede e sistemas distribuídos e governança/gestão de dados na operação. O módulo cobre o ciclo de exploração–defesa de *SQLi* (demonstrações com `curl`, múltiplas instruções, modificação de base, causa fundamental e contramedidas robustas) e consolida arquitetura Web segura sobre **TCP**/**IP**, protocolos e *sockets*, além de fundamentos de sistemas distribuídos (concorrência, sincronização, objetos/-componentes, segurança). Integra aspectos organizacionais (contratos, direitos e deveres trabalhistas), governança de dados e indicadores/OKRs, liderança (adaptabilidade e vulnerabilidade) e fundamentos político-econômicos (Direitos Humanos e economia sustentável) para sustentar decisões técnicas e de gestão.

Objetivos de Aprendizagem

Ao término do módulo, o discente deverá ser capaz de:

1. Explicar o modelo de ameaças Web para **CSRF** e **XSS** e projetar controles (tokens, *same-site*, CSP, sanitização/escape).
2. Diferenciar serviços *HTTP GET/POST*, identificar superfícies de ataque e construir provas de conceito controladas.
3. Modelar dados e selecionar **bancos de dados** (relacional/não relacional) e arquiteturas *cloud* adequadas ao contexto da aplicação.
4. Aplicar boas práticas de **SQL seguro** (validação, *encoding*, *prepared statements*) e reconhecer as causas fundamentais da *SQL Injection*.

5. Utilizar ferramentas de colaboração e estratégias de comunicação para conduzir rituais de projeto e registrar decisões.

6. Conduzir, em ambiente controlado, **ataques de SQL Injection** (incluindo múltiplas instruções) e projetar/validar defesas (*prepared statements*, validação/encoding, *least privilege* na base).

7. Integrar arquitetura Web segura a **redes** (TCP/UDP, IPv4/IPv6, QoS, sem fio/IP móvel, compressão, multiplexação, P2P) e programar *sockets* básicos.

8. Projetar componentes em **sistemas distribuídos** (modelos de arquitetura, concorrência, comunicação/sincronização, segurança) e serviços Web com políticas de acesso e *logging*.

9. Estabelecer práticas de **gestão e governança de dados** e definir **indicadores/metas** para operação segura de aplicações.

10. Analisar cenários (tecnológicos e sociais) e articular requisitos de diversidade, sustentabilidade e inovação ao desenho de soluções Web.

11. Contextualizar decisões técnicas com noções de contratos, relações de trabalho, liderança e marcos político-econômicos (Direitos Humanos/economia sustentável).

Conteúdos Programáticos

1. Web Security — CSRF

- Requisições *cross-site* e problemas; ataques **CSRF** em serviços *GET*/*POST*; construção de *POST* via JavaScript; estudo de caso (ex.: *add-friend*/*edit-profile*).
- Contramedidas: cabeçalho `Referer`, *Same-Site Cookies*, *secret tokens*/anti-CSRF; estudo de caso de contramedidas.

2. Web Security — XSS

- XSS refletido, persistente e *DOM-based*; danos potenciais; demonstrações de ataque e autoprogação (*worm* por DOM e por link).
- Prevenção: remoção de código em entradas; *output encoding*; *Content Security Policy* (CSP) e experimentação.

3. Bancos de Dados para Aplicações Web

- Modelo relacional e não relacional (documentos/colunas/grafos – visão); arquitetura de banco de dados em *cloud*.
- **SQL Essencial**: criação/seleção/atualização; *prepared statements*, *filtering*/*encoding* como base para defesa contra injeção.

4. Web Security — SQL Injection (exploração e defesa)

- Tutorial breve de SQL (revisão): criar base/tabela, inserir/selecionar/atualizar, cláusula `WHERE`, comentários.
- Interação Web–BD: coleta de dados do usuário e acesso ao BD; lançamento de ataques de **SQL Injection**; uso de `curl`; modificação de base; múltiplas instruções.
- Causa fundamental; contramedidas: *filtering*/*encoding*; *prepared statements*; política de privilégios; auditoria e trilhas.

5. Redes de Computadores para Aplicações Web

- Arquitetura **TCP**/**IP** e modelo **OSI**; TCP e UDP; IPv4/IPv6; QoS.
- Redes sem fio e IP móvel; **compressão** e **multiplexação**; paradigma **P2P**.
- *Sockets* e protocolos de aplicação; topologias de rede e implicações para Web segura; gerenciamento e segurança de redes.

6. Sistemas Distribuídos e Serviços Web

- Modelos de arquitetura; comunicação e sincronização de processos; controle de concorrência.
- Objetos e componentes distribuídos; **serviços Web**; segurança em sistemas distribuídos; *logging*/observabilidade.

7. Projetos, Governança e Dimensões Humanas

- Projetos, processos e operações: **contratos diversos**; direitos e deveres trabalhistas na operação de produtos digitais.
- **Gestão e governança de dados**; **indicadores, metas e objetivos** (OKRs/KPIs) para segurança e desempenho.
- Teorias de liderança: adaptabilidade e vulnerabilidade na liderança técnica.
- Teorias político-econômicas: Direitos Humanos como paradigma global; **economia sustentável**.

8. Comunicação, Diversidade e Estratégia

- Comunicação, linguagem e design de projetos: ferramentas de colaboração, bloqueios e intencionalidade na comunicação.
- Diversidade social no Brasil (visão aplicada a produtos e comunicação).
- Estratégia e inovação: análise de cenário, transformação digital, inovação aberta; (tópico transversal) poluição e ecotoxicologia como estudo de impacto em soluções digitais.

Metodologia

Aprendizagem baseada em projetos (*PBL*) com *sprints*; laboratórios de CSRF/XSS (ambiente controlado); *code reviews*; exercícios de modelagem de dados; experimentos com CSP; laboratórios com *SQLi* (ambiente seguro), *hardening* de camadas Web–BD; exercícios de *networking* (diagnóstico/profiling) e *sockets*; estudos de caso em sistemas distribuídos e serviços Web; oficinas de comunicação/colaboração; aprendizagem guiada por inteligência artificial e estudos de caso de diversidade e estratégia; oficinas de governança de dados e definição de indicadores; seminários sobre contratos e liderança.

Avaliação

A avaliação do estudante se dá através de três caminhos:

40% Avaliação das atividades de autoestudo e atividades definidas no *backlog* de cada estudante;

30% Avaliação formativa e somativa do projeto baseada em: (i) PoCs e *write-ups* reprodutíveis (CSRF/XSS); (ii) protótipo Web com controles implementados (tokens, CSP, *same-site*); (iii) desenho de dados e consulta SQL segura; (iv) relatório de comunicação/colaboração; (v) participação e colaboração; (vi) avaliação do projeto desenvolvido;

30% Avaliação formativa e somativa do projeto baseada em: (i) PoCs e *write-ups* reprodutíveis de **SQLi** e mitigação; (ii) protótipo cliente–servidor com BD e controles implementados; (iii) relatório técnico de arquitetura de rede/distribuída e políticas de acesso/registro; (iv) plano de governança de dados e indicadores; (v) participação e colaboração; (vi) avaliação do projeto desenvolvido.

Competências Desenvolvidas (síntese)

Modelagem de ameaças Web (CSRF/XSS) e controles; fundamentos de bancos de dados e SQL seguro; comunicação e colaboração; análise de cenário, diversidade e inovação.

Exploração/defesa de **SQL Injection**; integração segura Web–rede–BD; fundamentos de sistemas distribuídos e serviços Web; governança e indicadores de dados; leitura de contratos e relações de trabalho; liderança adaptativa e visão político-econômica aplicada; comunicação e documentação técnica; ética aplicada e responsabilidade ética, uso da inteligência artificial no processo de aprendizagem e desenvolvimento de projetos.

Bibliografia Básica

ALCORN, W.; FRICHOT, C.; ORRU, M. *The Browser Hacker's Handbook*. Indianapolis: Wiley, 2014.

ANDERSON, R. *Security Engineering*. 3rd ed. Cambridge: Cambridge University Press, 2020.

BEAULIEU, A. *Learning SQL*. 3rd ed. Sebastopol: O'Reilly, 2020. CLARKE-SALT, J. (ed.). *SQL Injection Attacks and Defense*. 2nd ed. Waltham: Syngress/Elsevier, 2012.

GOURLEY, D.; TOTTY, B.; SAYER, M.; AGARWAL, A.; RUTLEDGE, B. *HTTP: The Definitive Guide*. Sebastopol: O'Reilly, 2002.

HOFFMAN, A. *Web Application Security: Exploitation and Countermeasures for Modern Web Applications*. San Francisco: No Starch Press, 2020 (ed. atualizada recomendada).

KLEPPMANN, M. *Designing Data-Intensive Applications*. Sebastopol: O'Reilly, 2017.

KUROSE, J. F.; ROSS, K. W. *Redes de Computadores e a Internet: uma abordagem top-down*. 6. ed. São Paulo: Pearson, 2013.

McDONALD, M. *Web Security for Developers*. San Francisco: No Starch Press, 2020.

RICHARDSON, L.; AMUNDSEN, M.; RUBY, S. *RESTful Web APIs*. Sebastopol: O'Reilly, 2013.

ROBINSON, I.; WEBBER, J.; EIFREM, E. *Graph Databases*. 2nd ed. Sebastopol: O'Reilly, 2015.

SILBERSCHATZ, A.; KORTH, H. F.; SUDARSHAN, S. *Sistemas de Banco de Dados*. 7. ed. Rio de Janeiro: LTC, 2020.

STUTTARD, D.; PINTO, M. *The Web Application Hacker's Handbook*. 2nd ed. Indianapolis: Wiley, 2011.

ZALEWSKI, M. *The Tangled Web: A Guide to Securing Modern Web Applications*. San Francisco: No Starch Press, 2012.

CLARKE-SALT, J. (ed.). *SQL Injection Attacks and Defense*. 2nd ed. Waltham: Syngress/Elsevier, 2012.

KARWIN, B. *SQL Antipatterns: Avoiding the Pitfalls of Database Programming*. Dallas: Pragmatic Bookshelf, 2010.

STUTTARD, D.; PINTO, M. *The Web Application Hacker's Handbook*. 2nd ed. Indianapolis: Wiley, 2011.

STEVENS, W. R. *TCP/IP Illustrated, Volume 1: The Protocols*. 2nd ed. Upper Saddle River: Addison-Wesley, 2011.

STEVENS, W. R.; FENNER, B.; RUDOFF, A. M. *UNIX Network Programming, Volume 1: The Sockets Networking API*. 3rd ed. Upper Saddle River: Addison-Wesley, 2003.

TANENBAUM, A. S.; VAN STEEN, M. *Distributed Systems: Principles and Paradigms*. 2nd/3rd ed. Upper Saddle River/Cambridge: Pearson/Addison-Wesley, 2007/2017.

ABNT. *NBR ISO/IEC 27001:2022 — Tecnologia da informação — Segurança da informação, cibersegurança e proteção da privacidade — SGSI — Requisitos*. Rio de Janeiro: ABNT, 2022.

ABNT. *NBR ISO/IEC 27002:2023 — Tecnologia da informação — Segurança da informação, cibersegurança e proteção da privacidade — Controles de segurança da informação*. Rio de Janeiro: ABNT, 2023.

DOERR, J. *Measure What Matters: OKRs — The Simple Idea that Drives 10x Growth*. New York: Portfolio/Penguin, 2018.

DAMA INTERNATIONAL. *DAMA-DMBOK2: Data Management Body of Knowledge*. 2nd ed. Technics Publications, 2017.

Bibliografia Complementar

AMUNDSEN, M. *Designing Web APIs*. Sebastopol: O'Reilly, 2020.

BALL, C. *Hacking APIs*. Shelter Island: Manning, 2022.

BIONI, B. R. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2021.

DELAMARO, M. E.; MALDONADO, J. C.; JINO, M. *Introdução ao Teste de Software*. 2. ed. Rio de Janeiro: Elsevier, 2014.

FOWLER, M. *Patterns of Enterprise Application Architecture*. Boston: Addison-Wesley, 2003.

GRIGORIK, I. *High Performance Browser Networking*. Sebastopol: O'Reilly, 2013.

KARWIN, B. *SQL Antipatterns: Avoiding the Pitfalls of Database Programming*. Dallas: Pragmatic Bookshelf, 2010.

LI, V. *Bug Bounty Bootcamp*. San Francisco: No Starch Press, 2021.

MADDEN, N. *API Security in Action*. Shelter Island: Manning, 2020.

MUNZNER, T. *Visualization Analysis and Design*. Boca Raton: CRC Press, 2014.

O'NEIL, C. *Algoritmos de Destruição em Massa*. São Paulo: Rua do Sabão, 2017.

QUINN, M. J. *Ethics for the Information Age*. 8th ed. Boston: Pearson, 2020.

ROSEN, K. H. *Matemática Discreta e suas Aplicações*. 7. ed. Porto Alegre: AMGH, 2011.

STEFANOV, S. *JavaScript Patterns*. Sebastopol: O'Reilly, 2010.

STUTTARD, D. *The Art of Application Security Testing (A Practical Guide)*. Indianapolis: Wiley, 2014.

TANENBAUM, A. S.; WETHERALL, D. *Redes de Computadores*. 5. ed. São Paulo: Pearson, 2011.

YAWORSKI, P. *Real-World Bug Hunting*. San Francisco: No Starch Press, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27001:2022 — Tecnologia da informação — Segurança da informação, cibersegurança e proteção da privacidade — SGSI — Requisitos*. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27002:2023 — Controles de segurança da informação*. Rio de Janeiro: ABNT, 2023.

GOURLEY, D.; TOTTY, B.; SAYER, M.; AGARWAL, A.; RUTLEDGE, B. *HTTP: The Definitive Guide*. Sebastopol: O'Reilly, 2002.

SHEA, M. *Hacking Web Apps: Detecting and Preventing Web Application Security Problems*. Waltham: Syngress/Elsevier, 2012.

ANDERSON, R. *Security Engineering*. 3rd ed. Cambridge: Cambridge University Press, 2020.

CIS. *CIS Controls v8*. Center for Internet Security, 2021.

NIST. *SP 800-53 Rev. 5 — Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg: NIST, 2020.

NIST. *SP 800-63-3 — Digital Identity Guidelines*. Gaithersburg: NIST, 2017 (atualizações).

AMUNDSEN, M.; RICHARDSON, L.; RUBY, S. *RESTful Web APIs*. Sebastopol: O'Reilly, 2013.

SEINER, R. S. *Non-Invasive Data Governance*. Technics Publications, 2014.

PECK PINHEIRO, P. *Direito Digital*. 7. ed. São Paulo: Saraiva, 2021. (Contratos de TI, compliance, evidências digitais.)

BIONI, B. R. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2021.

GOOGLE SRE. *Site Reliability Engineering: How Google Runs Production Systems*. Sebastopol: O'Reilly, 2016. (Observabilidade, *logging* e indicadores operacionais.)

SIGELMAN, B.; et al. *Distributed Tracing in Practice*. Sebastopol: O'Reilly, 2020. (Observabilidade para serviços distribuídos.)

HEIFETZ, R.; LINSKY, M.; GRASHOW, A. *The Practice of Adaptive Leadership*. Boston: Harvard Business Press, 2009. (Liderança adaptativa.)

BROWN, B. *Dare to Lead*. New York: Random House, 2018. (Vulnerabilidade aplicada à liderança técnica.)

RAWORTH, K. *Doughnut Economics: Seven Ways to Think Like a 21st-Century Economist*. London: Random House, 2017. (Economia sustentável.)

SEN, A. *Development as Freedom*. New York: Knopf/Anchor, 1999. (Direitos humanos e desenvolvimento.)

Módulo 4 — Hardware e Segurança de Sistemas

Carga horária: 300 horas

Ementa

O módulo introduz, em ambiente controlado de laboratório, os fundamentos de *software security* em plataformas Unix/Linux, com foco nos mecanismos de privilégio (Set-UID/Set-GID), variáveis de ambiente, *dynamic linker* e superfícies de ataque associadas. São estudados e reproduzidos, com instrumentação, vetores clássicos como Shellshock, *buffer overflow* (parte I), *format string* (parte I), *race conditions* (parte I) e *reverse shell* básico, articulando princípios de mitigação inicial (ASLR, *stack canaries*, isolamento e menor privilégio). Integram-se fundamentos analíticos (probabilidade e estatística aplicadas), algoritmos e estruturas de dados (grafos, guloso, complexidade, *hash*), paradigmas de programação (funcional e lógica).

Exploração e defesa de sistemas através de **técnicas avançadas de software** (*return-to-libc*, *Return-Oriented Programming — ROP*, *format string*—parte II, *race*—parte II, Dirty COW completa, *reverse shell* com redirecionamentos TCP) e **segurança de hardware** com foco no **Spectre**: predição de desvio, *out-of-order execution*, desenho experimental, coleta/estatística e variantes/mitigações.

Complementam-se fundamentos de algoritmos (programação dinâmica/linear, recursão/indução), pesquisa operacional e otimização (modelos de decisão, otimização linear/discreta) e gestão por processos (BPM), além de finanças gerenciais (balanço, custos, DRE, ROI/EBITDA), liderança (propósito de grupo, mudança organizacional), dimensões ético-profissionais, de produto e mercado (ética, blockchain/cripto, marketing e vendas, metadesign, licenciamento/open source), conectando engenharia segura a decisões de negócio.

Objetivos de Aprendizagem

Ao término do módulo, o discente deverá ser capaz de:

1. Explicar e aplicar os mecanismos Set-UID/Set-GID e analisar suas superfícies de ataque (entradas explícitas, do sistema e variáveis de ambiente).

2. Identificar riscos em invocação de programas externos (`system()` versus `execve()`), *dynamic linking* e variáveis como `PATH`, propondo reduções de superfície.

3. Reproduzir, em laboratório, Shellshock, *buffer overflow* (básico), *format string* (básico), *race* (TOCTOU) e *reverse shell* simples, documentando exploração e mitigação inicial.

4. Empregar noções de probabilidade/estatística, análise de algoritmos e estruturas de dados para qualificar evidências e decisões técnicas.
5. Conduzir cadeias de exploração avançadas em *software* (*return-to-libc*/ROP; *format string*/*race* em profundidade; Dirty COW) e discutir limites de contramedidas (ASLR, canários, endurecimento).
6. Projetar e executar experimentos de **Spectre**, explicando predição de desvio, treino de preditor, medição de canal lateral e análise estatística dos sinais.
7. Implementar *reverse shells* com redirecionamento de E/S sobre TCP e discutir detecção/forense e impactos operacionais.
8. Aplicar PD/PL, pesquisa operacional e BPM à otimização de processos de segurança e priorização de riscos.
9. Relacionar segurança de *software* a ética profissional, conformidade e estratégia de produto/mercado (funil, indicadores, CRM, modelos de negócio).
10. Elaborar análises financeiras para justificar investimentos/mudanças organizacionais em segurança (ROI/EBITDA etc.).

Conteúdos Programáticos

1. Núcleo de Segurança de Software — fundamentos e ataques clássicos

- Programas privilegiados: necessidade de privilégio; tipos; mecanismo Set-UID/Set-GID; funcionamento; exemplo; segurança; estudo “Superman”; o que pode dar errado; superfícies de ataque.
- Entradas e ambiente: entradas do usuário e do sistema; variáveis de ambiente (acesso, herança, localização em memória; *shell* vs. ambiente); vazamento de capacidades; *locale* e uso de `getenv()`.
- *Dynamic linker*: estática vs. dinâmica; estudos de caso como `LD_PRELOAD` e `LD_LIBRARY_PATH` e *dynamic linker* do macOS.
- Invocação externa: `system()` (inseguro) vs. `execve()` (seguro); casos envolvendo `PATH`; redução de superfície.
- Shellshock: funções de *shell*; vulnerabilidade no `bash`; exploração em Set-UID e CGI/PHP; *reverse shell*; cadeia HTTP→CGI→`bash`.
- *Buffer overflow* (parte I): *memory layout*; pilha; *frame pointer*; programa vulnerável; desativação de aleatoriedade; achar endereço de *shellcode*; estratégias com endereços/tamanhos incertos.
- *Format string* (parte I): funções variádicas; `printf()` e acesso a argumentos; exploração para travar, ler pilha e alterar dados; contramedidas iniciais.

- *Race conditions* (parte I): conceito; instalação; exploração básica; seleção de alvo; execução/monitoramento; mitigação inicial (operações atômicas, repetir verificar/usar, *sticky symlink protection*, menor privilégio).
- *Reverse shell* (fundamentos): descritores de arquivo; redirecionamento; E/S padrão; conexão TCP; *redirect* a partir do *shell*.

2. Fundamentos Analíticos e Computacionais

- Probabilidade e estatística: estatística descritiva; conceito de probabilidade; variáveis aleatórias; distribuições; estimação pontual/intervalar; testes de hipóteses; teoremas fundamentais (visão).
- Algoritmos: em grafos; gulosos; análise de complexidade de algoritmos.
- Estruturas de dados: *hash* (tabelas de espalhamento).
- Paradigmas e linguagens: programação funcional e lógica (noções e aplicações).

3. Núcleo de Segurança de Software — exploração avançada e defesa

- BOF—parte II: pilha não executável; *return-to-libc* (endereços `system()`, setup; e `"/bin/sh"`; prólogo/epílogo, *stack frame*); construção do *payload*.
- ROP: rastreamento `esp`/`ebp`; encadeamento sem/com argumentos (pular prólogo; `leave`/`ret`); *gadgets*; obtenção de *root shell*.
- *Format string*—parte II: escrita seletiva rápida; injeção via *format string*; contramedidas (dev/compilador); relação com BOF e ASLR.
- *Race conditions*—parte II: instrumentação e monitoramento; contramedidas (atômicas, *retry*, *sticky symlink*, menor privilégio).
- Dirty COW—parte II: `mmap()`, `MAP_SHARED`/`MAP_PRIVATE`/COW; análise/mitigação; alvo `/etc/passwd`; threads `write`/`madvise`.
- *Reverse shell*—parte II: redirecionamentos de saída/entrada/erro padrão; canal TCP; considerações EDR/forense; *code injection* sob restrições.
- Contramedidas e limitações: ASLR, *stack canaries*/StackGuard, endurecimento de compilação/SO; isolamento e menor privilégio (síntese).

4. Núcleo de Segurança de Hardware — Spectre e variantes

- Introdução; *out-of-order execution* e **branch prediction**; montagem do experimento; programa de teste; coleta e resultados.
- **Spectre**—desenho do ataque: treinar preditor, desviar checagens de limites especulativamente, vazar via canal de cache.

- Abordagem estatística para robustez (múltiplas amostras, *noise handling*); comparação com Meltdown.
- Variantes do Spectre e mitigação (noções): barreiras, retpoline, isolamento, *fencing*, ruído temporal e atualizações de microcódigo/SO.

5. Algoritmos, Pesquisa Operacional e Otimização

- Algoritmos: programação dinâmica; programação linear; projeto de algoritmos; recursão e indução.
- PO/Otimização: classificação de modelos; modelos de decisão; otimização linear e discreta; pacotes computacionais para PO.

6. Finanças, Processos e Liderança

- Finanças/contabilidade gerencial: balanço; custos; DRE (lucros e perdas); rentabilidade; ROI; EBITDA.
- Processos e operações: análise de processos; BPM (gestão por processos de negócio) para fluxos de segurança.
- Liderança: propósito de grupo; liderança e mudança organizacional.

7. Ética, Produto e Mercado

- Ética profissional em computação e tecnologia; diversidade e liderança em equipes diversas.
- Blockchain e criptomoedas; operações privadas e mercados de capitais.
- Marketing e vendas: funil de *leads*, indicadores de marketing digital, pesquisa de mercado e tendências, marketplace/*two-sided markets*, CRM, satisfação/reputação/fidelidade.
- Metadesign e política; patentes, licenciamento e *open source*.
- Técnicas de visualização e representação: facilitação gráfica; técnicas de negociação.

Metodologia

Aprendizagem baseada em projetos e laboratórios práticos; *sprints* com rituais ágeis; instrumentação (`gdb`, *tracing*); *code review*; estudos de caso, aprendizagem guiada por inteligência artificial e *write-ups* reprodutíveis; debates éticos e de produto/mercado; laboratórios avançados com `gdb`, *tracing* e *timing* de cache; engenharia reversa orientada a hipóteses; *blue/red/purple teaming* e *tabletop* de incidentes; oficinas de PO/BPM e finanças aplicadas; *code review* e demonstrações técnicas.

Avaliação

40% Avaliação das atividades de autoestudo e atividades definidas no *backlog* de cada estudante;

30% Avaliação formativa e somativa do projeto baseada em: (i) Entregas de laboratório (exploits/PoCs e contramedidas); (ii) relatórios técnicos com análise de risco/mitigação; (iii) demonstrações e *debriefs*; (iv) participação e colaboração; (v) avaliação do projeto desenvolvido.

30% Avaliação formativa e somativa do projeto baseada em: (i) *Write-ups* reprodutíveis (software e Spectre), *exploits* e contramedidas; (ii) relatórios risco/impacto com análise custo–benefício; (iii) *post-mortems* de incidentes simulados; (iv) apresentações técnicas e executivas; (v) avaliação do projeto desenvolvido.

Competências Desenvolvidas (síntese)

Mecanismos de privilégio e ambiente; *dynamic linking*; exploração clássica (BOF, Shellshock, *format string*, *race*, *reverse shell*); Exploração/defesa avançada (Dirty COW, ret2libc/ROP, *format string*, *race*, *reverse shell*); **segurança de hardware com *Spectre***, medição/estatística de canais laterais; desenho/avaliação de contramedidas; raciocínio probabilístico/estatístico; algoritmos/estruturas (grafos, *hash*); otimização (PD/PL/PO/BPM); ética e produto/mercado; literacia financeira aplicada; liderança e gestão da mudança; comunicação técnica e trabalho em equipe, uso da inteligência artificial no processo de aprendizagem e desenvolvimento de projetos.

Bibliografia Básica

BRYANT, R. E.; O'HALLARON, D. R. Computer Systems: A Programmer's Perspective. 3rd ed. Boston: Pearson, 2016.

DOWD, M.; McDONALD, J.; SCHUH, J. The Art of Software Security Assessment. Boston: Addison-Wesley, 2006.

ERICKSON, J. Hacking: The Art of Exploitation. 2nd ed. San Francisco: No Starch Press, 2008.

KERRISK, M. The Linux Programming Interface. San Francisco: No Starch Press, 2010.

KOZIOL, J. et al. The Shellcoder's Handbook: Discovering and Exploiting Security Holes. 2nd ed. Indianapolis: Wiley, 2007.

LEVINE, J. R. Linkers and Loaders. San Francisco: Morgan Kaufmann, 2000. (Essencial para dynamic linking/loader, ELF e superfície via `LD_PRELOAD`.)

SEACORD, R. C. Secure Coding in C and C++. 2nd ed. Boston: Addison-Wesley, 2013.

SEACORD, R. C. The CERT C Secure Coding Standard. 2nd ed. Boston: Addison-Wesley, 2014.

STEVENS, W. R.; RAGO, S. A. Advanced Programming in the UNIX® Environment. 3rd ed. Boston: Addison-Wesley, 2013. (Execução, `execve()`, `setuid()`, ambiente, `getenv()`.)

ANDRIESSE, D. Practical Binary Analysis. San Francisco: No Starch Press, 2018.

SUTTON, M.; GREENE, A.; AMINI, P. Fuzzing: Brute Force Vulnerability Discovery. Boston: Addison-Wesley, 2007.

ARPACI-DUSSEAU, R. H.; ARPACI-DUSSEAU, A. C. Operating Systems: Three Easy Pieces. 2nd ed. Madison: Arpaci-Dusseau Books, 2020. (Memória, processos, ASLR em visão, race e concorrência.)

TANENBAUM, A. S.; BOS, H. Modern Operating Systems. 4th ed. Boston: Pearson, 2015.

GARFINKEL, S.; SPAFFORD, G.; SCHWARTZ, A. Practical UNIX and Internet Security. 3rd ed. Sebastopol: O'Reilly, 2003.

GREGG, B. Systems Performance. 2nd ed. Boston: Addison-Wesley, 2020. (Apoia instrumentação, tracing e evidências quantitativas.)

HENNESSY, J. L.; PATTERSON, D. A. Computer Architecture: A Quantitative Approach. 6th ed. San Francisco: Morgan Kaufmann, 2019.

SHEN, J. P.; LIPASTI, M. H. Modern Processor Design: Fundamentals of Superscalar Processors. Long Grove: Waveland, 2013.

KOZIOL, J. et al. The Shellcoder's Handbook: Discovering and Exploiting Security Holes. 2nd ed. Indianapolis: Wiley, 2007.

PERLA, E.; OLDANI, M. A Guide to Kernel Exploitation: Attacking the Core. Indianapolis: Wiley, 2010.

ARPACI-DUSSEAU, R. H.; ARPACI-DUSSEAU, A. C. Operating Systems: Three Easy Pieces. 2nd ed. Madison: Arpaci-Dusseau Books, 2020.

BOVET, D. P.; CESATI, M. Understanding the Linux Kernel. 3rd ed. Sebastopol: O'Reilly, 2005.

JAIN, R. The Art of Computer Systems Performance Analysis. New York: Wiley, 1991. (para desenho experimental, timing e estatística em canais laterais)

Bibliografia Complementar

HOG LUND, G.; McGRAW, G. Exploiting Software: How to Break Code. Boston: Addison-Wesley, 2004.

DANG, B.; GUDERIAN, A.; SKALSKI, E. Practical Reverse Engineering. Indianapolis: Wiley, 2014.

EAGLE, C. The IDA Pro Book. 2nd ed. No Starch Press, 2011.

EILAM, E. Reversing: Secrets of Reverse Engineering. Indianapolis: Wiley, 2005.

ANDERSON, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Cambridge: Cambridge University Press, 2020.

KLEPPMANN, M. Designing Data-Intensive Applications. Sebastopol: O'Reilly, 2017. (Para logging, integridade e decisões de persistência/mitigação.)

LOVE, R. Linux System Programming. 2nd ed. Sebastopol: O'Reilly, 2013.

NEMETH, E.; SNYDER, G.; HEIN, T.; WHALEY, B.; MACKIN, D. UNIX and Linux System Administration Handbook. 5th ed. Boston: Addison-Wesley, 2017.

KAUFFMAN, D.; ALTHEIDE, C. Linux Forensics. Burlington: Syngress/Elsevier, 2008. (Ou Practical Linux Forensics, No Starch, 2022, se preferir edição mais recente.)

SILBERSCHATZ, A.; GALVIN, P.; GAGNE, G. Fundamentals of Operating Systems. 9th ed. Hoboken: Wiley, 2012. (Base complementar em SO.)

ROSEN, L. Open Source Licensing: Software Freedom and Intellectual Property Law. Upper Saddle River: Prentice Hall, 2004.

RAYMOND, E. S. The Cathedral and the Bazaar. Sebastopol: O'Reilly, 2001. (Cultura e modelos de desenvolvimento open source.)

NARAYANAN, A. et al. Bitcoin and Cryptocurrency Technologies. Princeton: Princeton University Press, 2016. (Blockchain/cripto em visão crítica.)

CROLL, A.; YOSKOVITZ, B. Lean Analytics. Sebastopol: O'Reilly, 2013. (Funil, métricas, indicadores para produto/segurança.)

MOORE, G. A. Crossing the Chasm. 3rd ed. New York: HarperBusiness, 2014.

QUINN, M. J. Ethics for the Information Age. 8th ed. Boston: Pearson, 2020.

MONTGOMERY, D. C.; RUNGER, G. C. Estatística Aplicada e Probabilidade para Engenheiros. 6. ed. Rio de Janeiro: LTC, 2018. (Fundamentos analíticos.)

ROSEN, K. H. Matemática Discreta e suas Aplicações. 7. ed. Porto Alegre: AMGH, 2011. (Relações, grafos, contagem e hash.)

SAVAGE, S.; BURKE, T. The Ghidra Book: The Definitive Guide. No Starch Press, 2020.

GREGG, B. BPF Performance Tools. Boston: Addison-Wesley, 2019. (Tracing e evidência quantitativa em Linux.)

SAVAGE, S.; BURKE, T. The Ghidra Book: The Definitive Guide. San Francisco: No Starch Press, 2020.

CORBET, J.; RUBINI, A.; KROAH-HARTMAN, G. Linux Device Drivers. 3rd ed. Sebastopol: O'Reilly, 2005.

GREGG, B. BPF Performance Tools. Boston: Addison-Wesley, 2019.

GREGG, B. Systems Performance. 2nd ed. Boston: Addison-Wesley, 2020.

O'FLYNN, C.; VAN WOUDENBERG, J. The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks. San Francisco: No Starch Press, 2021. (side-channels e fault injection — dialoga com Spectre)

TEHRANIPOOR, M.; WANG, C. Introduction to Hardware Security and Trust. New York: Springer, 2012.

TEHRANIPOOR, M.; WANG, C. (eds.). Hardware Security: A Hands-on Learning Approach. Boca Raton: CRC Press, 2017.

CORMEN, T. H.; LEISERSON, C. E.; RIVEST, R. L.; STEIN, C. *Algoritmos: teoria e prática*. 4. ed. Rio de Janeiro: Grupo GEN, 2022. (PD, recursão/indução)

BERTSIMAS, D.; TSITSIKLIS, J. Introduction to Linear Optimization. Belmont: Athena Scientific, 1997.

HILLIER, F. S.; LIEBERMAN, G. J. Introduction to Operations Research. 10th ed. New York: McGraw-Hill, 2015.

WINSTON, W. L. Operations Research: Applications and Algorithms. 4th ed. Belmont: Duxbury, 2004.

DUMAS, M.; LA ROSA, M.; MENDLING, J.; REIJERS, H. A. Fundamentals of Business Process Management. 2nd ed. Berlin: Springer, 2018.

KOLLER, T.; GOEDHART, M.; WESSELS, D. Valuation: Measuring and Managing the Value of Companies. 7th ed. Hoboken: Wiley, 2020.

BREALEY, R. A.; MYERS, S. C.; ALLEN, F. Princípios de Finanças Corporativas. 12. ed. Porto Alegre: AMGH, 2019.

HEIFETZ, R.; LINSKY, M.; GRASHOW, A. The Practice of Adaptive Leadership. Boston: Harvard Business Press, 2009.

BROWN, B. Dare to Lead. New York: Random House, 2018.

Módulo 5 — Segurança de Redes

Carga horária: 300h

Ementa

Fundamentos práticos de *Network Security* com foco em captura e forja de pacotes (sniffing/spoofing), interfaces e filtros de baixo nível (NIC, BPF), *sockets* (crus e de alto nível), *pcap* e *Scapy*, além de ataques e diagnósticos no protocolo TCP (SYN Flooding, *reset*, *session hijacking* e *reverse shell*). Os laboratórios cobrem construção e análise de pacotes (ICMP/UDP/TCP), cálculos de *checksum*, *endianness* e instrumentação de tráfego. *Network Security* com ênfase em **firewalls** (filtro de pacotes, *stateful*, aplicação/*proxy*), **Netfilter/iptables** e **connection tracking**, evasão por **SSH tunneling/VPN**, e segurança de **DNS** (cache poisoning local e remoto, Kaminsky, *rebinding*, forja de respostas, DNSSEC, TLS/SSL para proteção, DoS) em ambiente de laboratório. Complementa com construção de **VPN** (interfaces virtuais TUN, *túnel* TLS/SSL, roteamento e testes) e análise do **Heartbleed** (protocolo *Heartbeat*, exploração e correção). Integram-se tópicos de engenharia de *software* (requisitos, qualidade e arquitetura), bancos de dados (modelagem e DDL/DML), fundamentos de **teoria da computação** (computabilidade, decidibilidade, Máquina de Turing, métodos de prova, notação formal, recursão, redutibilidade, Tese de Church) para sustentar limites e garantias de segurança, comunicação e persuasão em projetos, aprendizagem pessoal/organizacional e análise de cenário para conectar decisões técnicas de segurança às necessidades de produto e operação.

Objetivos de Aprendizagem

Ao término do módulo, o discente deverá ser capaz de:

1. Empregar NIC/BPF, *sockets* e *pcap/Scapy* para **capturar**, **processar** e **forjar** pacotes (ICMP/UDP/TCP) com precisão temporal.
2. Construir **PoCs** de sniffing/spoofing (incl. “sniffar e depois forjar”), calculando *checksums* e tratando *endianness*.
3. Analisar o funcionamento interno do TCP (3-way handshake, transmissão, cabeçalho) e conduzir ataques controlados: **SYN Flooding**, **TCP Reset** e **Session Hijacking**, incluindo criação de *reverse shell* em ambiente seguro.
4. Documentar riscos e controles compensatórios iniciais (limitação de taxa, backlog/filas, aleatorização de números de sequência, filtros).
5. Projetar e implementar **firewalls** em Linux (**Netfilter/iptables**), incluindo **stateful** com **connection tracking** e políticas por cadeia/regra.

6. Construir e avaliar **web proxies**/*application firewalls* e discutir cenários de evasão (SSH tunneling, *reverse* e *dynamic port forwarding*, VPN).
7. Configurar laboratório de **DNS** (hierarquia, zonas, servidores) e conduzir/examinar ataques (cache poisoning local/remoto, Kaminsky, *rebinding*, forja em seções *Answer*/*Authority*/*Additional*) e defesas (DNSSEC, TLS/SSL).
8. Construir uma **VPN** TLS/SSL de ponta a ponta usando interface **TUN** (estabelecer túnel, encaminhar pacotes, testes *ping*/*telnet*, *egress* bypass).
9. Analisar e reproduzir, em ambiente controlado, o **Heartbleed**, compreendendo sua causa e a correção.
10. Aplicar princípios de **engenharia de requisitos**, qualidade e arquitetura de sistemas, bem como modelagem de dados (conceitual, lógica e física) e DDL/DML, ao planejamento de controles de rede.
11. Conduzir rituais e comunicações de projeto com **persuasão empática** e técnicas de negociação, integrando práticas de aprendizagem individual e de organizações que aprendem.
12. Relacionar limites de solução e decidibilidade (Teoria da Computação) à definição de políticas e verificações de segurança.

Conteúdos Programáticos

1. Sniffing e Spoofing de Pacotes

- Recepção de pacotes; **NIC**; **BSD Packet Filter (BPF)**.
- **Packet Sniffing**: *sockets* de recepção; *raw sockets*; API **pcap**; processamento de pacotes capturados.
- **Packet Spoofing**: envio com *socket* normal; envio forjado com *raw sockets*; construção de pacotes **ICMP**/**UDP**; *sniffing then spoofing*.
- **Scapy** em Python: instalação; exemplo; sniffing; spoofing (ICMP/UDP); envio/recepção; **abordagem híbrida** (template em Scapy + envio em C).
- **Endianness** e **cálculo de checksum**.

2. Ataques ao Protocolo TCP

- Funcionamento do TCP; cliente/servidor; transmissão “under the hood”; cabeçalho TCP.
- **SYN Flooding**: protocolo de *handshake*, lançamento do ataque (incl. em C) e contramedidas iniciais.
- **TCP Reset**: encerramento de conexões; ataque e *setup*; cenários em Telnet/SSH/*streaming*.

- **TCP Session Hijacking**: conceito e execução; impactos; escalada de dano; **reverse shell**.

3. Firewalls e Evasão

- Tipos de **firewalls**: *packet filter*, **stateful**, aplicação/*proxy*.
- **Netfilter**: *hooks* IPv4; módulos de kernel (escrita, compilação, instalação); implementação de *packet filter*.
- **iptables**: estrutura (tabelas/cadeias), travessia e *matching* de regras; extensões; construção de firewall simples.
- **Stateful firewall**: *connection tracking* no Linux; exemplo prático de configuração.
- Evasão: **SSH tunneling** (port forwarding dinâmico e reverso), **VPN** para evasão de *egress* firewall.

4. DNS e Ataques

- Hierarquia de DNS, zonas e servidores; servidores autoritativos; arquivos locais; servidor local e consulta iterativa.
- Laboratório: configurar máquina do usuário; servidor DNS local; zonas. **Scapy**: construção de *request*/*reply*; cabeçalho/regs de DNS.
- Ataques: **cache poisoning** local; remoto e **Kaminsky**; forja de respostas (seções *Answer*/*Authority*/*Additional*); **DNS rebinding**.
- Defesa: mitigação de **rebinding**; proteção contra **spoofing**; **DNSSEC**; solução TLS/SSL; DoS contra servidores (raiz/TLD/dominios).

5. VPN (TLS/SSL) e Interfaces Virtuais

- Conceitos de **VPN** e funcionamento; visão de **TLS/SSL VPN**.
- Interfaces virtuais: **TUN**; criação e roteamento para a TUN; leitura/escrita; passagem do TUN ao túnel e vice-versa; agregação do sistema.
- Montagem de laboratório: configuração de servidor/cliente/host; testes (*ping* e *telnet*); uso de VPN para *egress bypass*.

6. Vulnerabilidade Heartbleed

- Protocolo *Heartbeat*; ambiente e *setup*; lançamento do ataque; validação do resultado; correção do bug.

7. Engenharia de Software, Dados e Comunicação (apoio ao módulo)

- **Elicitação/engenharia de requisitos**; requisitos funcionais e não funcionais; **reuso**; qualidade e documentação de projeto; projeto e arquitetura de sistemas.
- Bancos de dados: modelagem **conceitual, lógica e física**; linguagem de **criação e manipulação** (DDL/DML).
- Comunicação, linguagem e design de projetos: **persuasão e convencimento empático**; modelos de negociação; aprendizagem pessoal/profissional; organizações que aprendem.
- Estratégia e inovação: **análise de cenário**.

8. Teoria da Computação (fundamentos para segurança)

- **Computabilidade** e **decidibilidade**; **Máquina de Turing**; métodos de prova; notação formal; recursão; redutibilidade; **Tese de Church**.

Metodologia

Laboratórios *hands-on* (sniffing/spoofing, TCP attacks) com `pcap`, *Scapy* e C; *code reviews*; estudos de caso; *write-ups* reprodutíveis; oficinas de requisitos/-qualidade e modelagem de dados; simulações de comunicação/negociação em incidentes; laboratórios avançados de *firewalling* (Netfilter/iptables), DNS (configuração/ataques/defesas), VPN com TUN/TLS, e análise do Heartbleed; *code reviews* e *write-ups*; aprendizagem guiada por inteligência artificial; debates sobre limites computacionais de verificação e políticas.

Avaliação

40% Avaliação das atividades de autoestudo e atividades definidas no *backlog* de cada estudante;

30% Avaliação formativa e somativa do projeto baseada em: (i) PoCs de captura/forja de pacotes e ataques TCP; (ii) relatório técnico com análise de tráfego e contramedidas iniciais; (iii) artefatos de requisitos/qualidade e modelo de dados; (iv) apresentação e participação colaborativa; (v) avaliação do projeto desenvolvido.

30% Avaliação formativa e somativa do projeto baseada em: (i) Configurações funcionais de **firewall** e **VPN** com testes; (ii) PoCs de **DNS attacks** e mitigação; (iii) demonstração/relato do **Heartbleed**; (iv) ensaio técnico relacionando teoria da computação a políticas de segurança; (v) participação e colaboração; (vi) avaliação do projeto desenvolvido.

Competências Desenvolvidas (síntese)

Instrumentação de rede (NIC/BPF/pcap/Scapy), construção/análise de pacotes, ataques TCP e mitigação inicial, *Firewalling* (packet/stateful/proxy), Netfilter/iptables e connection tracking, evasão (SSH/VPN), operação segura de DNS e mitigação de ataques (Kaminsky/rebinding/DNSSEC), construção de VPN TLS/SSL com TUN, análise de vulnerabilidades de protocolo (Heartbleed), fundamentos teóricos (decidibilidade/MT/Church) aplicados a políticas de segurança, documentação técnica, engenharia de requisitos/qualidade, modelagem de dados, comunicação persuasiva e negociação, visão de cenário para decisões de segurança, uso da inteligência artificial no processo de aprendizagem e desenvolvimento de projetos.

Bibliografia Básica

STEVENS, W. R. TCP/IP Illustrated, Volume 1: The Protocols. 2nd ed. Upper Saddle River: Addison-Wesley, 2011.

STEVENS, W. R.; FENNER, B.; RUDOFF, A. M. UNIX Network Programming, Volume 1: The Sockets Networking API. 3rd ed. Upper Saddle River: Addison-Wesley, 2003.

DONAhoo, M. J.; CALVERT, K. L. TCP/IP Sockets in C: Practical Guide for Programmers. 2nd ed. Amsterdam: Morgan Kaufmann, 2009.

SANDERS, C. Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems. 3rd ed. San Francisco: No Starch Press, 2017.

CHAPPELL, L. Wireshark Network Analysis. 2nd ed. Chappell University, 2017.

GREGG, B. BPF Performance Tools. Boston: Addison-Wesley, 2019.

CALAVERA, D.; FONTANA, L. Linux Observability with BPF: Advanced Programming for Performance Analysis and Networking. Sebastopol: O'Reilly, 2019.

BENVENUTI, C. Understanding Linux Network Internals. Sebastopol: O'Reilly, 2006.

ROSEN, R. Linux Kernel Networking: Implementation and Theory. New York: Apress, 2014.

KOZIEROK, C. M. The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference. San Francisco: No Starch Press, 2005.

SEITZ, J.; SEITZ, J. (eds.) / SEITZ, J. (capítulos Scapy). Black Hat Python: Python Programming for Hackers and Pentesters. 2nd ed. San Francisco: No Starch Press, 2021. (Scapy para sniffing/spoofing e automação.)

VAN WINKLE, L. Hands-On Network Programming with C. Birmingham: Packt, 2019.

McNAB, C. Network Security Assessment: Know Your Network. 3rd ed. Sebastopol: O'Reilly, 2016.

KUROSE, J. F.; ROSS, K. W. Redes de computadores e a Internet: uma abordagem top-down. 6. ed. São Paulo: Pearson, 2013.

BRYANT, R. E.; O'HALLARON, D. R. Computer Systems: A Programmer's Perspective. 3rd ed. Boston: Pearson, 2016. (suporte a endianness, checksums e manipulação binária.)

LIU, C.; ALBITZ, P. **DNS and BIND**. 5th ed. Sebastopol: O'Reilly, 2006.

LUCAS, M. W. **DNSSEC Mastery: Securing the Domain Name System with BIND**. 2nd ed. Tilted Windmill Press, 2022.

RISTIĆ, I. **Bulletproof SSL and TLS**. 2nd ed. London: Feisty Duck, 2017.

RESCORLA, E. **SSL and TLS: Designing and Building Secure Systems**. Boston: Addison-Wesley, 2001.

FEILNER, M. **OpenVPN: Building and Integrating Virtual Private Networks**. Birmingham: Packt, 2006.

SNADER, J. C. **VPNs Illustrated: Tunnels, VPNs, and IPsec**. Boston: Addison-Wesley, 2005.

SIPSER, M. **Introduction to the Theory of Computation**. 3rd ed. Boston: Cengage, 2012.

Bibliografia Complementar

LYON, G. F. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Sunnyvale: Insecure, 2009.

ERICKSON, J. Hacking: The Art of Exploitation. 2nd ed. San Francisco: No Starch Press, 2008. (sockets, reverse shell, payloads.)

WRIGHT, G.; STEVENS, W. R. TCP/IP Illustrated, Volume 2: The Implementation. Reading: Addison-Wesley, 1995.

TANENBAUM, A. S.; WETHERALL, D. Redes de Computadores. 5. ed. São Paulo: Pearson, 2011.

KOCHER, P.; et al. (referências secundárias em canais e mitig.) – Wireshark 101: Essential Skills for Network Analysis. Chappell University, 2013.

RASH, M. Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort. 3rd ed. San Francisco: No Starch Press, 2007.

HANSTEEN, P. N. The Book of PF: A No-Nonsense Guide to the OpenBSD Firewall. 3rd ed. San Francisco: No Starch Press, 2014.

BEJTLICH, R. The Practice of Network Security Monitoring. San Francisco: No Starch Press, 2013.

SCAPY PROJECT (PHILIPPE BIONDI; C. LEVY). Scapy Documentation. Paris: scapy.net, edições contínuas. (referência prática para laboratórios.)

LOVE, R. Linux System Programming. 2nd ed. Sebastopol: O'Reilly, 2013.

WRIGHT, C.; DAVE, S.; COUGHLIN, A. Networking for Systems Administrators. Scotts Valley: Leanpub, 2014.

PRESSMAN, R. S.; MAXIM, B. R. Engenharia de Software: uma abordagem profissional. 9. ed. Porto Alegre: AMGH, 2021. (requisitos/qualidade/arquitetura.)

SOMMERVILLE, I. Engenharia de Software. 10. ed. São Paulo: Pearson, 2019.

SILBERSCHATZ, A.; KORTH, H. F.; SUDARSHAN, S. Sistema de Banco de Dados. 7. ed. Rio de Janeiro: LTC, 2020. (modelagem/DDL/DML.)

BEAULIEU, A. Learning SQL. 3rd ed. Sebastopol: O'Reilly, 2020.

FISHER, R.; URY, W.; PATTON, B. Como Chegar ao Sim (Getting to Yes). 3. ed. Rio de Janeiro: Sextante, 2011. (negociação.)

ROSENBERG, M. Comunicação Não-Violenta. 3. ed. São Paulo: Ágora, 2015. (persuasão empática.)

SENGE, P. A Quinta Disciplina: Arte e Prática da Organização que Aprende. 8. ed. Rio de Janeiro: BestSeller, 2006. (aprendizagem pessoal/organizacional.)

FOWLER, M. UML Essencial: Um breve guia para a Linguagem de Modelagem Unificada (UML Distilled). 3. ed. Porto Alegre: Bookman, 2005. (documentação de arquitetura.)

HANSTEEN, P. N. **The Book of PF: A No-Nonsense Guide to the OpenBSD Firewall**. 3rd ed. San Francisco: No Starch Press, 2014.

WRIGHT, C.; DAVE, S.; COUGHLIN, A. **Networking for Systems Administrators**. Scotts Valley: Leanpub, 2014.

ECKERSLEY, P.; PETERSON, Z.; et al. **HTTP/2 in Action**. Shelter Island: Manning, 2016. (apoio a proxies de aplicação e TLS moderno.)

FERGUSON, N.; SCHNEIER, B.; KOHNO, T. **Cryptography Engineering**. Indianapolis: Wiley, 2010.

PAAR, C.; PELZL, J. **Understanding Cryptography**. Heidelberg: Springer, 2010.

DORASWAMY, N.; HARKINS, D. **IPsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks**. 2nd ed. Upper Saddle River: Prentice Hall, 2003.

CARPENTER, T.; LOUKAS, G. **OpenVPN Cookbook**. 2nd ed. Birmingham: Packt, 2016.

BIONDI, P.; LEVY, C. (eds.). **Scapy Documentation**. Paris: scapy.net, várias edições. (referência prática para laboratórios DNS/ICMP/UDP/TCP.)

RASH, M. **Linux iptables Pocket Reference**. Sebastopol: O'Reilly, 2004.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores**. 5. ed. São Paulo: Pearson, 2011.

HOPCROFT, J. E.; MOTWANI, R.; ULLMAN, J. D. **Introduction to Automata Theory, Languages, and Computation**. 3rd ed. Boston: Pearson, 2006.

LEWIS, H. R.; PAPADIMITRIOU, C. H. **Elements of the Theory of Computation**. 2nd ed. Upper Saddle River: Prentice Hall, 1997.

ARORA, S.; BARAK, B. **Computational Complexity: A Modern Approach**. Cambridge: Cambridge University Press, 2009.

ANDERSON, R. **Security Engineering**. 3rd ed. Cambridge: Cambridge University Press, 2020. (integra políticas, ameaças e engenharia de defesas.)

RISTIĆ, I. **OpenSSL Cookbook**. 3rd ed. London: Feisty Duck, 2014. (diagnóstico TLS, *heartbeat*/Heartbleed, configuração segura.)

Módulo 6 — Criptografia e Segurança Blockchain

Carga horária: 300h

Ementa

Fundamentos de **criptografia de chave simétrica** e **funções hash** com foco em construção segura, modos de operação e uso correto de APIs, preparando o discente para aplicações reais (integridade, autenticação de mensagens e armazenamento seguro de senhas). Estuda cifras clássicas (substituição mono/polialfabética, *Enigma*) e algoritmos modernos (DES, AES), modos **AEAD** (GCM) e ECB/CBC/CFB/OFB/CTR, **IV** e erros comuns. Cobre hash criptográfico (famílias MD/SHA), propriedades, desempenho e aplicações; **MAC**/**HMAC**, *length extension* e colisões (visão). Integra **Bitcoin e Blockchain** no que tange a *hash chain*, chaves/endereços, carteiras e *scripts* de transação (P2PKH, P2MS, P2SH) para motivar o uso dos primitivos.

Criptografia de chave pública, **PKI** e **TLS** em **blockchain e Bitcoin** no plano de transações, *mining*, árvore de Merkle e consenso. Estuda-se **DH**, **RSA** (fundamentos matemáticos, desempenho, **híbrido**), preenchimentos seguros (PKCS /#1 v1.5, OAEP) e ataques ao "*textbook RSA*". Cobre **assinaturas digitais** (RSA/DSA/outras), programação com APIs de criptografia assimétrica, **PKI** (certificados X.509, CAs raiz/intermediárias, cadeia de confiança), **MITM** e ataques à infraestrutura; **TLS**: *handshake*, verificação de *hostname*, transmissão de dados e programação cliente/servidor.

Em blockchain, aprofunda carteira→transações→**propagação**, **mineração**, **recompensa**, **árvore de Merkle**, **duplo gasto**, **maioria de poder de hash** e estudos de caso. Integra temas de **estratégia e inovação** (análise de cenário), **ESG/-sustentabilidade**, **arquitetura empresarial** (Gartner/TOGAF/FEA), **CRM e vendas**, **pesquisa científica** (hipóteses/teorias) e **sistemas distribuídos** (modelos, comunicação, concorrência, invocação remota, objetos/componentes, serviços Web, segurança, sistema de arquivos distribuído, tolerância a falhas, computação móvel/ubíqua).

Complementa-se com algoritmos (lógica algorítmica, E/S, estruturas de controle, análise de complexidade, programação dinâmica/linear, projeto de algoritmos), aprendizagem pessoal/profissional, e **arquitetura da informação em nuvem** (dados→informação→conhecimento; *datalake*, *data warehouse*/*data mart*; anonimização).

Objetivos de Aprendizagem

Ao término do módulo, o discente deverá ser capaz de:

1. Explicar e aplicar cifras de **chave simétrica** (DES/AES) e selecionar **modos de operação** adequados, justificando segurança e desempenho.
2. Usar **APIs criptográficas** com **IV** aleatório/único, **AEAD**/**GCM** e *key management* básico, evitando armadilhas (ECB, IV previsível/repetido).
3. Empregar **hash** e **HMAC** para integridade/autenticação; discutir *length extension* e colisões (impacto e mitigação).
4. Implementar **verificação de senha** (com *salt*/*KDF*), **verificação de integridade**, **timestamping confiável** e **commitment** de segredos.
5. Explicar **endereços Bitcoin** (chaves privadas/públicas, *hashing* para endereço), carteiras e o papel de **scripts** (P2PKH, P2MS, P2SH) em transações.
6. Executar **DH** e **RSA** com preenchimentos seguros (PKCS /#1 v1.5, **OAEP**); discutir ataques e **híbridos** (simétrica+assimétrica).
7. Produzir/validar **assinaturas digitais** (RSA/DSA/EC, conforme API), e utilizar **OpenSSL**/APIs para geração de chaves, criptografia e assinatura.
8. Projetar e operar **PKI**: emitir/instalar certificados **X.509**, compreender cadeia de confiança (CAs raiz/intermediárias), e analisar **ataques à PKI** e **MITM**.
9. Implementar **TLS** (cliente/servidor): *handshake*, verificação de certificado/*hostname*, transmissão segura, testes e experimentos de **MITM** controlado.
10. Explicar detalhadamente **Bitcoin**/**Blockchain**: transações e *scripts*, **propagação**, **mineração**, **árvore de Merkle**, **consenso**, **duplo gasto** e **ataques de maioria**, avaliando riscos/mitigações.
11. Integrar segurança criptográfica com **sistemas distribuídos**, **ESG** e estratégia de adoção (arquitetura empresarial, CRM/vendas, pesquisa científica).
12. Modelar soluções considerando arquitetura de dados em nuvem, anonimização e boas práticas de organização da informação.

Conteúdos Programáticos

1. Criptografia de Chave Secreta

- Cifras de substituição (mono/polialfabética) e *Enigma* (motivação histórica).
- **DES** e **AES**; modos **ECB**/**CBC**/**CFB**/**OFB**/**CTR**; **padding**; **IV** e erros comuns (IV repetido/previsível).
- **AEAD** e **GCM**; programação usando GCM e práticas de API.

2. Funções Hash e MAC

- Propriedades (pré-imagem, segunda pré-imagem, colisão); famílias **MD** e **SHA**; como os algoritmos funcionam; desempenho.
- Comandos e uso em programas; aplicações: integridade, **commitment**, **password hashing**, **trusted timestamping**.
- **MAC**: construção e ataques; **HMAC**; *length extension* (experimento guiado) e impacto.
- Colisões (visão): impacto de colisão MD5; exemplos famosos (arquivos/-programas/certificados) — discussão conceitual.

1. Criptografia de Chave Pública e Assinaturas

- **Diffie–Hellman**; transformar DH em criptografia assimétrica (visão); **RSA**: aritmética modular, Teorema de Euler, Euclidiano estendido; exercícios (pequenos/grandes).
- Desempenho e **criptografia híbrida**; outros algoritmos de chave pública (visão).
- **OpenSSL**/APIs: geração de chaves; extração de chave pública; cifrar/decifrar; **paddings** (PKCS #1 v1.5/**OAEP**); ataques ao *textbook RSA*.
- **Assinatura digital**: RSA/DSA/EC (conforme disponibilidade de API); programação de assinatura/verificação.

2. PKI e TLS

- **PKI**: certificados públicos; X.509; obtenção de certificado; **CA** (raiz/intermediária); cadeia de confiança; implantação em servidor Web.
- **MITM** e defesa com PKI: encaminhar certificado autêntico; certificados falsos; *MITM proxy*; ataques ao processo de verificação/assinatura/usuário.
- Tipos de certificado: **DV**/**OV**/**EV**; CAs confiáveis no mundo real.
- **TLS**: visão; *handshake*; verificação de certificado; geração/troca de chaves; registro e transporte de dados; programação (cliente/servidor), verificação de *hostname*, testes.

3. Bitcoin e Blockchain — Fundamentos Criptográficos

- **Hash chain** e **blockchain**; “dificultar o encadeamento”; incentivos (visão).
- Endereços Bitcoin: geração de chaves privadas/públicas; *hashing* para endereço; carteiras.
- Transações e *scripts*: **P2SH**, **P2PKH** (Pay-to-Pubkey-Hash), **P2MS** (multisig); exemplo guiado de desbloqueio de saída.

4. Bitcoin e Blockchain — Operação e Segurança

- História; fundamentos de criptografia e endereços; carteiras.
- **Transações**: entradas/saídas; desbloqueio; variações e exemplos reais.
- **Propagação** de transações; **mineração**, **recompensa**; **árvore de Merkle**.
- **Consenso**, **duplo gasto** e **maioria do poder de *hash***; estudos de caso.

5. Algoritmos e Arquitetura da Informação (apoio)

- Lógica algorítmica; entrada/saída; estruturas de controle/repetição; análise de complexidade; **programação dinâmica** e **linear**; projeto de algoritmos.
- Arquitetura da informação: dados, informação e conhecimento; **datalake**, **data warehouse**/**data mart**; **anonimização**; arquitetura de dados em nuvem.
- Diversidades: linguagem e relações de poder; aprendizagem pessoal e profissional.

6. Estratégia, ESG e Arquitetura para Adoção

- **Estratégia e inovação**: análise de cenário; ESG/sustentabilidade (gestão ambiental; impactos e métricas).
- **Arquitetura empresarial**: frameworks (Gartner, TOGAF, FEA) para integração de soluções criptográficas/distribuídas.
- **CRM e vendas**: relacionamento com clientes; rotinas de vendas (rotas/monitoramento/incentivos); satisfação, reputação e fidelidade.
- Pesquisa científica: construção de hipóteses; papel das teorias.

7. Sistemas Distribuídos (integração com segurança)

- Modelos de arquitetura; algoritmos distribuídos; comunicação/sincronização; comunicação indireta; controle de concorrência; invocação remota.
- Objetos/componentes distribuídos; **serviços Web**; **sistemas de arquivos distribuídos**; **tolerância a falhas**; **computação móvel**/**ubíqua**; **segurança em sistemas distribuídos**.

Metodologia

Laboratórios *hands-on* com bibliotecas criptográficas (AES/GCM, HMAC), *kits* de hash/MAC, exercícios de *commitment*/timestamping e protótipos de carteira/endereços Bitcoin; *code reviews* focados em uso correto de APIs; aprendizagem guiada por inteligência artificial; estudos de caso; laboratórios com **DH**/**RSA**, assinatura digital e **OpenSSL**/APIs; montagem de **PKI** educativa (CA intermediária,

cadeia e implantação Web); **TLS** cliente/servidor com experimento de **MITM** controlado; simulações de transações/mineração e visualização de **Merkle**; seminários de adoção (ESG/arquitetura/CRM) e integração com sistemas distribuídos.

Avaliação

40% Avaliação das atividades de autoestudo e atividades definidas no *backlog* de cada estudante;

30% Avaliação formativa e somativa do projeto baseada em: (i) Artefatos de código (AES/GCM, HMAC, KDF); (ii) *write-ups* reprodutíveis (integridade/timestamping, *length* extension conceitual); (iii) mini-*wallet* educacional (chave/endereço/transação de exemplo); (iv) relatório de arquitetura de dados/anonimização; (v) avaliação do projeto desenvolvido.

30% Avaliação formativa e somativa do projeto baseada em: (i) Artefatos de código (DH/RSA, assinatura, TLS cliente/servidor); (ii) emissão e implantação de certificados (cadeia X.509) e relatório de segurança/ataques à PKI; (iii) *write-up* de MITM controlado; (iv) estudo aplicado de transações/mineração/consenso; (v) ensaio técnico sobre estratégia/ESG/arquitetura; (vi) avaliação do projeto desenvolvido.

Competências Desenvolvidas (síntese)

Cifras simétricas e modos; AEAD/GCM e IV seguro; hash/HMAC e aplicações; fundamentos de endereços/roteiros Bitcoin; criptografia assimétrica e assinaturas; **PKI** e **TLS** operacionais; segurança e operação de **blockchain**/**Bitcoin** (transações, mineração, consenso, riscos); integração com **sistemas distribuídos**; análise de complexidade e técnicas algorítmicas; arquitetura de informação em nuvem e anonimização; comunicação técnica e boas práticas de API; visão de **ESG**, estratégia e arquitetura empresarial; comunicação técnica e responsabilidade ética, uso da inteligência artificial no processo de aprendizagem e desenvolvimento de projetos.

Bibliografia Básica

KATZ, J.; LINDELL, Y. *Introduction to Modern Cryptography*. 3rd ed. Boca Raton: CRC Press, 2021.

STINSON, D. R.; PATERSON, M. B. *Cryptography: Theory and Practice*. 4th ed. Boca Raton: CRC Press, 2018.

MENEZES, A.; VAN OORSCHOT, P.; VANSTONE, S. *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1996.

AUMASSON, J.-P. *Serious Cryptography: A Practical Introduction to Modern Encryption*. San Francisco: No Starch Press, 2017.

FERGUSON, N.; SCHNEIER, B.; KOHNO, T. *Cryptography Engineering: Design Principles and Practical Applications*. Indianapolis: Wiley, 2010.

PAAR, C.; PELZL, J. *Understanding Cryptography*. Berlin: Springer, 2010.

WONG, D. *Real-World Cryptography*. Shelter Island: Manning, 2021.

BONEH, D.; SHOUP, V. *A Graduate Course in Applied Cryptography*. 2020. (Independente/Disponível em livro digital; cobre AEAD, MAC/HKDF, segurança de APIs.)

SHOUP, V. *A Computational Introduction to Number Theory and Algebra*. 2nd ed. Cambridge: Cambridge University Press, 2009.

ANTONOPOULOS, A. M. *Mastering Bitcoin: Programming the Open Blockchain*. 2nd ed. Sebastopol: O'Reilly, 2017.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University Press, 2016.

KLEPPMANN, M. *Designing Data-Intensive Applications*. Sebastopol: O'Reilly, 2017. (apoio a integridade, hashing, *commitment*/carimbos do tempo e armazenamento seguro)

KIMBALL, R.; ROSS, M. *The Data Warehouse Toolkit*. 3rd ed. Hoboken: Wiley, 2013. (modelagem dimensional, DW/DM para "dados→informação→conhecimento")

BEAULIEU, A. *Learning SQL*. 3rd ed. Sebastopol: O'Reilly, 2020. (apoio leve a consultas para checagens de integridade/registro de evidências)

Bibliografia Complementar

SCHNEIER, B. *Applied Cryptography*. 2nd ed. New York: Wiley, 1996.

MAO, W. *Modern Cryptography: Theory and Practice*. Upper Saddle River: Prentice Hall, 2004.

BRANDS, S. *Rethinking Public Key Infrastructures and Digital Certificates*. Cambridge, MA: MIT Press, 2000. (para discutir *timestamping*, *commitment* e identidade, ainda que o foco aqui seja simétrico/MAC)

KAUFMAN, C.; PERLMAN, R.; SPECINER, M. *Network Security: Private Communication in a Public World*. 3rd ed. Upper Saddle River: Prentice Hall, 2010.

PAAR, C.; PELZL, J.; PFITZMANN, A. (orgs.). *Understanding Cryptography – Exercises and Solutions*. Berlin: Springer, 2011. (exercícios adicionais sobre modos, MAC, KDF)

AUMASSON, J.-P. *The Crypto Dictionary*. San Francisco: No Starch Press, 2020. (terminologia prática para APIs e padrões)

DWORK, C.; ROTH, A. *The Algorithmic Foundations of Differential Privacy*. Boston: Now Publishers, 2014. (anonimização forte; dialoga com a parte de arquitetura de dados em nuvem)

EL EMAM, K.; ARBuckle, T. *Anonymizing Health Data*. Sebastopol: O'Reilly, 2013. (práticas de anonimização/risco de reidentificação)

BERTONI, G.; DAEMEN, J.; PEETERS, M.; VAN ASSCHE, G. *The Keccak Reference*. 2011. (referência técnica ao SHA-3/Shake — complementar para hash moderno)

KATZ, J.; LINDELL, Y. *Introduction to Modern Cryptography – Solutions Manual / Student Resources*. CRC Press, 2021. (apoio didático)

CORMEN, T. H.; LEISERSON, C. E.; RIVEST, R. L.; STEIN, C. *Algoritmos: teoria e prática*. 4. ed. Rio de Janeiro: Grupo GEN, 2022. (PD/PL, análise de complexidade – suporte aos tópicos de algoritmos do módulo)

DASGUPTA, S.; PAPADIMITRIOU, C.; VAZIRANI, U. *Algorithms*. New York: McGraw-Hill, 2008. (abordagem conceitual e provas por indução)

ROSEN, K. H. *Discrete Mathematics and Its Applications*. 8th ed. New York: McGraw-Hill, 2018. (estruturas de hash, probabilidade básica para colisões)

SINGH, S. *The Code Book*. New York: Anchor, 1999. (história das cifras – ideal para contextualização das clássicas)

KAHN, D. *The Codebreakers*. Rev. ed. New York: Scribner, 1996. (história aprofundada; leitura de apoio)

BASHIR, I. *Mastering Blockchain*. 3rd ed. Birmingham: Packt, 2020. (panorama — usar seletivamente; o foco do módulo é criptografia e Bitcoin básico)

ANTONOPOULOS, A. M.; WOOD, G. *Mastering Ethereum*. Sebastopol: O'Reilly, 2018. (opcional para ampliar visão de *scripts*/VM em comparação a Bitcoin)

ROSENBERG, B. (ed.). *Handbook of Financial Cryptography and Security*. Boca Raton: CRC Press, 2011.

WALLACE, D.; ENGLEHARDT, S. *The Joy of Cryptography*. 2nd ed. 2024 (draft/-book). (texto didático moderno; MAC/PRFs, AEAD, provas simples)

WONG, D. *Real-World Cryptography — Early Access Companion Code/Notes*. Manning, 2021+. (material complementar de exercícios e práticas)

VIEGA, John; MESSIER, Matt; CHANDRA, Pravir. *Network Security with OpenSSL*. Sebastopol: O'Reilly, 2002.

RISTIĆ, Ivan. *OpenSSL Cookbook*. 3rd ed. London: Feisty Duck, 2014.

SCHNEIER, Bruce. *Applied Cryptography*. 2nd ed. New York: Wiley, 1996.

MAO, Wenbo. *Modern Cryptography: Theory and Practice*. Upper Saddle River: Prentice Hall, 2004.

BRANDS, Stefan. *Rethinking Public Key Infrastructures and Digital Certificates*. Cambridge, MA: MIT Press, 2000.

FORD, Warwick; BAUM, Michael. *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*. 2nd ed. Upper Saddle River: Prentice Hall PTR, 2001.

HANKERSON, Darrel; MENEZES, Alfred; VANSTONE, Scott. *Guide to Elliptic Curve Cryptography*. New York: Springer, 2004.

SMART, Nigel P. *Cryptography Made Simple*. Cham: Springer, 2016.

HOFFSTEIN, Jeffrey; PIPHER, Jill; SILVERMAN, Joseph H. *An Introduction to Mathematical Cryptography*. 2nd ed. New York: Springer, 2014.

BERNSTEIN, Daniel J.; BUCHMANN, Johannes; DAHMEN, Erik (eds.). *Post-Quantum Cryptography*. Berlin: Springer, 2009.

LUCAS, Michael W. *SSH Mastery*. 2nd ed. Tilted Windmill Press, 2018. (apoio a chaves, agentes, *forwarding* e MITM controlado)

ANDERSON, Ross. *Security Engineering*. 3rd ed. Cambridge: Cambridge University Press, 2020. (falhas de PKI, engenharia de defesas)

TANENBAUM, Andrew S.; VAN STEEN, Maarten. *Distributed Systems*. 3rd ed. DistributedOpen, 2017. (modelos, comunicação, tolerância a falhas – integra com blockchain/TLS)

SONG, Jimmy. *Programming Bitcoin: Learn How to Program Bitcoin from Scratch*. Sebastopol: O'Reilly, 2019.

BASHIR, Imran. *Mastering Blockchain*. 3rd ed. Birmingham: Packt, 2020.

ANTONOPOULOS, Andreas M.; O'HARA, Olaoluwa; NARAYANAN, Rene. *Mastering the Lightning Network*. Sebastopol: O'Reilly, 2021. (opcional, para ampliar segurança e roteamento em camadas)

WONG, David. *Real-World Cryptography*. Shelter Island: Manning, 2021. (APIs modernas, AEAD, KDF, erros comuns em produção – dialoga com TLS/PKI)

KAHN, David. *The Codebreakers*. Rev. ed. New York: Scribner, 1996. (história, contexto; uso complementar)

Módulo 7 — Inteligência Artificial em Cibersegurança

Carga horária: 300 horas

Ementa

Fundamentos de **IA e Aprendizado de Máquina** aplicados à defesa cibernética. O módulo integra modelagem supervisionada, não supervisionada e semissupervisionada para detecção de intrusões, classificação de malware, detecção de phishing, análise de *logs* e anomalias em redes/sistemas. Cobre **engenharia de atributos**, preparação de dados de segurança, avaliação robusta (ROC/PR, *calibration*, *ablation*), **explainability** (LIME/SHAP) e noções de **MLOps/LLMOps** para operação segura em ambientes de missão crítica. Introduz **Deep Learning** (perceptrons, MLP, RNN/LSTM, noções de CNN e *Transformers*) e **IA Generativa** (embeddings, RAG básico) para triagem de incidentes e apoio a SOC. Aborda princípios de **Segurança de IA**: *data governance*, *dataset shift*, viés, **envenenamento de dados** (visão), **ataques de evasão** e **privacidade diferencial** (fundamentos); técnicas **avançadas** de **Deep Learning**, **IA Generativa** e **Segurança de IA** para defesa de alto desempenho. Aprofunda **Transformers**, **Autoencoders/VAEs**, **GANs** e **Modelos de Difusão** aplicados a detecção, síntese de dados e simulação de ameaças. Estuda **ataques adversariais** (FGSM/PGD/C&W), **poisoning/backdoor**, **model stealing**, **membership inference** e **model inversion**, com **defesas** (adversarial training, *certified robustness* — visão, *input filtering*, ensembling). Cobre **DP-SGD** e **federated learning seguro**, **watermarking/proveniência** e segurança de **LLMs/RAG** (prompt injection, *data exfiltration*, jailbreaks, *guardrails*, avaliação e *red teaming*). Integra **MLOps/LLMOps** avançado (governança, auditoria, detecção de *drift*/ataques, SLOs), conectando com conteúdos prévios de redes, web, criptografia e sistemas distribuídos.

Objetivos de Aprendizagem

Ao término do módulo, o discente deverá ser capaz de:

1. Planejar **pipelines** de IA para cibersegurança: coleta/curadoria de dados (rede, *logs*, binários), engenharia de atributos, validação e implantação inicial.

2. Selecionar e treinar modelos clássicos (Regressão, SVM, Árvores/Florestas, kNN, Naive Bayes, k-means, GMM, PCA/UMAP) para problemas de detecção/diagnóstico de segurança.

3. Construir **detectores de anomalia** (Isolation Forest, *autoencoders* rasos) e classificadores de malware/phishing com avaliação adequada (AUC-PR, F1, custo de erro).

4. Aplicar **explainability** e *model risk management* básico a decisões de segurança; identificar *drift* e riscos de dados.
5. Integrar **embeddings** e **RAG** introdutório para sumarização de eventos e consulta de inteligência de ameaças.
6. Descrever fundamentos de **privacidade diferencial** e **ataques a dados/-modelos** (visão), indicando estratégias iniciais de mitigação.
7. Projetar e treinar **modelos profundos** (Transformers, autoencoders/VAEs, CNNs, seq2seq) para detecção de intrusões, malware e anomalias em grande escala.
8. Conduzir **ataques adversariais** (FGSM/PGD/C&W) e **poisoning/backdoor** em ambiente controlado; avaliar impacto operacional e propor **defesas**.
9. Implementar **privacidade diferencial** prática (DP-SGD) e **aprendizado federado** com salvaguardas (agregação segura, auditoria).
10. Construir **pipelines RAG/LLM** seguros com **guardrails**, detecção de *prompt injection*, políticas de *data access* e validação de respostas.
11. Operar **MLOps/LLMOps** de nível produção (monitorar *drift*/ataques, *canary* de modelos, reprodutibilidade, *incident response* de modelos).

Conteúdos Programáticos

1. Fundamentos de IA/ML para Segurança

- Tarefas e dados em segurança: *logs*, *flows* (NetFlow), PCAP, binários, *URLs*/e-mails; curadoria, rotulagem e *weak supervision*.
- Supervisionado: Regressão, SVM, Árvores/Florestas, Naive Bayes, kNN; métricas (ROC vs PR), *calibration*, *thresholding*.
- Não/semissupervisionado: k-means, GMM, DBSCAN (visão), **PCA**/UMAP; **Isolation Forest**; *one-class SVM*.

2. Deep Learning (noções) e Sequências

- MLP; **RNN**/LSTM/GRU para séries de eventos e *logs*; noções de CNN para binários/pe & tráfego.
- *Transformers* (visão) e *tokenização* de *logs*; embeddings de sentenças para correlação de alertas.

3. IA Generativa aplicada

- Embeddings, vetorização e **RAG** básico (consulta de runbooks, playbooks, *threat intel*); avaliação de respostas e contornos de segurança; avaliação formativa e somativa do projeto desenvolvido.

4. Segurança de IA (fundamentos)

- **Envenenamento de dados** (visão), **evasão** na inferência (noções), **membership inference**/**model inversion** (conceitos).
- **Privacidade Diferencial**: intuição, ruído e ε; DP-SGD (ideia); trocas entre utilidade e privacidade.
- Dados, viés e justiça; *dataset shift* e *concept drift*.

5. MLOps/LLMOps (noções) em ambientes seguros

- Versionamento de dados/modelos, rastreabilidade, auditoria, *model cards*; monitoramento e alerta por *drift*.

6. Deep Learning Avançado para Segurança

- **Transformers** para *logs*/sequências e *threat intel*; **CNNs** para binários/tráfego; **Autoencoders**/**VAEs** para anomalia; **GNNs** (visão) para grafos de comunicação.
- **IA Generativa**: **GANs** e **Modelos de Difusão** para dados sintéticos controlados; avaliação de utilidade/privacidade e *risk of leakage*.

7. Adversarial ML e Defesa

- **Evasão**: FGSM, PGD, C&W; **Poisoning**/**Backdoor**; **Model Stealing**; **Membership Inference**/**Model Inversion**.
- Defesas: **adversarial training**, *input preprocessing*, *ensembles*, *confidence scoring*, *certified robustness* (visão), **detecção de backdoor**.

8. Privacidade, Federado e Proveniência

- **DP-SGD**, composição e orçamento de privacidade; *hyperparameters* vs utilidade.
- **Aprendizado Federado**: agregação (FedAvg, visão), *byzantine-robust*, *secure aggregation*; auditoria e *attestation*.
- **Watermarking** de modelos e saídas; **proveniência** de conteúdo (*content authenticity*).

9. Segurança de LLMs/RAG

- **Prompt injection**, *indirect injection*, *data exfiltration*, **jailbreaks**.
- **Guardrails**: políticas, checagens estruturadas, **tool-use** seguro, filtragem e validação; **red teaming** e avaliação.
- **LLMOps**: *observability*, *feedback loops*, *canary*, *rollback*, auditoria e governança.

10. Operação Segura de Modelos

- Monitoramento de *drift*/ataques, *SLOs* de segurança/latência/qualidade, *post-incident reviews*; integração com SIEM/SOAR.
- Forense Digital e Resposta a Incidentes; preservação de evidências; cadeia de custódia; aquisição (disco/memória/rede); análise de artifacts (Windows/Linux/macOS); timeline; triage; IR: preparação, identificação, contenção, erradicação, recuperação; post-mortem.

Metodologia

Laboratórios *hands-on* com notebooks reprodutíveis; estudos de caso (IDS baseado em *flows*, phishing por NLP simples, *autoencoder* para anomalia em *logs*); *code reviews*; **ablation studies** e relatórios de risco; laboratórios avançados: ataques/defesas adversariais, **DP-SGD** em *logs* sensíveis, **federated** com agregação segura, **RAG**/**LLM** com *guardrails*; *benchmarks* com PR-AUC/F1 e *calibration*; *red teaming* técnico; *code reviews*; *runbooks* de operação e aprendizagem guiada por inteligência artificial.

Avaliação

40% Avaliação das atividades de autoestudo e atividades definidas no *backlog* de cada estudante;

30% Avaliação formativa e somativa do projeto baseada em: (i) *PoCs* de detecção (supervisionado e anomalia); (ii) relatório técnico com métricas, *explainability* e análise de erro; (iii) protótipo RAG para SOC; (iv) nota de risco sobre dados/privacidade; (v) participação e colaboração; (vi) avaliação do projeto desenvolvido.

30% Avaliação formativa e somativa do projeto baseada em: (i) *Write-ups* reprodutíveis de ataques/defesas; (ii) **capstone** curto: detector profundo (Transformers/AE) com operação e monitoramento; (iii) DP-SGD ou FL seguro aplicado; (iv) RAG/LLM com *guardrails* e relatório de risco; (v) participação e colaboração; (vi) avaliação do projeto desenvolvido.

Competências Desenvolvidas (síntese)

Modelagem estatística e de ML para segurança; preparo/qualidade de dados; DL básico para sequências; RAG introdutório; avaliação robusta e interpretabilidade; noções de privacidade diferencial, envenenamento/evasão; operações iniciais de MLOps seguro; DL avançado e IA generativa para segurança; Adversarial ML (ataque/defesa); privacidade diferencial e aprendizado federado; avaliação robusta, segurança de LLMs/RAG; MLOps/LLMOps de produção; auditoria e resposta a incidentes de modelos, uso da inteligência artificial no processo de aprendizagem e desenvolvimento de projetos; conduzir investigação repetível, redigir laudos, acionar playbooks e comunicação de crise.

Bibliografia Básica

CHIO, C.; FREEMAN, D. *Machine Learning and Security: Protecting Systems with Data and Algorithms*. O'Reilly, 2018.

RUSSELL, S.; NORVIG, P. *Inteligência Artificial: Uma Abordagem Moderna*. 4. ed. Rio de Janeiro: LTC, 2022.

AGGARWAL, C. C. *Outlier Analysis*. 2nd ed. Springer, 2017.

GÉRON, A. *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*. 3rd ed. O'Reilly, 2022.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. *Deep Learning*. MIT Press, 2016.

BISHOP, C. M. *Pattern Recognition and Machine Learning*. Springer, 2006.

JAMES, G.; WITTEN, D.; HASTIE, T.; TIBSHIRANI, R. *An Introduction to Statistical Learning*. 2nd ed. Springer, 2021.

MOLNAR, C. *Interpretable Machine Learning*. 2nd ed. Independente, 2022. (LIME/SHAP, regras e confiança de predição.)

HUYEN, C. *Designing Machine Learning Systems*. O'Reilly, 2022. (MLOps: dados, monitoramento, drift, model cards.)

DWORK, C.; ROTH, A. *The Algorithmic Foundations of Differential Privacy*. Now Publishers, 2014.

LESKOVEC, J.; RAJARAMAN, A.; ULLMAN, J. D. *Mining of Massive Datasets*. 3rd ed. Cambridge, 2020. (mineração para grandes volumes de logs/flows.)

JURAFSKY, D.; MARTIN, J. *Speech and Language Processing*. 3rd ed. (draft). Prentice Hall, 2023–. (NLP aplicado a phishing/URLs/e-mails.)

RUDIS, B.; JACOBS, J. *Data-Driven Security*. Wiley, 2014. (pipeline de dados de segurança, visualização e métricas.)

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. *Deep Learning*. MIT Press, 2016.

CHOLLET, François. *Deep Learning with Python*. 2nd ed. Manning, 2021.

STEVENS, Eli; ANTIGA, Luca; VIEHMANN, Thomas. *Deep Learning with PyTorch*. Manning, 2020.

TUNSTALL, Lewis; VON WERRA, Leandro; WOLF, Thomas. *Natural Language Processing with Transformers*. O'Reilly, 2022. (Transformers para logs/URLs/e-mails e RAG)

FOSTER, David. *Generative Deep Learning*. 2nd ed. O'Reilly, 2023. (GANs e Difusão, avaliação e riscos de vazamento)

CHEN, Pin-Yu; HSIEH, Cho-Jui. *Adversarial Robustness for Deep Learning*. Morgan & Claypool, 2020.

VOROBEYCHIK, Yevgeniy; KANTARCIOGLU, Murat. *Adversarial Machine Learning*. Morgan & Claypool, 2018.

YANG, Qiang; LIU, Yang; CHEN, Tianjian; TONG, Yongxin. *Federated Learning*. Morgan & Claypool, 2019.

CACCIA, Massimo; TU, Stephen; et al. *Reliable Machine Learning: Applying SRE Principles to ML in Production*. O'Reilly, 2023. (observabilidade/incident response de modelos)

HUYEN, Chip. *Designing Machine Learning Systems*. O'Reilly, 2022. (MLOps/LLMOps: governança, drift, reprodutibilidade)

COX, Ingemar; MILLER, Matt; BLOOM, Jeffrey; FRIDRICH, Jessica; KALKER, Ton. *Digital Watermarking and Steganography*. 2nd ed. Morgan Kaufmann, 2008. (proveniência e marca d'água)

Bibliografia Complementar

MURPHY, K. P. *Probabilistic Machine Learning: An Introduction*. MIT Press, 2022.

SHALEV-SHWARTZ, S.; BEN-DAVID, S. *Understanding Machine Learning: From Theory to Algorithms*. Cambridge, 2014.

ZHENG, A. *Evaluating Machine Learning Models*. O'Reilly, 2015. (métricas, curvas PR/ROC e calibração.)

CASARI, A.; ZHENG, A. *Feature Engineering for Machine Learning*. O'Reilly, 2018.

AGGARWAL, C. C. *Machine Learning for Text*. Springer, 2018. (NLP prático para phishing.)

PATEL, A. *Hands-On Unsupervised Learning with Python*. O'Reilly, 2019. (k-means, GMM, DBSCAN, PCA/UMAP.)

LAKSHMANAN, V.; TIGHE, S.; BRYNJOLFSSON, S. *Machine Learning Design Patterns*. O'Reilly, 2020. (MLOps e anti-padrões.)

GIFT, N.; BEHRMAN, K. *Practical MLOps*. O'Reilly, 2021.

VOROBEYCHIK, Y.; KANTARCIOGLU, M. *Adversarial Machine Learning*. Morgan & Claypool, 2018. (poisoning/evasion, bases para o módulo II.)

SANDERS, C.; SMITH, J. *Applied Network Security Monitoring*. Syngress, 2013. (coleta/rotulagem de dados para IDS.)

COLLINS, M. *Network Security Through Data Analysis*. 2nd ed. O'Reilly, 2017.

FACELI, K.; LORENA, A. C.; GAMA, J.; DE CARVALHO, A. C. P. L. F. *Inteligência Artificial: Uma Abordagem de Aprendizado de Máquina*. 2. ed. LTC, 2021.

HAN, J.; KAMBER, M.; PEI, J. *Data Mining: Concepts and Techniques*. 4th ed. Morgan Kaufmann, 2022.

BAROCAS, S.; HARDT, M.; NARAYANAN, A. *Fairness and Machine Learning*. MIT Press (open book), 2023. (viés e justiça.)

CHEN, Y.; WU, J.; YU, P.; WANG, X. *Network Security Empowered by AI*. Springer, 2024.

STAMP, M.; VISAGGIO, C. A.; MERCALDO, F.; DI TROIA, F. *Artificial Intelligence for Cybersecurity*. Springer, 2022.

HALDER, S.; OZDEMIR, S. *Hands-On Machine Learning for Cybersecurity*. Packt, 2018. (exemplos práticos de malware/phishing.)

KLEPPMANN, M. *Designing Data-Intensive Applications*. O'Reilly, 2017. (linhagens, logs, tolerância a falhas – suporte ao SOC.)

WALLACE, D.; ENGLEHARDT, S. *The Joy of Cryptography*. 2nd ed., 2024. (fundamentos de segurança/PRFs/MACs úteis a pipelines.)

MURPHY, Kevin P. *Probabilistic Machine Learning: Advanced Topics*. MIT Press, 2023.

HAMILTON, William L. *Graph Representation Learning*. Morgan & Claypool, 2020. (GNNs para grafos de comunicação)

RUBINSTEIN, Benjamin I. P.; NELSON, Blaine; JOSEPH, Anthony D.; et al. *Adversarial Machine Learning*. Morgan & Claypool, 2019. (coletânea complementar a Vorobeychik & Kantarcioglu)

LI, Qinbin; YANG, Yiqun; SONG, Shusen; et al. *Federated Learning: Algorithms, Systems, and Applications*. Springer, 2022.

VAIDYA, Jaideep; CLIFTON, Chris; ZHU, Michael. *Privacy-Preserving Machine Learning*. Morgan & Claypool, 2020.

BAROCAS, Solon; HARDT, Moritz; NARAYANAN, Arvind. *Fairness and Machine Learning*. MIT Press (open), 2023.

GIFT, Noah; DEZA, Alfredo. *Practical MLOps*. O'Reilly, 2021.

PARISI, Antonio G. *Hands-On Artificial Intelligence for Cybersecurity*. Packt, 2019.

ROTHMAN, Denis. *Transformers for Natural Language Processing*. 3rd ed. Packt, 2023.

ULLMAN, Jonathan; STEFANOV, Emil; et al. *Differential Privacy for Databases, Data Analysis, and Machine Learning*. Morgan & Claypool, 2023. (visão prática complementar a Dwork–Roth)

FARID, Hany. *Photo Forensics*. MIT Press, 2016. (detecção de manipulações; apoio a proveniência/anti-deepfake)

Módulo 8 — Projeto de Graduação I

Carga horária: 150 horas

Ementa

Integração e aplicação dos conhecimentos acumulados nos módulos anteriores por meio de um projeto de graduação orientado em uma de três trilhas: **Acadêmica**, **Corporativa** ou **Empreendedora**. Ênfase em *scoping*, formulação de problema, levantamento do estado da arte/estado da prática, desenho metodológico, plano de projeto (backlog, cronograma, riscos) e governança (ética, conformidade, segurança e proteção de dados). O módulo estabelece bases sólidas para desenvolvimento, avaliação e transferência de resultados nos módulos subsequentes.

Objetivos de Aprendizagem

Ao término do módulo, o discente deverá ser capaz de:

1. Selecionar a trilha (Acadêmica, Corporativa ou Empreendedora) e formular um **problema bem-definido** alinhado a requisitos técnicos e de impacto.
2. Elaborar **revisão de literatura/benchmark** (acadêmico e/ou industrial), identificando lacunas e hipóteses/testáveis ou metas de negócio/usuário.
3. Construir **plano de projeto** com escopo, objetivos, *WBS*, backlog priorizado, cronograma (sprints), custos/recursos, riscos e métricas de sucesso.
4. Definir **métodos de coleta/análise** (científicos ou de engenharia) e estratégia de avaliação (métricas, experimentos, pilotos, aceites).
5. Atender a **critérios éticos**, de segurança e proteção de dados (consentimento, confidencialidade, LGPD, biossegurança quando aplicável).

Conteúdos Programáticos

1. Fundamentos comuns ao projeto

- Formulação de problema, objetivo geral/específicos, indicadores de valor.
- Estado da arte e da prática; *gap analysis*; definição de hipóteses/OKRs.
- Planejamento: WBS, cronograma por sprints, orçamento/recursos, matriz de riscos.
- Governança: ética, integridade acadêmica, LGPD e gestão de dados.

2. Trilhas e ênfases

- **Acadêmica**: metodologia científica; desenho experimental; pré-projeto de artigo; prospecção de programas de pós (POSCOMP e seleções).
- **Corporativa**: estudo de mercado; requisitos de negócio; desenho de *pipeline* e SLA/SLO; mapeamento de certificações e processos seletivos.
- **Empreendedora**: problema de cliente; proposta de valor; *lean canvas*; modelagem de produto/serviço; PI (patente/software) e responsabilidade social.

Metodologia

Aprendizagem baseada em projetos com *sprints* quinzenais; encontros de orientação (10h) e desenvolvimento (140h); *design reviews*, *risk reviews*; *ethics check* e aprendizagem guiada por inteligência artificial.

Avaliação

(i) **Plano de Projeto** completo (backlog, cronograma, riscos, métricas) e *baseline*; (ii) **Revisão Crítica** do estado da arte/prática; (iii) **Protocolo Metodológico**/Plano de Avaliação; (iv) apresentação pública de *scoping*. Participação e assiduidade contam.

Competências Desenvolvidas (síntese)

Formulação de problemas; planejamento e gestão por sprints; análise crítica de literatura/mercado; ética e governança de dados; comunicação técnica e tomada de decisão, uso da inteligência artificial no processo de aprendizagem e desenvolvimento de projetos.

Bibliografia Básica

BOOTH, W. C.; COLOMB, G. G.; WILLIAMS, J. M.; et al. *The Craft of Research*. 4. ed. University of Chicago Press, 2016.

CRESWELL, J. W.; CRESWELL, J. D. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5. ed. SAGE, 2018.

KITCHENHAM, B.; BUDGEN, D.; BRERETON, P. *Evidence-Based Software Engineering and Systematic Reviews*. CRC Press, 2015.

WOHLIN, C.; et al. *Experimentation in Software Engineering*. Springer, 2012.

RUNESON, P.; HÖST, M.; RAINER, A.; REGNELL, B. *Case Study Research in Software Engineering: Guidelines and Examples*. Wiley/IEEE, 2012.

PRESSMAN, R. S.; MAXIM, B. R. *Engenharia de Software: Uma Abordagem Profissional*. 9. ed. AMGH, 2021.

PMI. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*. 7. ed. PMI, 2021.

COHN, M. *User Stories Applied: For Agile Software Development*. Addison-Wesley, 2004.

DOERR, J. *Measure What Matters: How Google, Bono, and the Gates Foundation Rock the World with OKRs*. Penguin, 2018.

KENDRICK, T. *Identifying and Managing Project Risk*. 4. ed. Amacom, 2019.

ZOBEL, J. *Writing for Computer Science*. 3. ed. Springer, 2014.

QUINN, M. J. *Ethics for the Information Age*. 8. ed. Pearson, 2020.

MONTEIRO, R. L. (org.). *LGPD – Lei Geral de Proteção de Dados Pessoais Comentada*. 2. ed. Revista dos Tribunais/Thomson Reuters, 2022. (ou edição equivalente atualizada)

WILSON, J.; DROUIN, J. *Research Data Management: Practical Strategies for Information Professionals*. ALA/Neal-Schuman, 2021.

GASTEL, B.; DAY, R. A. *How to Write and Publish a Scientific Paper*. 9. ed. ABC-CLIO, 2022.

Bibliografia Complementar

SUTHERLAND, J. *SCRUM: A Arte de Fazer o Dobro do Trabalho na Metade do Tempo*. Alta Books, 2016.

HUMBLE, J.; FARLEY, D. *Continuous Delivery*. Addison-Wesley, 2010.

BEYER, B.; et al. *Site Reliability Engineering*. O'Reilly, 2016. (SLA/SLO, incidentes – útil para trilha Corporativa)

FORSGREN, N.; HUMBLE, J.; KIM, G. *Accelerate: The Science of Lean Software and DevOps*. IT Revolution, 2018.

OSTERWALDER, A.; PIGNEUR, Y.; et al. *Value Proposition Design*. Wiley, 2014.

RIES, E. *The Lean Startup*. Crown, 2011.

MAURYA, A. *Running Lean*. 2. ed. O'Reilly, 2012.

CROLL, A.; YOSKOVITZ, B. *Lean Analytics*. O'Reilly, 2013.

SAURO, J.; LEWIS, J. R. *Quantifying the User Experience*. 2. ed. Morgan Kaufmann, 2016. (avaliação de UX e métricas)

PORTIGAL, S. *Interviewing Users: How to Uncover Compelling Insights*. 2. ed. Rosenfeld, 2023.

KITCHENHAM, B.; CHARTERS, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. EBSE Tech. Report, 2007. (apoio à SLR)

SHADISH, W. R.; COOK, T. D.; CAMPBELL, D. T. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. 2. ed. Houghton Mifflin, 2021.

FIELD, A.; HOLE, G. *How to Design and Report Experiments*. Sage, 2003.

KNUTH, D. E.; LARRABEE, T.; ROBERTS, P. M. *Mathematical Writing*. MAA, 1989. (comunicação técnica precisa)

KAPLAN, R. S.; NORTON, D. P. *The Balanced Scorecard*. Harvard Business Review Press, 1996. (métricas e desdobramento de objetivos)

WIMMER, M.; MENDES, L.; DONEDA, D. (org.). *Proteção de Dados Pessoais: Comentários à LGPD*. Juspodivm, 2021. (alternativa/compl. em LGPD)

TENOPIR, C.; LEVINE, K. *Data Management: A Practical Guide for Librarians*. Rowman & Littlefield, 2016.

O'CONNOR, R. V.; BASRI, S.; et al. *Practice-Driven Research on Enterprise Transformation*. Springer, 2018. (ponte Academia–Indústria)

OECD. *Good Research Practices for Research Integrity*. OECD, 2023. (integridade, reprodutibilidade)

Módulo 9 — Projeto de Graduação II

Carga horária: 150 horas

Ementa (revisada)

Consolidação e defesa do projeto de graduação com entrega de **relatório/artigo final**, demonstração pública e documentação completa. O módulo integra evidências técnicas, impacto e conformidade. **Exigência adicional:** apresentação de um **Memorial** descrevendo as atividades de extensão realizadas ao longo do curso, comprovando o cumprimento de, no mínimo, **405 horas** de extensão aprovadas.

Objetivos de Aprendizagem

1. Produzir **relatório técnico ou artigo científico** final, com reprodutibilidade, análise crítica e discussão de limitações.
2. Realizar **defesa pública** (banca) com demonstração e arguição.
3. Entregar **documentação completa** (manual do usuário, instalação/operação, segurança/privacidade, manutenção).
4. Compilar e defender o **Memorial de Extensão** (com carga-horário mínima de 405h), articulando impactos para comunidade e aprendizagem.
5. Elaborar **plano de continuidade** (pesquisa, carreira corporativa ou empreendedorismo).

Conteúdos Programáticos

1. Encerramento técnico

- Consolidação de resultados; análise de sensibilidade/ameaças à validade; *postmortem* e lições aprendidas.
- Pacote de entrega: código/dados, versões, licenças, guia de operação/segurança, *SLA/SLO* (quando aplicável).

2. Comunicação e defesa

- Escrita científica/relatório executivo; visualização e narrativa técnica.
- Preparação para banca: *rehearsal*, gestão do tempo, respostas a críticas.

3. Extensão universitária

- Estrutura do **Memorial de Extensão**: objetivos, atividades, horas, evidências/documentos, impactos e reflexão crítica.
- Integração ensino–pesquisa–extensão; princípios éticos e avaliação de impacto social.

Metodologia

Sprints finais orientadas a entrega/defesa; *peer reviews*; simulações de banca e *pitch*; oficinas de escrita e de memorial de extensão; mentoria individual e aprendizagem guiada por inteligência artificial.

Avaliação

(i) **Relatório**/**Artigo Final** com material suplementar reprodutível; (ii) **Defesa Pública** (banca); (iii) **Dossiê de Documentação** (operação/segurança/PI quando aplicável); (iv) **Memorial de Extensão** comprovando carga horária superior ou igual a **405h**; (v) participação e cumprimento de marcos.

Competências Desenvolvidas (síntese)

Entrega e defesa de projetos complexos; comunicação técnica de alto impacto; documentação e reprodutibilidade; avaliação de impacto social; planejamento de continuidade acadêmica/corporativa/empreendedora, uso da inteligência artificial no processo de aprendizagem e desenvolvimento de projetos.

Bibliografia Básica

BOOTH, W. C.; COLOMB, G. G.; WILLIAMS, J. M.; et al. *The Craft of Research*. 4. ed. University of Chicago Press, 2016.

CRESWELL, J. W.; CRESWELL, J. D. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5. ed. SAGE, 2018.

KITCHENHAM, B.; BUDGEN, D.; BRERETON, P. *Evidence-Based Software Engineering and Systematic Reviews*. CRC Press, 2015.

WOHLIN, C.; et al. *Experimentation in Software Engineering*. Springer, 2012.

RUNESON, P.; HÖST, M.; RAINER, A.; REGNELL, B. *Case Study Research in Software Engineering: Guidelines and Examples*. Wiley/IEEE, 2012.

PRESSMAN, R. S.; MAXIM, B. R. *Engenharia de Software: Uma Abordagem Profissional*. 9. ed. AMGH, 2021.

PMI. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*. 7. ed. PMI, 2021.

COHN, M. *User Stories Applied: For Agile Software Development*. Addison-Wesley, 2004.

DOERR, J. *Measure What Matters: How Google, Bono, and the Gates Foundation Rock the World with OKRs*. Penguin, 2018.

KENDRICK, T. *Identifying and Managing Project Risk*. 4. ed. Amacom, 2019.

ZOBEL, J. *Writing for Computer Science*. 3. ed. Springer, 2014.

QUINN, M. J. *Ethics for the Information Age*. 8. ed. Pearson, 2020.

MONTEIRO, R. L. (org.). *LGPD – Lei Geral de Proteção de Dados Pessoais Comentada*. 2. ed. Revista dos Tribunais/Thomson Reuters, 2022. (ou edição equivalente atualizada)

WILSON, J.; DROUIN, J. *Research Data Management: Practical Strategies for Information Professionals*. ALA/Neal-Schuman, 2021.

GASTEL, B.; DAY, R. A. *How to Write and Publish a Scientific Paper*. 9. ed. ABC-CLIO, 2022.

Bibliografia Complementar

SUTHERLAND, J. *SCRUM: A Arte de Fazer o Dobro do Trabalho na Metade do Tempo*. Alta Books, 2016.

HUMBLE, J.; FARLEY, D. *Continuous Delivery*. Addison-Wesley, 2010.

BEYER, B.; et al. *Site Reliability Engineering*. O'Reilly, 2016. (SLA/SLO, incidentes – útil para trilha Corporativa)

FORSGREN, N.; HUMBLE, J.; KIM, G. *Accelerate: The Science of Lean Software and DevOps*. IT Revolution, 2018.

OSTERWALDER, A.; PIGNEUR, Y.; et al. *Value Proposition Design*. Wiley, 2014.

RIES, E. *The Lean Startup*. Crown, 2011.

MAURYA, A. *Running Lean*. 2. ed. O'Reilly, 2012.

CROLL, A.; YOSKOVITZ, B. *Lean Analytics*. O'Reilly, 2013.

SAURO, J.; LEWIS, J. R. *Quantifying the User Experience*. 2. ed. Morgan Kaufmann, 2016. (avaliação de UX e métricas)

PORTIGAL, S. *Interviewing Users: How to Uncover Compelling Insights*. 2. ed. Rosenfeld, 2023.

KITCHENHAM, B.; CHARTERS, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. EBSE Tech. Report, 2007. (apoio à SLR)

SHADISH, W. R.; COOK, T. D.; CAMPBELL, D. T. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. 2. ed. Houghton Mifflin, 2021.

FIELD, A.; HOLE, G. *How to Design and Report Experiments*. Sage, 2003.

KNUTH, D. E.; LARRABEE, T.; ROBERTS, P. M. *Mathematical Writing*. MAA, 1989. (comunicação técnica precisa)

KAPLAN, R. S.; NORTON, D. P. *The Balanced Scorecard*. Harvard Business Review Press, 1996. (métricas e desdobramento de objetivos)

WIMMER, M.; MENDES, L.; DONEDA, D. (org.). *Proteção de Dados Pessoais: Comentários à LGPD*. Juspodivm, 2021. (alternativa/compl. em LGPD)

TENOPIR, C.; LEVINE, K. *Data Management: A Practical Guide for Librarians*. Rowman & Littlefield, 2016.

O'CONNOR, R. V.; BASRI, S.; et al. *Practice-Driven Research on Enterprise Transformation*. Springer, 2018. (ponte Academia–Indústria)

OECD. *Good Research Practices for Research Integrity*. OECD, 2023. (integridade, reprodutibilidade)

Referências Bibliográficas

[1] Richard P. Feynman. *Só Pode Ser Brincadeira, Sr. Feynman!* Intrínseca, Rio de Janeiro, 2018. Tradução de: Surely You're Joking, Mr. Feynman!: Adventures of a Curious Character.

[2] J. Pacheco and M. de Fátima Pacheco. *Escola da ponte: Uma escola pública em debate*. Cortez Editora, 2018.

FACULDADE DE ENGENHARIA ELÉTRICA
UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Uberlândia/MG, Brasil
http://www.feelt.ufu.br

Universidade Federal de Uberlândia