

UNIVERSIDADE FEDERAL DO SUL DA BAHIA - UFSB
CENTRO MULTIDISCIPLINAR CIÊNCIA E SOCIEDADE - CMCS
CAMPUS JEQUIÉ

PROJETO PEDAGÓGICO DE CURSO DO BACHARELADO EM
ENGENHARIA EM CIBERSEGURANÇA

JEQUIÉ-BA
SETEMBRO DE 2025

Reitora da UFSB

Profª Drª Joana Angélica Guimarães

Pró-Reitor de Gestão Acadêmica

Prof. Francesco Lanciotti Júnior

Decanato do CMCS

Prof. Dr. Roberlaine Ribeiro Jorge (Decano Pró-tempore)

Equipe de Trabalho

Profa. Dra. Mydiã Falcão Freitas – SIAPE N.º 1426246 (Coordenadora)

Prof. Dr. Edcarllos Gonçalves dos Santos – SIAPE N.º 1716516

Prof. Dr. Roberlaine Ribeiro Jorge - SIAPE N.º 1850817

TAE Jenner da Cruz de Souza – SIAPE N.º 2413424

Sumário

1. DADOS DA INSTITUIÇÃO	1
2. IDENTIFICAÇÃO DO CURSO	3
3. BASES LEGAIS DO PROJETO PEDAGÓGICO DE CURSO	4
4. APRESENTAÇÃO	8
5. JUSTIFICATIVA DE OFERTA DO CURSO.....	10
5.1 Histórico de Implantação do Curso	10
5.2 Justificativa de Oferta	11
6. POLÍTICAS INSTITUCIONAIS NO ÂMBITO DO CURSO.....	13
6.1 Políticas de Acesso ao Curso e de Mobilidade Acadêmica	13
6.2 Políticas de Ensino	15
6.3 Políticas de Pesquisa	17
6.4 Políticas de Extensão.....	19
6.5 Políticas de Atendimento ao/à Estudante.....	20
6.6 Políticas de Internacionalização	23
7. OBJETIVOS DO CURSO.....	25
7.1 Objetivo Geral	25
7.2 Objetivos Específicos	25
8. PERFIL DO/A EGRESSO/A	27
8.1 Campos de Atuação Profissional.....	28
9. PROPOSTA PEDAGÓGICA.....	30
10. ARQUITETURA CURRICULAR.....	34
10.1 Atividades e Componentes Curriculares de Extensão	46
10.2 Estágio Curricular	49
10.3 Atividades Complementares.....	51
10.4 Trabalho de Conclusão de Curso	51

SUMARIO

10.5 Matriz Curricular	53
10.6 Ensino à Distância.....	55
11. AVALIAÇÃO DOS PROCESSOS DE ENSINO-APRENDIZAGEM	60
12. PROCESSOS DE AVALIAÇÃO DO PROJETO PEDAGÓGICO DE CURSO	62
13. GESTÃO DO CURSO	64
13.1 Coordenação do Colegiado de Curso	64
13.2 Colegiado de Curso	65
13.3 Núcleo Docente Estruturante (NDE).....	66
13.4 Coordenação de Extensão e Comissão Própria de Assessoria.....	68
14. INFRAESTRUTURA	70
14.1 Infraestrutura Física.....	70
14.2 Acervo Bibliográfico	71
15. CATÁLOGO DE EMENTAS DOS COMPONENTES CURRICULARES ..	72
15.1 Componentes Curriculares da Formação Geral.....	72
15.2 Componentes Curriculares Obrigatórios.....	101
15.3 Componentes Curriculares Optativos.....	147
.....	157
15.4 Componentes Curriculares de Extensão	169
16. REFERÊNCIAS BIBLIOGRÁFICAS.....	174

1. DADOS DA INSTITUIÇÃO

Instituição de Ensino Superior:	Universidade Federal do Sul da Bahia
Sigla:	UFSB
CNPJ:	18.560.547/0001-07
Categoria Administrativa:	Pública Federal
Organização Acadêmica:	Universidade
Lei de Criação:	Lei nº 12.818, de 05 de junho de 2013
Endereço do sítio:	http://www.ufsb.edu.br

Para operação institucional da oferta diversificada dos Cursos em Regime de Ciclos, a estrutura institucional da UFSB compreende quatro esferas de organização, respeitando a ampla cobertura regional da instituição, com a seguinte distribuição de Unidades Acadêmicas:

CAMPUS JEQUIÉ

Km 3 BR 116, S/N, Bairro Mandacaru, 45200-000, Jequié-BA

- Centro Multidisciplinar Ciência e Sociedade (CMCS)

CAMPUS JORGE AMADO - ILHÉUS

Rodovia Ilhéus/Itabuna - km 22 - Ilhéus/BA, CEP: 45600-970

- Centro de Formação em Ciências Agroflorestais (CFCAf)
- Centro de Formação em Políticas Públicas e Tecnologias Sociais (CFPPTS)
- Centro de Formação em Tecnociências e Inovação (CFTCI)
- Instituto Jorge Amado de Humanidades, Artes e Ciências (IHAC)
- Rede CUNI Litoral Sul [Coaraci, Ibicaraí, Ilhéus e Itabuna]

CAMPUS PAULO FREIRE - TEIXEIRA DE FREITAS

Praça Joana Angélica, 250, São José, Teixeira de Freitas/BA, CEP: 45988-058

- Centro de Formação em Ciências da Saúde (CFCS)

- Centro de Formação em Desenvolvimento Territorial (CFDT)
- Instituto Paulo Freire de Humanidades, Artes e Ciências (IHAC)
- Rede CUNI Extremo Sul [Itamaraju, Posto do Mata, Teixeira de Freitas, Helvécia e Medeiros Neto]

CAMPUS SOSÍGENES COSTA - PORTO SEGURO

Rodovia Porto Seguro/Eunápolis - km 10, Porto Seguro/BA, CEP: 45810-000

- Centro de Formação em Artes e Comunicação (CFAC)
- Centro de Formação em Ciências Ambientais (CFCAm)
- Centro de Formação em Ciências Humanas e Sociais (CFCHS)
- Instituto Sosígenes Costa de Humanidades, Artes e Ciências (IHAC)
- Rede CUNI Costa do Descobrimento [Eunápolis, Porto Seguro, Santa Cruz Cabrália]

2. IDENTIFICAÇÃO DO CURSO

Curso:	Bacharelado em Engenharia em Cibersegurança
Diplomação:	Bacharel/la em Engenharia em Cibersegurança
Carga Horária Total do Curso:	3600 horas
Tempo Mínimo para Integralização:	04 anos e 06 meses ou 9 semestres
Tempo Máximo para Integralização:	09 anos ou 18 semestres
Estágio Obrigatório:	160 horas
Extensão:	380 horas
Atividades Complementares:	120 horas
Turno de Oferta:	Integral
Número de Vagas:	40 vagas
Campus de Oferta:	Campus Jequié/BA

3. BASES LEGAIS DO PROJETO PEDAGÓGICO DE CURSO

A elaboração do Projeto Pedagógico de Curso (PPC) do Bacharelado em Engenharia em Cibersegurança foi norteadada por diretrizes estabelecidas pelo Governo Federal, pelo Conselho Nacional de Educação da Câmara de Educação Superior (CNE/CES) e pelo Conselho Federal da Engenharia, Arquitetura e Agronomia (CONFEA), assim como atende ao modelo pedagógico preconizado pela UFSB. Neste contexto, a organização curricular proposta assenta-se em várias diretrizes e resoluções:

- Lei 5.194, de 24 de Dezembro de 1966, que regula o exercício das profissões de Engenheiro, e dá outras providências;
- Lei nº 9.394, de 20 de Dezembro de 1996, que estabelece as diretrizes e bases da educação nacional;
- Lei nº 9.795, de 27 de Abril de 1999, que institui a Política Nacional de Educação Ambiental, e o Decreto nº 4.281, de 25 de Junho de 2002, que institui a Política Nacional de Educação Ambiental;
- Lei nº 10.098, de 19 de Dezembro de 2000, que estabelece normas gerais e critérios básicos para a promoção da acessibilidade das pessoas portadoras de deficiência ou com mobilidade reduzida, e dá outras providências;
- Lei nº 10.639, de 09 de Janeiro de 2003, que altera a Lei nº 9.394, de 20 de Dezembro de 1996, para incluir no currículo oficial da Rede de Ensino a obrigatoriedade da temática "História e Cultura Afro-Brasileira", e dá outras providências;
- Lei nº 11.645, de 10 de Março de 2008, que altera a Lei nº 9.394 para incluir no currículo oficial da rede de ensino a obrigatoriedade da temática “História e Cultura Afro-Brasileira e Indígena”;
- Lei nº 12.764, de 27 de Dezembro de 2012, que institui a Política Nacional de Proteção dos Direitos da Pessoa com Transtorno do Espectro Autista;
- Lei nº 13.005, de 25 de Junho de 2014, que aprova o Plano Nacional de Educação - PNE e dá outras providências;
- Decreto nº 5.626, de 22 de Dezembro de 2005, que dispõe sobre a Língua Brasileira de Sinais - Libras;
- Decreto nº 9.057, de 25 de maio de 2017, que regulamenta o artigo 80 da Lei nº 9.394, de 20 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional;

- Decreto nº 12.456, de 19 de maio de 2025, que dispõe sobre a oferta de educação a distância por instituições de educação superior em cursos de graduação;
- Portaria Normativa nº 40, de 12 de Dezembro de 2007, que institui o e-MEC, sistema eletrônico de fluxo de trabalho e gerenciamento de informações relativas aos processos de regulação, avaliação e supervisão da educação superior no sistema federal de educação, e o Cadastro e-MEC de Instituições e Cursos Superiores e consolida disposições; sobre indicadores de qualidade, banco de avaliadores (Basis) e o Exame Nacional de Desempenho de Estudantes (ENADE) e outras disposições.
- Resolução CNAES nº 01, de 17 de junho de 2010, que normatiza o Núcleo Docente Estruturante e dá outras providências;
- Resolução CNE/CES nº 11, de 11 de Março de 2002 que institui as diretrizes curriculares do curso de graduação em Engenharia;
- Resolução CNE/CES nº 01, de 17 de Junho de 2004, que institui Diretrizes Curriculares Nacionais para a Educação das Relações Étnico-Raciais e para o Ensino de História e Cultura Afro-Brasileira e Africana;
- Resolução CNE/CES nº 02, de 18 de Junho de 2007 e Parecer CNE/CES nº 441, de 10 de Julho de 2020 que dispõe sobre carga horária mínima e procedimentos relativos à integralização e duração dos cursos de Engenharia;
- Resolução CNE/CES nº 03, de 02 de Julho de 2007, que dispõe sobre procedimentos a serem adotados quanto ao conceito de hora-aula, e dá outras providências;
- Resolução CNE/CP nº 03, de 10 de Março de 2004, que institui Diretrizes Curriculares Nacionais para a Educação das Relações Étnico-Raciais e para o Ensino de História e Cultura Afro-Brasileira e Africana;
- Resolução CNE/CP nº 01, de 30 de Maio de 2012, que estabelece Diretrizes Nacionais para a Educação em Direitos Humanos;
- Resolução CNE/CES nº 05, de 16 de Novembro de 2016, que institui as Diretrizes Curriculares Nacionais para os cursos de graduação na área da Computação, abrangendo os cursos de bacharelado em Ciência da Computação, em Sistemas de Informação, em Engenharia de Computação, em Engenharia de Software e de licenciatura em Computação, e dá outras providências;
- Resolução CNE/CES nº 07, de 18 de Dezembro de 2018, que estabelece as diretrizes para a Extensão na Educação Superior Brasileira;

- Resolução CNE/CES nº 02, de 24 de Abril de 2019, que institui as Diretrizes Curriculares Nacionais do Curso de Graduação em Engenharia;
- Resolução CNE/CES nº 01, de 29 de Dezembro de 2020, que dispõe sobre prorrogação de prazo de implantação das novas Diretrizes Curriculares Nacionais (DCNs);
- Resolução CNE/CES nº 01, de 26 de Março de 2021, que altera o Art. 9º, § 1º da Resolução CNE/CES nº 02, de 24 de Abril de 2019, que institui as Diretrizes Curriculares Nacionais do Curso de Graduação em Engenharia;
- Parecer CNE/CES nº 776, de 3 de Dezembro de 1997, sobre as Diretrizes Curriculares dos cursos de graduação;
- Parecer CNE/CES nº 1362, de 12 de Dezembro de 2001, sobre as Diretrizes Curriculares Nacionais dos Cursos de Engenharia;
- Parecer CNE/CES nº 153, de 7 de Agosto de 2008, sobre a consulta quanto a carga horária mínima do curso de Engenharia da Computação;
- Parecer CNE/CES nº 266, de 6 de Julho de 2011, sobre os referenciais orientadores para os Bacharelados Interdisciplinares e similares das IES;
- Parecer CNE/CES nº 136, de 9 de Março de 2012, sobre as Diretrizes Curriculares Nacionais para os cursos de graduação em Computação;
- Parecer CNE/CES nº 01, de 23 de Janeiro de 2019, sobre as Diretrizes Curriculares Nacionais do Curso de Graduação em Engenharia;
- Parecer CNE/CES nº 334, de 8 de Maio de 2019, que institui a Orientação às Diretrizes Curriculares Nacionais dos Cursos Superiores;
- Parecer CNE/CES nº 948, de 9 de Outubro de 2019, que altera a Resolução CNE/CES nº 2, de 24 de abril de 2019, que institui as Diretrizes Curriculares Nacionais do Curso de Graduação em Engenharia, em virtude de decisão judicial transitada em julgado.
- Referenciais orientadores para os Bacharelados Interdisciplinares e similares, de novembro de 2010;
- Resolução CONFEA nº 218, de 29 de Junho de 1973 que discrimina atividades das diferentes modalidades profissionais da Engenharia;
- Resolução CONFEA nº 473, de 26 de Novembro de 2002, que institui a tabela de títulos profissionais do sistema Confea/Crea, e dá outras providências;

- Resolução CONFEA nº 1073, de 19 de Abril de 2016, que regulamenta a atribuição de títulos, atividades, competências e campos de atuação aos profissionais registrados no Sistema Confea/Crea para efeito de fiscalização do exercício profissional no âmbito da Engenharia;
- Carta de Fundação da UFSB;
- Plano Orientador da UFSB;
- Relatório do I Fórum Social da UFSB (2015);
- Resolução CONSUNI nº 24, de 17 de Outubro de 2019, que dispõe sobre as normas que regulamentam as Atividades de Extensão;
- Resolução CONSUNI nº 13, de 29 de Junho de 2021, que dispõe sobre a curricularização das Atividades de Extensão nos cursos de graduação;
- Resolução CONSUNI nº 14, de 02 de Agosto de 2021, que dispõe sobre as normas que regulamentam as Atividades de Extensão;
- Resolução CONSUNI nº 06, de 06 de Junho de 2024, que dispõe sobre criação e extinção de cursos de graduação, elaboração e reformulação de projetos pedagógico de cursos da UFSB;
- FORPROEX. Política Nacional de Extensão Universitária. Gráfica da UFRGS. Porto Alegre, RS, 2012 (Coleção Extensão Universitária; v. 7.).

4. APRESENTAÇÃO

O presente documento apresenta o Projeto Pedagógico de Curso (PPC) do Bacharelado em Engenharia em Cibersegurança (BECiber), ofertado pelo Centro Multidisciplinar Ciência e Sociedade (CMCS) da Universidade Federal do Sul da Bahia (UFSB). A proposta foi construída por um grupo de trabalho formado por docentes e técnicos-administrativos da instituição, com ampla experiência em Computação e Segurança da Informação. O objetivo é atender às demandas regionais, nacionais e internacionais por profissionais preparados para atuar em um mundo globalizado e em constante transformação tecnológica.

A concepção deste PPC segue os princípios e diretrizes das Diretrizes Curriculares Nacionais (DCN) para os cursos de Engenharia, estabelecidas pelo Ministério da Educação (MEC), e está alinhada às políticas institucionais da UFSB, que priorizam uma formação interdisciplinar, crítica e ética. O curso busca formar engenheiros com perfil multidisciplinar, capazes de atuar em áreas como segurança de redes, criptografia, forense computacional, confiança digital e engenharia de software seguro, desenvolvendo competências para enfrentar os desafios da inovação tecnológica. A matriz curricular proposta combina os fundamentos básicos da engenharia com disciplinas específicas de segurança da informação, articulando ensino, pesquisa e extensão em consonância com as diretrizes nacionais.

Um dos pilares da proposta é a articulação com o setor produtivo, em especial com as demandas regionais relacionadas à segurança cibernética. Localizado em Jequié, no sudoeste baiano, o curso oferece condições para que os futuros engenheiros contribuam com soluções inovadoras para o desenvolvimento econômico sustentável da região. A formação possibilitará que os egressos atuem no mapeamento de riscos, no desenvolvimento de sistemas seguros, na concepção de soluções de defesa cibernética e em projetos colaborativos com empresas e instituições locais, sempre com responsabilidade social e ética profissional.

A elaboração do documento seguiu princípios que garantem uma estrutura curricular sólida e atualizada, entre os quais se destacam:

- domínio das ciências básicas e das engenharias;
- integração contínua entre os ciclos de formação (básico, profissionalizante e específico);
- desenvolvimento das capacidades de análise, associação e síntese;

- estímulo a práticas que fortaleçam a capacidade individual e coletiva de resolução de problemas;
- estreita integração com o setor produtivo e a comunidade local, por meio de estágios supervisionados, trabalhos de conclusão de curso e atividades extensionistas;
- articulação entre os conteúdos das disciplinas, de forma a evitar fragmentação;
- valorização dos princípios de desenvolvimento sustentável.

Assim, o Projeto Pedagógico de Curso foi estruturado considerando aspectos sociais, ambientais, políticos, humanísticos e éticos, traduzindo-se na formação de profissionais generalistas, humanistas, críticos e reflexivos, com uma base teórico-prática sólida em Engenharia em Cibersegurança. Essa proposta reafirma o compromisso do Centro Multidisciplinar Ciência e Sociedade (CMCS) da UFSB em ofertar um curso de excelência, alinhado às necessidades contemporâneas da sociedade e do mercado de trabalho, e comprometido com o avanço científico e tecnológico do Brasil.

5. JUSTIFICATIVA DE OFERTA DO CURSO

5.1 Histórico de Implantação do Curso

A Universidade Federal do Sul da Bahia (UFSB) foi criada pela Lei nº 12.818/2013 e iniciou suas atividades acadêmicas em 8 de setembro de 2014. Desde então, consolidou sua presença em diferentes municípios, com a sede em Itabuna e *campi* em Porto Seguro e Teixeira de Freitas, além da Rede Anísio Teixeira de Colégios Universitários (Rede CUNI), que funciona em escolas da rede pública estadual de ensino médio. Mais recentemente, a UFSB expandiu sua atuação com a implantação do *Campus* em Jequié, consolidando sua presença estratégica também no sudoeste baiano.

Desde sua criação, tornou-se evidente a necessidade de estruturar cursos capazes de responder às demandas regionais e nacionais, em consonância com os princípios do desenvolvimento sustentável e da inovação tecnológica. Diversas discussões foram realizadas ao longo dos anos, envolvendo a comunidade acadêmica, representantes da sociedade civil e instituições parceiras, a fim de definir áreas prioritárias para a formação de profissionais.

No caso específico do *Campus* Jequié, a definição dos cursos partiu de estudos regionais e de um amplo processo de escuta qualificada. Esse processo contemplou a aplicação de formulários eletrônicos à população, bem como reuniões com setores representativos da região. Além disso, foram considerados a oferta já existente de cursos superiores no território, como aqueles promovidos pelo IFBA e pela UESB, de modo a evitar sobreposição e buscar complementaridade. Dessa análise, destacaram-se alguns pontos centrais:

- as licenciaturas e cursos da área da saúde já se encontram bem contemplados pela UESB;
- a região já possui cursos de engenharia ofertados pelo IFBA e por instituições privadas instaladas em Jequié.

A partir dessas constatações, delineou-se a proposta inicial de cursos do novo *campus*, orientada pelo modelo pedagógico-administrativo da UFSB, baseado na lógica dos Centros de Formação e na integração entre formação geral e específica.

Nesse contexto, o curso de Engenharia em Cibersegurança emergiu como uma demanda prioritária, amplamente apoiada pela comunidade consultada. Sua escolha refletiu a percepção da relevância crescente da área em um mundo cada vez mais digitalizado, no qual

conectividade, proteção de dados e resiliência cibernética são elementos centrais para o desenvolvimento econômico, social e tecnológico.

A formalização da implantação do curso foi resultado de debates acadêmicos e deliberações institucionais, nos quais a comunidade universitária, pautada pelas consultas regionais, definiu a prioridade da formação em cibersegurança. Dessa forma, a criação do curso em Jequié não apenas responde às exigências locais e regionais, mas também consolida a UFSB como um polo de inovação tecnológica, segurança digital e desenvolvimento científico no sudoeste da Bahia.

5.2 Justificativa de Oferta

A criação do curso de Engenharia em Cibersegurança na UFSB fundamenta-se em uma análise ampla das necessidades sociais, econômicas e tecnológicas, considerando tanto o contexto regional quanto o cenário nacional. Trata-se de uma resposta estratégica à crescente demanda por profissionais altamente qualificados em defesa digital, em um ambiente no qual ataques e riscos cibernéticos se consolidaram como ameaças críticas à soberania, à continuidade de negócios e à proteção de infraestruturas vitais da sociedade.

No Brasil e no mundo, a intensificação da digitalização e a rápida incorporação de tecnologias emergentes — como inteligência artificial, internet das coisas, computação em nuvem, 5G e blockchain — ampliaram de forma significativa a superfície de ataque, assim como a sofisticação das ameaças digitais. Casos de ransomware, invasões em cadeias de suprimentos, exploração de vulnerabilidades em dispositivos IoT, fraudes digitais e violações de privacidade evidenciam a urgência de formar engenheiros capazes de projetar, implementar e gerenciar soluções inovadoras de proteção e resiliência.

O déficit de profissionais especializados é expressivo. Relatórios nacionais e internacionais indicam que centenas de milhares de vagas permanecem abertas por falta de formação específica em cibersegurança. Nesse cenário, a oferta do curso pela UFSB surge como medida estratégica para reduzir essa lacuna de talentos e fortalecer a resiliência digital brasileira. Os engenheiros formados estarão aptos a atuar em diversos segmentos — desde indústrias e empresas de serviços até órgãos públicos — contribuindo de forma direta para a segurança digital e a inovação tecnológica.

Além disso, o curso dialoga com as vocações econômicas da região sudoeste da Bahia, como o agronegócio, o turismo e os serviços, setores cada vez mais dependentes de soluções

digitais seguras. A presença de um curso pioneiro em cibersegurança possibilita a formação de profissionais preparados para atender às demandas específicas desses segmentos, incentivando o empreendedorismo, a pesquisa aplicada e o desenvolvimento de soluções tecnológicas adaptadas ao contexto regional.

Outro aspecto relevante é o alinhamento da proposta com os compromissos de sustentabilidade e inclusão social. O curso busca formar engenheiros que dominem tanto os aspectos técnicos da defesa digital quanto os impactos sociais e éticos do uso das tecnologias, incentivando soluções responsáveis, que respeitem a privacidade, a transparência e a confiança digital. A proposta também visa reduzir desigualdades, ampliar a inclusão e fortalecer a soberania tecnológica do país.

Nesse sentido, a Engenharia em Cibersegurança da UFSB contribui diretamente para os Objetivos de Desenvolvimento Sustentável (ODS) da Agenda 2030 da ONU:

- **ODS 4 – Educação de Qualidade:** amplia o acesso a cursos tecnológicos avançados no ensino superior público, em uma região historicamente carente dessas formações, promovendo inclusão e redução de desigualdades.
- **ODS 8 – Trabalho Decente e Crescimento Econômico:** prepara jovens para um mercado em franca expansão, reduzindo o desemprego regional e incentivando empregos de alta qualificação.
- **ODS 9 – Indústria, Inovação e Infraestrutura:** qualifica profissionais para proteger infraestruturas críticas, estimular a inovação em setores estratégicos e apoiar a modernização digital de organizações públicas e privadas.
- **ODS 11 – Cidades e Comunidades Sustentáveis:** contribui para a segurança digital em cidades inteligentes e serviços públicos digitalizados, essenciais para o desenvolvimento urbano sustentável.
- **ODS 16 – Paz, Justiça e Instituições Eficazes:** fortalece instituições públicas e privadas contra crimes digitais, promovendo governança digital, proteção de dados e transparência.

Com essa iniciativa, a UFSB amplia sua capacidade formativa, consolida o sudoeste da Bahia como referência em formação em cibersegurança e projeta-se nacionalmente como protagonista no enfrentamento dos desafios da transformação digital.

6. POLÍTICAS INSTITUCIONAIS NO ÂMBITO DO CURSO

O Projeto Pedagógico Institucional (PPI) define as políticas gerais que orientam o desenvolvimento das ações acadêmicas da UFSB. O documento serve como guia estratégico para a criação de projetos e iniciativas de caráter sociocultural, sempre articulados às necessidades do contexto regional em que a universidade está inserida.

Nele, estão estabelecidos os caminhos a serem seguidos pela instituição para o cumprimento de sua missão e o alcance de seus objetivos de médio e longo prazo. O PPI explicita a missão e o perfil institucional da UFSB, além de apresentar orientações sobre as diretrizes pedagógicas, as atividades acadêmicas e a infraestrutura existente ou planejada para o período de vigência. Também contempla a programação da oferta de cursos, em suas diferentes modalidades, de forma a assegurar expansão e consolidação ao longo do tempo.

É importante destacar que todas as políticas institucionais adotadas nos cursos da UFSB estão alinhadas às diretrizes do PPI, reafirmando sua função como documento norteador da formação acadêmica e do desenvolvimento institucional.

6.1 Políticas de Acesso ao Curso e de Mobilidade Acadêmica

O Curso de Engenharia em Cibersegurança está alicerçado nas políticas de acesso ao Curso e de mobilidade acadêmica, constantes no PDI da UFSB, geridas pela Pró-Reitoria de Gestão Acadêmica (PROGEAC). Serão ofertadas anualmente 40 vagas para o Curso, presencialmente, no *Campus* Jequié, BA. Os processos seletivos para ingresso serão realizados por meio de editais de seleção gerenciados pela PROGEAC.

Para acessar o Curso, os/as estudantes poderão ingressar das seguintes formas: Entrada direta pelo SISU, Transferência interna, Transferência de outra IES, Admissão de portadores de diploma, seleção interna para cursos de segundo ciclo e ingresso por edital da Rede Anísio Teixeira de Colégios Universitários (Rede CUNI). Pela entrada direta, as vagas são ofertadas pelo Sistema de Seleção Unificada (SiSU), utilizando-se as notas obtidas pelo/a estudante no ENEM. As demais formas de ingresso são viabilizadas mediante editais específicos e regulamentação da Instituição.

Para participar do processo seletivo SiSU, o estudante deverá se inscrever no sítio do SiSU com o número de inscrição e senha do ENEM. O sistema do SiSU irá recuperar as notas do Enem da edição mais recente para o candidato concorrer às vagas disponíveis. Após a

divulgação dos candidatos aprovados, os mesmos devem comparecer para a matrícula presencial no *Campus* de lotação do Curso na UFSB.

O ingresso através da Rede Anísio Teixeira de Colégios Universitários (Rede CUNI) utiliza as notas das quatro edições anteriores do Enem, sendo a maior nota escolhida como nota classificatória no processo. Os Colégios Universitários (CUNI) visam contribuir para ampliar a inclusão social através da educação superior de estudantes que tenham cursado todo o ensino médio em escolas públicas da Região. São implantados em municípios com mais de 20.000 habitantes, estão organizados em rede (institucional e digital), que oferecem programas descentralizados e metapresenciais de educação superior. Os CUNIs funcionam em turno noturno e os Institutos de Humanidades, Artes e Ciências (IHAC) coordenam os colégios em sua área de abrangência, a partir das sedes estabelecidas em cada um dos *Campi* da UFSB.

A Inscrição Especial em Componentes Curriculares possibilita o ingresso do público interessado em cursar componentes com vagas não ocupadas pelos/as estudantes regularmente matriculados/as em seus respectivos processos. O/A estudante em Inscrição Especial fará jus à declaração comprobatória dos CC 's cursados, com a respectiva carga horária e nota obtida.

O preenchimento das vagas no Curso atende aos critérios estabelecidos para as diferentes modalidades de ingresso da Universidade, conforme resolução específica que dispõe sobre a política de ações afirmativas para os processos seletivos aos cursos de graduação da UFSB, com os seguintes tipos de cotas, a saber:

- I. Candidatos/as com renda familiar bruta per capita igual ou inferior a 1,5 salário mínimo que tenham cursado integralmente o ensino médio em escolas públicas.
- II. Candidatos/as autodeclarados/as negros/as (pretos/as e pardos/as) ou indígenas, com renda familiar bruta per capita igual ou inferior a 1,5 salário mínimo e que tenham cursado integralmente o ensino médio em escolas públicas.
- III. Candidatos/as que, independentemente da renda, tenham cursado integralmente o ensino médio em escolas públicas.
- IV. Candidatos/as autodeclarados/as negros/as (pretos/as e pardos/as) ou indígenas que, independentemente da renda tenham cursado integralmente o ensino médio em escolas públicas.

- V. Candidatos/as com deficiência, nos termos da legislação, que tenham renda familiar bruta per capita igual ou inferior a 1,5 salário mínimo e que tenham cursado integralmente o ensino médio em escolas públicas.
- VI. Candidatos/as com deficiência, nos termos da legislação, autodeclarados/as negros/as (pretos/as e pardos/as) ou indígenas, que tenham renda familiar bruta per capita igual ou inferior a 1,5 salário mínimo e que tenham cursado integralmente o ensino médio em escolas públicas.
- VII. Candidatos/as com deficiência, nos termos da legislação, que, independentemente da renda, tenham cursado integralmente o ensino médio em escolas públicas.
- VIII. Candidatos/as com deficiência, nos termos da legislação, autodeclarados/as negros/as (pretos/as e pardos/as) ou indígenas que, independentemente da renda, tenham cursado integralmente o ensino médio em escolas públicas.

O Programa de Mobilidade Acadêmica tem como objetivo possibilitar aos/às discentes regularmente matriculados/as em cursos de graduação nas Instituições Federais de Ensino Superior (IES) que participam do convênio ANDIFES, cursar componentes curriculares na UFSB, conforme regulamentação que consta no convênio assinado pela ANDIFES e Colégio de Pró-Reitores de Graduação (COGRAD) com o intuito de fomentar a cooperação técnico-científica.

O/A discente poderá realizar mobilidade na UFSB por até dois semestres letivos, (totalizando 1 ano de intercâmbio acadêmico), de acordo com os critérios estabelecidos em cada convênio e concordância da instituição de origem e de destino. Estudantes da UFSB interessados/as em participar do Programa de Mobilidade Acadêmica em outras IES deverão consultar o Coordenador do seu curso para elaborar o plano de estudos seguindo o modelo proposto pela instituição pleiteada, observando as ementas dos Componentes Curriculares que serão cursados em mobilidade para fins de aproveitamento quando do retorno.

6.2 Políticas de Ensino

As diretrizes educacionais aplicáveis ao Curso de Bacharelado em Engenharia em Cibersegurança são as mesmas estabelecidas pela UFSB, as quais são gerenciadas pela Câmara de Graduação da Pró-Reitoria de Gestão Acadêmica.

Na UFSB, o/a estudante pode cursar sua graduação em dois ciclos, sendo que é conferido um diploma após o cumprimento dos requisitos para cada curso. Ao concluir um

curso de primeiro ciclo, o/a estudante poderá optar, de acordo com o seu percurso e o cumprimento das exigências para ingresso, por realizar um curso de segundo ciclo ofertado nos Centros de Formação (CF), dentre eles, o Curso de Engenharia em Cibersegurança. No primeiro ciclo, são ofertados cursos interdisciplinares, os Bacharelados (BI) e Licenciaturas (LI), que darão uma formação generalista, polivalente para atuar em uma grande área de formação. Dentre os Cursos de 1º Ciclo, o Bacharelado Interdisciplinar em Ciências (BiC) proporciona uma formação abrangente, cuja estrutura curricular contempla uma base sólida em disciplinas fundamentais, alinhadas em grande parte às exigências do Curso de Engenharia em Cibersegurança, favorecendo uma transição acadêmica consistente e bem fundamentada. A partir da conclusão do BIC, o/a estudante que ingressar em um curso de 2º Ciclo poderá prosseguir com seus estudos para obtenção de uma graduação profissional voltada para atuação em campos ou áreas de formação mais específicas, como é o caso do Curso de Engenharia em Cibersegurança, que contempla conteúdos voltados à proteção de sistemas digitais e infraestruturas críticas, incluindo áreas como Engenharia de Software Segura, Redes e Sistemas Computacionais, Criptografia e Segurança de Dados, Inteligência Artificial aplicada à defesa cibernética, Sistemas Eletrônicos, Computação em Nuvem e Gerenciamento de Riscos e Incidentes de Segurança.

O Programa de Monitoria Acadêmica da UFSB é uma prática pedagógica exercida por estudantes de graduação em componente curricular, supervisionada por docente responsável pela submissão de projeto de monitoria, cujo planejamento deve almejar os objetivos de formação acadêmica do/a discente que se habilita ao papel de monitor/a, do/a docente ofertante da monitoria e dos/as discentes matriculados/as no componente curricular ao qual se vincula. A monitoria tem por objetivos possibilitar aos/as estudantes da graduação experiências relacionadas à docência, assim como ampliar os conhecimentos relacionados ao componente curricular e estimular a integração entre o corpo docente e discente.

O Programa de Acompanhamento Acadêmico (PROA) é uma política institucional de permanência estudantil da UFSB que tem como objetivo instruir as trajetórias acadêmicas e proporcionar aos/as estudantes de graduação um maior conhecimento do modelo institucional da UFSB e das possibilidades de construção de percurso formativo. São objetivos específicos de destaque do PROA: a viabilização da filiação acadêmica dos/as ingressantes, com o acolhimento no seu contexto universitário; a contribuição para a realização profissional e acadêmica dos/as discentes, com orientações sobre o currículo do Curso e os percursos

formativos; e a redução da retenção, da evasão e do abandono. O PROA é executado de dois modos, um caracterizado pela orientação coletiva por meio de cursos, oficinas, palestras, rodas de conversa e workshops, realizados periodicamente, e o outro configurado como uma orientação individualizada por meio de relação direta entre orientador/a e estudante.

O Programa de Tutorias consiste em um conjunto de ações que visam dar apoio acadêmico-pedagógico em áreas de conhecimento para aprimorar o desempenho de estudantes ingressantes ou veteranos/as que apresentam dificuldades de aprendizagem. A implementação desse programa visa enfatizar a importância da valorização de práticas pedagógicas que estimulam a solidariedade e a coletividade acadêmica, tais como as Estratégias de Aprendizagem Compartilhada (EAC), as Equipes de Aprendizagem Ativa (EAA) e a aprendizagem interpares (*peer-instruction*). Cabe destacar que tais estratégias estão previstas no Plano Orientador da UFSB e foram reforçadas como Políticas de Ensino no PDI (2020-2024). O programa em questão se propõe a oferecer suporte aos/às estudantes em sua transição entre níveis de ensino, visando promover o nivelamento de conhecimentos, orientar a organização da rotina de estudos e incentivar a criação de grupos de estudo. Além disso, busca colaborar para a redução dos índices de reprovação em CCs e, consequentemente, reduzir a evasão, o que pode contribuir para o aumento da permanência de estudantes na universidade e, por consequência, para o aumento da taxa de formação.

Por fim, ainda segundo o PDI 2020-2024, o Programa de Reestruturação e Consolidação dos Cursos de Primeiro e Segundo Ciclo, o Programa de Qualificação das Atividades Práticas e de Estágio e o Programa Educação em Rede são também integrantes das políticas de ensino da UFSB que integram o Curso de Bacharelado em Engenharia em Cibersegurança em suas ações ou que tem as suas ações elegíveis para este.

6.3 Políticas de Pesquisa

As diretrizes de pesquisa no contexto do Curso de Bacharelado em Engenharia em Cibersegurança seguem as mesmas políticas estabelecidas pela Universidade Federal do Sul da Bahia (UFSB), as quais são gerenciadas pela Pró-Reitoria de Pesquisa e Pós-Graduação (PROPPG).

O Programa de Iniciação à Pesquisa Criação e Inovação (PIPCI) tem como objetivo primordial incentivar o desenvolvimento de atividades de pesquisa, criação e inovação pelos/as discentes da UFSB, oportunizando-lhes a aquisição de conhecimentos teóricos e

práticos, o desenvolvimento de habilidades e competências, além de contribuir para a produção de conhecimento científico e tecnológico relevante para a sociedade.

A seleção dos/as estudantes para o programa ocorre anualmente através de editais públicos, os quais contemplam a concessão de bolsas de pesquisa. A execução dos projetos de pesquisa é conduzida sob a orientação de um/a docente-pesquisador/a da UFSB e possibilita a participação de estudantes em eventos acadêmicos e científicos, a exemplo do Congresso de Iniciação à Pesquisa, Criação e Inovação (CIPCI) da UFSB e da Semana Nacional de Ciência e Tecnologia, bem como a publicação de artigos em revistas especializadas. O PIPCI ainda promove a interação entre a universidade e a sociedade, estimulando a elaboração de projetos que objetivem solucionar questões locais, regionais e nacionais, o que contribui para o desenvolvimento econômico, social e cultural da região.

A região Sul da Bahia oferece um campo vasto de pesquisas enquadradas nos eixos temáticos da Engenharia em Cibersegurança, pois há grande potencial para o estudo e o desenvolvimento de soluções voltadas à proteção de sistemas digitais, infraestruturas críticas e serviços essenciais. A diversidade socioeconômica, geográfica e cultural da região cria um ambiente propício para pesquisas em defesa digital e inovação tecnológica, com foco na criação de estratégias de segurança cibernética aplicadas à agricultura, indústria, serviços e gestão pública.

Além disso, setores como saúde, educação e logística apresentam crescente demanda por soluções digitais confiáveis, que garantam privacidade, integridade e disponibilidade de informações. Nesse contexto, a Engenharia em Cibersegurança pode atuar no desenvolvimento de plataformas digitais seguras, sistemas de gestão com camadas de proteção avançada, redes de sensores resilientes e soluções de inteligência artificial aplicadas à defesa cibernética, atendendo aos desafios regionais com inovação e responsabilidade.

A UFSB adota uma política de pesquisa que visa fortalecer a integração entre os diferentes níveis de ensino e promover a inovação tecnológica, incentivando os estudantes do curso de Engenharia em Cibersegurança a participarem ativamente de projetos de pesquisa e extensão. Essa abordagem reforça o compromisso da UFSB em preparar profissionais altamente qualificados, conectados com as demandas regionais e globais, e capazes de contribuir para o avanço tecnológico e o desenvolvimento sustentável da região sul da Bahia.

6.4 Políticas de Extensão

As políticas de extensão no âmbito do Curso de Bacharelado em Engenharia em Cibersegurança são regidas pelas mesmas diretrizes aplicáveis à UFSB. Essas políticas são geridas pela Pró-Reitoria de Extensão e Cultura (PROEX).

A PROEX tem como objetivo fomentar e incentivar atividades de extensão universitária que promovam práticas emancipatórias com forte impacto social, em consonância com a renovação e revalorização da extensão universitária no âmbito brasileiro. O órgão disponibiliza cadastro em fluxo contínuo para programas, projetos, eventos, cursos e produtos, além de lançar editais para bolsas e apoio a atividades de maneira pontual. A PROEX tem como base práticas que ultrapassam o enfoque unicamente centrado na difusão do conhecimento acadêmico e busca a inserção da universidade na realidade social e política brasileira por meio de projetos que valorizem práticas dialógicas, a formação discente e o tripé ensino-pesquisa-extensão.

Com o objetivo de assegurar a consolidação de um projeto universitário que contemple a justiça e os direitos sociais, a PROEX é encarregada de elaborar, administrar, propor, coordenar, implementar, monitorar, avaliar e atualizar as políticas, diretrizes e normas de extensão e cultura, com ações voltadas para uma relação horizontal com as comunidades não universitárias dos territórios Sul e Extremo Sul da Bahia, enfatizando as comunidades tradicionais e os povos originários, as populações em situação de vulnerabilidade social, econômica, cultural e ambiental, as comunidades de periferias urbanas e outros grupos historicamente excluídos.

Um curso da área de cibersegurança tem, por natureza, uma tendência forte de envolvimento e desenvolvimento em ações de extensão, antes percebidas isoladamente pela realização destas por docentes que possuem um perfil voltado à extensão, a partir de agora inseridas no currículo obrigatório da formação dos/as estudantes. A consolidação de práticas extensionistas é essencial para estabelecer um diálogo efetivo entre universidade e sociedade, sobretudo em regiões que apresentam indicadores socioeconômicos desfavoráveis e que demandam soluções para superar tais desafios, como é o caso da região Sul Baiana. Nesse contexto, ações de extensão são fundamentais no intuito de contribuir para o desenvolvimento sustentável da região, por meio da realização de projetos que busquem soluções inovadoras e eficientes para os problemas existentes. Além disso, a participação de estudantes em ações de extensão contribui para a formação de profissionais mais engajados e conscientes do seu papel

na sociedade e capazes de aplicar seus conhecimentos de forma mais prática e efetiva.

As políticas extensionistas do Curso atendem ao Plano Nacional da Educação 2014/2024, aprovado pela Lei nº 13.005/2014, e regulamentada pela Resolução CNE/CES/MEC nº 07/2018, que assegura no mínimo, 10% do total de créditos curriculares da graduação em programas e projetos de extensão universitária. Vale ressaltar que são atendidas os regimentos internos da instituição no âmbito da extensão, a saber, a resolução que dispõe sobre a curricularização das Atividades de Extensão nos cursos de graduação, e a resolução, que dispõe sobre as normas que regulamentam as Atividades de Extensão.

De modo específico o Curso de Engenharia em Cibersegurança conta com 380 horas destinadas à prática de ações de extensão. Neste sentido, entende-se por extensão qualquer atividade que envolva o público externo da UFSB e que o/a estudante desempenhe atuação protagonista sendo este o agente da atividade com participação em etapas significativas do processo, e não apenas ouvinte ou cursista. Vale ressaltar que este processo permite ao estudante reconhecer seu papel como agente de garantia de direitos e deveres e de transformação social.

6.5 Políticas de Atendimento ao/à Estudante

No âmbito do Curso de Bacharelado em Engenharia em Cibersegurança, as políticas de atendimento aos estudantes são gerenciadas pela Pró-Reitoria de Ações Afirmativas (PROAF) e são as mesmas políticas gerais adotadas pela UFSB. Dentre as políticas de atendimento aos discentes, destaca-se o Programa de Apoio à Permanência, que oferece bolsas e auxílios nas seguintes modalidades:

- **Bolsa de Apoio à Permanência (BAP):** destinada a prover as condições para a manutenção dos/as estudantes em situação de vulnerabilidade socioeconômica. Possui um duplo caráter: caráter social, pois se utiliza de critérios socioeconômicos para selecionar bolsistas e contribuir com a permanência destas/es na UFSB, e caráter acadêmico, pois possibilita às/aos estudantes desenvolver atividades de pesquisa, extensão, ensino, gestão, sustentabilidade, orientados/as por docentes ou técnico-administrativos/as da UFSB.
- **Auxílio Instalação:** consiste em subvenção financeira com periodicidade de desembolso mensal e por tempo determinado, em que o/a estudante recém-ingresso/a na UFSB poderá obter um auxílio, mediante a comprovação de gastos com moradia,

enquanto aguarda a realização do processo regular de seleção para os Auxílios Alimentação, Transporte e Moradia. O Auxílio Instalação é destinado aos/às estudantes ingressantes na modalidade de reserva de vagas (estudantes com deficiência ou autodeclarados/as pretos/as, pardos/as ou indígenas), com renda familiar bruta per capita igual ou inferior a 1,5 salário mínimo e que tenham cursado integralmente o ensino médio em escolas públicas.

- **Auxílio Eventos:** consiste em apoio à realização e à participação de estudantes ou de entidades estudantis reconhecidas pela UFSB em eventos culturais, políticos e esportivos nacionais ou internacionais, em valores pré-fixados pela Instituição, na forma de cessão de transporte, alimentação, hospedagem, infraestrutura, pagamento de inscrição em eventos e/ou material de divulgação, sendo que cada estudante pode receber o auxílio até duas vezes por ano.
- **Auxílio Emergencial:** consiste em subvenção financeira, com periodicidade de desembolso mensal e por tempo determinado, destinada a casos excepcionais de vulnerabilidade e risco social avaliados pela equipe multiprofissional da PROAF. O auxílio emergencial possui caráter diferenciado em relação aos demais auxílios, devendo ser utilizado em situações de extrema vulnerabilidade ou risco à permanência de estudantes da UFSB que não sejam atendidos no Programa de Apoio à Permanência.
- **Auxílio Creche:** destinado à/ao estudante que tenha filho/a em idade pré-escolar (zero a cinco anos e onze meses) e necessite de apoio de instituições ou terceiros para desempenhar suas atividades acadêmicas para subsidiar despesas com creche ou outras relacionadas aos cuidados com a guarda e a manutenção infantil.
- **Auxílio Alimentação:** com valores pagos por dia letivo conforme a faixa de renda familiar per capita do/a estudante, destina-se à complementação de despesas com alimentação, aportando recursos financeiros complementares para a melhoria das condições de alimentação, com prioridade àqueles/as em situação de maior vulnerabilidade socioeconômica.
- **Auxílio Transporte:** dividido em quatro modalidades com valores diferenciados conforme a distância entre cidades até às sedes ou à Rede CUNI, tem por objetivo subsidiar as despesas com transporte de estudantes no deslocamento de casa ou do trabalho para desempenhar suas atividades acadêmicas.

- **Auxílio Moradia:** consiste em subvenção financeira, pré-fixada pela Universidade, destinando-se ao apoio ao/a estudante para que possa se alojar em condições satisfatórias nos municípios sede da UFSB, individual ou coletivamente, com o intuito de auxiliar na cobertura de despesas com locação e eventuais gastos relacionados à moradia, prioritariamente as de uso coletivo. A UFSB ainda não dispõe de moradias universitárias, sendo que o auxílio permite que o/a estudante tenha autonomia para escolher com quem dividir as despesas de habitação. Destaca-se que este auxílio também é pago no período de férias.
- **Bolsa Monitoria Inclusiva:** tem como objetivo auxiliar na permanência, participação e aprendizagem de estudante com deficiência, transtornos globais do desenvolvimento, altas habilidades e superdotação na UFSB. As principais ações desenvolvidas pelos/as monitores/as são: acompanhar o/a estudante com deficiência presencialmente nos espaços acadêmicos, além de auxiliá-los/as na realização de atividades de rotina identificadas como barreiras pedagógicas, arquitetônicas e atitudinais e adaptar o material acadêmico utilizado.

Em 2018, foi implementado o Programa TRANSforme, que reúne ações voltadas à permanência de pessoas trans na UFSB, dentre elas a adoção do uso do nome social nos documentos oficiais e a política que determina o uso dos banheiros por identidade de gênero. Os objetivos do Programa de Inclusão e Ações Afirmativas são:

- Consolidar o modelo de inclusão de estudantes egressos/as de escola pública, sobretudo jovens negros/as e indígenas de acordo com o estabelecido na Lei de Cotas;
- Qualificar os regulamentos internos do programa de ações afirmativas e os programas de elucidações sobre o modelo de ingresso e os mecanismos de controle social da política de cotas; e
- Ampliar o interesse institucional em desenvolver ações específicas voltadas à promoção da diversidade étnica e cultural, por meio de ações de diálogo interacadêmico, de divulgação institucional e de permanência e fortalecimento de identidades de grupos com histórico de exclusão e/ou silenciamento no espaço universitário.

Também no PDI, especifica-se o Programa de Inclusão e Ações Afirmativas, que visa à ampliação e democratização das condições de acesso e permanência do/a estudante

comprovadamente em situação de vulnerabilidade socioeconômica. E, ainda, as políticas de acessibilidade e inclusão da Universidade, como o Plano de promoção da acessibilidade e atendimento diferenciado a pessoas com deficiência, que atua com o objetivo de executar ações, tais como aquisição de tecnologias assistivas/execução com o intuito de garantir o acesso e a permanência dos estudantes com deficiência.

6.6 Políticas de Internacionalização

No âmbito do Curso de Bacharelado em Engenharia em Cibersegurança, as políticas de internacionalização são gerenciadas pela Assessoria de Relações Internacionais (ARI) e são as mesmas políticas gerais adotadas pela UFSB. A ARI é um órgão suplementar da UFSB vinculado à Reitoria e que tem por objetivo planejar, coordenar, implementar, promover e acompanhar a política de internacionalização, nos âmbitos do ensino, pesquisa, inovação, cultura, extensão e gestão universitária, em especial no plano internacional, junto a outras instituições universitárias, órgãos públicos, entidades privadas e sociedade em geral. Além disso, a ARI tem o objetivo de fomentar a internacionalização contínua das atividades da UFSB por meio da definição e realização de metas e objetivos.

No âmbito institucional da UFSB, é prevista durante a Formação Geral a oferta de Componentes Curriculares voltados para o ensino de línguas estrangeiras, os quais são implementados em todos os cursos de graduação. Ademais, no que tange às políticas institucionais, em resolução específica, a UFSB estabelece a sua Política de Internacionalização, além de instituir o Comitê de Internacionalização. A referida política visa ampliar a atuação da universidade no cenário internacional, por meio do estímulo à mobilidade acadêmica e científica, intercâmbio de conhecimentos e cooperação com instituições estrangeiras. Por outro lado, a criação do Comitê de Internacionalização tem como objetivo principal assessorar as ações relacionadas à internacionalização, promovendo a articulação entre as Unidades Acadêmicas e fomentando a construção de estratégias e parcerias para a inserção da UFSB no contexto internacional.

Entre as iniciativas promovidas pela ARI, destaca-se a elaboração de editais para intercâmbio, seja de forma presencial ou virtual, envolvendo docentes, discentes e técnicos-administrativos. É importante destacar que este tipo de mobilidade internacional deve seguir as normas estabelecidas nos editais das instituições promotoras. No caso, os/as estudantes que, tendo sua permanência no Brasil devidamente legalizada, poderão ingressar nos cursos da UFSB pelos processos de seleção regulares, por programas ou acordos de cooperação dos

quais a UFSB seja signatária ou por programas específicos para refugiados.

Outro tipo de atividade conduzida pela ARI refere-se à elaboração de parcerias internacionais de cooperação técnica e científica com outras instituições, por meio da celebração de convênios e acordos, devidamente respaldados pela legislação brasileira. Essas iniciativas poderão ser utilizadas para o financiamento de projetos e programas, incluindo aqueles voltados para áreas acadêmicas, científicas, técnicas, de mobilidade ou outras, tendo estabelecidas as normas e as responsabilidades das partes envolvidas.

Em resumo, a ARI desempenha um papel fundamental na promoção de uma política de internacionalização da UFSB, tendo como objetivo fomentar a integração e o intercâmbio com outras instituições de ensino e pesquisa em nível global. Portanto, as políticas de internacionalização implantadas até o momento, são uma forma de expandir as fronteiras acadêmicas e científicas da instituição e, assim, contribuem para o desenvolvimento regional.

7. OBJETIVOS DO CURSO

7.1 Objetivo Geral

O curso de Engenharia em Cibersegurança da UFSB tem como objetivo geral formar profissionais altamente qualificados para conceber, projetar, implementar e gerenciar soluções de defesa digital, capazes de proteger dados, sistemas e infraestruturas críticas contra ameaças cibernéticas. Esses profissionais estarão preparados para atuar de forma ética, inovadora e responsável, promovendo a resiliência tecnológica em diferentes setores da sociedade e contribuindo para a soberania digital do país. O curso busca, ainda, estimular a pesquisa e o desenvolvimento de novas tecnologias, respondendo aos desafios locais, regionais e globais, e contribuindo para a melhoria da qualidade de vida da população por meio da promoção da confiança e da segurança no uso das tecnologias digitais.

7.2 Objetivos Específicos

- **Projetar Soluções em Defesa Digital:** desenvolver tecnologias e práticas inovadoras para prevenção, detecção e resposta a incidentes cibernéticos, utilizando metodologias atuais e adequadas às necessidades do setor público e privado.
- **Proteger Dados e Infraestruturas Críticas:** atuar na preservação da confidencialidade, integridade e disponibilidade de informações e sistemas, assegurando a resiliência de serviços essenciais em diferentes contextos organizacionais.
- **Incorporar Tecnologias Emergentes com Segurança:** aplicar e proteger inovações tecnológicas como inteligência artificial, blockchain, computação em nuvem e internet das coisas (IoT), garantindo sua adoção responsável frente a riscos digitais.
- **Contribuir para a Governança e a Soberania Digital:** elaborar políticas, normas e estratégias de segurança cibernética que assegurem conformidade regulatória e apoiem a maturidade organizacional, com foco em responsabilidade social e fortalecimento institucional.
- **Atuar na Análise e Gestão de Riscos Cibernéticos:** empregar ferramentas de monitoramento, análise de dados e inteligência artificial para identificar vulnerabilidades, prever ataques e propor medidas de mitigação proativas.

- **Promover a Sustentabilidade e a Inclusão Digital:** fomentar soluções tecnológicas que reduzam impactos ambientais, respeitem princípios éticos e ampliem o acesso seguro às tecnologias digitais para comunidades diversas.
- **Integrar Formação Técnica e Humanista:** preparar engenheiros capazes de articular competências técnicas com valores éticos, liderança e trabalho em equipe, colaborando em projetos interdisciplinares voltados à inovação e ao desenvolvimento sustentável.
- **Responder a Demandas Locais, Regionais e Globais:** contribuir com soluções que atendam aos desafios socioeconômicos do Sul da Bahia e, ao mesmo tempo, possibilitar a inserção dos egressos em um mercado global, em cooperação com redes nacionais e internacionais de cibersegurança.

8. PERFIL DO/A EGRESSO/A

O egresso do Bacharelado em Engenharia Cibernética (BECiber) da UFSB, será um profissional estratégico, inovador e orientado à prática, preparado para enfrentar um cenário global de intensas transformações tecnológicas e ameaças digitais em constante evolução. Reconhecido pela atuação *hands-on*, esse profissional integrará conhecimento técnico avançado a competências interpessoais e visão estratégica, consolidando-se como protagonista na área da Engenharia Cibernética.

Do ponto de vista das Competências Técnicas e Estratégicas, o egresso será capaz de:

- Projetar, implementar e gerenciar sistemas de segurança cibernética, alinhados às melhores práticas internacionais e às tecnologias emergentes.
- Desenvolver soluções inovadoras para a proteção de dados, redes e infraestruturas críticas, aplicando metodologias ágeis e ferramentas de ponta.
- Identificar vulnerabilidades em sistemas complexos e propor estratégias eficazes de mitigação, com foco em resiliência e continuidade de negócios.
- Integrar conhecimentos de segurança digital a áreas como inteligência artificial, blockchain e internet das coisas (IoT), enfrentando desafios interdisciplinares.

Do ponto de vista das Habilidades Interpessoais e de Liderança, o egresso será um profissional colaborativo e adaptável, capaz de:

- Atuar em equipes multidisciplinares, promovendo a integração entre especialistas técnicos, gestores e demais atores estratégicos.
- Comunicar ideias complexas de forma clara e acessível, dialogando com diferentes públicos, de equipes técnicas a tomadores de decisão.
- Exercitar empatia, escuta ativa e negociação em ambientes corporativos, acadêmicos e de inovação.

Do ponto de vista da Resolução de Problemas e Proatividade, com uma abordagem orientada à prática, o egresso será um solucionador de problemas, apto a:

- Responder com rapidez a incidentes cibernéticos, aplicando soluções criativas e eficazes para mitigar danos e restabelecer a confiança digital.
- Antecipar tendências e ameaças emergentes, propondo medidas preventivas que assegurem a integridade das operações organizacionais.
- Liderar projetos inovadores voltados a desafios locais, regionais e globais, criando soluções práticas e sustentáveis.

Do ponto de vista do Impacto e Sustentabilidade, o egresso do BECiber estará comprometido com o uso ético e responsável da tecnologia, contribuindo para:

- A promoção da sustentabilidade digital, reduzindo impactos ambientais das soluções tecnológicas.
- O desenvolvimento de sistemas seguros que respeitem a privacidade e os direitos dos usuários, em conformidade com padrões globais de segurança e governança digital.

8.1 Campos de Atuação Profissional

O/A egresso/a do Bacharelado em Engenharia Cibernética da UFSB terá um campo de atuação amplo e estratégico, voltado para setores que demandam soluções em segurança digital, inovação tecnológica e proteção de infraestruturas críticas. Sua formação técnico-científica possibilitará atuar em diferentes contextos profissionais, em consonância com as competências definidas pelas Diretrizes Curriculares Nacionais para os cursos de Engenharia (Resolução CNE/CES nº 2/2019) e pelas atribuições estabelecidas pelo CONFEA (Resolução nº 1.073/2016).

Entre os principais campos de atuação, destacam-se:

- **Agências reguladoras e órgãos governamentais:** atuação em instituições federais, estaduais e municipais responsáveis por regular, fiscalizar e implementar políticas públicas relacionadas à segurança da informação, telecomunicações, defesa cibernética e proteção de dados.
- **Empresas de tecnologia e desenvolvimento de software:** criação de soluções digitais, plataformas seguras e sistemas críticos em áreas como saúde, transporte, logística, educação e finanças.
- **Consultorias e serviços técnicos especializados:** apoio estratégico em segurança digital, gestão de riscos, conformidade regulatória e implementação de soluções de proteção cibernética em organizações públicas e privadas.
- **Centros de pesquisa científica e tecnológica:** desenvolvimento de inovações em cibersegurança, inteligência artificial aplicada à proteção de sistemas, IoT segura, criptografia avançada e defesa cibernética.

- **Indústrias e organizações com uso intensivo de tecnologia:** proteção de ambientes de automação industrial, sistemas embarcados, redes corporativas, infraestrutura de nuvem e dispositivos conectados.
- **Instituições financeiras, de saúde, educação e gestão pública:** implementação de políticas e sistemas de segurança digital voltados para a proteção de dados sensíveis, a prevenção de fraudes e a garantia da continuidade de serviços essenciais.
- **Startups de base tecnológica e inovação:** desenvolvimento de soluções disruptivas em cibersegurança, produtos digitais inovadores e tecnologias aplicadas a mercados emergentes.
- **Universidades e centros de ensino e pesquisa:** docência, formação de profissionais, além da pesquisa e desenvolvimento de metodologias e tecnologias voltadas à proteção digital.
- **Empreendedorismo e atuação autônoma:** criação de empresas próprias ou prestação de serviços como consultor/a em cibersegurança, auditoria de sistemas, desenvolvimento de softwares seguros e soluções inovadoras.

A formação em Engenharia Cibernética capacita os/as egressos/as não apenas para o exercício profissional, mas também para atuarem como agentes de transformação social, comprometidos com a inovação, a sustentabilidade e a ética, pilares essenciais para o fortalecimento da soberania digital e para o enfrentamento dos desafios da sociedade contemporânea.

9. PROPOSTA PEDAGÓGICA

A proposta pedagógica do Curso de Bacharelado em Engenharia Cibernética foi elaborada em conformidade com as Diretrizes Curriculares Nacionais (DCNs) para os cursos de Engenharia, estabelecidas pelo Conselho Nacional de Educação, e está plenamente alinhada ao modelo pedagógico da UFSB.

Nesse contexto, o curso prioriza o desenvolvimento da autonomia discente, a capacidade de resolver problemas de forma dinâmica e complexa, o trabalho em equipes multidisciplinares, bem como valores fundamentais como solidariedade, liderança e espírito empreendedor.

Com foco na inovação tecnológica e na vanguarda acadêmica, a formação estimula o uso de metodologias ativas, em que o/a estudante assume papel de protagonista do próprio aprendizado. Essas metodologias são planejadas para integrar conteúdos, competências e habilidades exigidas pelo mercado de trabalho contemporâneo, fortalecendo a inserção dos egressos em diferentes setores estratégicos.

Dessa forma, as atividades de ensino do curso deverão adotar práticas que favoreçam a participação ativa dos/das estudantes, sempre de acordo com os objetivos pedagógicos estabelecidos. Para isso, serão empregados os instrumentos pedagógicos prioritários do modelo institucional da UFSB, detalhados a seguir:

- **Equipes de Aprendizagem Ativa** – grupos formados por estudantes de diferentes ciclos de formação e períodos de ingresso, criados para o desenvolvimento das atividades didáticas. Essas equipes são acompanhadas por pós-graduandos/as, no âmbito dos estágios docentes, e supervisionadas por docentes da universidade.
- **Estratégia de Aprendizagem Compartilhada** – consiste na divisão das responsabilidades pedagógicas entre pares. Nesse modelo, estudantes mais avançados no curso assumem o papel de tutores/as (coeducadores/as) para apoiar os/as colegas em etapas iniciais da formação, fortalecendo a colaboração e a troca de saberes.
- **Espaços de Diversidade** – ambientes de integração entre estudantes de diferentes cursos, períodos e ciclos formativos. Seu objetivo é promover a resolução de problemas acadêmicos de caráter interdisciplinar e multidisciplinar, em atividades realizadas tanto dentro quanto fora da universidade.
- **Aprendizagem Baseada em Problemas Concretos** – abordagem que integra o PBL (*Problem-Based Learning*) clássico com o estudo de casos reais, estimulando maior

interação entre estudantes, docentes supervisores/as, monitores/as de pós-graduação e tutores/as. Essa estratégia contribui para o desenvolvimento de competências ligadas ao trabalho colaborativo e à resolução prática de desafios.

- **Competência Socialmente Referenciada** – os problemas propostos nas atividades de aprendizagem são extraídos da realidade social, ampliando o diálogo com a comunidade universitária e com a sociedade em geral. Dessa forma, os/as estudantes desenvolvem competências voltadas para a aplicação prática do conhecimento, com impacto social direto.
- **Articulação Interciclos** – a formação de equipes com estudantes de graduação e pós-graduação possibilita a integração entre diferentes níveis de ensino. Combinada às Estratégias de Aprendizagem Compartilhada e às práticas baseadas em problemas reais, essa articulação potencializa a troca de experiências e o aprofundamento acadêmico.
- **Articulação de Diferentes Ambientes de Aprendizagem** – envolve a utilização de múltiplos espaços de ensino-aprendizagem: salas de aula e laboratórios da universidade, ambientes externos para aulas práticas e visitas técnicas, além de plataformas virtuais e recursos digitais de apoio ao ensino.

O Bacharelado em Engenharia Cibernética (BECiber) adotará um conjunto robusto de metodologias ativas e instrumentos pedagógicos inovadores, em consonância com as Diretrizes Curriculares Nacionais para Engenharia e com o modelo pedagógico institucional. O curso priorizará a autonomia discente, a resolução de problemas complexos, o trabalho em equipe e o espírito empreendedor, alinhando conteúdos, habilidades e competências às exigências contemporâneas da transformação digital.

Um princípio estruturante da concepção do curso será a indissociabilidade entre ensino, pesquisa e extensão. Essa integração ocorrerá não apenas em sala de aula, mas também em atividades extraclasse, nas quais a prática, a investigação e a descoberta farão parte do processo formativo. O BECiber integrará docentes, discentes e técnicos em projetos extracurriculares e contemplará Componentes Curriculares (CCs) com caráter interdisciplinar, reforçando a integração ensino-pesquisa-extensão e conectando o aprendizado às demandas sociais.

As atividades práticas poderão acontecer em laboratórios e ambientes virtuais, somadas a visitas técnicas, aproximando os/as estudantes dos desafios concretos da área

cibernética. Essas práticas abrangerão desde fundamentos (matemática, física e bases de computação) até conteúdos profissionalizantes (segurança da informação, redes, IA, automação e engenharia de software). Além disso, estudos de caso e simulações explorarão cenários complexos — como violações em sistemas ciberfísicos e análises forenses — permitindo exercitar a tomada de decisão sob pressão e desenvolver competências técnicas e estratégicas em situações realistas.

O curso poderá contar com Laboratórios Avançados de Cibersegurança e Ciberfísica, equipados com simuladores de ataques, ferramentas de análise de tráfego e plataformas de testes de resiliência. Nesses espaços, os/as estudantes participarão de hackathons, competições de captura de bandeira (CTFs) e práticas integradas de defesa e ataque, inspiradas em centros de inovação internacionais. Essas experiências oferecerão vivências imersivas, alinhadas às práticas do mercado.

Para favorecer o engajamento, a proposta pedagógica incluirá gamificação, incorporando desafios, rankings e jogos de estratégia digital que reforçarão conceitos teóricos de forma lúdica. Será adotada ainda a metodologia da sala de aula invertida, estruturada em três momentos: pré-aula, em que o estudante terá contato inicial com o conteúdo por meio de vídeos, leituras e exercícios; aula, dedicada ao feedback, às discussões e ao aprofundamento; e pós-aula, voltada ao reforço e à preparação para os conteúdos seguintes.

A Aprendizagem Baseada em Problemas (ABP) será utilizada para propor desafios socialmente referenciados, conectando a formação às necessidades da comunidade regional e nacional. Em complemento, os jogos de guerra cibernética (*cyber war games*) serão integrados às atividades, permitindo que os/as estudantes assumam papéis de atacantes, defensores e analistas, ampliando a compreensão sobre ameaças e estratégias de defesa.

A proposta também valorizará a colaboração interdisciplinar e a aprendizagem por pares, com a formação de grupos interciclos, reunindo graduação e pós-graduação. Essa prática estimulará a troca de conhecimentos e o desenvolvimento de competências interpessoais. Projetos de extensão universitária realizados em parceria com empresas, órgãos governamentais e comunidades locais possibilitarão a aplicação prática dos conhecimentos, como em auditorias de segurança, implantação de soluções digitais e capacitações comunitárias.

O curso incentivará ainda convênios e intercâmbios institucionais, inclusive em nível internacional, garantindo aos/às estudantes experiências acadêmicas globais e oportunidades de construir redes profissionais em centros de excelência em segurança cibernética.

Entre as ações pedagógicas previstas, destacam-se:

- induzir a inter-relação entre conteúdos dos CCs básicos e profissionalizantes;
- promover a integração entre teoria e prática por meio de laboratórios, projetos de pesquisa e extensão;
- estimular a participação em monitorias, bolsas de iniciação científica, tecnológica e de extensão;
- realizar visitas técnicas planejadas para integrar múltiplos CCs, favorecendo a experimentação de processos em diferentes escalas.

A flexibilidade curricular será um princípio orientador, permitindo que o/a estudante construa sua trajetória de forma ativa e responsável, ajustando-a às suas necessidades e interesses. Essa flexibilidade assegurará a integração entre teoria e prática, além de consolidar o protagonismo discente no processo formativo.

As tecnologias de informação e comunicação terão papel central, com uso de ambientes virtuais de aprendizagem, simuladores, softwares e aplicativos, ampliando as possibilidades de ensino presencial e remoto. A UFSB, por meio de sua infraestrutura de rede digital, garantirá as condições para esse modelo pedagógico, sustentada pelo backbone da Rede Nacional de Ensino e Pesquisa (RNP), que assegura transmissão de dados em alta velocidade.

10. ARQUITETURA CURRICULAR

O currículo do Curso de Bacharelado em Engenharia em Cibersegurança (BECiber) foi concebido com base em uma perspectiva multidisciplinar, em consonância com as diretrizes estabelecidas pelo Ministério da Educação. Sua organização busca garantir um sequenciamento lógico e progressivo na distribuição dos Componentes Curriculares (CCs), de modo a preparar os/as discentes para atuar em diferentes áreas de conhecimento da Engenharia em Cibersegurança, com ênfase no desenvolvimento das competências técnicas, científicas e éticas exigidas pelo campo da segurança digital.

A UFSB adota uma arquitetura curricular progressiva estruturada no regime de ciclos de formação, que compreende três fases distintas:

- **Primeiro Ciclo** – acesso à universidade, por meio dos Bacharelados Interdisciplinares (BIs);
- **Segundo Ciclo** – formação profissionalizante, no qual se insere o BECiber;
- **Terceiro Ciclo** – formação em nível de pós-graduação, acadêmica e/ou profissional (mestrado e doutorado).

Cada ciclo possui certificação própria, permitindo ao/à estudante percorrer diferentes trajetórias formativas, alinhadas a seus interesses e objetivos.

Os/as concluintes dos cursos de Primeiro Ciclo da UFSB, ou de outras instituições, que ingressarem no BECiber e já tenham cursado os componentes obrigatórios previstos poderão solicitar aproveitamento direto ao Colegiado. Caso contrário, os componentes faltantes deverão ser cursados após a matrícula no curso. Nesse processo, recomenda-se atenção às indicações de componentes precedentes, de modo que sejam respeitadas as ordens de progressão vertical do conhecimento.

Cabe destacar que, entre os cursos de Primeiro Ciclo, o Bacharelado Interdisciplinar em Ciências contempla em sua matriz curricular grande parte dos componentes obrigatórios exigidos pelo curso de Engenharia em Cibersegurança, o que facilita a continuidade acadêmica dos/as estudantes que optem por essa trajetória.

O Curso de Engenharia em Cibersegurança possui carga horária total de 3.600 horas. Considerando a necessidade de que o/a engenheiro/a em cibersegurança tenha uma formação básica sólida e abrangente, capaz de prepará-lo/a para atuar em diferentes áreas do campo da computação, da segurança da informação e das tecnologias digitais, adota-se um modelo curricular estruturado em eixos de conteúdos e atividades. Esse modelo garante uma formação

equilibrada, integrando fundamentos científicos, habilidades técnicas específicas e competências transversais, elementos indispensáveis para a atuação em um mercado cada vez mais dinâmico, desafiador e orientado à inovação.

A matriz curricular do Curso de Bacharelado em Engenharia em Cibersegurança organiza-se em eixos temáticos, que agrupam os conteúdos curriculares de forma coerente e integrada, cada qual relacionado a um campo específico de conhecimento. Esses eixos visam assegurar a progressão lógica da formação, desde os fundamentos científicos e técnicos até os conteúdos avançados e aplicados, preparando os/as estudantes para atuar em um cenário tecnológico dinâmico e em constante transformação.

Os eixos propostos são: Bases da Cibersegurança e Desenvolvimento Seguro; Governança, Conformidade e Resiliência Cibernética; Computação e Infraestruturas de TI; Forense Digital e Defesa de Infraestruturas Críticas; Inteligência Aplicada e Simulação em Cibersegurança; Integração e Prática Profissional.

Essa estrutura favorece uma formação interdisciplinar e integrada, permitindo que os/as estudantes desenvolvam competências que vão desde a base científica até a aplicação prática em problemas reais. Por exemplo, a capacitação em inteligência artificial possibilitará a criação de soluções para automação e análise de dados; e os conhecimentos em engenharia de software habilitarão os/as formandos/as a projetar sistemas escaláveis e seguros.

Dessa forma, alinhada aos preceitos pedagógicos institucionais, a arquitetura curricular do Curso de Engenharia em Cibersegurança integra teoria e prática, respondendo às necessidades formativas do profissional moderno e às exigências crescentes da sociedade digital.

O currículo do Curso de Bacharelado em Engenharia em Cibersegurança foi organizado de modo a contemplar apenas os pré-requisitos essenciais para garantir o desenvolvimento lógico e progressivo dos conteúdos. Assim, a matriz curricular do curso apresentada em forma de fluxograma (Figura 1), encontra-se em plena conformidade com as diretrizes estabelecidas pela Resolução CNE/CES nº 01/2021.

Figura 1.
do perfil
formação
de

1º ANO		2º ANO		3º ANO		4º ANO		5º ANO
1º Semestre	2º Semestre	3º Semestre	4º Semestre	5º Semestre	6º Semestre	7º Semestre	8º Semestre	9º Semestre
330 horas	330 horas	300 horas	300 horas	360 horas	360 horas	360 horas	330 horas	430 horas
Tendências em TI (30h)	Programação I (60h)	Programação II (60h)	Estatística para Análises de Segurança II (60h)	Banco de Dados (60h)	Sistemas Operacionais (60h)	Aprendizado Profundo (60h)	Trabalho de Conclusão de Curso I (30h)	Trabalho de Conclusão de Curso II (30h)
Eixo Matemática e Computação (60h)	Cálculo I (60h)	Cálculo II (60h)	Arquitetura de Computadores (60h)	Criptografia e Segurança de Dados (60h)	Engenharia de Software Seguro (60h)	Projeto e Modelagem de Sistemas Seguros (60h)	Segurança de IA e Mitigação de Riscos (60h)	Estágio Obrigatório (160h)
Eixo Línguas Estrangeiras (60h)	Física I (60h)	Física II (60h)	Álgebra Linear (60h)	Estrutura de Dados II (60h)	Aprendizado de Máquina (60h)	Laboratório de Invasão e Defesa (60h)	Simulações e Gamificação em Ambientes Seguros (60h)	Optativo (60h)
Eixo Ciências na Formação Cidadã (60h)	Laboratório de Projeto I (30h)	Laboratório de Projeto II (30h)	Design Thinking para Soluções de Segurança (30h)	Programação Orientada a Objetos (60h)	Big Data (60h)	Análise de Malware e Engenharia Reversa (60h)	Segurança em Infraestruturas Críticas (60h)	Optativo (60h)
Eixo Produções Textuais Acadêmicas (60h)	Geometria Analítica (60h)	Fundamentos de Cibersegurança (60h)	Estrutura de Dados I (30h)	Inteligência Artificial e Análise de Dados Aplicada à Segurança (60h)	Inteligência em Segurança e Gestão de Ameaças (60h)	Computação em Nuvem e Segurança em Ambientes Distribuídos (60h)	Políticas de Conformidade e Regulação em Segurança (60h)	Forense Computacional (60h)
Eixo Artes e Humanidades (60h)	Análise e Comunicação de Dados (60h)	Estatística para Análises de Segurança I (30h)	Optativo (60h)	Redes de Computadores I (60h)	Redes de Computadores II (60h)	Visão Computacional (60h)	Resiliência e Continuidade de Negócios (60h)	Métodos Avançados em Defesa Cibernética (60h)
Extensão (380 horas) + Atividades Complementares (120 horas)								

Legenda	
Formação Geral	
Núcleo Básico	
Núcleo Específico	Consulte Eixos Temáticos

Legenda - Núcleo Específico Eixos Temáticos	
Computação e Infraestruturas de TI	Forense Digital e Defesa de Infraestruturas Críticas
Bases da Cibersegurança e Desenvolvimento Seguro	Inteligência Aplicada e Simulação em Cibersegurança
Governança, Conformidade e Resiliência Cibernética	Integração e Prática Profissional

Bacharelado em Engenharia em Cibersegurança da UFSB.

Currículo
de
do Curso

A carga horária do Curso de Engenharia em Cibersegurança está organizada em três núcleos formativos: Formação Geral, Núcleo Básico e Núcleo Específico.

A Formação Geral corresponde a um currículo comum a todos os cursos da UFSB, constituído por uma carga horária obrigatória de Componentes Curriculares (CCs) que têm como finalidade apoiar a transição da educação básica para o ensino superior. Essa etapa formativa parte do reconhecimento da universidade como um espaço heterogêneo de produção e compartilhamento de saberes, fundamentado na interação dialógica, criativa e crítica.

A Formação Geral tem como objetivo preparar o/a estudante para a vida acadêmica e cidadã, enfatizando a complexidade das relações entre ciência, tecnologia e sociedade, o aprimoramento de práticas contemporâneas de interação e o reconhecimento da relevância da arte e da cultura na constituição dos sujeitos. Os CCs que a compõem devem valorizar a interdisciplinaridade, constituindo um campo de saberes capaz de auxiliar no entendimento do modelo institucional da universidade e de promover uma formação integral.

Os objetivos de aprendizagem dos diferentes eixos que estruturam a Formação Geral visam ao letramento acadêmico e científico, possibilitando ao estudante a construção de um arcabouço conceitual e prático essencial para superar eventuais lacunas oriundas da educação básica, ao mesmo tempo em que favorecem um melhor desempenho no ensino superior.

A Formação Geral é organizada em cinco eixos temáticos, cada um composto por um conjunto de CCs que podem ser escolhidos pelo/a estudante, preferencialmente no início do curso (primeiros semestres letivos). O Quadro 2 apresenta o conjunto de CCs da Formação Geral, divididos por eixos temáticos, que deverão ser cursados no percurso do Curso de Engenharia em Cibersegurança.

É importante destacar que, de acordo com a Resolução CONSUNI nº 02/2023, é obrigatório para o/a estudante cumprir um total de 60 horas por eixo temático, totalizando uma carga horária total de 300 horas a serem cumpridas na Formação Geral.

Quadro 2. CCs da Formação Geral.

EIXO TEMÁTICO	COMPONENTE CURRICULAR	CARGA HORÁRIA
Artes e Humanidades na Formação Cidadã	Arte e território	60 horas
	Brasil: Cidadania, Democracia e Políticas Públicas	45 horas
	Experiência do sensível	60 horas
	Humanidades, Interculturalidades e Metamorfoses Sociais	60 horas
	Introdução à Administração	60 horas
	Territorialidades e Sustentabilidade no Contexto Regional	45 horas
	Universidade e Sociedade	60 horas
Eixo Ciências na Formação Cidadã	Ciência e Cotidiano	60 horas
	Ciência, Sociedade e Ética	60 horas
	Ética e Responsabilidade Sócio-Ambiental	60 horas
	Processos Filosóficos e Metodológicos das Ciências	60 horas
	Saúde Única: Humana, Animal e Ambiental	60 horas
Matemática e Computação	Ambientes Virtuais e Colaborativos de Ensino Aprendizagem	30 horas
	Ciência dos Dados	60 horas
	Fundamentos da Computação	30 horas
	Fundamentos de Matemática	30 horas
	Fundamentos de Estatística	30 horas
	Introdução a Lógica	60 horas
	Matemática e Cotidiano	30 horas
	Pré-Cálculo	60 horas
Línguas Estrangeiras	Estratégias de Leitura em Língua Espanhola	45 horas
	Estratégias de Leitura em Língua Inglesa	60 horas
	Língua Espanhola em Nível Básico	60 horas
	Língua Inglesa e Cultura	60 horas
Produções Textuais Acadêmicas	Artigo Científico e Exposição Oral	30 horas
	Autoria na Produção do Texto Acadêmico	30 horas
	Metodologia Científica e Tecnológica	60 horas
	Oficina de Escrita Criativa	75 horas
	Oficina de Textos Acadêmicos	60 horas

Os CCs do Núcleo Básico reúnem conteúdos obrigatórios ligados aos fundamentos científicos e tecnológicos que sustentam a formação em Engenharia. Esse núcleo contempla disciplinas introdutórias das áreas de Matemática, Física e Estatística, essenciais para o

desenvolvimento do raciocínio lógico e para a construção de uma base sólida que dará suporte às competências técnicas do/a engenheiro/a em cibersegurança.

Nesse sentido, o arranjo dos CCs do Núcleo Básico foi estruturado para favorecer a progressão lógica do aprendizado e proporcionar aos/as estudantes as condições necessárias para o domínio dos conteúdos específicos do curso. Fazem parte desse núcleo as disciplinas: Cálculo I e II, Física I e II, Geometria Analítica, Álgebra Linear, Análise e Comunicação de Dados, além dos Laboratórios de Projeto I e II.

Essas disciplinas foram distribuídas, em sua maioria, ao longo dos quatro primeiros semestres, de modo a garantir uma formação inicial robusta em ciências exatas e metodológicas, consolidando os alicerces para os conteúdos profissionalizantes e específicos da área de cibersegurança.

A carga horária total do Núcleo Básico no Bacharelado em Engenharia em Cibersegurança é de 480 horas, conforme detalhado no Quadro 3.

Quadro 3. Listagem de CCs do Núcleo Básico.

EIXO TEMÁTICO	COMPONENTE CURRICULAR	CARGA HORÁRIA
Matemática	Geometria Analítica	240 horas
	Álgebra Linear	
	Cálculo I	
	Cálculo II	
Física	Física I	120 horas
	Física II	
Métodos Analíticos e Projetos Integradores	Análise e Comunicação de Dados	120 horas
	Laboratório de Projeto I	
	Laboratório de Projeto II	
CARGA HORÁRIA TOTAL		480 HORAS

O Núcleo Específico constitui a etapa central da formação do/a engenheiro/a em cibersegurança, reunindo os componentes curriculares que abordam de forma aprofundada os conteúdos profissionalizantes e especializados da área. Trata-se do núcleo que consolida as competências técnicas e científicas necessárias à atuação no campo da segurança digital, proteção de sistemas e defesa cibernética.

Nesse núcleo, os/as estudantes têm contato com temas avançados, como Criptografia e Segurança de Dados, Segurança em Infraestruturas Críticas, Forense Computacional, Engenharia de Software Seguro, entre outros. Esses conteúdos são estruturados para articular

teoria e prática, proporcionando experiências de aprendizagem que simulam cenários reais de ataque, defesa e gestão da segurança da informação.

O Núcleo Específico busca não apenas o domínio técnico, mas também o desenvolvimento de competências estratégicas e éticas, como a análise crítica de riscos, a elaboração de políticas de conformidade, a continuidade de negócios em ambientes digitais e a capacidade de inovação em soluções seguras. Com uma carga horária total de 1.980 horas, conforme detalhado no Quadro 4, o Núcleo Específico representa a maior parte da matriz curricular do curso, consolidando-se como o espaço formativo em que os conhecimentos adquiridos nos núcleos de Formação Geral e Básico são plenamente aplicados, orientando-se para a prática profissional em cibersegurança.

Quadro 4. CCs do Núcleo Específico.

EIXO TEMÁTICO	COMPONENTE CURRICULAR	CARGA HORÁRIA
Computação e Infraestruturas de TI	Tendências em TI	660 horas
	Programação I	
	Programação II	
	Estrutura de Dados I	
	Estrutura de Dados II	
	Banco de Dados	
	Arquitetura de Computadores	
	Programação Orientada a Objetos	
	Redes de Computadores I	
	Redes de Computadores II	
	Sistemas Operacionais	
	Computação em Nuvem e Segurança de Ambientes Distribuídos	
Bases da Cibersegurança e Desenvolvimento Seguro	Fundamentos de Cibersegurança	300 horas
	Criptografia e Segurança de Dados	
	Engenharia de Software Seguro	
	Projeto e Modelagem de Sistemas Seguros	
	Segurança de IA e Mitigação de Riscos	
Governança, Conformidade e Resiliência Cibernética	Resiliência e Continuidade de Negócios	180 horas
	Políticas de Conformidade e Regulação em	

	Segurança	
	Métodos Avançados em Defesa Cibernética	
Forense Digital e Defesa de Infraestruturas Críticas	Análise de Malware e Engenharia Reversa	180 horas
	Segurança em Infraestruturas Críticas	
	Forense Computacional	
Inteligência Aplicada e Simulação em Cibersegurança	Estatística para Análises de Segurança I	600 horas
	Estatística para Análises de Segurança II	
	Design Thinking para Soluções de Segurança	
	Inteligência em Segurança e Gestão de Ameaças	
	Aprendizado de Máquina	
	Big Data	
	Aprendizado Profundo	
	Inteligência Artificial e Análise de Dados Aplicada à Segurança	
	Laboratório de Invasão e Defesa	
	Visão Computacional	
	Simulações e Gamificação em Ambientes Seguros	
Integração e Prática Profissional	Trabalho de Conclusão de Curso I	60 horas
	Trabalho de Conclusão de Curso II	
CARGA HORÁRIA TOTAL		1980 HORAS

Além dos CCs apresentados nos Quadros 1, 2, 3 e 4, o/a estudante deverá cumprir, para a integralização do curso, um mínimo de 180 horas em CCs optativos, 120 horas em atividades complementares, 380 horas em atividades de extensão e 160 horas de estágio supervisionado obrigatório. A relação detalhada dos CCs optativos encontra-se no Quadro 5.

Quadro 5. Listagem de CCs optativos.

COMPONENTE CURRICULAR	CARGA HORÁRIA	PRÉ-REQUISITOS
Blockchain e Segurança em Criptomoedas	60	Criptografia e Segurança de Dados
Desenvolvimento de Malware Controlado	60	Sistemas Operacionais; Laboratório de Invasão e Defesa; Análise de Malware e Engenharia Reversa
Segurança em Redes Sociais	60	Redes de Computadores II; Fundamentos de Cibersegurança
Gerenciamento de Identidade e Acesso	60	Fundamentos de Cibersegurança; Políticas de Conformidade e Regulação em

		Segurança
Segurança em Sistemas Operacionais Abertos	60	Sistemas Operacionais
Privacidade e Proteção de Dados Pessoais	60	Criptografia e Segurança de Dados; Políticas de Conformidade e Regulação em Segurança
Segurança em Dispositivos IoT e Sistemas Ciberfísicos	60	Redes de Computadores II; Laboratório de Projeto II
Cibersegurança em Redes 5G e Futuras Gerações	60	Redes de Computadores II; Computação em Nuvem e Segurança em Ambientes Distribuídos
Segurança Ofensiva e Testes de Intrusão	60	Laboratório de Invasão e Defesa; Métodos Avançados em Defesa Cibernética
Segurança em Aplicações Web e Mobile	60	Engenharia de Software Seguro; Programação Orientada a Objetos
Impactos Sociais e Éticos da Privacidade Digital	60	-
Engenharia de Privacidade e Tecnologias de Preservação de Dados	60	Criptografia e Segurança de Dados; Análise e Comunicação de Dados
Engenharia de Dados	60	Banco de Dados; Big Data
Inteligência Artificial e as Redes Neurais	60	Aprendizado de Máquina; Inteligência Artificial e Análise de Dados Aplicada à Segurança
Introdução à Ciência de Dados com Python	60	Programação II; Estrutura de Dados II
Língua Brasileira de Sinais - Libras	60	-
Pesquisa Operacional	60	Álgebra Linear; Estatística para Análises de Segurança II
Tópicos Avançados em Engenharia de Software	60	Engenharia de Software Seguro; Projeto e Modelagem de Sistemas Seguros
Tópicos Avançados em Inteligência Artificial	60	Aprendizado de Máquina; Aprendizado Profundo
Educação Ambiental e Sustentabilidade Tecnológica	60	-
Direitos Humanos, Ética e Tecnologia	60	-
História e Cultura Afro-Brasileira, Africana e Indígena na Sociedade Digital	60	-

No Quadro 6 apresenta os CCs obrigatórios e seus respectivos pré-requisitos, detalhando de forma textual as informações representadas graficamente no fluxograma da matriz curricular e descritas de maneira aprofundada no catálogo de ementas.

Quadro 6. Listagem de CCs obrigatórios.

COMPONENTE CURRICULAR	CH TOTAL (horas)	PRÉ-REQUISITOS
Álgebra Linear	60	-
Análise de Malware e Engenharia Reversa	60	Sistemas Operacionais
Análise e Comunicação de Dados	60	-
Aprendizado de Máquina	60	Inteligência Artificial e Análise de Dados Aplicada à Segurança
Aprendizado Profundo	60	Álgebra Linear; Aprendizado de Máquina
Arquitetura de Computadores	60	Programação II
Banco de Dados	60	Estrutura de Dados I
Big Data	60	Banco de Dados
Cálculo I	60	-
Cálculo II	60	Cálculo I
Computação em Nuvem e Segurança em Ambientes Distribuídos	60	Redes de Computadores II
Criptografia e Segurança de Dados	60	Cálculo II; Álgebra Linear
Design Thinking para Soluções de Segurança	30	-
Engenharia de Software Seguro	60	Programação Orientada a Objetos; Estrutura de Dados I
Estágio Obrigatório	160	Consultar regimento interno
Estatística para Análises de Segurança I	30	-
Estatística para Análises de Segurança II	60	Estatística para Análises de Segurança I

ARQUITETURA CURRICULAR

Estrutura de Dados I	30	Programação II
Estrutura de Dados II	60	Estrutura de Dados I
Física I	60	-
Física II	60	Física I; Cálculo I
Forense Computacional	60	Fundamentos de Cibersegurança
Fundamentos de Cibersegurança	60	-
Geometria Analítica	60	-
Inteligência Artificial e Análise de Dados Aplicada à Segurança	60	Estatística para Análises de Segurança II
Inteligência em Segurança e Gestão de Ameaças	60	Inteligência Artificial e Análise de Dados Aplicada à Segurança
Laboratório de Invasão e Defesa	60	Redes de Computadores II; Sistemas Operacionais
Laboratório de Projeto I	30	-
Laboratório de Projeto II	30	Laboratório de Projeto I
Métodos Avançados em Defesa Cibernética	60	Laboratório de Invasão e Defesa
Políticas de Conformidade e Regulação em Segurança	60	-
Programação I	60	-
Programação II	60	Programação I
Programação Orientada a Objetos	60	Estrutura de Dados I
Projeto e Modelagem de Sistemas Seguros	60	Engenharia de Software Seguro
Redes de Computadores I	60	-
Redes de Computadores II	60	Redes de Computadores I
Resiliência e Continuidade de Negócios	60	-
Segurança de IA e Mitigação de Riscos	60	Aprendizado de Máquina
Segurança em Infraestruturas Críticas	60	Redes de Computadores II
Simulações e Gamificação em Ambientes Seguros	60	Laboratório de Invasão e Defesa; Inteligência em Segurança e Gestão de Ameaças
Sistemas Operacionais	60	Arquitetura de Computadores

Tendências em TI	30	-
Trabalho de Conclusão de Curso I	30	-
Trabalho de Conclusão de Curso II	30	Trabalho de Conclusão de Curso I
Visão Computacional	60	Álgebra Linear; Aprendizado de Máquina

10.1 Atividades e Componentes Curriculares de Extensão

Com base na legislação que regulamenta as Atividades Curriculares de Extensão (ACEEx) e considerando a obrigatoriedade de destinar no mínimo 10% da carga horária total do curso a ações extensionistas, o Curso de Bacharelado em Engenharia em Cibersegurança organiza suas atividades de extensão em sete modalidades principais:

- **Clínicas de Segurança Digital para Micro e Pequenas Empresas:** Os/as estudantes podem oferecer serviços de consultoria para pequenos negócios locais, que muitas vezes não possuem infraestrutura própria de TI. As clínicas podem abordar: segurança em redes Wi-Fi, gestão de senhas, uso seguro de sistemas de gestão, conformidade com a LGPD e boas práticas em backup de dados.
 - Benefício para a comunidade: fortalecimento da economia local com empresas mais protegidas contra golpes e ataques digitais.
 - Benefício para o/a estudante: aplicação prática de conhecimentos técnicos em cenários reais e desenvolvimento de competências de comunicação e consultoria.
- **Hackathons e Competições de Cibersegurança:** Organização de eventos como *Capture the Flag* (CTF) e maratonas de inovação em segurança digital, abertos à comunidade acadêmica e também a estudantes da rede pública. Nessas competições, os/as participantes podem resolver desafios de invasão ética, criptografia, engenharia reversa e proteção de sistemas.
 - Benefício para a comunidade: disseminação da cultura de inovação e segurança digital.
 - Benefício para o/a estudante: desenvolvimento de habilidades técnicas sob pressão, trabalho em equipe e visibilidade no mercado de trabalho.

- **Observatório de Cibersegurança e Privacidade:** Criação de um núcleo extensionista dedicado ao monitoramento e análise de incidentes de segurança digital. O observatório pode produzir relatórios periódicos, boletins educativos, guias de boas práticas e alertas de ameaças voltados para empresas, escolas e órgãos públicos da região.
 - Benefício para a comunidade: acesso a informações confiáveis e contextualizadas sobre riscos digitais.
 - Benefício para o/a estudante: experiência em coleta, análise e comunicação de dados, além do contato com metodologias de inteligência cibernética.
- **Campanhas de Conscientização em Escolas e Órgãos Públicos:** Ações educativas em escolas municipais, estaduais e órgãos públicos, promovendo palestras e oficinas sobre uso responsável da internet, *cyberbullying*, proteção de dados pessoais, combate a *fake news* e golpes digitais.
 - Benefício para a comunidade: maior preparo de jovens e servidores para lidar com os riscos do ambiente digital.
 - Benefício para o/a estudante: prática de comunicação clara, empatia social e fortalecimento do compromisso ético da profissão.
- **Laboratórios Abertos de Inovação em Segurança Digital:** Espaços colaborativos que podem ser abertos à comunidade para testes e prototipagem de soluções tecnológicas, como dispositivos IoT seguros, aplicativos com autenticação robusta e simulações de ataques/defesas cibernéticas.
 - Benefício para a comunidade: acesso a soluções inovadoras em segurança e inclusão digital.
 - Benefício para o/a estudante: contato com metodologias ágeis de inovação e prática de empreendedorismo em segurança digital.
- **Extensão Internacional em Cibersegurança:** Desenvolvimento de projetos colaborativos com universidades e organizações internacionais, em temas como privacidade transnacional, ética em IA, combate a crimes cibernéticos globais e regulação digital.
 - Benefício para a comunidade: inserção da região em redes internacionais de conhecimento.

- Benefício para o/a estudante: experiência internacional, desenvolvimento de competências interculturais e networking em um setor estratégico.
- **Atuação em Incubadoras e Startups de Segurança Digital:** Parceria com incubadoras e parques tecnológicos para que os/as estudantes contribuam com startups em projetos de análise de vulnerabilidades, soluções de autenticação, sistemas de proteção em nuvem e análise de malware.
 - Benefício para a comunidade: estímulo à inovação tecnológica e fortalecimento do ecossistema empreendedor regional.
 - Benefício para o/a estudante: imersão em ambientes de negócio reais, experiência em inovação e possibilidade de geração de propriedade intelectual.

Além destas atividades, os/as alunos/as poderão cumprir até 50% da carga horária destinada à extensão em Componentes Curriculares de Extensão (CCEX). O Quadro 7 lista os Componentes Curriculares de extensão do Curso de Engenharia em Cibersegurança.

Quadro 7. Componentes curriculares de extensão.

COMPONENTE CURRICULAR	CH TOTAL (horas)	PRÉ-REQUISITO
CCEX - Saúde Digital e Proteção de Dados	60	Fundamentos de Cibersegurança
CCEX - Cibersegurança em Cidades Inteligentes	60	Redes de Computadores II
CCEX - Defesa Digital e Direitos Humanos	60	-
CCEX - Educação Continuada em Segurança Digital	60	-
CCEX - Análise de Incidentes Cibernéticos	60	Fundamentos de Cibersegurança; Sistemas Operacionais; Redes de Computadores I.

Para o currículo do Bacharelado em Engenharia em Cibersegurança, a carga horária obrigatória destinada à extensão corresponde a 10% da matriz curricular, totalizando 380 horas. É fundamental que os/as estudantes se engajem em atividades extensionistas desde os primeiros anos do curso, de modo a garantir uma formação integral, articulada com as

demandas da sociedade, e cumprir adequadamente a carga horária exigida dentro do prazo estabelecido.

A gestão da extensão será coordenada por um/a docente designado/a pelo Colegiado do Curso de Engenharia em Cibersegurança, responsável pelo planejamento, acompanhamento e organização da oferta curricular extensionista. A creditação das atividades será registrada no histórico acadêmico do/a estudante e ocorrerá nas seguintes modalidades:

- Componentes Curriculares de Extensão (CCEx) - de natureza optativa, desenvolvidos por meio de projetos e ações junto à comunidade externa, com atribuição de carga horária e avaliação formal.
- Atividades Curriculares de Extensão (ACEx) - realizadas na forma de programas, projetos, cursos, eventos ou produtos, em que o/a estudante atue como protagonista em interação direta com a comunidade externa, com atribuição de carga horária correspondente.

As atividades de extensão poderão ser realizadas no âmbito do curso, em outras Unidades Acadêmicas da UFSB ou em instituições externas públicas e privadas, bem como em programas institucionais e acadêmicos (como PIBID, PET, Residência Pedagógica, entre outros). Também poderão ser consideradas atividades provenientes de políticas públicas em parceria com a universidade.

Para fins de creditação, deverão ser observados os seguintes critérios:

- As atividades devem estar alinhadas aos eixos temáticos do Curso de Engenharia em Cibersegurança;
- A carga horária não poderá ser validada em duplicidade com outros processos formativos já contemplados na matriz curricular;
- É indispensável a comprovação do protagonismo do/a estudante e da efetiva realização em conjunto com a comunidade externa à UFSB.

O aproveitamento de CCEx e ACEx seguirá as normas estabelecidas em Resoluções específicas da UFSB e do Conselho Superior pertinentes à curricularização da extensão.

10.2 Estágio Curricular

A carga horária mínima do estágio curricular supervisionado obrigatório do Curso de Bacharelado em Engenharia em Cibersegurança é de 160 horas, conforme estabelecido pelas

normativas da UFSB. Esse estágio tem como objetivo possibilitar ao/à estudante a aplicação prática dos conhecimentos teóricos adquiridos ao longo do curso, em ambientes reais de trabalho vinculados à área da cibersegurança e da engenharia de sistemas digitais.

As diretrizes que regem essa atividade estão descritas em resolução específica da UFSB, que institui normas para a realização de estágios obrigatórios. Além disso, as regras e condições para a prática constam no regulamento de estágio do curso.

O estágio curricular obrigatório constitui uma etapa fundamental na formação do/a estudante, permitindo o desenvolvimento de habilidades técnicas, sociais e profissionais, bem como o amadurecimento necessário para a atuação como engenheiro/a em cibersegurança. Ele é também uma oportunidade para o fortalecimento de competências em comunicação, trabalho em equipe, liderança, gestão de projetos e resolução de problemas, aspectos indispensáveis à inserção qualificada no mercado de trabalho.

Durante o estágio, os/as estudantes poderão, entre outras atividades:

- Participar de projetos práticos em segurança da informação e defesa cibernética;
- Desenvolver e aplicar soluções tecnológicas em redes de computadores, sistemas em nuvem, IoT e dispositivos ciberfísicos;
- Atuar em análises de vulnerabilidades, auditorias de conformidade, desenvolvimento seguro de software e implementação de políticas de proteção de dados;
- Colaborar em projetos de forense computacional, inteligência artificial aplicada à segurança e investigação de incidentes;
- Contribuir com o planejamento, gestão e execução de projetos de engenharia cibernética, como modelagem de sistemas resilientes, testes de invasão controlados e avaliação de riscos em infraestruturas críticas.

Essa experiência proporciona ao/à estudante a vivência de situações reais do mercado, promovendo a integração entre teoria e prática, e ampliando suas competências profissionais e éticas diante dos desafios da sociedade digital contemporânea.

O estágio supervisionado será acompanhado por um/a Coordenador/a de Estágio, designado/a pelo Colegiado do Curso, e por docentes orientadores/as responsáveis pela supervisão pedagógica da atividade, vinculados ao Componente Curricular Estágio Obrigatório.

Por fim, vale ressaltar que os estágios não obrigatórios são incentivados e poderão ser reconhecidos como atividades complementares, desde que atendam às disposições previstas no regulamento do curso e contribuam para a formação em cibersegurança.

10.3 Atividades Complementares

As Atividades Complementares constituem um componente fundamental na formação dos/as estudantes do Curso de Bacharelado em Engenharia em Cibersegurança, pois ampliam e enriquecem o processo formativo para além do currículo regular. Por meio delas, os/as discentes têm a oportunidade de vivenciar experiências adicionais de aprendizado, desenvolver novas habilidades e consolidar competências que fortalecem tanto a sua atuação profissional quanto a sua formação cidadã.

Essas atividades permitem que os/as estudantes participem de projetos, eventos e iniciativas que dialogam com o campo da cibersegurança e com sua inserção social, estimulando o engajamento comunitário, a responsabilidade ética na proteção de dados, a consciência socioambiental e a atuação em projetos de impacto social. Ao integrar dimensões técnicas, sociais e humanas, as Atividades Complementares contribuem para uma formação mais crítica, interdisciplinar e alinhada às demandas contemporâneas do mundo digital.

De acordo com o currículo estabelecido, a carga horária destinada às Atividades Complementares no curso de Engenharia em Cibersegurança corresponde a 120 horas.

As diretrizes que regulamentam essas atividades na UFSB estão definidas em resolução específica e complementadas por normas internas do curso. Destaca-se que o/a estudante deve cumprir atividades diversificadas, não sendo permitido utilizar apenas um único tipo de experiência para integralizar a carga horária prevista. Essa diversidade assegura que a formação seja abrangente e equilibrada, contemplando aspectos acadêmicos, científicos, tecnológicos, culturais e sociais.

As condições e critérios para a creditação das Atividades Complementares constam no regulamento interno do curso, que define os tipos de atividades aceitas, os limites de carga horária por modalidade e os procedimentos de registro no histórico acadêmico.

10.4 Trabalho de Conclusão de Curso

O Trabalho de Conclusão de Curso (TCC) constitui uma etapa fundamental e obrigatória no Curso de Bacharelado em Engenharia em Cibersegurança, tendo como

propósito consolidar e aplicar os conhecimentos adquiridos ao longo da graduação. Essa atividade proporciona aos/as estudantes a oportunidade de desenvolver competências em pesquisa, análise crítica, síntese, organização e apresentação de resultados, habilidades indispensáveis para o exercício profissional e para a atuação ética e responsável na área da cibersegurança.

O objetivo central do TCC é permitir que os/as estudantes aprofundem seus conhecimentos em temas específicos da área, aplicando-os em um projeto de pesquisa, estudo de caso ou desenvolvimento tecnológico voltado à solução de problemas concretos relacionados à segurança digital, proteção de dados, defesa cibernética e inovação tecnológica. Ao propor soluções ou desenvolver projetos aplicados, o/a estudante vivencia a aplicação prática de conceitos teóricos em contextos reais, preparando-se para os desafios contemporâneos da vida profissional e do mercado de trabalho.

Além disso, o TCC contribui para o desenvolvimento de habilidades de comunicação oral e escrita, uma vez que o trabalho deverá ser apresentado e defendido publicamente perante uma banca avaliadora.

O/A orientador/a do TCC deverá ser um/a docente da UFSB com experiência na área de Engenharia em Cibersegurança e será indicado/a pelo/a estudante. O aceite da orientação será formalizado por meio de termo de responsabilidade, sujeito à aprovação do Colegiado do Curso. O TCC deverá ser realizado individualmente e seu tema deve estar relacionado a um dos eixos temáticos do curso, garantindo a aderência à especificidade e à complexidade da formação em cibersegurança, sempre com foco no equilíbrio entre tecnologia, segurança e sustentabilidade social.

O TCC será desenvolvido em duas etapas, distribuídas em dois Componentes Curriculares:

- Trabalho de Conclusão de Curso I (TCC I) – ofertado no 8º semestre, com carga horária de 30h;
- Trabalho de Conclusão de Curso II (TCC II) – ofertado no 9º semestre, também com carga horária de 30h.

A oficialização da matrícula nos componentes será realizada em conformidade com o planejamento acadêmico, cabendo ao/a estudante solicitar a abertura da turma junto ao Colegiado do Curso. O/A docente responsável pelos CCs de TCC deverá:

- acompanhar a lista de matriculados;

- organizar e divulgar a lista de orientadores/as disponíveis;
- orientar os prazos para entrega e defesa;
- receber os trabalhos escritos e encaminhá-los ao Colegiado para cadastramento e arquivamento.

A avaliação do TCC compreenderá duas etapas: a entrega do trabalho escrito e a sua defesa pública. A banca avaliadora será composta por, no mínimo, três membros, sendo o/a orientador/a o presidente da banca. As regras específicas relacionadas ao TCC estão dispostas em resolução interna do curso, aprovada pelo Colegiado.

10.5 Matriz Curricular

O Quadro 8 apresenta a ilustração do percurso formativo do Curso de Engenharia em Cibersegurança.

Quadro 8. Matriz Curricular.

PERÍODO	COMPONENTE CURRICULAR OU ATIVIDADE	NÚCLEO DE CONTEÚDO	CARGA HORÁRIA (horas)	PRÉ-REQUISITOS
1º	Tendências em TI	Específico	30	-
1º	Eixo Artes e Humanidades na Formação Cidadã	Formação Geral	60	-
1º	Eixo Ciências na Formação Cidadã	Formação Geral	60	-
1º	Eixo Línguas Estrangeiras	Formação Geral	60	-
1º	Eixo Matemática e Computação	Formação Geral	60	-
1º	Eixo Produções Textuais Acadêmicas	Formação Geral	60	-
2º	Programação I	Específico	60	-
2º	Cálculo I	Básico	60	-
2º	Física I	Básico	60	-
2º	Laboratório de Projeto I	Básico	30	-
2º	Geometria Analítica	Básico	60	-
2º	Análise e Comunicação de Dados	Básico	60	-
3º	Física II	Básico	60	Física I; Cálculo I
3º	Programação II	Específico	60	Programação I
3º	Cálculo II	Básico	60	Cálculo I
3º	Laboratório de Projeto II	Básico	30	Laboratório de Projeto I
3º	Fundamentos de Cibersegurança	Específico	60	-

ARQUITETURA CURRICULAR

3º	Estatística para Análises de Segurança I	Específico	30	-
4º	Estatística para Análises de Segurança II	Específico	60	Estatística para Análises de Segurança I
4º	Arquitetura de Computadores	Específico	60	Programação II
4º	Álgebra Linear	Básico	60	-
4º	Design Thinking para Soluções de Segurança	Específico	30	-
4º	Estrutura de Dados I	Específico	30	Programação II
4º	Optativo	-	60	Consultar requisitos na ementa do componente
5º	Banco de Dados	Específico	60	Estrutura de Dados I
5º	Criptografia e Segurança de Dados	Específico	60	Cálculo II; Álgebra Linear
5º	Estrutura de Dados II	Específico	60	Estrutura de Dados I
5º	Programação Orientada a Objetos	Específico	60	Estrutura de Dados I
5º	Inteligência Artificial e Análise de Dados Aplicada à Segurança	Específico	60	Estatística para Análises de Segurança II
5º	Redes de Computadores I	Específico	60	-
6º	Sistemas Operacionais	Específico	60	Arquitetura de Computadores
6º	Engenharia de Software Seguro	Específico	60	Programação Orientada a Objetos; Estrutura de Dados I
6º	Aprendizado de Máquina	Específico	60	Inteligência Artificial e Análise de Dados Aplicada à Segurança
6º	Big Data	Específico	60	Banco de Dados
6º	Inteligência em Segurança e Gestão de Ameaças	Específico	60	Inteligência Artificial e Análise de Dados Aplicada à Segurança
6º	Redes de Computadores II	Específico	60	Redes de Computadores I
7º	Aprendizado Profundo	Específico	60	Álgebra Linear; Aprendizado de Máquina
7º	Projeto e Modelagem de Sistemas Seguros	Específico	60	Engenharia de Software Seguro
7º	Laboratório de Invasão e Defesa	Específico	60	Redes de Computadores II; Sistemas Operacionais
7º	Análise de Malware e Engenharia Reversa	Específico	60	Sistemas Operacionais
7º	Computação em Nuvem e Segurança em Ambientes Distribuídos	Específico	60	Redes de Computadores II
7º	Visão Computacional	Específico	60	Álgebra Linear; Aprendizado de Máquina
8º	Trabalho de Conclusão de Curso I	Específico	30	-
8º	Segurança de IA e Mitigação de Riscos	Específico	60	Aprendizado de Máquina

8º	Simulações e Gamificação em Ambientes Seguros	Específico	60	Laboratório de Invasão e Defesa; Inteligência em Segurança e Gestão de Ameaças
8º	Segurança em Infraestruturas Críticas	Específico	60	Redes de Computadores II
8º	Políticas de Conformidade e Regulação em Segurança	Específico	60	-
8º	Resiliência e Continuidade de Negócios	Específico	60	-
9º	Trabalho de Conclusão de Curso II	Específico	30	Trabalho de Conclusão de Curso I
9º	Estágio Obrigatório	-	160	Consultar regimento interno
9º	Optativo	-	60	Consultar requisitos na ementa do componente
9º	Optativo	-	60	Consultar requisitos na ementa do componente
9º	Forense Computacional	Específico	60	Fundamentos de Cibersegurança
9º	Métodos Avançados em Defesa Cibernética	Específico	60	Laboratório de Invasão e Defesa
-	Atividades de Extensão	-	380	-
-	Atividades Complementares	-	120	-
TOTAL	54 CCs e 2 Atividades	-	3600 horas	-

10.6 Ensino à Distância

A proposta pedagógica do Bacharelado em Engenharia em Cibersegurança prevê a possibilidade de oferta de parte de sua carga horária por meio da modalidade de Ensino à Distância (EaD), em conformidade com o Decreto nº 12.456/2025, com atos normativos complementares do MEC, com as Diretrizes Curriculares Nacionais para os cursos de Engenharia e com as resoluções internas da UFSB que regulamentam a temática.

Todas as atividades realizadas em EaD são estruturadas com rigor metodológico, contemplando acompanhamento contínuo por meio de tutoria especializada, suporte constante no Ambiente Virtual de Aprendizagem (AVA) — integrado ao Sistema Integrado de Gestão de Atividades Acadêmicas (SIGAA) — e o uso articulado de Tecnologias da Informação e Comunicação (TICs) adequadas aos objetivos pedagógicos do curso. Essa abordagem busca assegurar a qualidade acadêmica, a flexibilidade no processo de aprendizagem e a conformidade com os padrões legais vigentes.

O Quadro 9 apresenta detalhadamente os Componentes Curriculares (CCs) que poderão ser ofertados parcial ou integralmente na modalidade EaD, bem como o percentual de carga horária permitido para essa oferta.

Quadro 9. Componentes curriculares opcionais para a modalidade de ensino à distância.

PERÍODO	COMPONENTE CURRICULAR OU ATIVIDADE	NÚCLEO DE CONTEÚDO	CARGA HORÁRIA (horas)
2º	Análise e Comunicação de Dados	Básico	60
2º	Programação I	Específico	60
3º	Programação II	Específico	60
3º	Estatística para Análises de Segurança I	Específico	30
4º	Arquitetura de Computadores	Específico	60
4º	Estatística para Análises de Segurança II	Específico	60
4º	Estrutura de Dados I	Específico	30
5º	Inteligência Artificial e Análise de Dados Aplicada à Segurança	Específico	60
5º	Banco de Dados	Específico	60
5º	Programação Orientada a Objetos	Específico	60
5º	Estrutura de Dados II	Específico	60
5º	Redes de Computadores I	Específico	60
6º	Sistemas Operacionais	Específico	60
6º	Redes de Computadores II	Específico	60
6º	Aprendizado de Máquina	Específico	60
7º	Aprendizado Profundo	Específico	60
7º	Visão Computacional	Específico	60
8º	Políticas de Conformidade e Regulação em Segurança	Específico	60
8º	Resiliência e Continuidade de Negócios	Específico	60
TOTAL	19 Componentes Curriculares		1080 horas ou 30% da carga horário total do curso

As atividades em Educação a Distância (EaD) no Curso de Bacharelado em Engenharia em Cibersegurança contemplam apenas os Componentes Curriculares (CCs) cujo conteúdo pode ser efetivamente transmitido por esta modalidade, sem prejuízo para a formação. Os CCs de caráter estritamente prático, que demandam laboratórios especializados

ou ambientes de simulação controlados, permanecerão ofertados presencialmente, de modo a resguardar a qualidade acadêmica e a formação aplicada essencial ao/à engenheiro/a em cibersegurança.

A metodologia adotada para os CCs ofertados total ou parcialmente em EaD privilegia:

- Aulas virtuais síncronas (videoconferências e webconferências), que promovem interação em tempo real entre docentes, tutores/as e discentes;
- Recursos de interação (fóruns, chats, e-mails e ferramentas no AVA), favorecendo a construção coletiva do conhecimento;
- Atividades práticas orientadas, como projetos, estudos de caso, simulações e uso de laboratórios remotos ou virtuais, sempre que aplicável;
- Materiais de apoio (artigos científicos, podcasts, tutoriais em vídeo, apostilas digitais, roteiros práticos), alinhados às ementas e adaptados à linguagem inclusiva e acessível.

Essa abordagem busca assegurar que os/as estudantes desenvolvam as competências e habilidades inerentes à Engenharia em Cibersegurança, inclusive quando parte da aprendizagem ocorre fora do ambiente presencial.

O PPC reconhece que a EaD exige o envolvimento de diferentes profissionais da educação, cada qual com atribuições específicas:

- O/A Professor/a Regente e o/a Professor/a Conteudista são responsáveis pelo planejamento, execução e atualização do ciclo ensino-aprendizagem, garantindo coerência pedagógica e qualidade dos materiais.
- O/A Mediador/a Pedagógico/a — docente ou tutor/a designado/a — desempenha funções de acompanhamento didático, esclarecimento de dúvidas e condução de atividades síncronas, respeitando a proporção máxima de 70 estudantes por atividade.
- O/A Tutor/a Administrativo/a responde pela gestão logística e operacional do curso (inscrições, prazos, envio de materiais e controle de frequência), assegurando suporte contínuo aos discentes e docentes.

No que se refere ao uso de Ambientes Virtuais de Aprendizagem (AVA), o curso poderá adotar plataformas institucionais ou complementares, mantendo o SIGAA como apoio central. O SIGAA possibilita a:

- hospedagem de conteúdos (planos de ensino, materiais didáticos, atividades e avaliações);

- promoção de fóruns de discussão;
- submissão e correção de trabalhos;
- acompanhamento de notas, frequência e engajamento dos/as estudantes.

Todos os recursos digitais devem estar em conformidade com as Diretrizes de Acessibilidade para Conteúdo Web (WCAG 2.1 nível AA), garantindo inclusão e usabilidade plena, além de respeitar a identidade visual institucional da UFSB.

Complementarmente, as Tecnologias de Informação e Comunicação (TICs) serão utilizadas para dinamizar o processo de ensino, incluindo:

- plataformas de videoconferência para aulas síncronas e orientações de TCC;
- ferramentas colaborativas (repositórios de código, editores coletivos, quadros virtuais) para o desenvolvimento de projetos;
- laboratórios virtuais e simuladores para apoiar atividades práticas em hardware, software e segurança cibernética.

Os Polos de EaD vinculados à UFSB devem dispor de infraestrutura mínima que inclua:

- salas com internet de alta velocidade e recursos de videoconferência;
- mobiliário ergonômico para docentes e discentes;
- acesso a laboratórios ou simuladores especializados, quando necessário;
- conformidade com normas de acessibilidade e inclusão.

A manutenção e atualização desses Polos é responsabilidade da UFSB, com suporte técnico local, manutenção periódica e monitoramento contínuo. O Colegiado do Curso é responsável por acompanhar a qualidade acadêmica, fiscalizar a infraestrutura e avaliar a satisfação de docentes e discentes.

Nos Planos de Ensino e Aprendizagem (PEAs) dos CCs ofertados na modalidade EaD, deverão constar com clareza as metodologias, os instrumentos de avaliação e a divisão entre atividades presenciais e a distância. A frequência discente será aferida por meio da participação em AVAs (fóruns, quizzes, submissões) e pela presença em aulas síncronas, com registro eletrônico auditável.

As avaliações finais ocorrerão presencialmente na sede ou em polos conveniados, sendo obrigatório que no mínimo 50% da nota seja atribuída em provas presenciais, das quais pelo menos 1/3 do conteúdo deve ser discursivo, assegurando profundidade e autenticidade no processo avaliativo.

A gestão das atividades EaD no Curso de Engenharia em Cibersegurança será realizada pelo Colegiado do Curso, com atribuições de:

- monitorar a qualidade acadêmica e os indicadores de desempenho;
- promover formação continuada de docentes e tutores/as em TICs e metodologias inovadoras;
- atualizar os recursos tecnológicos de suporte;
- elaborar relatórios periódicos de avaliação e melhoria contínua.

Assim, o PPC do Bacharelado em Engenharia em Cibersegurança garante que a oferta de carga horária na modalidade EaD esteja em consonância com a legislação vigente, mantendo o equilíbrio entre a formação presencial — indispensável para disciplinas práticas e experimentais — e o uso estratégico da EaD, que amplia a flexibilidade, promove autonomia discente e fortalece a inovação pedagógica.

11. AVALIAÇÃO DOS PROCESSOS DE ENSINO-APRENDIZAGEM

A avaliação do processo de ensino-aprendizagem no Curso de Bacharelado em Engenharia em Cibersegurança possui caráter diagnóstico, processual, cumulativo e formativo, fundamentando-se em um trabalho contínuo de ação-reflexão por parte dos/as docentes, a fim de acompanhar e promover os avanços alcançados pelos/as discentes em sua formação técnico-científica, ética e cidadã.

Os instrumentos de avaliação são definidos em consonância com as especificidades de cada Componente Curricular (CC), a metodologia de ensino empregada e a concepção pedagógica adotada. Dessa forma, a avaliação considera tanto o processo de aprendizagem quanto o produto final.

No processo de aprendizagem, a avaliação busca identificar potencialidades, dificuldades e necessidades dos/as estudantes, permitindo que docentes elaborem estratégias diferenciadas para superação de desafios e consolidem a evolução das competências.

No produto da aprendizagem, a avaliação visa mensurar a apropriação dos conhecimentos e habilidades previstos nos objetivos do curso e de cada CC. Entre os instrumentos utilizados, destacam-se:

- questionários e provas escritas, com ou sem consulta a materiais bibliográficos;
- arguições orais;
- experimentações monitoradas em laboratórios;
- relatórios técnicos e descrições de processos produtivos;
- visitas técnicas e relatórios de campo;
- elaboração e apresentação de pôsteres e materiais científicos;
- fichas de aula e instrumentos de autoavaliação;
- relatórios de estágio;
- monografias e projetos de conclusão.

Ao atribuir nota, o/a docente deve explicitar de forma clara os critérios adotados, em alinhamento com os objetivos de aprendizagem definidos no Plano de Ensino-Aprendizagem (PEA). Esses critérios devem ser apresentados no início do semestre, garantindo transparência, justiça, imparcialidade e objetividade no processo avaliativo.

As notas são expressas em escala numérica de 0 (zero) a 10 (dez), com uma casa decimal. O/A discente será considerado/a aprovado/a em um CC quando cumprir simultaneamente dois requisitos:

- frequência mínima de 75% da carga horária do componente;
- nota final igual ou superior a 6,0 (seis).

Para estudantes que obtiverem desempenho insatisfatório, a instituição assegura o direito à Recuperação por Crédito Condicional (RCC). Este recurso aplica-se quando a nota final do discente situa-se entre 3,0 e 5,9, permitindo sua aprovação condicionada à realização de atividades avaliativas adicionais, definidas pelo/a docente ou equipe responsável, dentro do prazo estipulado no calendário acadêmico da UFSB.

Além das avaliações internas, o curso considera como referências externas a avaliação institucional da UFSB, conduzida periodicamente pela Comissão Própria de Avaliação (CPA), e os resultados do Exame Nacional de Desempenho dos Estudantes (ENADE), que funcionam como balizadores importantes para o aprimoramento contínuo do processo de ensino-aprendizagem.

12. PROCESSOS DE AVALIAÇÃO DO PROJETO PEDAGÓGICO DE CURSO

O Projeto Pedagógico do Curso (PPC) do Bacharelado em Engenharia em Cibersegurança será avaliado periodicamente, de modo a acompanhar as transformações significativas nas atribuições profissionais, especialmente diante dos rápidos avanços tecnológicos e das constantes mudanças no cenário da cibersegurança. Essa atualização contínua é essencial para assegurar que o curso permaneça alinhado às demandas do mercado, às inovações científicas e às necessidades sociais.

A responsabilidade por conduzir essas avaliações é do Núcleo Docente Estruturante (NDE), que realizará revisões regulares do PPC ao longo do tempo.

Outro aspecto central desse processo consiste na análise da adequação do corpo docente e da infraestrutura do curso, incluindo salas de aula, laboratórios especializados em cibersegurança, bibliotecas físicas e digitais e recursos tecnológicos. Nesse sentido, serão realizadas avaliações anuais, voltadas para:

- Estrutura física e tecnológica: análise das condições de infraestrutura do curso, incluindo laboratórios de redes e cibersegurança, ambientes de simulação, biblioteca e recursos digitais necessários para uma formação atualizada e prática.
- Inserção no mercado de trabalho: acompanhamento dos egressos, avaliando sua atuação profissional, as áreas de inserção e o grau de satisfação com a formação recebida, identificando pontos de melhoria e fortalecimento.

O curso será avaliado por meio de instâncias internas e externas:

- Avaliação interna: realizada anualmente por meio de consultas a discentes e egressos, buscando identificar potencialidades e fragilidades. Essas informações são utilizadas tanto para correções de rumo quanto para potencializar aspectos positivos do curso. A participação ativa dos/as estudantes é essencial, uma vez que suas percepções fundamentam o processo de evolução contínua do PPC.
- Avaliação externa: conduzida conforme os padrões estabelecidos pelo Ministério da Educação (MEC), por meio do Exame Nacional de Desempenho dos Estudantes (ENADE) e das avaliações realizadas pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), ambas de caráter obrigatório para o curso.

Além disso, a UFSB adota um sistema de avaliação institucional, coordenado pela Comissão Própria de Avaliação (CPA), que realiza diagnósticos críticos e coletivos sobre a coerência entre as práticas institucionais e os princípios e políticas definidas no Estatuto, no

Regimento Geral, no Plano de Desenvolvimento Institucional (PDI) e nas deliberações dos órgãos colegiados da universidade.

As avaliações institucionais seguem as diretrizes do Sistema Nacional de Avaliação da Educação Superior (SINAES) e abrangem a análise do perfil institucional, dos processos de funcionamento, dos resultados obtidos e de seu impacto acadêmico e social. O objetivo é fomentar uma reflexão crítica permanente, que permita aperfeiçoar a qualidade da formação, promover a inovação pedagógica e fortalecer o papel estratégico do curso na formação de profissionais de excelência em cibersegurança.

13. GESTÃO DO CURSO

O Centro Multidisciplinar Ciência e Sociedade (CMCS), unidade acadêmica responsável pela oferta do Curso de Bacharelado em Engenharia em Cibersegurança, é administrado por um órgão colegiado denominado Congregação do CMCS. Esse colegiado conta com representações dos três segmentos da comunidade acadêmica — docente, discente e técnico-administrativo —, além de representantes dos colegiados dos cursos vinculados ao centro. A direção da Congregação é exercida pelo/a decano/a e pelo/a vice-decano/a, que também representam o decanato do CMCS.

No âmbito do curso, a gestão direta é exercida pelo Colegiado do Curso de Engenharia em Cibersegurança, instância responsável pela coordenação e acompanhamento de todas as atividades acadêmicas e administrativas relacionadas à graduação. O Colegiado é igualmente composto por representantes docentes, discentes e técnico-administrativos, e possui uma Coordenação de Curso, formada por um/a coordenador/a e um/a vice-coordenador/a, designados/as conforme as normativas institucionais vigentes.

As atividades da Congregação e do Colegiado são conduzidas por meio de reuniões ordinárias mensais, convocadas com antecedência e acompanhadas da documentação pertinente à pauta definida. Essas reuniões têm como objetivo deliberar sobre temas previamente estabelecidos, garantindo a participação democrática dos segmentos representados e a transparência das decisões acadêmico-administrativas. Além disso, sempre que necessário, são convocadas reuniões extraordinárias, destinadas ao tratamento de questões emergenciais que exigem deliberação imediata.

Toda a administração do curso é regida pelas resoluções específicas da UFSB, que regulamentam os órgãos de gestão acadêmica das unidades universitárias, assegurando que as práticas de governança estejam alinhadas às diretrizes institucionais e aos princípios de gestão participativa.

13.1 Coordenação do Colegiado de Curso

O Colegiado do Curso de Engenharia em Cibersegurança conta com uma Coordenação, composta por um/a Coordenador/a e um/a Vice-Coordenador/a, escolhidos/as entre os/as docentes do quadro efetivo da UFSB, para mandatos de dois anos, sendo permitida uma única recondução ao mesmo cargo.

O/A Coordenador/a deve ser um/a docente diretamente envolvido/a no desenvolvimento do curso, com perfil de liderança acadêmica e compromisso institucional. Suas atribuições seguem a resolução específica que regulamenta os Órgãos de Gestão Acadêmica das Unidades Universitárias, abrangendo:

- Convocar e presidir as reuniões do Colegiado, com direito a voto e ao voto de qualidade em casos de empate;
- Zelar pela correta aplicação do Projeto Pedagógico do Curso (PPC);
- Designar relatores/as para assuntos de pauta que demandem análise detalhada e deliberação;
- Participar como membro nato da Congregação do Centro Multidisciplinar Ciência e Sociedade (CMCS);
- Representar o Colegiado do Curso junto aos demais órgãos da UFSB e a instituições externas.

Além das funções deliberativas e de representação, o/a Coordenador/a exerce papel estratégico de articulação e comunicação, mantendo contato frequente com discentes, docentes e técnicos/as administrativos/as. Esse diálogo constante permite compreender demandas e inquietações, difundir informações relevantes e estimular a participação ativa da comunidade acadêmica em instâncias avaliativas e decisórias.

Todas essas práticas, realizadas em conformidade com as normas e regulamentos institucionais, têm como objetivo assegurar a efetividade da gestão acadêmica e garantir a qualidade e a consolidação do Curso de Engenharia em Cibersegurança.

13.2 Colegiado de Curso

O Colegiado do Curso de Engenharia em Cibersegurança é o órgão de gestão acadêmica responsável por planejar, executar e supervisionar as atividades universitárias do curso, exercendo as atribuições previstas em resoluções específicas do CONSUNI e demais normativas institucionais aplicáveis. Sua finalidade principal é assegurar a articulação entre docentes e discentes, promovendo aprendizagens significativas pautadas em práticas solidárias, críticas e interdisciplinares, em consonância com o Projeto Pedagógico do Curso (PPC).

A composição mínima do Colegiado é definida da seguinte forma:

- Cinco docentes com atuação comprovada em Componentes Curriculares vinculados ao curso;
- Um/a representante técnico-administrativo/a;
- Um/a representante discente do curso.
- O mandato dos membros é de dois anos, sendo permitida uma única recondução.

Compete ao Colegiado do Curso:

- Coordenar e zelar pelas atividades de ensino-aprendizagem, assegurando conformidade com o PPC;
- Implementar e acompanhar o PPC aprovado pelo CONSUNI;
- Analisar e emitir parecer sobre propostas de atualização do PPC elaboradas pelo Núcleo Docente Estruturante (NDE);
- Propor políticas de incentivo ao ensino, à pesquisa, à inovação, à criação e à cooperação técnica no âmbito do curso;
- Sugerir a expansão, modificação ou extinção do curso, bem como ajustes na oferta de vagas;
- Apreçar e aprovar os Planos de Ensino-Aprendizagem (PEAs), propondo alterações quando necessário;
- Avaliar a execução dos PEAs e propor medidas de aperfeiçoamento;
- Apresentar propostas de atividades extracurriculares que contribuam para o fortalecimento da formação acadêmica;
- Promover o planejamento pedagógico dos Componentes Curriculares ofertados a cada semestre, realizando revisões anuais para ajustes e melhorias;
- Deliberar sobre processos administrativos de natureza acadêmica relacionados ao curso.

O Colegiado reúne-se ordinariamente uma vez ao mês e, em caráter extraordinário, sempre que houver necessidade, sendo suas deliberações tomadas por maioria simples dos votos.

13.3 Núcleo Docente Estruturante (NDE)

A regulamentação interna da UFSB estabelece a criação e a composição do Núcleo Docente Estruturante (NDE) para todos os cursos de 1º e 2º Ciclo de Graduação. O NDE

possui caráter consultivo, propositivo e de assessoramento em questões acadêmicas, sendo responsável pela elaboração, implementação, acompanhamento, atualização e consolidação do Projeto Pedagógico de Curso (PPC). No caso do Curso de Engenharia em Cibersegurança, o NDE desempenha papel estratégico no acompanhamento contínuo do PPC, assegurando sua adequação às Diretrizes Curriculares Nacionais (DCNs) e às demandas contemporâneas da área.

São atribuições do NDE do Curso de Engenharia em Cibersegurança:

- Acompanhar o desenvolvimento do PPC, promovendo reflexão permanente sobre sua atualidade e recomendando ajustes e inovações sempre que necessários para seu aperfeiçoamento;
- Favorecer a integração interdisciplinar entre as diferentes atividades de ensino-aprendizagem previstas na arquitetura curricular, em consonância com a lógica de flexibilização curricular da UFSB;
- Assessorar o Colegiado do Curso em mudanças estruturais ou transitórias, sempre que demandado;
- Propor políticas e estratégias que garantam atributos como qualidade, criatividade, criticidade e inovação do curso;
- Contribuir para a consolidação do perfil profissional do egresso, considerando as especificidades do sistema de ciclos da UFSB e as competências necessárias para a atuação social, ética e profissional no campo da cibersegurança;
- Zelar pelo cumprimento das Diretrizes Curriculares Nacionais para os cursos de Engenharia.

A composição do NDE do Curso de Engenharia em Cibersegurança inclui:

- O/A Coordenador/a do Curso (membro nato do NDE);
- O/A Vice-Coordenador/a do Curso;
- Três docentes efetivos/as, em regime de dedicação exclusiva, com reconhecida liderança acadêmica, demonstrada por sua produção científica, atuação no desenvolvimento do ensino e contribuição em outras dimensões relevantes para a consolidação do curso.

Essa configuração assegura que o NDE atue de forma colegiada, integrando lideranças acadêmicas capazes de orientar, avaliar e propor continuamente melhorias no desenvolvimento pedagógico e institucional do curso.

13.4 Coordenação de Extensão e Comissão Própria de Assessoria

A regulamentação vigente da UFSB estabelece diretrizes para a integralização e validação das atividades de extensão, em conformidade com as normas institucionais e as resoluções específicas do CONSUNI. No âmbito do Curso de Engenharia em Cibersegurança, o Colegiado do Curso designará um/a Coordenador/a de Extensão, responsável por organizar o planejamento e a oferta curricular relacionada à extensão universitária.

São atribuições do/a Coordenador/a de Extensão do curso:

- Presidir a Comissão Própria de Assessoria;
- Reunir os/as docentes para planejar a oferta das Atividades Curriculares de Extensão (ACEx) e dos Componentes Curriculares de Extensão (CCEx) em cada período letivo;
- Orientar os/as estudantes quanto ao cumprimento obrigatório da creditação em extensão;
- Apoiar a divulgação de editais de fomento e apoio à extensão lançados pela Pró-Reitoria de Extensão e Cultura (PROEX);
- Estimular a integração e a colaboração entre as equipes executoras das diferentes atividades de extensão do curso;
- Aprovar, em conjunto com a Comissão Própria de Assessoria, a creditação de atividades de extensão realizadas fora do escopo direto do curso, desde que atendam aos critérios institucionais.

Para apoiar as atribuições da Coordenação de Extensão, será instituída uma Comissão Própria de Assessoria, com funções específicas de acompanhamento e validação das atividades extensionistas.

São atribuições da Comissão Própria de Assessoria:

- Auxiliar o/a Coordenador/a de Extensão nas atividades de planejamento, acompanhamento e supervisão;
- Realizar a avaliação documental apresentada pelos/as estudantes para a integralização da carga horária obrigatória em extensão;

- Garantir que as atividades credenciadas estejam em conformidade com os eixos temáticos do curso, mantendo a qualidade e a pertinência acadêmica e social da formação extensionista.

A atuação integrada do/a Coordenador/a de Extensão e da Comissão Própria de Assessoria contribui para assegurar que as atividades de extensão:

- Tenham relevância social e acadêmica;
- Promovam impacto positivo na comunidade;
- Atendam ao mínimo de 10% da carga horária total do curso, conforme previsto na legislação e nas normativas internas da UFSB;
- Reforcem o compromisso da Engenharia em Cibersegurança com a formação cidadã, crítica e socialmente referenciada.

14. INFRAESTRUTURA

14.1 Infraestrutura Física

O *Campus* Jequié – Centro Multidisciplinar Ciência e Sociedade (CMCS) – está instalado provisoriamente na antiga sede da Escola Estadual Luiz Navarro de Brito, localizada na Praça Antônio Camilo, no bairro Km3, em Jequié. O terreno possui área total de 1.772,55 m², contemplando ambientes adequados para o funcionamento inicial das atividades acadêmicas, administrativas e extensionistas.

O prédio dispõe de oito salas de aula amplas, todas com piso de alta resistência, cerâmica até a meia altura das paredes, forro de PVC e sistema de ventilação natural reforçado por ar-condicionado. As salas contam com iluminação adequada e janelas em alumínio e vidro, assegurando conforto térmico e luminoso. A presença de instalações elétricas e de internet recentemente renovadas possibilita o uso de recursos multimídia e tecnológicos, apoiando a qualidade das atividades de ensino. Há também uma sala de informática equipada, destinada a práticas de apoio ao ensino, acesso a plataformas digitais e suporte a atividades de pesquisa e extensão.

A infraestrutura administrativa é composta por seis salas destinadas a setores de gestão, coordenação e apoio técnico-administrativo, permitindo o funcionamento organizado das rotinas institucionais. Entre essas salas, destaca-se uma sala de reuniões, adequada para encontros de colegiados, planejamentos acadêmicos e atendimentos administrativos. A existência de uma copa favorece o suporte às equipes técnicas e docentes, contribuindo para a rotina de trabalho e acolhimento da comunidade universitária.

Os sanitários masculinos e femininos, em bom estado de conservação, atendem às necessidades básicas de estudantes, servidores e visitantes. O prédio dispõe ainda de uma guarita de acesso, garantindo maior segurança e controle do fluxo de pessoas, e de área livre externa cimentada, que pode ser utilizada para circulação, convivência e eventos de pequeno porte. Uma área verde ajardinada complementa o espaço, servindo como ambiente de integração e bem-estar para a comunidade acadêmica.

Embora seja uma instalação provisória, o prédio da Escola Luiz Navarro de Brito apresenta condições estruturais sólidas e adaptações recentes, o que garante funcionalidade imediata para abrigar atividades do CMCS. As salas de aula asseguram o início do ciclo formativo dos discentes, enquanto as áreas administrativas e de reuniões oferecem suporte à atuação dos docentes e técnicos, viabilizando a gestão acadêmica e institucional.

As instalações definitivas do *Campus Jequié* estão previstas para serem construídas em área contígua ao Instituto Federal da Bahia (IFBA), no bairro Cidade Nova, em terreno cedido pela instituição. O projeto inclui a construção de blocos pedagógicos, laboratórios multidisciplinares, biblioteca, restaurante universitário, auditório, áreas esportivas e culturais, além de infraestrutura urbana completa (acessos, drenagem, energia e saneamento). Com investimentos estimados em R\$ 60 milhões, as futuras instalações integram o Programa de Aceleração do Crescimento (Novo PAC), assegurando condições ideais de ensino, pesquisa, extensão e assistência estudantil.

14.2 Acervo Bibliográfico

Enquanto o prédio definitivo do Centro Multidisciplinar Ciência e Sociedade (CMCS) é estruturado, o *campus* contará com uma biblioteca em espaço adaptado na Escola Estadual Luiz Navarro de Brito, plenamente integrada ao Sistema de Bibliotecas da UFSB.

O acervo geral encontra-se catalogado no Sistema Pergamum, permitindo consulta por meio do catálogo online de acesso público. Parte dos títulos está disponível em acesso aberto na íntegra, ampliando as possibilidades de estudo remoto. A rede de serviços informatizados garante acesso, compartilhamento e disseminação do conhecimento científico-tecnológico entre docentes e discentes, assegurando apoio ao ensino, à pesquisa e à extensão.

O Sistema de Bibliotecas da UFSB é um órgão complementar vinculado à Reitoria, responsável por coordenar os processos, atividades e recursos das bibliotecas dos *campi* Jorge Amado (Itabuna), Sosígenes Costa (Porto Seguro), Paulo Freire (Teixeira de Freitas) e, agora, do *Campus Jequié*. Seu objetivo principal é oferecer apoio integral às atividades de ensino, pesquisa, extensão, inovação e criação em todos os ciclos de formação acadêmica, garantindo:

- Amplo acesso à informação;
- Disseminação abrangente do conhecimento;
- Promoção ativa da leitura e da cultura científica.

Dessa forma, mesmo em caráter provisório, a biblioteca do CMCS assegura aos/às estudantes e docentes da Engenharia em Cibersegurança um ambiente estruturado e conectado às demandas de formação e investigação acadêmica.

15. CATÁLOGO DE EMENTAS DOS COMPONENTES CURRICULARES

O currículo do Curso de Bacharelado em Engenharia em Cibersegurança é constituído pelos CCs que tem as ementas detalhadas a seguir.

15.1 Componentes Curriculares da Formação Geral

COMPONENTE CURRICULAR: Ambientes Virtuais e Colaborativos de Ensino-aprendizagem				
EIXO TEMÁTICO: FG - Matemática e Computação				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Conhecimentos necessários para o uso de tecnologias digitais no processo de aprendizagem. Ambientes colaborativos e sistemas de gerenciamento de conteúdo digital. Interação e comunicação em ambientes virtuais. Monitoramento de atividades e recursos para avaliação. Produção e desenvolvimento de conteúdos digitais. Tecnologias digitais na universidade: direitos e deveres de estudantes e professores. Ambientes colaborativos mediados por tecnologias digitais: limites e possibilidades.				
BIBLIOGRAFIA BÁSICA: BEHAR, P. A. Modelos pedagógicos em educação a distância. Porto Alegre: ArtMed, 2011. RIBEIRO, A. E. Letramento digital: aspectos sociais e possibilidades pedagógicas. 3ª ed. São Paulo: Autêntica, 2007. TAJRA, S. F. Desenvolvimento de projetos educacionais: mídias e tecnologias. São Paulo: Erica, 2014.				
BIBLIOGRAFIA COMPLEMENTAR: BEHAR, P. A. Competências em educação a distância. Porto Alegre: Penso, 2013. CARMO, V. O. Tecnologias educacionais. São Paulo: Cengage Learning, 2015. FERREIRA, A. R. Comunicação e aprendizagem: mecanismos, ferramentas e comunidades digitais. São Paulo: Erica, 2014. ROSINI, A. M. As novas tecnologias da informação e a educação a distância. 2ª ed. São Paulo: Cengage Learning, 2014. VELOSO, R. Tecnologia da informação e comunicação. São Paulo: Saraiva, 2008.				

COMPONENTE CURRICULAR: Arte e Território				
EIXO TEMÁTICO: FG - Artes e Humanidades na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Discussões em torno dos conceitos de arte, território e paisagem. Modos de atuação das artes na paisagem contemporânea, tendo como enfoque as relações territoriais tratadas pela geografia humana. Presença das artes na investigação acadêmica, na educação, nos saberes e práticas dos povos tradicionais e dos povos marginais ao campo urbano e em pesquisas das humanidades de modo geral.				
BIBLIOGRAFIA BÁSICA: CAUQUELIN, A. A invenção da paisagem. Trad. M. Marcionilo. São Paulo: Martins Fontes, 2007. LAGROU, E. Arte indígena no Brasil: agência, alteridade e relação. Belo Horizonte: C/Arte, 2009. SANTOS, M. Metamorfoses do espaço habitado. 6ª ed. São Paulo: Edusp, 2014.				
BIBLIOGRAFIA COMPLEMENTAR: AUGÉ, M. Não-lugares: introdução a uma antropologia da supermodernidade. Trad. M. L. Pereira. 9ª ed. Campinas: Papirus, 2012. GOMBRICH, E. H. A história da arte. Trad. A. Cabral. 16ª ed. São Paulo: LTC, 2000. NAVARRO, L.; FRANCA, P. (org.). Concepções contemporâneas da Arte. Belo Horizonte: UFMG, 2006. PEIXOTO, N. B. Intervenções urbanas: arte/cidade. 2ª ed. São Paulo: SENAC, 2012. SCHAFER, R. M. A afinação do mundo. Trad. M. T. de O. Fonterrada. 2ª ed. São Paulo: UNESP, 2001.				

COMPONENTE CURRICULAR: Artigo Científico e Exposição Oral				
EIXO TEMÁTICO: FG - Produções Textuais Acadêmicas				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Leitura, compreensão e análise de artigos científicos. Práticas de retextualização a partir de diferentes propósitos comunicativos: do artigo científico à exposição oral.				
BIBLIOGRAFIA BÁSICA: MACHADO, A. R. (coord.); LOUSADA, E.; ABREU-TARDELLI, L. S. Trabalhos de pesquisa: diários de leitura para a revisão bibliográfica. São Paulo: Parábola Editorial, 2007. MARCUSCHI, L. A. Da fala para a escrita: atividades de retextualização. 10. ed. São Paulo: Cortez, 2017. MOTTA-ROTH, D.; HENDGES, G. R. Produção textual na universidade. São Paulo: Parábola Editorial, 2010.				
BIBLIOGRAFIA COMPLEMENTAR: GUSTAVII, B. Como escrever e ilustrar um artigo científico. Trad. M. Marcionilo. São Paulo: Parábola Editorial, 2017. MACHADO, A. R. (coord.); LOUSADA, E.; ABREU-TARDELLI, L. S. Planejar gêneros acadêmicos. São Paulo: Parábola Editorial, 2005. MATTOSO CÂMARA, J. Manual de expressão oral & escrita. 27ª ed. Petrópolis: Vozes, 2010. PRODANOV, C. C.; FREITAS, E. C. de. Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico. 2ª ed. Novo Hamburgo: Feevale, 2013. Disponível em: https://www.feevale.br/institucional/editora-feevale/metodologia-do-trabalho-cientifico---2-edicao RIBEIRO, R. M. A construção da argumentação oral no contexto de ensino. São Paulo: Cortez, 2009.				

COMPONENTE CURRICULAR: Autoria na Produção do Texto Acadêmico				
EIXO TEMÁTICO: FG - Produções Textuais Acadêmicas				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Autoria na produção dialógica do texto escrito. Os usos da palavra do outro: paráfrase, citação e plágio. Processos de revisão e reescrita.				
BIBLIOGRAFIA BÁSICA: KROKOSCH, M.. Autoria e plágio: um guia para estudantes, professores, pesquisadores e editores. São Paulo: Atlas, 2012. PERROTTA, C.. Um texto para chamar de seu: preliminares sobre a produção do texto acadêmico. São Paulo: Martins Fontes, 2004. VIEIRA, F. E.; FARACO, C. A.. Escrever na universidade 1 – fundamentos. São Paulo: Parábola, 2019.				
BIBLIOGRAFIA COMPLEMENTAR: D’ALMEIDA, M.. A revisão do texto: parte integrante do processo de produção textual. São Paulo: Scortecci Editora, 2017. HARTMANN, S. H. G.; SANTAROSA, S. D.. Práticas de escrita para o letramento no ensino superior. Curitiba: InterSaberes, 2015. KOCH, I. V.; ELIAS, V. M.. Escrever e argumentar. São Paulo: Editora Contexto, 2016. QUEIROZ, A. S.. Autoria e produção de texto: uma perspectiva discursiva. São Paulo: Pimenta cultural, 2021. VIEIRA, F. E.; FARACO, C. A.. Escrever na universidade 2 – Texto e discurso. São Paulo: Parábola, 2019.				

COMPONENTE CURRICULAR: Brasil: Cidadania, Democracia e Políticas Públicas				
EIXO TEMÁTICO: FG - Artes e Humanidades na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
45	0	45	CRÉDITOS:	3
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: A construção da cidadania no Brasil: dimensões políticas, sociais, raciais e jurídicas. A Constituição Federal de 1988: Constituição cidadã e democrática. Representação política e participação popular no Brasil. Movimentos sociais, conquista de direitos e participação cidadã. Políticas públicas, Estado e sociedade civil no contemporâneo.				
BIBLIOGRAFIA BÁSICA: AVRITZER, Leonardo. Experiência democrática, sistema político e participação popular. São Paulo: Perseu Abramo, 2013. CARVALHO, José Murilo de. Cidadania no Brasil: o longo caminho. Rio de Janeiro: Civilização Brasileira, 2021, 27a ed. SANTOS, Boaventura Souza; CHAUI, Marilena. Direitos Humanos, Democracia e Desenvolvimento. São Paulo: Cortez, 2013.				
BIBLIOGRAFIA COMPLEMENTAR: ALMEIDA, Silvio Luiz. Racismo estrutural. São Paulo: Pólen, 2019. BENEVIDES, Maria Victoria de Mesquita. Cidadania e Democracia. In: Lua Nova, nº 33, 94. Disponível em: http://www.scielo.br/pdf/ln/n33/a02n33.pdf BONETI, Lindomar Wessler. Políticas Públicas por dentro. Ijuí: Ed. Unijuí, 2018.				

COMPONENTE CURRICULAR: Ciência dos Dados				
EIXO TEMÁTICO: FG - Matemática e Computação				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Tecnologia e sociedade através dos dados. Organização, resumo e apresentação de dados estatísticos. Organização de tabelas. Estatística Descritiva. Noções e distribuição de probabilidade e amostras. Tipos de Variáveis. Entendendo a confiança dos dados. Teste de hipóteses. Introdução aos testes estatísticos. Aplicações na atualidade				
BIBLIOGRAFIA BÁSICA: PINHEIRO, R., CUNHA, G., Estatística Básica, a arte de trabalhar com dados, Editora <i>Campus</i> , 2008. MORETTIN, Pedro A; BUSSAB, Wilton de O. Estatística básica. 9. ed. São Paulo: Saraiva, 2017. DEVORE, J. L., Probabilidade e Estatística para engenharia e ciências, Tradução da 8ª edição americana, Cengage Learning, 2015.				
BIBLIOGRAFIA COMPLEMENTAR: BECKER, J.L. Estatística básica: transformando dados em informação. Porto Alegre: Bookman. 2015. OLIVEIRA, P. H. F. C. Amostragem básica: aplicação em auditoria com práticas em microsoft excel e aql. 2ª ed. Rio de Janeiro: Ciência Moderna, 2014. MOORE, David S. A estatística básica e sua prática. 7. Rio de Janeiro: LTC. 2017. MORETTIN, P. A.; BUSSAB, W. O. Estatística básica. 9ª ed. São Paulo: Saraiva, 2017. TRIOLA, M. F. Introdução à estatística. 12ª ed. Rio de Janeiro: LTC, 2017.				

COMPONENTE CURRICULAR: Ciência e Cotidiano				
EIXO TEMÁTICO: FG - Ciências na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: O que é ciência. Introdução às diversas áreas da ciência. Papel do cientista na sociedade. Cultura científica e cidadania. Análise crítica de temas atuais relacionados à ciência e tecnologia no cotidiano.				
BIBLIOGRAFIA BÁSICA: CHALMERS, A. F. O que é ciência, afinal? Trad. R. Filker. São Paulo: Brasiliense, 1993. FOUREZ, G. A construção das ciências: uma introdução à filosofia e ética das ciências. Trad. L. P. Rouanet. São Paulo: Editora Unesp, 1995. PASTERNAK, N.; ORSI, C. Ciência no cotidiano: Viva a razão. Abaixo a ignorância! São Paulo: Editora Contexto, 2020.				
BIBLIOGRAFIA COMPLEMENTAR: BACHELARD, G. A formação do espírito científico: contribuição para uma psicanálise do conhecimento. Trad. E. dos S. Abreu; A. L. de A. Guerreiro. Rio de Janeiro: Contraponto, 1996. CARNEIRO DA CUNHA, M. Cultura com aspas e outros ensaios. São Paulo: Cosac e Naify, 2009. DAWKINS, R. Desvendando o arco-íris. Trad. R. Eichenberg. 1ª ed. São Paulo: Companhia das Letras, 2000. PINKER, S. O novo iluminismo. Trad. L. T. Motta; P. M. Soares. 1ª ed. São Paulo: Companhia das Letras, 2018. SAGAN, C. O mundo assombrado pelos demônios: a ciência vista como uma vela acesa no escuro. Trad. R. Eichenberg. São Paulo: Companhia das Letras, 1999.				

COMPONENTE CURRICULAR: Ciência, Sociedade e Ética				
EIXO TEMÁTICO: FG - Ciências na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Tipos de conhecimento. Qual a utilidade do conhecimento científico? O método científico e a observação. A ética na produção, aplicação e publicação do conhecimento científico. A relação entre ciência e as transformações da sociedade: desenvolvimento, paradigma biotecnocientífico, biossegurança e pós-modernidade. Proposição das políticas de ciência, tecnologia e inovação: formação de recursos humanos e financiamento de pesquisa. A importância das universidades públicas na produção do conhecimento científico.				
BIBLIOGRAFIA BÁSICA: CLOTET, J. Ciência e ética: onde estão os limites? Episteme, Porto Alegre, n. 10, pp. 23-29, 2000. FEYERABEND, P. A ciência em uma sociedade livre. São Paulo: Ed. Unesp, 2011. VOLPATO, G. Ciência: da filosofia à publicação. São Paulo: Ed. Cultura Acadêmica, 2013.				
BIBLIOGRAFIA COMPLEMENTAR: ALVES-MAZZOTTI, A. J.; GEWANDSZNAJDER, F. O método nas ciências naturais e sociais: pesquisa quantitativa e qualitativa. São Paulo: Pioneira, 1998. BUZZI, A. Introdução ao pensar: o ser, o conhecimento. 35ª ed. São Paulo: Vozes, 2012. COMTE-SPONVILLE, A. A felicidade, desesperadamente. São Paulo: Martins Fontes, 2015. KUHN, T. S. A estrutura das revoluções científicas. São Paulo: Pioneira.1992. OLIVA, A. É a ciência a razão em ação ou ação social sem razão? Scientiae Studia, v. 7, n. 1, pp. 105-134, 2009. SANTOS, B. de S. Um discurso sobre as ciências. 7ª ed. São Paulo: Cortez, 2010.				

COMPONENTE CURRICULAR: Estratégias de Leitura em Língua Espanhola				
EIXO TEMÁTICO: FG - Línguas Estrangeiras				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
45	0	45	CRÉDITOS:	3
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Técnicas e estratégias de leitura de textos em língua espanhola e compreensão de estruturas linguísticas básicas com vistas ao desenvolvimento de habilidades interculturais.				
BIBLIOGRAFIA BÁSICA: AMENDOLA, Roberta. Nuevo Listo: español a través de textos. São Paulo: Moderna, 2012 PINHEIRO-CORREA, Paulo; LAGARE, Xoán Carlos. Confluencia ? Língua Estrangeira moderna ? Espanhol. São Paulo: Moderna, 2018. MATTE BON, Francisco. Gramática comunicativa del español - tomo I. Madrid: Edelsa, 2020.				
BIBLIOGRAFIA COMPLEMENTAR: BRANDÃO, E.; BELINER, C. (trad.). SEÑAS. Diccionario para la enseñanza de la lengua española para brasileños. Universidad de Alcalá de Henares. 3. ed. São Paulo: Editora WMF Martins Fontes, 2010. FRAGO GARCIA, Juan Antonio. Historia del espanol de America: textos y contextos. Madrid: Gredos, 1999. CORPAS, Jaime. Socios 2: nueva edition ? cuaderno de ejercicios. Buenos Aires: Difusion, 2008. COXMAN, Monica. Voces del sur I. Buenos Aires: Suvoces del Sur, 2010. ESPAÑOL LENGUA VIVA 2: libro del alumno. Moderna, 2015.				

COMPONENTE CURRICULAR: Estratégias de Leitura em Língua Inglesa				
EIXO TEMÁTICO: FG - Línguas Estrangeiras				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Técnicas e estratégias de leitura de textos em língua inglesa e compreensão de estruturas linguísticas básicas com vistas ao desenvolvimento de habilidades interculturais.				
BIBLIOGRAFIA BÁSICA: NASH, G. M.; FERREIRA, W. R. Real English. Vocabulário, gramática e funções a partir de textos em inglês. Barueri, SP: Disal, 2010. PASSWORD – English Dictionary for Speakers of Portuguese. 4ª edição. São Paulo: Martins Fontes, 2013. SOUZA, A. G. F. et al. Leitura em Língua Inglesa: uma abordagem instrumental. 2ª edição atualizada. Barueri, SP: DISAL, 2010.				
BIBLIOGRAFIA COMPLEMENTAR: CIRANDA CULTURAL. Dicionário Escolar Português-Inglês / Inglês-Português. Barueri, SP: Ciranda Cultural, 2015. LOPES, M. C. (coord.) Dicionário da Língua Inglesa. Inglês-Português, Português-Inglês. São Paulo: Rideel/Bicho Esperto, 2015. MORAES, R. De C. B. T. de. Ler para compreender textos em inglês: algumas estratégias. São Carlos, SP: UAB-UFSCar, 2014. THOMPSON, M. A. Inglês instrumental: estratégias de leitura para informática e internet. São Paulo: Érica, 2016. TORRES, N. Gramática prática da língua inglesa: o inglês descomplicado. 11ª ed. São Paulo: Saraiva, 2014.				

COMPONENTE CURRICULAR: Ética e Responsabilidade Sócio-ambiental				
EIXO TEMÁTICO: FG - Ciências na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Conceitos e princípios da ética. Ética profissional. Ética na engenharia de produção. Ética nas empresas. Ética na sociedade. Relação entre o social e o ambiental. Responsabilidade socioambiental nas organizações. Legislação e normas relacionadas a ética e responsabilidade socioambiental.				
BIBLIOGRAFIA BÁSICA: BAUMAN, Z. A ética é possível num mudo de consumidores. Rio de Janeiro: Zahar, 2011 SANTOS, F. A.. Ética empresarial política de responsabilidade social em 5 dimenções: sustentabilidade, respeito à multicultural, aprendizado contínuo, inovação, governança corporativa. São Paulo Atlas 2014 TACHIZAWA, T.. Gestão ambiental responsabilidade social corporativa. 9. São Paulo Atlas 2019				
BIBLIOGRAFIA COMPLEMENTAR: ANTONIK, L. R.. Compliance, ética, responsabilidade social e empresarial uma visão prática. Rio de Janeiro Alta Books 2016 DIAS, R.. Gestão ambiental responsabilidade social e sustentabilidade. 3. São Paulo Atlas 2017 WEBER, M. Ética protestante e o espírito capitalista. São Paulo: Companhia das letras, 2004				

COMPONENTE CURRICULAR: Experiência do Sensível				
EIXO TEMÁTICO: FG - Artes e Humanidades na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Construção, análise, diálogo e articulação de experiências sensíveis destinadas a instigar a curiosidade e a formulação de saberes corporalizados. Atravessamentos do tempo, da memória, da cultura e do território por experiências do sensível e pelos modos de subjetivação. Observação de matizes e processos do sensível que tensionam os métodos científicos normativos e fundamentam formas de investigação sobre o mundo.				
BIBLIOGRAFIA BÁSICA: BADIOU, A. Pequeno manual de inestética. Trad. M. Appenzeller. São Paulo: Estação Liberdade, 2002. DUARTE JÚNIOR, J. F. A montanha e o videogame: escritos sobre educação. Campinas, SP: Papirus, 2010. RANCIÈRE, J. A partilha do sensível: estética e política. Trad. M. C. Netto. 2ª ed. São Paulo: Ed. 34, 2009.				
BIBLIOGRAFIA COMPLEMENTAR: AGAMBEN, G. Infância e história – Destruição da experiência e origem da história. Trad. H. Burigo. Belo Horizonte: Editora UFMG, 2005. DIDI-HUBERMAN, G. Sobrevivência dos vaga-lumes. Trad. V. Casa Nova e M. Arbex. Belo Horizonte: Editora UFMG, 2011. GUIMARÃES, C.; MENDONÇA, C.; SOUSA LEAL, B. (org.). Entre o sensível e o comunicacional. Belo Horizonte: Autêntica, 2010. LEVI-STRAUSS, C. O pensamento selvagem. Trad. T. Pelegrini. 12ª ed. Campinas, SP: Papirus, 2012. MATURANA, H.; VARELA, F. A árvore do conhecimento: as bases biológicas da compreensão humana. 9ª ed. São Paulo: Palas Athena, 2011.				

COMPONENTE CURRICULAR: Fundamentos da Computação				
EIXO TEMÁTICO: FG - Matemática e Computação				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Formação Geral	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Como funciona o computador. Em que se baseia. Como se chegou ao computador contemporâneo. Seus sistemas de representação: números binários, cores. Suas operações lógicas e aritméticas. Exemplo de arquitetura e organização de um computador. Para quê um sistema operacional. O algoritmo e suas estruturas. Processo de compilação: do algoritmo às operações. Processo de comunicação em redes. A Internet, a World Wide Web. Muitos dados, o que fazer com eles? Grandes aplicações de Sistemas Inteligentes. Realização de atividades desplugadas e manipulações de objetos no processo de ensino e aprendizagem. Discussão de questões históricas, sociais e filosóficas dos temas tratados.				
BIBLIOGRAFIA BÁSICA: BARICHELO, Leonardo; MORAES, Jéssica B. de; LANCINI, Isabella C.; SANTOS, Marina B. dos. Computação desplugada. 2020. Disponível em: https://desplugada.ime.unicamp.br/. Acesso em 14 de março de 2022. DALE, N.. Ciência da computação. Rio de Janeiro: LTC, 2010. (Disponível em e-book) WEBER, R. F.. Fundamentos de arquitetura de computadores. Vol. 8. Porto Alegre: Bookman, 2012. (Disponível em e-book)				
BIBLIOGRAFIA COMPLEMENTAR: BELL, T.; WITTEN, Ian H.; FELLOWS, Mike. Computer science unplugged. Department of Computer Science, University of Canterbury, Christchurch, New Zealand, 2002. Disponível em: https://www.csunplugged.org/en/. Acesso em: 14 de março de 2022. BROOKSHEAR, J. Glenn. Ciência da computação - uma visão abrangente. 11 ed. Porto Alegre: Bookman, 2013. LÉVY, P.. As tecnologias da inteligência: o futuro do pensamento na era da informática. 2. ed. São Paulo: Ed. 34, 2010. TANENBAUM, A. S.; AUSTIN, T.. Organização estruturada de computadores. 6 ed. Rio de Janeiro: Pearson, 2013. WAZLAWICK, R. S.. História da computação. Rio de Janeiro: GEN, LTC, 2016.				

COMPONENTE CURRICULAR: Fundamentos de Estatística				
EIXO TEMÁTICO: FG - Matemática e Computação				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Leitura e interpretação de textos multimodais (infográficos e tabelas). Estatística descritiva: conceitos fundamentais.				
BIBLIOGRAFIA BÁSICA: DEVORE, J. L. Probabilidade e estatística para engenharia e ciências. 2ª ed. São Paulo: Cengage Learning, 2017. MORETTIN, P. A.; BUSSAB, W. O. Estatística básica. 9ª ed. São Paulo: Saraiva, 2017. TRIOLA, M. F. Introdução à estatística. 12ª ed. Rio de Janeiro: LTC, 2017.				
BIBLIOGRAFIA COMPLEMENTAR: CAMPOS, C. R.; WODEWOTZKI, M. L. L.; JACOBINI, O. R. Educação estatística: teoria e prática em ambientes de modelagem matemática. Belo Horizonte: Autêntica, 2011. COSTA, S. F. Introdução ilustrada à estatística. 5ª ed. São Paulo: Harbra, 2013. GUPTA, B. C.; GUTTMAN, I. Estatística e probabilidade com aplicações para engenheiros e cientistas. Rio de Janeiro: LTC, 2017. NOVAES, D. V.; COUTINHO, C. Q. S. Estatística para educação profissional e tecnológica. 2ª ed. São Paulo: Atlas, 2013. OLIVEIRA, P. H. F. C. Amostragem básica: aplicação em auditoria com práticas em microsoft excel e aql. 2ª ed. Rio de Janeiro: Ciência Moderna, 2014.				

COMPONENTE CURRICULAR: Fundamentos de Matemática				
EIXO TEMÁTICO: FG - Matemática e Computação				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Conhecimentos e raciocínios matemáticos (aritmético, algébrico, proporcional e combinatório). Transição dos temas tratados na educação básica com aplicação de forma contextualizada nas diferentes áreas do conhecimento (Ciências, Humanidades, Saúde, Artes e Educação).				
BIBLIOGRAFIA BÁSICA: BATSCHULET, E. Introdução à matemática para biocientistas. Trad. V. M. A. P. da Silva; J. M. P. de A. Quitete. Rio de Janeiro: Interciência; São Paulo: Universidade de São Paulo, 1978. IEZZI, G.; MURAKAMI, C. Fundamentos de matemática elementar: conjuntos, funções. 9ª ed. São Paulo: Atual, 2013. SILVA, L. M. O.; MACHADO, M. A. S. Matemática aplicada à administração, economia e contabilidade: funções de uma e mais variáveis. São Paulo: Cengage Learning, 2016.				
BIBLIOGRAFIA COMPLEMENTAR: ARAÚJO, U. F.; SASTRE, G. (org.). Aprendizagem baseada em problemas no ensino superior. 3ª ed. São Paulo: Summus, 2016. ÁVILA, G.; ARAÚJO, J. L. L. Cálculo: ilustrado, prático e descomplicado. Rio de Janeiro: LTC, 2015. DEMANA, F. D.; WAITS, B. K.; FOLEY, G. D.; KENNEDY, D. Pré-cálculo. Trad. S. M. Yamamoto. 2ª ed. São Paulo: Pearson, 2013. HOFFMANN, L. D. et al. Cálculo: um curso moderno e suas aplicações. Trad. P. P. de Lima e Silva. 10ª ed. Rio de Janeiro: LTC, 2018. LANDAU, E. Teoria elementar dos números. Trad. G. dos S. Barbosa. Rio de Janeiro: Ciência Moderna, 2002. (Coleção clássicos da matemática)				

COMPONENTE CURRICULAR:			Humanidades, Interculturalidades e Metamorfoses Sociais	
EIXO TEMÁTICO: FG - Artes e Humanidades na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: A construção do conhecimento nas Humanidades. Experimentações de interdisciplinaridade, interculturalidade e territorialidade. Alteridade, diferença e convivência.				
BIBLIOGRAFIA BÁSICA: LARAIA, R. de B. Cultura: um conceito antropológico. 6ª ed. Rio de Janeiro: Zahar, 1992. NUNES, E. (org.) A aventura sociológica: objetividade, paixão, improviso e método na pesquisa social. Rio de Janeiro: Jorge Zahar Editor, 2019. SANTOS, M. Metamorfoses do espaço habitado: fundamentos teórico e metodológico da geografia. 6ª ed. São Paulo: EDUSP, 2014.				
BIBLIOGRAFIA COMPLEMENTAR: HOBSBAWN, E. A era dos extremos: o breve século XX. Trad. M. Santa Rita. 2ª ed. São Paulo: Companhia das Letras, 1995. REIS, J. C. As identidades do Brasil: de Varnhagen a FHC. 9ª ed. Rio de Janeiro: FGV, 2014. SANTOS, B. de S. Um discurso sobre as ciências. 7ª ed. São Paulo: Cortez, 2010. SENNETT, R. O declínio do homem público: as tiranias da intimidade. Trad. L. A. Watanabe. São Paulo: Companhia das Letras, 2014. WHYTE, W. F. Sociedade de esquina: a estrutura social de uma área urbana pobre e degradada. Trad. M. L. de Oliveira. Rio de Janeiro: Jorge Zahar, 2005.				

COMPONENTE CURRICULAR: Introdução à Administração				
EIXO TEMÁTICO: FG - Artes e Humanidades na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Conceitos fundamentais em Administração; funções básicas da administração; funções básicas da organização; as principais correntes do pensamento administrativo; administração, burocracia e processo de burocratização.				
BIBLIOGRAFIA BÁSICA: CHIAVENATO, I.. Introdução à teoria geral da administração. 9. ed. Barueri: Manole, 2014 GUERRINI, F. M.; ESCRIVÃO FILHO, E.; ROSIM, D.. Administração para engenheiros. Rio de Janeiro: Elsevier, 2016 WILLIAMS, C.. ADM - princípios de administração. 2. São Paulo Cengage Learning 2017				
BIBLIOGRAFIA COMPLEMENTAR: CHIAVENATO, I.. Administração geral e pública provas e concursos. 6. Rio de Janeiro Método 2021 MASIERO, G.. Administração de empresas. 3. São Paulo Saraiva 2012 OLIVEIRA, D. P. R.. Administração estratégica na prática a competitividade para administrar o futuro das empresas. 8. São Paulo Atlas 2013 OLIVEIRA, D. P. R.. Fundamentos da administração conceitos e práticas essenciais. São Paulo Atlas 2009				

COMPONENTE CURRICULAR: Introdução à Lógica				
EIXO TEMÁTICO: FG - Matemática e Computação				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Introdução à lógica: proposições, valor lógico, conectivos e tabelas-verdade. Lógica proposicional; Relações de equivalência e de implicação lógica; Lógica de primeira ordem; Técnicas de demonstração; Aplicação de lógica para a computação.				
BIBLIOGRAFIA BÁSICA: MORTARI, C. A.. Introdução à Lógica. 2ª edição, ed. São Paulo, Editora Unesp, 2017. NICOLETTI, M. do C. A Cartilha da Lógica. 3ª edição, ed. LTC, 2017. SILVA, F. S. C. D., FINGER, M., MELO, A. C. V. D. Lógica Para Computação. 2ª edição, ed. Cengage Learning, 2017.				
BIBLIOGRAFIA COMPLEMENTAR: BISPO, C., CASTANHEIRA, L., FILHO, O. Introdução à Lógica Matemática. 1ª edição ed. [S.l.], Cengage Learning, 2011. BOOLOS, G. S., BURGESS, J. P., JEFFREY, R. C., et al. Computabilidade e Lógica. 1ª edição ed. Editora Unesp, 2013. CARNIELLI, W., EPSTEIN, R. L.. Computabilidade, Funções Computáveis, Lógica e os Fundamentos da Matemática. 2ª edição ed. Unesp, 2012. COELHO, R. M.. Introdução à Lógica Matemática. 1ª edição ed. Edição do Autor, 2014. DAGHLIAN, J.. Lógica e Álgebra de Boole. Editora Atlas, 2018.				

COMPONENTE CURRICULAR: Língua Espanhola em Nível Básico				
EIXO TEMÁTICO: FG - Línguas Estrangeiras				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Estudo de estrutura da língua espanhola que levem à comunicação oral e escrita em nível básico. Desenvolvimento do espanhol nas suas diferentes variedades em nível elementar, conforme proposto pelo Quadro Comum Europeu de Referência para o nível A2. Estudo e prática das quatro habilidades comunicativas (compreensão e produção oral e escrita), da tradução e da competência intercultural de forma integrada a partir de situações sociodiscursivas voltadas para as negociações internacionais. Noções de fonética da língua espanhola.				
BIBLIOGRAFIA BÁSICA: FANJUL, Adrian (org.) Gramática y práctica de español. São Paulo: Santillana/Moderna, 2005. GÓMEZ TORREGO, Leonardo. Gramática didáctica del español. São Paulo: SM, 2005. PERIS, Ernesto M.; BAULENAS, Neus S. Gente Hoy 1: Curso de Español. Barcelona: Difusión, 2013.				
BIBLIOGRAFIA COMPLEMENTAR: CORPAS, Jaime et al. Aula internacional 1 PLUS. Difusión: Barcelona, 2021 CASSANY, D. (1995): La cocina de la escritura. Barcelona: Anagrama, 1995 Diccionario Clave. Disponível em: http://clave.smdiccionarios.com/app.php Diccionario RAE. Disponível em: http://www.rae.es/				

COMPONENTE CURRICULAR: Língua Inglesa e Cultura				
EIXO TEMÁTICO: FG - Línguas Estrangeiras				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Introdução às práticas de compreensão e produção oral e escrita da língua inglesa através do uso de estruturas linguísticas e funções comunicativas elementares em uma perspectiva cultural.				
BIBLIOGRAFIA BÁSICA: MILNER, M.; CHASE, R. T.; JOHANNSEN, K. L. World English. Heinle Cengage Learning, 2015. MURPHY, R. Essential Grammar in Use. 3ª ed. Cambridge: CUP, 2004 . SOARS, L.; SOARS J.; HANCOCK, P. Headway, Beginner, 5 th edition. Oxford: Oxford University Press, 2018.				
BIBLIOGRAFIA COMPLEMENTAR: BYRAM, M.; GRUNDY, P. Context and cultures in language teaching and learning. Clevedon: Multilingual Matters, 2003. CRYSTAL, D. English as a Global Language. Cambridge: Cambridge University Press, 1997. NASH, M. G.; FERREIRA, W. R. Real english: vocabulário, gramática e funções a partir de textos em inglês. São Paulo: Disal Editora, 2015. SPENCER-OATEY, H. What is culture? A compilation of quotations. Global PAD Core Concepts, 2012.				

COMPONENTE CURRICULAR: Matemática e Cotidiano				
EIXO TEMÁTICO: FG - Matemática e Computação				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Abordagem lógico-matemática de situações-problema cotidianas, contextualizadas em diferentes realidades socio-histórico-culturais. Números, conjuntos numéricos e sistemas de numeração. Sistemas de Orientação e Medida. Calendários. Operações e instrumentos matemáticos. Análise de fenômenos naturais.				
BIBLIOGRAFIA BÁSICA: Triola, Mario F. Introdução a Estatística. Rio de Janeiro: LTC, 2013. Disponível em: http://www.ebookspdf.org/download/mario-triola-estatistica.html . Acesso em: 8 set. 2014 Cenci, A; Costas, F.A.T. Matemática cotidiana e matemática científica. Ciências & Cognição, v.16, p.127-136, ... 2011 CARNIELLI, Walter A. Pensamento Crítico: o poder da lógica e da argumentação. São Paulo: Ridee. ... 2009				
BIBLIOGRAFIA COMPLEMENTAR: ARAÚJO, U. F.; SASTRE, G. (org.). Aprendizagem baseada em problemas no ensino superior. 3ª ed. São Paulo: Summus. ... 2016 CRAWLEY, Michael J. The R Book. West Sussex: Willey, 2007. Disponível em: http://javanan.moe.gov.ir/getattachment/2b6d2d65-d767-4232-9a62-3ef2ea9245cf/The-R-Book--1-.aspx . Acesso em: 8 set. 2014. SPIEGEL, Murray. Estatística. São Paulo: Mc Graw Hill do Brasil, 1985. Disponível em: http://www.ebookspdf.org/download/estatistica-spiegel.html . Acesso em: 8 set. 2014. LAKATOS, Imre. A Lógica do Descobrimento Matemático. Rio de Janeiro: Zahar. ... 1978 HOFSTADTER, Douglas. Gödel, Escher, Bach: um entrelaçamento de gênios brilhantes. Brasília: Editora da UnB. ... 2001				

COMPONENTE CURRICULAR: Metodologia Científica e Tecnológica				
EIXO TEMÁTICO: FG - Produções Textuais Acadêmicas				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS:				
EMENTA: Introdução à Filosofia da Ciência. A estruturação do Pensamento Científico. Ciência e Pseudociência. Falácias Argumentativas. Conhecimento Científico e outros Tipos de Conhecimentos. A Ciência Contemporânea: Concepção, Características e Divisão. Métodos de Pesquisa. Etapas do Processo de Revisão da Literatura. Habilidades de Redação Científica. Normas de Publicação Científica. Ética na Pesquisa.				
BIBLIOGRAFIA BÁSICA: BARROS, A. J. S., Fundamentos de Metodologia Científica, 3a Ed., Pearson Education, 2007. KOCHE, J. C., Fundamentos de Metodologia Científica ? Teoria da Ciência e Prática da Pesquisa, 32a Ed., Vozes, 2011. MARCONI, M. A. e LAKATOS, E. M., Metodologia Científica, 5a Ed., Atlas, 2007.				
BIBLIOGRAFIA COMPLEMENTAR: SANTOS, J. A. e PARRA FILHO, D., Metodologia Científica, 2a Ed., Cengage, 2012. MAIA, Raquel. G., Ciência, Pós-Ciência, Metaciência ? Tradição, Inovação e Renovação, Editora Livraria da Física, 2011. STOKES, D. E., O Quadrante de Pasteur ? A Ciência Básica e a Inovação Tecnológica, Unicamp, 2009.				

CATALOGO DE EMENTAS

COMPONENTE CURRICULAR: Oficina de Escrita Criativa				
EIXO TEMÁTICO: FG - Produções Textuais Acadêmicas				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
75	0	75	CRÉDITOS:	5
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Introdução à escrita criativa. Autoria e escrita. Gêneros literários. Tipologias textuais: descrição, narração e dissertação. Criação e criatividade. Experimentações com textos narrativos, poéticos, jornalísticos e imagéticos. Avaliação de textos literários. Ateliê de escrita.				
BIBLIOGRAFIA BÁSICA: ADICHIE, Chimamanda Ngozi. O perigo de uma história única. São Paulo: Companhia das Letras, 2019. PROSE, Francine. Ler como um Escritor. Rio de Janeiro: Zahar, 2008. BARTHES, Roland. Aula. Trad. Leyla Perrone-Moisés. São Paulo: Cultrix, 2013.				
BIBLIOGRAFIA COMPLEMENTAR: CHARTIER, Roger. "escutar os mortos com os olhos" In: http://www.scielo.br/pdf/ea/v24n69/v24n69a02.pdf FLUP 2016 - Desde que o samba é samba - Tenda Morangos Mofados https://www.youtube.com/watch?v=DCKpri9PgbA MIGLIAVACCA, Adriano Moraes. Um continente e sua escrita https://estadodaarte.estadao.com.br/um-continente-e-sua-escrita/ REINACH, Fernando. O cérebro não é uma folha de papel em branco. Estado de S. Paulo, 26jun. 2008. p.A-24. SQUARISI, Dad & SALVADOR, Ariete. A arte de escrever bem- um guia para jornalistas e profissionais do texto. São Paulo : Contexto, 2005.				

COMPONENTE CURRICULAR: Oficina de Textos Acadêmicos				
EIXO TEMÁTICO: FG - Produções Textuais Acadêmicas				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Integridade na pesquisa e na escrita científica. Estudos sobre construção frasal, paragrafação, coesão e coerência textuais com base na leitura e produção de gêneros acadêmicos: fichamento, resumo e resenha.				
BIBLIOGRAFIA BÁSICA: MACHADO, A. R. (coord.); LOUSADA, E.; ABREU-TARDELLI, L. S. Planejar gêneros acadêmicos. São Paulo: Parábola Editorial, 2005. MACHADO, A. R. (coord.); LOUSADA, E.; ABREU-TARDELLI, L. S. Resenha. São Paulo: Parábola Editorial, 2004. MACHADO, A. R. (coord.); LOUSADA, E.; ABREU-TARDELLI, L. S. Resumo. São Paulo: Parábola Editorial, 2004.				
BIBLIOGRAFIA COMPLEMENTAR: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6023: informação e documentação – referências – elaboração. Rio de Janeiro, 2002. MARCONI, M. de A.; LAKATOS, E. M. Fundamentos de metodologia científica. São Paulo: Atlas, 2003. MARCUSCHI, L. A. Da fala para a escrita: atividades de retextualização. 10ª ed. São Paulo: Cortez, 2017. MOTTA-ROTH, D.; HENDGES, G. R. Produção textual na universidade. São Paulo: Parábola Editorial, 2010. RESENDE, V. de M.; VIEIRA, V. Leitura e produção de texto na universidade: roteiros de aula. Brasília: EdUNB, 2014. WEG, R. M. Fichamento. São Paulo: Paulistana Editora, 2006.				

COMPONENTE CURRICULAR: Pré-cálculo				
EIXO TEMÁTICO: FG - Matemática e Computação				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Conjuntos numéricos e números reais. Radiciação e potenciação. Polinômios e fatoração. Expressões fracionárias. Equações e inequações. Sistema de coordenadas cartesianas. Funções e suas propriedades. Funções de primeiro e de segundo grau. Funções potência. Funções polinomiais. Funções exponenciais e logarítmicas. Noções de trigonometria e funções trigonométricas. Funções compostas. Uso de ferramentas computacionais.				
BIBLIOGRAFIA BÁSICA: CALDEIRA, A. M; SILVA, L. M. O.; MACHADO, M. A. S. Pré-Cálculo. 2. ed. São Paulo: Cengage Learning, 2010. DEMANA, F. D.; WAITS, K.; FOLEY, G. D.; KENNEDY, D. Pré-Cálculo. 2. ed. São Paulo: Pearson, 2013 IEZZI, G. e DOLCE, O., DEGENSZAJN, D., PERIGO, R. Fundamentos de Matemática Elementar, volume único. 6. ed. São Paulo: Atual, 2019				
BIBLIOGRAFIA COMPLEMENTAR: IEZZI, G.; DOLCE, O. e MURAKAMI, C. Fundamentos de Matemática Elementar, volume 2: Logaritmos. 10. ed. São Paulo: Saraiva, 2019 IEZZI, G.. Fundamentos de Matemática Elementar, volume 1: Conjuntos, Funções. São Paulo: 9. ed. São Paulo: Saraiva, 2019. IEZZI, G.. Fundamentos de Matemática Elementar, volume 3: Trigonometria. 9. ed. São Paulo: Saraiva, 2019 IEZZI, G.. Fundamentos de matemática elementar, volume 6: Complexos, polinômios, equações. 8. ed. São Paulo: Saraiva, 2019 LIMA, E; CARVALHO, P.C.P.; WAGNER, E. E C. A matemática no ensino Médio. Coleção do Professor de Matemática, volumes 1, 2, 3. Sociedade Brasileira de Matemática. Rio de Janeiro, 1999				

COMPONENTE CURRICULAR: Processos Filosóficos e Metodológicos das Ciências				
EIXO TEMÁTICO: FG - Ciências na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Formação Geral	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: O que é Ciência? Mito e Filosofia. Filosofia da Ciência: contribuições epistemológicas dos principais pensadores (Aristóteles, Descartes, Popper, Kuhn, Lakatos, Maturana e Mayr). O paradigma newtoniano-cartesiano. Paradigmas emergentes. Métodos científicos: Como se estrutura o pensamento científico? Regras da lógica argumentativa. Formato padrão dos argumentos. Critérios de validação de argumentos: aceitabilidade, relevância, suficiência e refutabilidade. Ciência e Pseudociência. Falácias argumentativas. Limites do pensamento lógico. Ética e investigação científica.				
BIBLIOGRAFIA BÁSICA: MOREIRA, M.A.; MASSONI, N.T. Epistemologias do século XX: Popper, Kuhn, Lakatos, Laudan, Bachelard, Toulmin, Feyerabend, Maturana, Bohm, Bungem Prigogine, Mayr. São Paulo: E.P.U., 2011, 207p. BUZZI, A. Introdução ao pensar: o ser, o conhecimento. São Paulo: Vozes. 35ª ed., 2010. SANTOS, J. A.; PARRA FILHO, D. Metodologia científica 2. ed. São Paulo: Cengage Learning, 2017. 251p.				
BIBLIOGRAFIA COMPLEMENTAR: DESCARTES, R, Discurso do Método, L& PM Editores, 2005. KANT, I., Crítica da Razão Pura, Ed. Vozes, 2012. KUHN, T. S., A Estrutura das Revoluções Científicas, Ed. Perspectiva, 2010. ALVES-MAZZOTTI, A. J., GEWANDSZNAJDER, F. O método nas ciências naturais e sociais: pesquisa quantitativa e qualitativa. São Paulo: Pioneira, 1998. BOOTH, W.C.; COLOMB, G.G.; WILLIAMS, J.M. A arte da pesquisa. 2ª Edição. São Paulo: Martins Fontes, 2005.				

COMPONENTE CURRICULAR: Saúde Única: Humana, Animal e Ambiental				
EIXO TEMÁTICO: FG - Ciências na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Conceitos básicos, histórico e contemporaneidade. Perspectiva holística, integrativa e interdisciplinar de temas atuais envolvendo Saúde Única e interfaces com a vida e os ecossistemas. Contribuições e impactos nos determinantes sociais, econômicos, culturais, políticos e ambientais dos seres vivos. Educação e tecnologias em Saúde Única.				
BIBLIOGRAFIA BÁSICA: BRONFENBRENNER, U. Bioecologia do desenvolvimento humano: tornando os seres humanos mais humanos. Trad. A. de Carvalho-Barreto. Porto Alegre: Artmed, 2011. GALVÃO, L. A. C.; FINKELMAN, J.; HENAO, S. Determinantes ambientais e sociais da saúde. Rio de Janeiro: Fiocruz, 2011. ROUQUAYROL, M. Z.; SILVA, M. G. C. (org.). Epidemiologia e saúde. 7ª ed. Rio de Janeiro:Medbook, 2013.				
BIBLIOGRAFIA COMPLEMENTAR: COURA, J. R. Dinâmica das doenças infecciosas e parasitárias. 2ª ed., vol. I e II. Rio de Janeiro: Guanabara Koogan, 2013. FORATTINI, O. P. Ecologia, epidemiologia e sociedade. São Paulo: Artes Médicas; Editora da Universidade de São Paulo, 1992. RICKLEFS, R.; RELYEA, R. A economia da natureza. 6ª ed. São Paulo: Guanabara Koogan, 2011.				

COMPONENTE CURRICULAR: Territorialidades e Sustentabilidade no Contexto Regional				
EIXO TEMÁTICO: FG - Artes e Humanidades na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Formação Geral	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
45	0	45	CRÉDITOS:	3
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Estudo de questões socioambientais de relevância planetária e suas incidências no Sul e Extremo Sul da Bahia. Possibilidades de atuação no território de abrangência da UFSB, guiada por reflexão crítica sobre conceitos de desenvolvimento e sustentabilidade, seus limites, contradições e alternativas.				
BIBLIOGRAFIA BÁSICA: MARQUES, Luiz. Capitalismo e colapso ambiental. Campinas: Unicamp, 2018. DOWBOR, Ladislao. O que é poder local. Imperatriz: Ética, 2016. Disponível em: https://dowbor.org/wp-content/uploads/2012/06/Dowbor-_Poder-Local-portal.pdf (acesso em 28/02/23) DILGER, Gerhard; LANG, Miriam; PEREIRA FILHO, Jorge (org.). Descolonizar o imaginário: debates sobre pós-extratativismo e alternativas ao desenvolvimento. São Paulo: Fundação Rosa Luxemburgo, 2016. Disponível em https://rosalux.org.br/wp-content/uploads/2016/08/Descolonizar_o_Imaginario_web.pdf (acesso em 28/02/23)				
BIBLIOGRAFIA COMPLEMENTAR: FURTADO, Celso. O Mito do Desenvolvimento Econômico. Rio de Janeiro, Paz e Terra. 1974. FERREIRA, Joelson e FELÍCIO, Erahsto. Por Terra e território. Arataca: Teia dos Povos, 2021. CANDEIAS, Cezar Nonato Bezerra. MACDONALD, José Brendan e MELO, José Francisco de (org.). Economia solidária e autogestão: ponderações teóricas e achados empíricos. Maceió: Editora da UFAL, 2005. Disponível em: https://www.rededegestoresecosol.org.br/wp-content/uploads/2015/11/livro_economia_solidaria_e_autogestao.pdf (acesso em 28/02/23) BAIARDI, A.; TEIXEIRA, F. O Desenvolvimento dos Territórios do Baixo Sul e do Litoral Sul da Bahia: a Rota da Sustentabilidade, Perspectivas e Vicissitudes, Salvador: Repositório UFBA, 2011.				

COMPONENTE CURRICULAR: Universidade e Sociedade				
EIXO TEMÁTICO: FG - Artes e Humanidades na Formação Cidadã				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Formação Geral	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Presença da Universidade no Ocidente, na América Latina e no Brasil. Universidade e Estado. Universidade e pluralismo dos saberes. Vida estudantil na formação da Universidade e da sociedade.				
BIBLIOGRAFIA BÁSICA: COULON, A. A condição de estudante: a entrada na vida universitária. Trad. G. G. dos Santos; S. M. R. Sampaio. Salvador: EDUFBA, 2008. SANTOS, M. O espaço do cidadão. 7ª ed. São Paulo: Edusp, 2014. TEIXEIRA, A.; FÁVERO, M. L.; BRITTO, J. M. (org.). Educação e Universidade. 2ª ed. Rio de Janeiro: UFRJ, 2010.				
BIBLIOGRAFIA COMPLEMENTAR: ARAÚJO, U. F.; SASTRE, G. Aprendizagem baseada em problemas no ensino superior. 3ª ed. São Paulo: Summus, 2016. FREIRE, P. Pedagogia da autonomia: saberes necessários à prática educativa. 52ª ed. Rio de Janeiro: Paz e Terra, 2015. SANTOS, B. de S. A Universidade no século XXI: para uma reforma democrática e emancipatória da universidade. 3ª ed. São Paulo: Editora Cortez, 2011.				

15.2 Componentes Curriculares Obrigatórios

COMPONENTE CURRICULAR:			Tendências em TI	
EIXO TEMÁTICO:			Computação e Infraestruturas de TI	
PERÍODO DE OFERTA:			1º Semestre	NÚCLEO DE CONTEÚDO: Específico
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA:			Presencial	
PRÉ-REQUISITOS:			-	
EMENTA: Estudo das principais tendências contemporâneas em Tecnologia da Informação (TI) e suas implicações técnicas, sociais e econômicas. Abordagem de tecnologias emergentes como computação em nuvem, inteligência artificial, aprendizado de máquina, big data, internet das coisas (IoT), redes 5G e futuras gerações, blockchain e realidade estendida (XR). Discussão sobre impactos da transformação digital em setores produtivos e na sociedade. Avaliação de cenários futuros e análise crítica de inovações disruptivas, considerando aspectos de segurança, privacidade, ética e sustentabilidade.				
BIBLIOGRAFIA BÁSICA: STAIR, R.; REYNOLDS, G. Princípios de Sistemas de Informação. 13. ed. Cengage Learning, 2020. GARTNER. Hype Cycle for Emerging Technologies 2024. Stamford: Gartner Inc., 2024. SCHWAB, K. A Quarta Revolução Industrial. São Paulo: Edipro, 2016.				
BIBLIOGRAFIA COMPLEMENTAR: NIST. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, 2018. IEEE COMPUTER SOCIETY. IEEE Future Directions: Technology Roadmaps. IEEE, 2022. BROOKS, Jennifer; WHELAN, Karl. Emerging Technologies: AI, IoT, and Beyond. Routledge, 2021. WESTERMAN, G.; BONNET, D.; MCAFEE, A. Leading Digital: Turning Technology into Business Transformation. Harvard Business Review Press, 2014. MIN, H. Artificial Intelligence in Supply Chain Management: Theory and Applications. Springer, 2021.				

COMPONENTE CURRICULAR: Álgebra Linear				
EIXO TEMÁTICO: Matemática				
PERÍODO DE OFERTA: 4º Semestre			NÚCLEO DE CONTEÚDO: Básico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Matrizes e Determinantes. Sistemas de equações lineares. Espaços e Subespaços vetoriais. Dependência e independência linear. Bases. Transformações lineares. Produtos internos. Núcleo e imagem de uma transformação linear. Autovalores e autovetores. Aplicações com o uso de softwares didáticos.				
BIBLIOGRAFIA BÁSICA: ANTON, H.; RORRES, C.. Álgebra Linear com Aplicações. 10. ed. Porto Alegre: Bookman, 2012. POOLE, D. Álgebra Linear: uma introdução moderna. 2. ed. São Paulo: Cengage Learning, 2016. STRANG, G., Álgebra Linear com Aplicações. 1.ed. São Paulo: Cengage Learning, 2010.				
BIBLIOGRAFIA COMPLEMENTAR: BOLDRINI, J. L. Álgebra Linear. 3. ed. São Paulo: Harbra, 1984. CALLIOLI C. C., DOMINGUES H., COSTA R. C. F. Álgebra Linear com Aplicações, Santos: 6a ed. reformulada. Atual Paradidático, 2009. LAY, D. C.; LAY, S. R.; DONALD, J. J. Álgebra Linear e suas Aplicações. 5.ed. São Paulo: LTC, 2018. STEINBRUCH, A.; WINTERLE, P. Álgebra Linear. São Paulo: Makron Books, 1995.				

COMPONENTE CURRICULAR: Aprendizado de Máquina				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 6º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Inteligência Artificial e Análise de Dados Aplicada à Segurança				
EMENTA: Introdução ao aprendizado de máquina e suas aplicações; aprendizado supervisionado: regressão linear e logística, árvores de decisão, máquinas de vetores de suporte (SVM); aprendizado não supervisionado: agrupamento, análise de componentes principais (PCA), redução de dimensionalidade; modelos probabilísticos e Naive Bayes; redes neurais; regularização e generalização de modelos; engenharia de atributos e pré-processamento de dados; avaliação e validação de modelos.				
BIBLIOGRAFIA BÁSICA: IZBICKI, R.; DOS SANTOS, T. M. Aprendizado de máquina: Uma abordagem estatística. UICLAP, 2022. FACELI, K.; LORENA, A. C.; GAMA, J.; ALMEIDA, T. A. D.; CARVALHO, A. C. P. D. L. F. D. Inteligência artificial: Uma abordagem de aprendizado de máquina. 2. ed. Rio de Janeiro, RJ: Ltc-Livros Tecnicos E Cientificos Editora Lda, 2022. 304 p. SERRANO, L. G. Grokking machine learning. Shelter Island: Manning Publications, 2021. 489 p.				
BIBLIOGRAFIA COMPLEMENTAR: PROVOST, F.; FAWCETT, T. Data science para negócios. Alta Books, 2016. MUELLER, J. P.; MASSARON, L.; TORTELLO, J. E. N. Aprendizado de máquina para leigos. Alta Books, 2019. DA SILVA, L. A.; PERES, S. M.; BOSCARIOLI, C. Introdução à mineração de dados - com aplicações em R. GEN LTC, 2016. ASSUNÇÃO, J. V. C. Uma breve introdução à mineração de dados: Bases para a ciência de dados, com exemplos em R. São Paulo, SP: Novatec Editora, 2021. DE CASTRO, L. N.; FERRARI, D. G. Introdução à mineração de dados. Saraiva Uni, 2017. 651 p.				

COMPONENTE CURRICULAR: Aprendizado Profundo				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 7º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Aprendizado de Máquina; Álgebra Linear.				
EMENTA: Introdução ao aprendizado profundo e redes neurais; blocos matemáticos das redes neurais; propagação direta e retropropagação; funções de ativação; regularização e técnicas de batch training; redes neurais convolucionais (CNNs) e aplicações em visão computacional; redes neurais recorrentes (RNNs) e aprendizado para séries temporais e texto; aprendizado profundo para linguagem natural e redes neurais que compreendem linguagem; modelos generativos e aprendizado profundo aplicado; frameworks de deep learning (Keras, TensorFlow); aprendizado federado e melhores práticas para uso real.				
BIBLIOGRAFIA BÁSICA: SILVA, I. N. da; SPATTI, D. H.; FLAUZINO, R. A. Redes neurais artificiais para engenharia e ciências aplicadas: Fundamentos teóricos e aspectos práticos. [s.l.] Artliber, 2019. TRASK, A. Grokking deep learning. New York: Manning, 2019. 336 p. MUELLER, J. P.; MASSARON, L. Aprendizado profundo para leigos. Alta Books, 2020.				
BIBLIOGRAFIA COMPLEMENTAR: GLASSNER, A. Deep learning: A visual approach. San Francisco, CA: No Starch Press, 2021. GOODFELLOW, I.; COURVILLE, A.; BENGIO, Y. Deep learning. Cambridge, Massachusetts: The MIT Press, 2016. 1 p. PRINCE, S. J. D. Understanding deep learning. Cambridge, Massachusetts London, England: MIT Press, 2023. CHOLLET, F.; KALINOWSKI, T.; ALLAIRE, J. j. Deep Learning with R, Second Edition. Shelter Island, NY: Manning Publications Co. LLC, 2022. 568 p.				

COMPONENTE CURRICULAR: Arquitetura de Computadores				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 4º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Programação II				
EMENTA: Fundamentos físicos e químicos dos dispositivos digitais: propriedades elétricas da matéria, semicondutores, circuitos integrados e componentes eletrônicos básicos. Estrutura e organização de computadores: modelo de Von Neumann, unidades funcionais e fluxo de dados. Aritmética computacional: representação numérica e operações. Conjunto de instruções: modos de endereçamento, tipos e formatos de instruções. Unidade de controle e processamento: registradores, barramentos e execução de instruções. Hierarquia de memória: cache, memória principal e memória virtual. Dispositivos de entrada e saída. Pipeline e paralelismo em nível de instrução. Arquiteturas CISC e RISC. Introdução à programação em linguagem de montagem.				
BIBLIOGRAFIA BÁSICA: STALLINGS, W. Arquitetura e Organização de Computadores. 8ª ed. São Paulo: Pearson, 10ª ed. 2017. TANENBAUM, A. S. Organização Estruturada de Computadores. 6ª ed. São Paulo: Pearson, 2015. HENNESSY, J. L.; PATTERSON, D. A. Arquitetura de Computadores: Uma Abordagem Quantitativa. 6ª ed. Rio de Janeiro: GEN LTC, 2019.				
BIBLIOGRAFIA COMPLEMENTAR: WEBER, R. F. Fundamentos de Arquitetura de Computadores. 4ª ed. Bookman, 2012. MONTEIRO, M. A. Introdução à Organização de Computadores. 5ª ed. Rio de Janeiro: LTC, 2014. PATTERSON, D. A.; HENNESSY, J. L. Organização e Projeto de Computadores: A Interface Hardware/Software. 5ª ed. Rio de Janeiro: GEN LTC, 2017. PAIXÃO, R. R. Arquitetura de Computadores: PCs. São Paulo: Érica, 2013. DELGADO, J.; RIBEIRO, C. Arquitetura de Computadores. 5ª ed. Rio de Janeiro: LTC, 2017.				

COMPONENTE CURRICULAR: Análise e Comunicação de Dados				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: 2º Semestre			NÚCLEO DE CONTEÚDO: Básico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: -				
EMENTA: Conceitos fundamentais de dados e informação, destacando as diferenças e a importância de sua distinção. Tipos de dados gerados nas áreas de saúde, segurança, administração e outras. Princípios da ciência aberta. Introdução à análise de dados como suporte à tomada de decisão baseada em evidências. Uso de ferramentas para análise de dados para explorar e manipular dados. Engenharia de prompts para chatbots inteligentes com aplicação prática em gestão, tecnologias e segurança. Técnicas de visualização e comunicação de dados: criação de relatórios, dashboards e apresentações. Aspectos éticos e legais no uso de dados e inteligência artificial. Desenvolvimento de projetos práticos e análise de estudos de caso aplicados a contextos específicos.				
BIBLIOGRAFIA BÁSICA: FINCH, V.. Data analytics for beginners: your ultimate guide to learn and master, data analysis - get your business intelligence right and accelerate growth. 2017. 128 p. SHARDA, R.; DELEN, D.; TURBAN, E.. Business intelligence e análise de dados para gestão do negócio. Bookman Editora, 2019. BAHGA, A.; MADISETTI, V.. Big data science & analytics: a hands-on approach. VPT, 2016.				
BIBLIOGRAFIA COMPLEMENTAR: BENGFORT, B.; KIM, J.. Data analytics with Hadoop: an introduction for data scientists. O'Reilly Media, Inc., 2016. SHARDA, R.; DELEN, D.; TURBAN, E. Business intelligence, analytics, and data science: a managerial perspective. 4th Ed., Pearson, 2018. KITCHIN, R. The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences. SAGE Publications, 2014. MAYER-SCHÖNBERGER, V.; CUKIER, K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt, 2013. GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. Deep Learning. MIT Press, 2016.				

COMPONENTE CURRICULAR: Banco de Dados				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 5º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Estrutura de Dados I.				
EMENTA: Sistemas de Gerência de Bancos de Dados (SGBDs). Conceitos básicos: independência de dados, modelos, abordagem relacional e relacional-orientada a objetos. abordagem relacional: modelo de dados e restrições de integridade, álgebra e cálculo relacional, SQL, normalização e dependências funcionais. Modelagem e projeto de Banco de Dados: modelagem entidade-relacionamento (projeto conceitual), Normalização como técnica de projeto, transformação do modelo conceitual para o relacional (projeto lógico). Aspectos de implementação dos SGBDs: integridade, segurança e privacidade.				
BIBLIOGRAFIA BÁSICA: ELMASRI, R.; NAVATHE, S. B.. Sistemas de Banco de Dados. 1. ed. Pearson Universidades, 2019. MACHADO, F. N. R.. Banco De Dados - Projetos E Implementação. 4ª edição ed. Editora Érica, 2020. SILBERSCHATZ, A., KORTH, H. F., SUDARSHAN, S. Sistema de Banco de Dados. 7ª edição ed. GEN LTC, 2020.				
BIBLIOGRAFIA COMPLEMENTAR: CARDOSO, V., CARDOSO, G. Linguagem SQL: Fundamentos e Práticas. 1ª edição ed. Saraiva Uni - Sob Demanda, 2013. DATE, C. J. Introdução a Sistemas de Bancos de Dados. 1ª edição ed. GEN LTC, 2023. HEUSER, C. A.. Projeto de Banco de Dados: Volume 4. 6ª edição ed. Bookman, 2008. NIELD, T.. Introdução à Linguagem SQL: Abordagem Prática Para Iniciantes. 1ª edição ed. Novatec Editora, 2016. RAMAKRISHNAN, R.; GEHRKE, J.; TANIWAKE, C.; et al.. Sistemas de Gerenciamento de Bancos de Dados. 3ª edição ed. AMGH, 2007.				

COMPONENTE CURRICULAR: Big Data				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 6º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Banco de Dados.				
EMENTA: Big Data: conceitos fundamentais e os 5Vs; tipos de dados: estruturados, semiestruturados e não estruturados; arquiteturas: Hadoop, Spark e armazenamento distribuído (HDFS, Amazon S3); bancos de dados NoSQL: MongoDB e Cassandra; processamento de dados: Pandas, Dask e PySpark; processos ETL: extração, transformação e carregamento; análise exploratória de dados: agregação, resumo e estatísticas descritivas; visualização de dados: Matplotlib, Seaborn e Plotly; computação em nuvem: AWS, Google Cloud e Azure; processamento em tempo real: Kafka e Apache Flink;				
BIBLIOGRAFIA BÁSICA: BAHGA, A.; MADISETTI, V. Big data science & analytics: A hands-on approach. Erscheinungsort nicht ermittelbar: VPT, 2016. 542 p. MAHESHWARI, A. Big data: Essentials. Taylor & Francis Group, 2016. 332 p. MARZ, N.; WARREN, J. Big data: Principles and best practices of scalable realtime data systems. New York: Manning Publications, 2015.				
BIBLIOGRAFIA COMPLEMENTAR: GROLINGER, K.; HIGASHINO, W. A.; TIWARI, A.; CAPRETZ, M. A. Data management in cloud environments: NoSQL and NewSQL data stores. Journal of Cloud Computing: Advances, Systems and Applications, v. 2, n. 1, p. 22, 18 dez. 2013. MONTEIRO, J. M.; BRAYNER, A. R. A.; TAVARES, J. A. What Comes After NoSQL? NewSQL: A New Era of Challenges in DBMS Scalable Data Processing. Em: Tópicos em Gerenciamento de Dados e Informações. Minicursos do XXXI Simpósio Brasileiro de Banco de Dados (SBBBD). Minicursos do XXV Simpósio Brasileiro de Banco de Dados (SBBBD). [s.l.: s.n.].p. 27–56. SOUSA, F. R. C.; MOREIRA, L. O.; DE MACÊDO, J. A. F. Gerenciamento de Dados em Nuvem: Conceitos, Sistemas e Desafios. Em: Tópicos em Sistemas Colaborativos, Interativos, Multimídia, Web e Bancos de Dados. Minicursos do XXV Simpósio Brasileiro de Banco de Dados (SBBBD). WHITE, T. Hadoop: The definitive guide: storage and analysis at internet scale. Beijing Cambridge Farnham Köln Sebastopol Tokyo: O'Reilly Media, 2015.				

COMPONENTE CURRICULAR: Cálculo I				
EIXO TEMÁTICO: Matemática				
PERÍODO DE OFERTA: 2º Semestre			NÚCLEO DE CONTEÚDO: Básico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Limites e continuidade. Derivada de funções de uma variável: Interpretações física e geométrica, propriedades, técnicas de diferenciação. Análise de funções: crescimento, decrescimento, pontos críticos, derivadas de ordem superior e concavidade. Cálculo Integral de funções de uma variável real: o problema das áreas, integral indefinida e definida, Teorema Fundamental do Cálculo. Aplicações ao cálculo de áreas e volumes. Técnicas de integração: integração por substituição, por partes, integrais trigonométricas, integração por substituição trigonométrica. Integrais impróprias.				
BIBLIOGRAFIA BÁSICA: ANTON, H.; BIVENS, I.; DAVIS, S.. Cálculo. 10. ed. Porto Alegre: Bookman, 2014. v. 1. FLEMMING, D. M.; GONÇALVES, M. B.. Cálculo A. 6. ed. São Paulo: Pearson, 2006. STEWART, J.. Cálculo. 8. ed. São Paulo: Cengage Learning, 2017.v. 1.				
BIBLIOGRAFIA COMPLEMENTAR: DEMANA, F. D.; WAITS, K.; FOLEY, G. D.; KENNEDY, D. Pré-Cálculo. 2. ed. São Paulo: Pearson, 2013. FINNEY, R. L.; WEIR, M. D.; GIORDANO, F. R. Cálculo de George B. Thomas Jr. São Paulo: Pearson, 2002.v. 1. GUIDORIZZI, H.. Um Curso de Cálculo. 5. ed. São Paulo: LTC, 2016. v. 1. LEITHOLD, L.. Cálculo com Geometria Analítica. 3. ed. São Paulo: Harbra, 1994. v. 1.				

COMPONENTE CURRICULAR: Cálculo II				
EIXO TEMÁTICO: Matemática				
PERÍODO DE OFERTA: 3º Semestre			NÚCLEO DE CONTEÚDO: Básico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Cálculo I.				
EMENTA: Funções de duas variáveis: definição, domínio e imagem, gráficos de superfícies (planos, esferas, cones, superfícies quádricas). Mapas de contorno, curvas e superfícies de nível. Limites e continuidade. Derivadas parciais. Aproximações lineares e diferenciais. Regra da cadeia. Derivadas direcionais e vetor gradiente. Máximos e mínimos. Extremos condicionados. Integrais duplas em coordenadas retangulares e polares. Integrais triplas em coordenadas retangulares, cilíndricas e esféricas. Mudança de variável. Aplicações ao cálculo de massa, carga, centro de massa, momento de inércia, probabilidade e outras.				
BIBLIOGRAFIA BÁSICA: ANTON, H.; BIVENS, I.; DAVIS, S.. Cálculo. 10. ed. Porto Alegre: Bookman, 2014. v. 2. FLEMMING, D. M.; GONÇALVES, M. B. Cálculo B. 6. ed. São Paulo: Pearson, 2006. STEWART, J.. Cálculo. 8. ed. São Paulo: Cengage Learning, 2017.v. 2.				
BIBLIOGRAFIA COMPLEMENTAR: ANTON, H.; BIVENS, I., e DAVIS, S.. Cálculo. 10. ed. Porto Alegre: Bookman, 2014. v. 1. FLEMMING, D. M.; GONÇALVES, M. B. Cálculo A. 6. ed. São Paulo: Pearson, 2006. GUIDORIZZI, H.. Um Curso de Cálculo. 5. ed. São Paulo: LTC, 2016. v. 2. LEITHOLD, L.. Cálculo com Geometria Analítica. 3. ed. São Paulo: Harbra, 1994. v. 1, 2. STEWART, J.. Cálculo. 8. ed. São Paulo: Cengage Learning, 2017.v. 1.				

COMPONENTE CURRICULAR: Laboratório de Projeto I				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: 2º Semestre			NÚCLEO DE CONTEÚDO: Básico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
15	15	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Conceituação de projeto. Estrutura de um projeto: objetivos e metas, justificativa, materiais e métodos, equipe, orçamento, cronograma de execução. Buscas bibliográficas usando terminologia/vocabulário controlado (Descritores em Ciências da Saúde [DeCS] e Medical Subject Headings [MeSH]). Fases de um projeto: definição do objeto, pesquisa bibliográfica, amostra, coleta e análise de dados. Ferramentas de gestão de projeto. Ferramentas para gerenciamento eletrônico de citações e referências. Ética na pesquisa científica e boas práticas de publicação. Plataforma Brasil. Formas de apresentação dos resultados. Redação técnica.				
BIBLIOGRAFIA BÁSICA: GRAY, D. E.. Doing research in the real world. 5th ed. SAGE Publications, 2022. MINAYO, M. C. S.; DESLANDES, S. F.; GOMES, R. Pesquisa social: teoria, método e criatividade. Vozes, 2025. CRESWELL, J. W.; CRESWELL, J. D. Research design: qualitative, quantitative, and mixed methods approaches. 6th ed. SAGE Publications, 2022				
BIBLIOGRAFIA COMPLEMENTAR: KUMAR, R. Research methodology: a step-by-step guide for beginners. Sage Publications, 2014. SCHILLING, M. A. Strategic management of technological innovation. McGraw-Hill Education, 2016. PMI. Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK®). 7. ed. Project Management Institute, 2021. LAKATOS, E. M.; MARCONI, M. A. Metodologia do Trabalho Científico: Projetos de Pesquisa e Relatórios. 9. ed. Atlas, 2021. HARRIS, M.; TAYLOR, G.; TAYLOR, R. Medical Statistics Made Easy. 4. ed. CRC Press, 2019.				

COMPONENTE CURRICULAR: Laboratório de Projeto II				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: 3º Semestre			NÚCLEO DE CONTEÚDO: Básico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
15	15	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Laboratório de Projeto I				
EMENTA: Definição de temas relevantes de projetos. Escolha de equipes. Elaboração de projetos. Normas técnicas de apresentação de trabalhos científicos. Uso de inteligência artificial na metodologia científica: ferramentas e aplicações. Seminários para apresentação das propostas. Execução e acompanhamento dos projetos. Relatórios finais. Seminários com apresentação dos resultados.				
BIBLIOGRAFIA BÁSICA: GRAY, D. E.. Doing research in the real world. 5th ed. SAGE Publications, 2022. SCHILLING, M. A.. Strategic management of technological innovation. McGraw-Hill Education, 2016. GIL, A. C.. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2017. 192 p.				
BIBLIOGRAFIA COMPLEMENTAR: CRESWELL, J. W.; CRESWELL, J. D.. Research design: qualitative, quantitative, and mixed methods approaches. 6th ed. SAGE Publications, 2022. MINAYO, M. C. S.; DESLANDES, S. F.; GOMES, R.. Pesquisa social: teoria, método e criatividade. Vozes, 2025. PMI. Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK®). 7. ed. Project Management Institute, 2021. LAKATOS, E. M.; MARCONI, M. A. Metodologia do Trabalho Científico: Projetos de Pesquisa e Relatórios. 9. ed. Atlas, 2021. KUMAR, R. Research methodology: a step-by-step guide for beginners. Sage Publications, 2014.				

COMPONENTE CURRICULAR: Estágio Obrigatório				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
0	160	160	CRÉDITOS:	-
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Tem por objetivo complementar e aperfeiçoar o ensino técnico-científico desenvolvendo os conhecimentos adquiridos através da vivência profissional na respectiva área de atividade. Esta integração com a teoria e a prática profissional proporcionará avaliar as habilidades profissionais diante das situações reais e de problemas encontrados na sociedade visando uma melhor integração entre a Universidade e a comunidade. Habilita avaliar as atividades práticas diante de situações reais, permitindo definir melhor suas preferências profissionais. O estágio obrigatório será acompanhado pelo professor orientador e supervisor que promoverão a atualização e o ajustamento do ensino a presentes e reais necessidades.				

COMPONENTE CURRICULAR: Estatística para Análises de Segurança I				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 3º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: -				
EMENTA: Estatística descritiva, probabilidade e distribuições de dados. Aplicação de conceitos estatísticos para análise de riscos. Conceitos fundamentais de estatística descritiva: medidas de tendência central e dispersão. Visualização de dados (histogramas, boxplots, violinplots). Distribuições de probabilidade e variáveis aleatórias (binomial, normal, exponencial). Modelagem de dados para identificação de padrões. Introdução à estatística inferencial: estimativas e intervalos de confiança. Ferramentas computacionais para estatística (Excel, Matplotlib, Python com pandas). Aplicações na análise de logs e detecção de anomalias.				
BIBLIOGRAFIA BÁSICA: MONTGOMERY, D. C.; RUNGER, G. C. Estatística Aplicada e Probabilidade para Engenheiros. 7a ed. Rio de Janeiro: LTC, 2021. DEVORE, J. L. Probabilidade e Estatística para Engenharia e Ciências. 8a ed. Cengage Learning, 2014. ROSS, S. M. Introduction to Probability and Statistics for Engineers and Scientists. 6th ed. Academic Press, 2020.				
BIBLIOGRAFIA COMPLEMENTAR: TRIVEDI, K. S. Probability and Statistics with Reliability, Queuing, and Computer Science Applications. 2nd ed. Wiley, 2016. WALPOLE, R. E.; MYERS, R. H.; MYERS, S. L.; YE, K. E. Probability & Statistics for Engineers & Scientists. 9th ed. Pearson, 2011. MOORE, D. S.; McCABE, G. P.; CRAIG, B. A. Introduction to the Practice of Statistics. 9th ed. W. H. Freeman, 2016. TAN, P. N.; STEINBACH, M.; KUMAR, V. Introduction to Data Mining. 2nd ed. Pearson, 2018. VANDERPLAS, J. Python Data Science Handbook: Essential Tools for Working with Data. O’Reilly, 2016.				

COMPONENTE CURRICULAR: Estatística para Análises de Segurança II				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 4º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Estatística para Análises de Segurança I				
EMENTA: Estatística inferencial, análise de regressão e testes de hipóteses aplicados à segurança digital. Testes de hipóteses e análise de variância. Regressão linear e logística na identificação de padrões de ataque. Séries temporais para análise de eventos de segurança. Algoritmos estatísticos para detecção de intrusões. Introdução a aprendizado de máquina com métodos estatísticos. Ferramentas computacionais para estatística aplicada à cibersegurança (SciPy, statsmodels, scikit-learn). Estudo de casos reais com estatística aplicada. Simulação de cenários baseados em dados.				
BIBLIOGRAFIA BÁSICA: HASTIE, T.; TIBSHIRANI, R.; FRIEDMAN, J. The Elements of Statistical Learning: Data Mining, Inference, and Prediction. 2nd ed. Springer, 2009. WASSERMAN, L. All of Statistics: A Concise Course in Statistical Inference. Springer, 2004. MURPHY, K. P. Machine Learning: A Probabilistic Perspective. MIT Press, 2012.				
BIBLIOGRAFIA COMPLEMENTAR: GERON, A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. 3rd ed. O’Reilly, 2022. BISHOP, C. M. Pattern Recognition and Machine Learning. Springer, 2006. STEWART, W. J. Probability, Markov Chains, Queues, and Simulation: The Mathematical Basis of Performance Modeling. Princeton University Press, 2009. BARBER, D. Bayesian Reasoning and Machine Learning. Cambridge University Press, 2012. AGGARWAL, C. C. Outlier Analysis. 2nd ed. Springer, 2017.				

COMPONENTE CURRICULAR: Estrutura de Dados I				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 4º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
15	15	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Programação II.				
EMENTA: Algoritmos de Ordenação; Conceitos Básicos de Complexidade; Recursão; Listas; Pilhas; Filas.				
BIBLIOGRAFIA BÁSICA: CORMEN, T. T.. Algoritmos: Teoria e Prática. 3. ed. Rio de Janeiro: GEN LTC, 2012. DROZDEK. Estrutura de Dados e Algoritmos em c++. 2ª edição ed. Cengage Learning, 2016. SZWARCFITER, J. L., MARKENZON, L. Estruturas de Dados e Seus Algoritmos. 3ª edição ed. LTC, 2010.				
BIBLIOGRAFIA COMPLEMENTAR: ASCENCIO, A. F. G., ARAÚJO, G. S. Estruturas de Dados: algoritmos, análise da complexidade e implementações em JAVA e C/C++. 1ª edição ed. Pearson, 2015. CELES, W. Introdução a Estruturas de Dados - Com Técnicas de Programação em C. 2º edição ed. GEN LTC, 2022. PUGA, S., RISSETTI, G. Lógica de Programação e Estruturas de Dados. 3ª edição ed. Pearson Universidades, 2016. TENENBAUM, A. M., LANGSAM, Y., AUGENSTEIN, M. J. Estruturas de Dados Usando C. 1ª edição ed. Pearson Universidades, 1995. WENGROW, J.. A Common-Sense Guide to Data Structures and Algorithms, Second Edition: Level Up Your Core Programming Skills. 2nd ed. edição ed. Raleigh, North Carolina, Pragmatic Bookshelf, 2020.				

COMPONENTE CURRICULAR: Estrutura de Dados II				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 5º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Estrutura de Dados I.				
EMENTA: Árvores binárias. Árvores de busca. Árvores balanceadas; Algoritmos para manipulação de estruturas: inserção, remoção, busca e percurso; Filas com prioridades; e Tabela Hash.				
BIBLIOGRAFIA BÁSICA: CORMEN, T. H.; LEISERSON, C. E.; RIVEST, R. L.; AL, et. Algoritmos. RIO DE JANEIRO, RJ: GEN LTC, 2024. DROZDEK. Estrutura de dados e algoritmos em c++. Cengage Learning, 2016. ZIVIANI, N. Projeto de algoritmos com implementações em pascal E C, 3ª ed. Rev. E ampl. Cengage Learning, 2010.				
BIBLIOGRAFIA COMPLEMENTAR: BACKES, A. R. Algoritmos e estruturas de dados em linguagem C. RIO DE JANEIRO, RJ: LTC, 2022. BHARGAVA, A. Y. Entendendo algoritmos: Um guia ilustrado para programadores e outros curiosos. [s.l.] Novatec Editora, 2017. CORMEN, T. H.; LEISERSON, C. E.; RIVEST, R. L.; STEIN, C. Introduction to algorithms, fourth edition. Cambridge, Massachusetts London: MIT Press, 2022. PREISS, B. R. Estruturas de dados e algoritmos. Elsevier, 2001. SEDGEWICK, R.; WAYNE, K. Algorithms. Upper Saddle River: Addison-Wesley Professional, 2011.				

COMPONENTE CURRICULAR: Design Thinking para Soluções de Segurança				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 4º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
15	15	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Metodologias de Design Thinking aplicadas à criação de soluções de segurança cibernética. Fundamentos, etapas e ferramentas do Design Thinking: empatia, definição, ideação, prototipagem e testes. Mapeamento de problemas e oportunidades (persona, jornada do usuário). Aplicação do Design Thinking à cibersegurança e ao desenvolvimento de soluções inovadoras e seguras. Sustentabilidade e impactos ambientais da infraestrutura digital: princípios de Green IT, eficiência energética em data centers e design ecológico de soluções tecnológicas. Prototipagem rápida e validação de ideias. Colaboração e trabalho em equipe multidisciplinar. Análise de casos reais e uso de ferramentas de design aplicadas à segurança (como Figma e Miro).				
BIBLIOGRAFIA BÁSICA: BERNARDA, Greg; OSTERWALDER, Alex. Value Proposition Design: Como construir propostas de valor inovadoras. HSM Editora, 2014. BROWN, Tim et al. Design thinking: uma metodologia poderosa para decretar o fim das velhas ideias. Rio de Janeiro: Elsevier, 2010. PLATTNER, H.; MEINEL, C.; LEIFER, L. (Orgs.). Design Thinking Research: Building Innovators. Springer, 2015.				
BIBLIOGRAFIA COMPLEMENTAR: MANZINI, E. Design para Inovação e Sustentabilidade: Comunidades Criativas e Organizações Colaborativas e Novas Redes Projetuais. Rio de Janeiro: E-papers, 2008. THACKARA, J. Plano B: O Design e as alternativas viáveis em um mundo complexo. São Paulo: Saraiva, 2008. VASCONCELOS, R. B. B. de.; OLIVEIRA, M. R. G. de. Determinantes da inovação em micro e pequenas empresas: Uma abordagem gerencial. RAE - REVISTA DE ADMINISTRAÇÃO DE EMPRESAS, v. 58, n. 4, July-August, p.349-364, 2018. KELLEY, T.; KELLEY, D. Creative Confidence: Unleashing the Creative Potential Within Us All. Crown Business, 2013. SEDDON, J.; CURTIS, K. Cybersecurity by Design. Routledge, 2019.				

COMPONENTE CURRICULAR: Fundamentos de Cibersegurança				
EIXO TEMÁTICO: Bases da Cibersegurança e Desenvolvimento Seguro				
PERÍODO DE OFERTA: 3º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Princípios básicos de cibersegurança, histórico de ataques e métodos de defesa. Introdução a frameworks de segurança. Histórico e evolução da cibersegurança. Tipos de ameaças cibernéticas (malware, phishing, ransomware, DoS, etc). Identificação e análise de vulnerabilidades. Fundamentos de proteção de dados e sistemas. Conceitos de confidencialidade, integridade e disponibilidade (triade CIA). Tecnologias de segurança: firewalls, antivírus, IDS/IPS. Introdução a frameworks de segurança. Legislação básica relacionada à segurança. Exemplos práticos de ataques cibernéticos. Técnicas básicas de mitigação e prevenção de incidentes.				
BIBLIOGRAFIA BÁSICA: SANTOS, A. R. & FERREIRA, J. R. . Cibersegurança: Fundamentos, Desafios e Estratégias. Editora Elsevier. 2021. KENNES, K. & PEROT, D. Fundamentals of Cyber Security: The Complete Guide for Beginners. Springer. 2020. ZENG, M. & ZHANG, Z. . Introduction to Cybersecurity: Protecting Critical Information. Springer. 2021.				
BIBLIOGRAFIA COMPLEMENTAR: KIZZA, J. M.. Computer Network Security and Cyber Ethics (4a ed.). Springer. 2022. MOURA, F. S., & GOMES, A. F. . Segurança Cibernética: Práticas e Tecnologias para Proteção de Sistemas. Editora Ciência Moderna. 2020. TAVARES, A. & RODRIGUES, C. . Cibersegurança para Iniciantes: Princípios, Riscos e Estratégias de Defesa. Editora Pearson. 2021. ANDERSON, R. . Security Engineering: A Guide to Building Dependable Distributed Systems (3a ed.). Wiley. 2020. STALLINGS, W. Fundamentos de Segurança da Computação: Princípios e Prática. 4. ed. Pearson, 2019.				

COMPONENTE CURRICULAR: Criptografia e Segurança de Dados				
EIXO TEMÁTICO: Bases da Cibersegurança e Desenvolvimento Seguro				
PERÍODO DE OFERTA: 5º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Cálculo II; Álgebra Linear.				
EMENTA: Fundamentos de criptografia, algoritmos de criptografia simétrica e assimétrica. Aplicação em comunicações seguras. História e evolução da criptografia. Algoritmos de criptografia simétrica (AES, DES). Algoritmos de criptografia assimétrica (RSA, ECC). Protocolos de chave pública e privada. Funções hash. Assinaturas digitais e certificados. Segurança em TLS/SSL e VPNs. Práticas de proteção de dados em sistemas críticos. Criptografia aplicada em IoT. Estudos de casos: ataques a criptografia e contramedidas.				
BIBLIOGRAFIA BÁSICA: PRENEEL, B.; PAAR, C.; PELZL, J. Understanding Cryptography: A Textbook for Students and Practitioners. 10a edição, Springer, 2014. STALLINGS, W. Criptografia e Segurança de Redes: Princípios e Práticas. Pearson, 6a edição, 2014. CORMEN, T.; LEISERSON, C.; RIVEST, R.; STEIN, C. Algoritmos - Teoria e Prática. Editora Campus, 2002.				
BIBLIOGRAFIA COMPLEMENTAR: SMART, N. Cryptography Made Simple. Springer, 2016. KATZ, J.; LINDELL, Y. Introduction to Modern Cryptography. CRC Press, 3rd edition, 2020. MAO, W. Modern Cryptography - Theory and practice. Pearson Education, 1st edition, 2004. BASTA, A.; BASTA, N.; BROWN, M. Segurança de computadores e teste de invasão. Cengage Learning; 1a edição, 2014. SHOUP, V. A Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2005.				

COMPONENTE CURRICULAR: Inteligência Artificial e Análise de Dados Aplicada à Segurança				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 5º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Estatística para Análises de Segurança II.				
EMENTA: Introdução à Inteligência Artificial (IA) e análise de dados aplicados à segurança. Análise de dados para detecção de anomalias e ameaças. Redes neurais e deep learning aplicados à segurança cibernética. Aplicações de IA em monitoramento e resposta a incidentes. Sistemas de recomendação e filtragem de conteúdo na segurança cibernética. Uso de big data e IA em sistemas de segurança escaláveis. Ética, privacidade e considerações legais no uso de IA para segurança. Estudo de casos e aplicações reais com uso de ferramentas e frameworks amplamente utilizados.				
BIBLIOGRAFIA BÁSICA: TAVARES, J. R., & SILVA, P. M.. Inteligência Artificial e Análise de Dados na Segurança Cibernética. Editora Atlas. 2021. SILVA, A. M., & LIMA, D. R. . Análise de Dados para Cibersegurança: Técnicas e Aplicações. Editora Saraiva. 2022. ZHAO, J., & LI, Y. . Artificial Intelligence in Cybersecurity: Fundamentals and Applications. Wiley. 2020.				
BIBLIOGRAFIA COMPLEMENTAR: HE, H., & XU, X. . Data Mining and Machine Learning in Cybersecurity. Springer. 2020 COHEN, A., & BASSI, A. . AI and Machine Learning for Cybersecurity: Applications and Techniques. Springer. 2018. ALVES, F. S., & PEREIRA, L. T. . Big Data e Inteligência Artificial na Defesa Cibernética. Editora Elsevier. 2021. GOMES, M. F., & OLIVEIRA, R. M. . Inteligência Artificial e Segurança Cibernética: Soluções e Desafios. Editora Pearson. 2020. ZHANG, Y.; ZHENG, Y.; JIANG, J. Artificial Intelligence for Security. Springer, 2021.				

COMPONENTE CURRICULAR: Física I				
EIXO TEMÁTICO: Física				
PERÍODO DE OFERTA: 2º Semestre			NÚCLEO DE CONTEÚDO: Básico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Medição: grandezas físicas, ordens de grandeza, sistemas de unidades, Algarismos significativos. Vetores: definição, componentes vetoriais, versores, operações com vetores. Movimento retilíneo. Movimentos em duas e três dimensões, Leis de Newton do movimento. Trabalho e Energia Cinética. Energia Potencial e Conservação da Energia. Centro de Massa e Movimento Linear. Rotação de Corpos Rígidos. Torque e Momento Angular.				
BIBLIOGRAFIA BÁSICA: RESNICK, R.; HALLIDAY, D.; KRANE, K. S. Física 1. 5. ed. Rio de Janeiro: LTC, 2015 SERWAY, R. A.. Física para Cientistas e Engenheiros, v. 1: Mecânica. 2. ed. São Paulo: Cengage Learning, 2013. YOUNG, H. D; FREEDMAN, R. A; SEARS, F. W.; ZEMANSKY, M. W.. Física I: mecânica. 14. ed. São Paulo: Pearson, 2016				
BIBLIOGRAFIA COMPLEMENTAR: BREITHAUPT, J.. Física. 4. Rio de Janeiro LTC 2018 CHAVES, A.. Física básica mecânica. Rio de Janeiro LTC 2007 CUTNELL, J. D; JOHNSON, K. W.. Física. 9. ed. Rio de Janeiro: LTC, 2016 JEWETT JUNIOR, J. W; SERWAY, R. A.. Física para cientistas e engenheiros: Mecânica. Rio de Janeiro: Cengage Learning, 2016 NUSSENZVEIG, H. M.. Curso de física básica 1: mecânica. 5. ed. Rio de Janeiro: Blucher, 2013				

COMPONENTE CURRICULAR: Física II				
EIXO TEMÁTICO: Física				
PERÍODO DE OFERTA: 3º Semestre			NÚCLEO DE CONTEÚDO: Básico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Física I; Cálculo I.				
EMENTA: Movimento harmônico simples, Energia no movimento harmônico simples, Aplicações do movimento harmônico simples, O pêndulo simples, O pêndulo físico, Oscilações amortecidas, Tipos de ondas mecânicas, Ondas periódicas, Descrição matemática das ondas, Energia no movimento ondulatório, Ondas Sonoras, Velocidade das ondas sonoras, Intensidade do som, O efeito Doppler, Pressão em um fluido, Fluido em repouso, Escoamento de um fluido, Equação da continuidade, Equação de Bernoulli, Temperatura, Dilatação térmica, Calor e Trabalho, Primeira Lei da Termodinâmica, Gases Ideais, A Segunda Lei de Termodinâmica, Máquinas Térmicas - Ciclo de Carnot, Entropia.				
BIBLIOGRAFIA BÁSICA: RESNICK, R.; HALLIDAY, D.; KRANE, K. S.. Física 2. 5. ed. Rio de Janeiro: LTC, 2017. TIPLER, P. A; MOSCA, G.. Física para cientistas e engenheiros: mecânica, oscilações e ondas, termodinâmica. 6. ed. Rio de Janeiro: LTC, 2016 YOUNG, H. D; FREEDMAN, R. A; SEARS, F. W.; ZEMANSKY, M. W.. Física II: termodinâmica e ondas. 14. ed. São Paulo: Pearson, 2016.				
BIBLIOGRAFIA COMPLEMENTAR: BAUER, W.; WESTFALL, G. D; DIAS, H.. Física para universitários: relatividade, oscilações, ondas e calor. Porto Alegre: AMGH, 2013 CHABAY, R. W.. Física básica matéria e interações, v. 2. 4. Rio de Janeiro LTC 2018 CHAVES, A.. Física Básica: gravitação, fluidos, ondas, termodinâmica. Rio de Janeiro: LTC, 2007 JEWETT JUNIOR, J. W; SERWAY, R. A.. Física para cientistas e engenheiros: oscilações, ondas e termodinâmica. Rio de Janeiro: Cengage Learning, 2011 NUSSENZVEIG, H. M.. Curso de física básica 2: fluidos, oscilações e ondas, calor. 5. ed. Rio de Janeiro: Blucher, 2014				

COMPONENTE CURRICULAR: Geometria Analítica				
EIXO TEMÁTICO: Matemática				
PERÍODO DE OFERTA: 2º Semestre			NÚCLEO DE CONTEÚDO: Básico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Vetores no plano e no espaço. Retas e planos. Posições relativas entre retas e planos. Distâncias e ângulos. Mudança de coordenadas: rotação e translação de eixos. Sistema de coordenadas polares e curvas polares. Cônicas: parábola, circunferência, elipse, hipérbole.				
BIBLIOGRAFIA BÁSICA: BOULOS, P.. Geometria analítica: Um tratamento vetorial. 3. ed. São Paulo: Pearson, 2005. LEITHOLD, L. Cálculo com Geometria Analítica. 3. ed. São Paulo: Harbra, 1994. v. 1. WINTERLE, P. Vetores e Geometria Analítica. 2. ed. São Paulo: Pearson, 2014.				
BIBLIOGRAFIA COMPLEMENTAR: BALDIN, Y. Y.; FURUYA, Y. K. S. Geometria Analítica para Todos e Atividades com Octave e Geogebra. 1. ed. São Carlos: EdufsCar, 2011. FERREIRA, P. C. P. Cálculo e Análise Vetoriais com Aplicações. Rio de Janeiro: Ciência Moderna, 2013, v.1. MACHADO, K. D. Cálculo Vetorial e Aplicações. 1. ed. Ponta Grossa: Toda Palavra Editora, 2014. STEINBRUCH, A.; WINTERLE, P., Geometria Analítica. 1. ed. São Paulo: Pearson, 1987.				

COMPONENTE CURRICULAR: Engenharia de Software Seguro				
EIXO TEMÁTICO: Bases da Cibersegurança e Desenvolvimento Seguro				
PERÍODO DE OFERTA: 6º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Programação Orientada a Objetos; Estrutura de Dados I				
EMENTA: Princípios de engenharia de software aplicados ao desenvolvimento de sistemas seguros.Técnicas de codificação segura. DevSecOps. Security by design. Testes de segurança estático (Static Application Security Testing - SAST) e dinâmico (Dynamic Application Security Testing - DAST).				
BIBLIOGRAFIA BÁSICA: KOHNFELDER, Loren. Designing Secure Software: A Guide for Developers. No Starch Press. 2021. SUEHRING, S. Learning DevSecOps: A Practical Guide to Processes and Tools. O'Reilly Media. 2024. DEOGUN, D. Secure by Design. Manning Publications. 2019.				
BIBLIOGRAFIA COMPLEMENTAR: GRAFF, M. Secure Coding – Principles & Practices: Principles and Practices. O'Reilly Media. 2003. ADKINS, H.; BEYER, B.; et. al. Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems. O'Reilly Media. 2020. JANCA, T. Alice and Bob Learn Secure Coding. Wiley. 2025. WILLIAMS, J.; WICHERS, D. OWASP Top 10: The Ten Most Critical Web Application Security Risks. OWASP Foundation. MYRBACKA, S.; ZACHARIAH, D. DevSecOps: A Leader’s Guide to Producing Secure Software Without Compromising Flow, Feedback and Continuous Improvement. Leanpub, 2021.				

COMPONENTE CURRICULAR: Inteligência em Segurança e Gestão de Ameaças				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 6º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Inteligência Artificial e Análise de Dados Aplicada à Segurança.				
EMENTA: Análise de dados para identificação de ameaças e vulnerabilidades. Gestão proativa de segurança. Introdução à inteligência cibernética e análise de ameaças. Tipos de ameaças: externas e internas. Ferramentas de inteligência em segurança (Threat Intelligence Platforms). Monitoramento de atividades suspeitas em redes. Técnicas de análise de comportamento de atacantes (TTPs). Modelagem de ameaças usando frameworks como MITRE ATT&CK. Estratégias de mitigação e resposta a ameaças. Relatórios de inteligência e comunicação para tomadores de decisão. Previsão de ataques com base em dados históricos. Estudo de casos de ameaças globais e seus impactos.				
BIBLIOGRAFIA BÁSICA: RODDIE, M.; DEYALSINGH, J.; KATZ, G. J. Practical Threat Detection Engineering: A hands-on guide to planning, developing, and validating detection capabilities. 1. ed. Packt Publishing, 2023. ISBN-13: 978-1801076715. THOMAS, P. T. Cyber Defence Strategy using NIST and MITRE ATT&CK Frameworks: A Senior Leader's Guide to Cybersecurity Excellence. 1. ed. Independently published, 2023. ISBN-13: 979-8389788794. KAPLAN, Jeff; HEILAND, Andy. Cyber Threat Intelligence: Leveraging Data for Threat Detection and Response. CRC Press, 2021.				
BIBLIOGRAFIA COMPLEMENTAR: MOTA FILHO, J. E. Análise de Tráfego em Redes TCP/IP: Utilize Tcpcdump na Análise de Tráfegos em Qualquer Sistema Operacional. 1. ed. Novatec, 2013. ISBN-13: 978-8575223758. SEITZ, J.; ARNOLD, T. Black Hat Python – 2a Edição: Programação Python para hackers e pentesters. 1. ed. Novatec, 2024. ISBN-13: 978-8575228890. WENDT, E.; JORGE, H. V. N. Crimes Cibernéticos. Ameaças e Procedimentos de Investigação. 2. ed. Brasport, 2013. ISBN-13: 978-8574526362. SKOULOLOS, Nikos. Threat Hunting with Elastic Stack. Packt Publishing, 2021. COLE, Eric. Cybersecurity Threats, Malware Trends, and Strategies. CRC Press, 2020.				

COMPONENTE CURRICULAR: Projeto e Modelagem de Sistemas Seguros				
EIXO TEMÁTICO: Bases da Cibersegurança e Desenvolvimento Seguro				
PERÍODO DE OFERTA: 7º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Engenharia de Software Seguro				
EMENTA: Técnicas avançadas de modelagem de sistemas com foco em segurança e resiliência. Modelos matemáticos e computacionais. Fundamentos de projeto de sistemas seguros. Modelagem de ameaças e análise de riscos. Princípios de arquitetura segura para sistemas distribuídos. Ferramentas de modelagem de segurança (STRIDE, LINDDUN). Implementação de medidas de proteção em sistemas críticos. Projeto de interfaces seguras para usuários finais. Simulação de sistemas seguros em ambientes ciberfísicos. Análise de custos versus segurança em projetos. Validação de sistemas seguros antes da implantação. Estudos de casos de falhas de segurança em projetos de sistemas seguros.				
BIBLIOGRAFIA BÁSICA: BLOKDYC, G. Security System Design: A Complete Guide. 1. ed. The Art of Service - Security System Design Publishing. ISBN-13: 978-1038803337. OLMSTED, A. Security-Driven Software Development: Learn to analyze and mitigate risks in your software projects. 1. ed. Packt Publishing, 2024. ANDERSON, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. 3ª ed. Wiley, 2020.				
BIBLIOGRAFIA COMPLEMENTAR: NORMAN, T. L. Integrated Security Systems Design: A Complete Reference for Building Enterprise-Wide Digital Security. 2. ed. Butterworth-Heinemann, 2014. ISBN-13: 978-0128000229. SHORTRIDGE, K.; RINEHART, A. Security Chaos Engineering: Sustaining Resilience in Software and Systems. 1. ed. O'Reilly Media, 2023. ISBN-13: 978-1098113827. TROST, H.; SHOSTACK, A. Human-Centered Security: How to Design Systems That Are Both Safe and Usable. 1. ed. Rosenfeld Media, 2024. ISBN-13: 978-1959029090. SALTER, Colleen; et al. LINDDUN Privacy Threat Modeling: Foundations and Practice. Springer, 2022. BISHOP, Matt. Computer Security: Art and Science. 2ª ed. Addison-Wesley, 2018.				

COMPONENTE CURRICULAR: Laboratório de Invasão e Defesa				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 7º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Redes de Computadores II; Sistemas Operacionais.				
EMENTA: Testes práticos de penetração e defesa. Análise de vulnerabilidades em redes e sistemas. Introdução ao ethical hacking e suas aplicações. Reconhecimento e coleta de informações. Exploração de vulnerabilidades em sistemas simulados. Testes de penetração em redes e aplicativos. Ferramentas de pentesting (Nmap, Metasploit, Burp Suite). Técnicas de defesa contra ataques detectados. Análise de logs de segurança. Criação de relatórios de vulnerabilidades. Introdução ao Red Team e Blue Team. Estudo prático de cenários de ataque e defesa.				
BIBLIOGRAFIA BÁSICA: STUTTARD, D.; PINTO, M. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. 2. ed. Wiley Publishing, 2011. ISBN-13: 978-1118026472. WEIDMAN, G. Testes de Invasão: uma Introdução Prática ao Hacking. 1. ed. Novatec Editora, 2014. ISBN-13: 978-8575224076. AYYASWAMY, K.; RAJ A, A.; KATHIRVEL, N. Sistema bancário seguro baseado em cadeia de blocos: Segurança e privacidade. 1. ed. Edições Nosso Conhecimento, 2025. ISBN-13: 978-6208636852.				
BIBLIOGRAFIA COMPLEMENTAR: BALL, C. J. Hacking APIs: Breaking Web Application Programming Interfaces. 1o ed. No Starch Press, 2022. ISBN-13: 978-1718502444. DA SILVA, C. F. G. Técnicas de invasão de sistemas e pentest: práticas detalhadas de hacker ético para os novos profissionais do mercado. 1. ed. Dialética, 2020. ISBN-13: 978-6587403151. MORENO, D. Introdução ao Pentest. 2. ed. Novatec Editora, 2019. ISBN-13: 978-8575228074. MORENO, D. Pentest em Aplicações web. 1. ed. Novatec Editora, 2017. ISBN-13: 978-8575226131. MORENO, D. Pentest em Redes sem fio. 1. ed. Novatec Editora, 2017. ISBN-13: 978-8575224830.				

COMPONENTE CURRICULAR: Análise de Malware e Engenharia Reversa				
EIXO TEMÁTICO: Forense Digital e Defesa de Infraestruturas Críticas				
PERÍODO DE OFERTA: 7º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Sistemas Operacionais				
EMENTA: Técnicas de análise de malware, identificação de comportamento malicioso e engenharia reversa para compreensão de ameaças. Definição e tipos de malware: vírus, worms, trojans, ransomware, adware e botnets. Análise das famílias de malware. Conceitos fundamentais de engenharia reversa. Criação e configuração de sandboxes e máquinas virtuais para análise segura. Técnicas de análise sem execução do malware. Métodos de execução controlada para observação do comportamento do malware. Análise de métodos de ofuscação usados por malwares. Identificação e catalogação de IoCs, como endereços IP, hashes de arquivos e nomes de domínios. Desenvolvimento de patches e contramedidas contra malware analisados. Estudo de Casos Reais.				
BIBLIOGRAFIA BÁSICA: RAINS, T. Cybersecurity Threats, Malware Trends, and Strategies. 1. ed. Packt, 2020. ISBN-13: 9781800205895. WONG, R. Mastering Reverse Engineering: Re-engineer your ethical hacking skills. 1. ed. Packt, 2018. ISBN-13: 9781788835299. BARBIERO, D. R. Implantação de Malwares em Investigações Complexas. 1. ed. Juruá Editora, 2021. ISBN-13: 978-6556057682.				
BIBLIOGRAFIA COMPLEMENTAR: MOHANTA, A. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware. 1. ed. Springer Nature BV, 2021. ISBN-13: 978-1484261927. PINHO FILHO, O. B.; PACHECO, J. E. C. Investigação Criminal Tecnológica - Infiltração por Malware nas Investigações Informáticas. 1. ed. Juruá Editora, 2022. ISBN-13: 978-8536299044. ALI, Mohamed Arezki (org.). Security and Information Technologies with AI, Internet Computing and Big-Data Applications: Proceedings of SITAIBA 2023. Singapore: Springer, 2023. HUANG, Joseph; BHARADWAJ, Sriram. AI Native LLM Security: A Comprehensive Guide to Secure Applications. Birmingham: Packt Publishing, 2024. SAUNDERS, Alex; REED, Joseph. Mastering Malware Analysis: A Malware Analyst’s Practical Cybercrime Guide. Birmingham: Packt Publishing, 2022.				

COMPONENTE CURRICULAR: Computação em Nuvem e Segurança em Ambientes Distribuídos				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 7º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Redes de Computadores II				
EMENTA: Estruturas de computação em nuvem, gerenciamento de segurança e proteção de dados em sistemas distribuídos. Modelos de serviço (IaaS, PaaS, SaaS) e implantação (pública, privada, híbrida). Virtualização e orquestração de recursos. Segurança em ambientes distribuídos: controle de acesso, criptografia, identidade e gerenciamento de chaves. Encriptação e proteção de dados em nuvem. Segurança de contêineres e microsserviços. Ameaças e vulnerabilidades em ambientes distribuídos. Conformidade e regulamentações de segurança. Monitoramento, auditoria e resposta a incidentes em nuvens públicas e privadas. Estudos de casos de violações em serviços de nuvem.				
BIBLIOGRAFIA BÁSICA: ERL, T.; MONROY, E. B. Cloud Computing: Concepts, Technology, Security, and Architecture. 2nd ed. Pearson, 2023. COMER, D. The Cloud Computing Book: The Future of Computing Explained. CRC Press, 2023. STALLINGS, W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Pearson, 2015.				
BIBLIOGRAFIA COMPLEMENTAR: KRUTZ, R. L.; VINES, R. D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley, 2010. GARRISON, J.; NOVA, K. Cloud Native Infrastructure. O'Reilly Media, 2017. DOTSON, C. Practical Cloud Security: A Guide for Secure Design and Deployment. O'Reilly Media, 2019. VEHENT, J. Securing DevOps: Security in the Cloud. Manning, 2018. ANDERSON, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Wiley, 2020.				

COMPONENTE CURRICULAR: Segurança de IA e Mitigação de Riscos				
EIXO TEMÁTICO: Bases da Cibersegurança e Desenvolvimento Seguro				
PERÍODO DE OFERTA: 8º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Aprendizado de Máquina.				
EMENTA: Segurança em sistemas de IA. DevSecOps em sistemas de IA. Gerenciamento de riscos de IA. Vulnerabilidades em soluções baseadas em IA.				
BIBLIOGRAFIA BÁSICA: BASS, L.; et al. Engineering AI Systems: Architecture and Devops Essential. Addison-Wesley Professional. 2025. SAYLES, J. Principles of AI Governance and Model Risk Management: Master the Techniques for Ethical and Transparent AI Systems. Apress. 2024. REZNIK, L. Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security. Wiley-IEEE Press. 2021.				
BIBLIOGRAFIA COMPLEMENTAR: SANTOS, O.; RADANLIEV, P. Beyond the Algorithm: AI, Security, Privacy, and Ethics. Addison-Wesley Professional. 2024. HUANG, K.; et. al. Generative AI Security: Theories and Practices. Springer. 2024. BRENES, J. AI Security for Businesses: Comprehensive Protection in the Age of Artificial Intelligence. Independently Published. 2025. SOTIROPOULOS, J. Adversarial AI Attacks, Mitigations, and Defense Strategies: A cybersecurity professional's guide to AI attacks, threat modeling, and securing AI with MLSecOps. Packt Publishing. 2024. SOOD. A. Combating Cyberattacks Targeting the AI Ecosystem: Assessing Threats, Risks, and Vulnerabilities. Mercury Learning and Information. 2024.				

COMPONENTE CURRICULAR: Programação I				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 2º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: -				
EMENTA: Noções de raciocínio computacional. Introdução ao desenvolvimento de algoritmos usando uma linguagem de programação estruturada. Construção de programas: variáveis, constantes, operadores aritméticos, expressões aritméticas, estruturas de controle (atribuição, sequência, seleção, repetição). Uso de raciocínio computacional para solução de problemas interdisciplinares.				
BIBLIOGRAFIA BÁSICA: DEITEL, H. M.. C++: Como Programar. 5ª edição ed. Pearson Universidades, 2006. MANZANO, J. A. N. G. Programação de Computadores com C/C++. 1ª edição ed. Editora Érica, 2014. ZIVIANI, N. Projeto de Algoritmos com Implementação em Java e c++. 1ª edição ed. Cengage Learning, 2006.				
BIBLIOGRAFIA COMPLEMENTAR: DROZDEK. Estrutura de Dados e Algoritmos em c++. 2ª edição ed. Cengage Learning, 2016. LIPPMAN, S. B., LAJOIE, J., MOO, B. E. C++ Primer. 5th Revised ed. edição ed. Upper Saddle River, NJ, Addison-Wesley Professional, 2012. MEYERS, S.. C++ Eficaz: 55 Maneiras de Aprimorar seus Programas e Projetos. 3ª edição ed. Bookman, 2011. PRESS, W. H.; TEUKOLSKY, S. A.; VETTERLING, W. T.; et al.. Métodos Numéricos Aplicados: Rotinas em C++. 3ª edição ed. Bookman, 2011. SOUZA, M. A. F.; GOMES, M. M.; SOARES, M. V.; et al.. Algoritmos e Lógica de Programação. 3ª edição ed. Cengage Learning, 2019.				

COMPONENTE CURRICULAR: Programação II				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 3º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Programação I.				
EMENTA: Uso de uma linguagem de programação estruturada; Estruturas Estáticas: Vetores, Matrizes e Strings; Construção de programas: modularização (função, procedimento e bibliotecas); Passagem de parâmetros; Arquivos.				
BIBLIOGRAFIA BÁSICA: DEITEL, H. M.. C++: Como Programar. 5ª edição ed. Pearson Universidades, 2006. MANZANO, J. A. N. G. Programação de Computadores com C/C++. 1ª edição ed. Editora Érica, 2014. ZIVIANI, N. Projeto de Algoritmos com Implementação em Java e c++. 1ª edição ed. Cengage Learning, 2006.				
BIBLIOGRAFIA COMPLEMENTAR: DROZDEK. Estrutura de Dados e Algoritmos em c++. 2ª edição ed. Cengage Learning, 2016. LIPPMAN, S. B., LAJOIE, J., MOO, B. E. C++ Primer. 5th Revised ed. edição ed. Upper Saddle River, NJ, Addison-Wesley Professional, 2012. MEYERS, S.. C++ Eficaz: 55 Maneiras de Aprimorar seus Programas e Projetos. 3ª edição ed. Bookman, 2011. PRESS, W. H.; TEUKOLSKY, S. A.; VETTERLING, W. T.; et al.. Métodos Numéricos Aplicados: Rotinas em C++. 3ª edição ed. Bookman, 2011. SOUZA, M. A. F.; GOMES, M. M.; SOARES, M. V.; et al.. Algoritmos e Lógica de Programação. 3ª edição ed. Cengage Learning, 2019.				

COMPONENTE CURRICULAR: Programação Orientada a Objetos				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 5º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Estrutura de Dados I.				
EMENTA: Elementos básicos de uma linguagem de programação orientada a objetos; Introdução à Orientação a Objetos; Encapsulamento; Construtores e Destrutores; Sobrecarga de operadores; Herança, Polimorfismo e Classes Abstratas; Tratamento de exceções; Coleções (Containers); Interfaces gráficas; Implementação de pequenos projetos usando OO.				
BIBLIOGRAFIA BÁSICA: KOFFMAN, E. B.; WOLFGANG, P. A. T. Objetos, Abstração, Estrutura de Dados e Projeto Usando C++. 1ª edição ed. LTC, 2008. DEITEL, H. M.. C++: Como Programar. 5ª edição ed. Pearson Universidades, 2006. GAMMA, E., HELM, R., JOHNSON, R., et al. Padrões de Projetos: Soluções Reutilizáveis de Software Orientados a Objetos. 1ª edição ed. Bookman, 2000.				
BIBLIOGRAFIA COMPLEMENTAR: FOWLER, M.. UML Essencial: Um Breve Guia para a Linguagem-Padrão de Modelagem de Objetos. 3ª edição ed. Bookman, 2005. GÓES, W. M. Aprenda UML por Meio de Estudos de Caso. 1ª edição ed. Novatec Editora, 2014. JR, O. S.. Introdução à Orientação a Objetos com C++ e Python: Uma abordagem prática. 1ª edição ed. Novatec Editora, 2017. MCLAUGHLIN, B.. Use A Cabeça Análise E Projeto Orientado ao Objeto. 1ª edição ed. Alta Books, 2008. PIZZOLATO, E. B.. Introdução à Programação Orientada a Objetos com C++ e Java. 1ª edição ed. EdUFSCar, 2021.				

COMPONENTE CURRICULAR: Redes de Computadores I				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 5º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: -				
EMENTA: Características Gerais e Aplicações: Estruturas Topologias e Meios de Transmissão; Protocolos de Comunicação; Departamento dos Níveis do Modelo OSI da ISSO; Análise de Algumas Redes do Ponto de Vist do Modelo OSI; Sistemas Operacionais para Redes: Desempenho, Custos e Segurança em Redes de Computadores: Aspectos de LAN’S, MAN’S e WAN’S; Estudos de Casos. Redes Novell. Redes TCP/IP. Redes ATM. Gerenciamento de Redes de Computadores: Aspectos da Gerência de Redes. Segurança em Redes de Computadores. Ferramentas para Gerenciamento de Redes.				
BIBLIOGRAFIA BÁSICA: TANENBAUM, Andrew S. COMPUTER NETWORKS. 3 ed. Prentice Hall, 1996. 813 pág. SOARES, Luiz F. G.; LEMOS, Guido; COLCHER, Sérgio. REDES DE COMPUTADORES Das LANs, MANs e WANs às Redes ATM. 2 ed. Editora CAMPUS, 1995. 705 pág. STALLINGS, William. DATA AND COMPUTER COMMUNICATIONS. 5 ed. Prentice Hall, 1996. 798 pág				
BIBLIOGRAFIA COMPLEMENTAR: KUROSE, James F.; ROSS, Keith W. Computer Networking: A Top-Down Approach. 8. ed. Boston: Pearson, 2021. FOROUZAN, Behrouz A. Data Communications and Networking. 6. ed. McGraw-Hill Education, 2018. COMER, Douglas E. Internetworking with TCP/IP Volume One: Principles, Protocols, and Architecture. 5. ed. Pearson, 2018. SCARFONE, Karen; MELL, Peter; COMPAGNO, Lisa. Guide to Network Security: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-41 Rev. 1. Gaithersburg: NIST, 2022. FILHO, J. E. M. Análise de tráfego em redes TCP/IP: Utilize tcpdump na análise de tráfegos em qualquer sistema operacional. Novatec Editora, 2013.				

COMPONENTE CURRICULAR: Redes de Computadores II				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 6º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Redes de Computadores I				
EMENTA: Introdução a redes de computadores. Conceituação de topologias de redes. Caracterização e análise de tecnologias (software e hardware) de redes de computadores. Caracterização e análise do modelo de referência TCP/IP. Caracterização e análise dos tipos de redes. Caracterização e análise de tecnologias de interconexão de redes. Caracterização e análise de aspectos de segurança.				
BIBLIOGRAFIA BÁSICA: COMER, D. E. Redes de Computadores, Porto Alegre, 2001: Bookman. GIBSON, Jerry D. The Communications Handbook. [S.l.]: CRC Press, 1997. 1598 p. TANNENBAUM, A. S. Redes de Computadores, Rio de Janeiro, 1997: Campus.				
BIBLIOGRAFIA COMPLEMENTAR: KUROSE, James F.; ROSS, Keith W. Computer Networking: A Top-Down Approach. 8. ed. Boston: Pearson, 2021. TANENBAUM, Andrew S.; WETHERALL, David J. Computer Networks. 6. ed. Boston: Pearson, 2019. FOROUZAN, Behrouz A. Data Communications and Networking. 6. ed. New York: McGraw-Hill Education, 2018. STALLINGS, William. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Pearson, 2017. CONTI, Mauro; DEGHANTANHA, Ali; FRANÇA, Francisco A. (Org.). Cybersecurity: Advances in Network Security and Threats. Cham: Springer, 2020.				

COMPONENTE CURRICULAR: Simulações e Gamificação em Ambientes Seguros				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 8º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial.				
PRÉ-REQUISITOS: Laboratório de Invasão e Defesa; Inteligência em Segurança e Gestão de Ameaças.				
EMENTA: Utilização de jogos e simulações para treinamento e avaliação de cenários de segurança. Conceitos de gamificação e sua aplicação em cibersegurança. Planejamento de cenários de ataque e defesa cibernética. Ferramentas e plataformas para simulação de ataque e defesa (Cyber Range, Capture The Flag - CTF).Desenvolvimento de jogos educacionais para segurança. Avaliação de habilidades em ambientes simulados.Modelagem de cenários em infraestruturas críticas. Estratégias de resposta a incidentes simulados.Estudos de caso baseados em ataques históricos.				
BIBLIOGRAFIA BÁSICA: KIM, S.; SONG, K.; LOCKEE, B.; BURTON, J. Gamification in Learning and Education: Enjoy Learning Like Gaming. Springer, 2018. LELEWSKI, R.; HOLLENBERGER, J. Cybersecurity Tabletop Exercises: From Planning to Execution. No Starch Press, 2024. ADARE, S.; SILVA, N. Gamification in Higher Education: A How-To Instructional Guide. Routledge, 2023.				
BIBLIOGRAFIA COMPLEMENTAR: RUSCH, D. C. Making Deep Games: Designing Games with Meaning and Purpose. Routledge, 2016. APPLEGET J.; BURKS, R.; CAMERON, F. The Craft of Wargaming: A Detailed Planning Guide for Defense Planners and Analysts. Naval Institute Press, 2020. ALDRICH, C. Learning Online with Games, Simulations, and Virtual Worlds: Strategies for Online Instruction. Jossey-Bass, 2009. SINGH, G. D. The Ultimate Kali Linux Book: Harness Nmap, Metasploit, Aircrack-ng, and Empire for cutting-edge pentesting. 3rd ed. Packt Publishing, 2024. KAPP, K. M.; BLAIR, L.; MESCH, R. The Gamification of Learning and Instruction Fieldbook: Ideas into Practice. Wiley, 2013.				

COMPONENTE CURRICULAR: Segurança em Infraestruturas Críticas				
EIXO TEMÁTICO: Forense Digital e Defesa de Infraestruturas Críticas				
PERÍODO DE OFERTA: 8º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial.				
PRÉ-REQUISITOS: Redes de Computadores II				
EMENTA: Estratégias para proteção de infraestruturas críticas, como energia, telecomunicações, transporte e saúde. Análise de vulnerabilidades em sistemas ciberfísicos. Definição e identificação de infraestruturas críticas. Modelos de proteção e normas internacionais de segurança. Ameaças e vulnerabilidades em sistemas industriais (ICS/SCADA). Estratégias de defesa cibernética e ferramentas de segurança para sistemas industriais. Monitoramento de sistemas ciberfísicos. Resiliência e continuidade operacional em infraestruturas críticas. Estratégias de resposta a incidentes e recuperação de desastres. Estudos de caso em infraestruturas críticas globais. Avaliação de impactos econômicos e sociais de falhas em infraestruturas críticas.				
BIBLIOGRAFIA BÁSICA: BRANQUINHO, T.; BRANQUINHO, M. Segurança Cibernética Industrial: As Infraestruturas Críticas Mundiais Correm Perigo. Aprenda a Proteger Redes e Sistemas de Controle com uma Metodologia Comprovada na Prática. Alta Books, 2022. LEWIS, T. G. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. 3rd ed. Wiley, 2019. KNAPP, E. D.; LANGILL, J. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 2nd ed. Syngress, 2014.				
BIBLIOGRAFIA COMPLEMENTAR: BODUNGEN, C.; SINGER, B.; SHBEEB, A.; WILHOIT, K.; HILT, S. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. McGraw-Hill Companies, 2016. MACAULAY, T.; SINGER, B. L. Cybersecurity for Industrial Control Systems. Auerbach Publications, 2016. SINGER, P. W.; FRIEDMAN, A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. WEISS, J. Protecting Industrial Control Systems from Electronic Threats. Momentum Press, 2010. KRUTZ, R. L. Securing SCADA Systems. Wiley, 2005.				

COMPONENTE CURRICULAR: Políticas de Conformidade e Regulação em Segurança				
EIXO TEMÁTICO: Governança, Conformidade e Resiliência Cibernética				
PERÍODO DE OFERTA: 8º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: -				
EMENTA: Conceitos fundamentais de governança, risco e conformidade (GRC) aplicados à segurança da informação. Normas, frameworks e regulamentações nacionais e internacionais de segurança cibernética: ISO/IEC 27001, ISO/IEC 27701, NIST Cybersecurity Framework, COBIT, GDPR (Regulamento Geral de Proteção de Dados), LGPD (Lei Geral de Proteção de Dados) e leis setoriais. Estruturação e implementação de programas de conformidade em segurança da informação. Auditoria e certificação em segurança. Políticas corporativas de segurança e privacidade. Métodos de avaliação e mitigação de riscos regulatórios. Ética, responsabilidade corporativa e impacto social das regulações em segurança. Estudos de casos práticos em conformidade e falhas de adequação regulatória em ambientes nacionais e globais.				
BIBLIOGRAFIA BÁSICA: ISO/IEC. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg: National Institute of Standards and Technology, 2018.				
BIBLIOGRAFIA COMPLEMENTAR: CALDER, Alan. ISO27001/ISO27002: A Pocket Guide. 4. ed. Ely: IT Governance Publishing, 2021. KOTULSKI, James; WITTEN, Charles. The NIST Cybersecurity Framework: A pocket guide. Ely: IT Governance Publishing, 2020. WHITMAN, Michael E.; MATTORD, Herbert J. Principles of Information Security. 7. ed. Boston: Cengage Learning, 2021. WEAVER, John; LALLIE, Harjinder. Cybersecurity Auditing and Monitoring. Cham: Springer, 2022. ROSS, Jeanne W.; SEIBEL, Christian. Governança de TI e Conformidade: estratégias para empresas digitais. São Paulo: Bookman, 2020.				

COMPONENTE CURRICULAR: Resiliência e Continuidade de Negócios				
EIXO TEMÁTICO: Governança, Conformidade e Resiliência Cibernética				
PERÍODO DE OFERTA: 8º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: -				
EMENTA: Gestão de continuidade de negócios e recuperação de desastres em ambientes cibernéticos. Planejamento, análise de impacto e definição de estratégias de resiliência para sistemas críticos. Ciber-resiliência e sua integração à governança de TI. Avaliação de riscos e priorização de ativos. Gestão econômica da segurança da informação: análise de custos de downtime, impactos financeiros de incidentes e otimização de investimentos em continuidade. Modelos e métricas de disponibilidade e recuperação. Planos de resposta a incidentes e testes de contingência. Estudos de caso sobre falhas e recuperação em organizações públicas e privadas.				
BIBLIOGRAFIA BÁSICA: MANOEL, S. S. Sistema de Gestão de Continuidade de Negócios: Esteja Preparado Para Salvar a sua Vida e os Negócios em Caso de um Incidente ou Desastre. Brasport. 2019. CRASK, J. Business Continuity Management: A Practical Guide to Organizational Resilience and ISO 22301. Kogan Page Ltd. 2021. MARINHO, F. Guia de Plano de Continuidade de Negócios (PCN). GEN Atlas. 2021.				
BIBLIOGRAFIA COMPLEMENTAR: OLIVEIRA, R. C. Q. Gestão de riscos e continuidade nos negócios. Editora Senac São Paulo. 2020. LINDSTEDT, D.; et. al. Adaptive Business Continuity. Rothstein Publishing. 2017. ELLIOT, D. Business Continuity Management: A Crisis Management Approach. Routledge. 2010. STERLING,S. Business Continuity for Dummies. For Dummies. 2012. SNEDAKER, S. Business Continuity and Disaster Recovery Planning for IT Professionals. Syngress Publishing. 2013.				

COMPONENTE CURRICULAR: Forense Computacional				
EIXO TEMÁTICO: Forense Digital e Defesa de Infraestruturas Críticas				
PERÍODO DE OFERTA: 9º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial.				
PRÉ-REQUISITOS: Fundamentos de Cibersegurança.				
EMENTA: Introdução à computação forense. Princípios e ética da computação forense. Fundamentos técnicos da forense digital. Técnicas de investigação digital, coleta de evidências e análise forense de incidentes cibernéticos. Investigação de ataques cibernéticos e incidentes de segurança. Análise forense de redes e comunicações. Análise forense de dispositivos móveis. Análise forense de nuvem e armazenamento de dados em ambientes distribuídos. Relatórios forenses e apresentação de evidências. Estudos de casos.				
BIBLIOGRAFIA BÁSICA: PEREIRA, A. J. & RIBEIRO, D. F. . Computação Forense e Investigação Cibernética: Fundamentos e Aplicações. Editora Pearson. 2021. BARROS, F. S. & COSTA, A. M. . Forense Digital: Fundamentos, Técnicas e Ferramentas para Investigação de Incidentes. Editora Ciência Moderna. 2021. SANTOS, G. L. & COSTA, A. R. . Computação Forense: Processos, Ferramentas e Investigação de Incidentes de Segurança. Editora Atlas. 2020.				
BIBLIOGRAFIA COMPLEMENTAR: ALTHEIDE, C., & CARVEY, H. . The Forensic Computer Examiner’s Handbook. Springer. 2020. KENNEALLY, E. . Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom. Elsevier. 2027. CASEY, E. . Handbook of Computer Crime Investigation: Forensic Tools and Technology. Academic Press. 2011. TAVARES, A. M. & SILVA, M. P. . Forense Digital e Investigação de Cibercrimes. Editora Elsevier. 2022. LIMA, L. R. & MOURA, F. S. . Introdução à Computação Forense: Técnicas e Aplicações. Editora Novatec. 2019.				

COMPONENTE CURRICULAR: Métodos Avançados em Defesa Cibernética				
EIXO TEMÁTICO: Governança, Conformidade e Resiliência Cibernética				
PERÍODO DE OFERTA: 9º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial.				
PRÉ-REQUISITOS: Laboratório de Invasão e Defesa.				
EMENTA: Estratégias de defesa cibernética para mitigação de ataques complexos. Desenvolvimento de sistemas resilientes e proativos. Detecção e prevenção de intrusões (IDS/IPS). Sistemas de defesa em profundidade. Técnicas de enganação (honeypots e honeynets). Análise de comportamento de atacantes (TTPs). Soluções SOAR (orquestração, automação e resposta de segurança). Ferramentas avançadas de monitoramento. Simulações de Red Team e Blue Team. Estratégias para mitigação de ataques DDoS. Estudos de casos de defesa contra ataques sofisticados. Avaliação de desempenho de sistemas de defesa.				
BIBLIOGRAFIA BÁSICA: SANS Institute. Advanced Network Defense: Advanced Persistent Threats, Network Security Monitoring, and Incident Response. SANS Institute. 2020. BUCHANAN, W. J., & ABAWAJV, J. H. Advances in Cyber Security: Applications, Techniques, and Research. Springer. 2017. SANTOS, G. L., & COSTA, A. R. Defesa Cibernética: Conceitos, Práticas e Aplicações Avançadas. Editora Elsevier. 2017.				
BIBLIOGRAFIA COMPLEMENTAR: MOURA, F. S., & GOMES, A. F. Segurança Cibernética: Práticas e Tecnologias para Proteção de Sistemas. Editora Ciência Moderna. 2020. KASPERSKY Lab. Advanced Persistent Threats: A Cybersecurity Guide. Kaspersky Lab. 2019. FREITAS, A. M., & LIMA, M. A. Cibersegurança Avançada: Análise de Ameaças, Resposta a Incidentes e Proteção de Infraestruturas Críticas. Editora Atlas. 2021. SHANNON, C. E. Communication Theory of Secrecy Systems. Bell System Technical Journal, 28(4), 656-715. STALLINGS, W. Network Security Essentials: Applications and Standards (6a ed.). Pearson. 2017.				

COMPONENTE CURRICULAR: Sistemas Operacionais				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: 6º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Arquitetura de Computadores.				
EMENTA: Conceitos fundamentais e evolução dos sistemas operacionais; processos e threads: gerenciamento, comunicação, sincronização e escalonamento; gerenciamento de memória: paginação, segmentação e memória virtual; sistemas de arquivos: estrutura, organização e segurança; entrada e saída: dispositivos, barramentos, interrupções e controle de E/S; sincronização, impasses (deadlocks) e estratégias de prevenção e recuperação; virtualização e containerização; estudo de casos de sistemas operacionais modernos.				
BIBLIOGRAFIA BÁSICA: TANENBAUM, A. S.; BOS, H. Sistemas Operacionais Modernos. 4ª ed. São Paulo: Pearson, 2016 SILBERSCHATZ, A.; GALVIN, P.; GAGNE, G. Fundamentos de Sistemas Operacionais. 9ª ed. Rio de Janeiro: LTC, 20175. MACHADO, F. B.; MAIA, L. P. Arquitetura de Sistemas Operacionais. 5ª ed. Rio de Janeiro: LTC, 2017.				
BIBLIOGRAFIA COMPLEMENTAR: DEITEL, H. M.; DEITEL, P. J.; CHOFFNES, D. R. Sistemas Operacionais. 3ª ed. São Paulo: Pearson, 2005. OLIVEIRA, R. S.; CARISSIMI, A. S.; TOSCANI, S. S. Sistemas Operacionais. 4ª ed. Porto Alegre: Bookman, 2010. STALLINGS, W. Arquitetura e Organização de Computadores. 11ª ed. Rio de Janeiro: Bookman, 2024. TANENBAUM, A. S.; WOODHULL, A. S. Sistemas Operacionais: Projeto e Implementação. 3ª ed. Porto Alegre: Bookman, 2008. MAZIERO, C. Sistemas Operacionais: Conceitos e Mecanismos. Editora da UFPR, 2019. 456 p.				

COMPONENTE CURRICULAR: Trabalho de Conclusão de Curso I				
EIXO TEMÁTICO: Integração Curricular				
PERÍODO DE OFERTA: 8º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Introdução à Ciência. Os tipos de conhecimento. Métodos de pesquisa. Normas da ABNT. Artigo Científica. A leitura e a escrita. Instrumentalização científica. Plágio: o que é e como evitar. Elaboração do Projeto do TCC.				
BIBLIOGRAFIA BÁSICA: MARCONI, M. A.; LAKATOS, E. M.. Metodologia do trabalho científico: procedimentos básicos, pesquisa bibliográfica, projeto e relatório, publicações e trabalhos científicos. 7. ed. São Paulo: Atlas, 2015. 225 p SEVERINO, A. J. Metodologia do trabalho científico. São Paulo: Cortez, 2016, 317 p. VOLPATO, G. L.. Guia prático para redação científica: publique em revistas internacionais. Botucatu: Ed. Best Writing, 2015, 267 p.				
BIBLIOGRAFIA COMPLEMENTAR: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 10520: informação e documentação – citações em documentos – apresentação. Rio de Janeiro: ABNT, 2002. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 14724: informação e documentação – trabalhos acadêmicos – apresentação. Rio de Janeiro: ABNT, 2011. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6023: informação e documentação – referências – elaboração. Rio de Janeiro, 2002. KOLLER, S.H.; COUTO, M.C.P; VON HOHENDORFF, J. Manual de produção científica. Porto Alegre: Ed. Penso, 2014. 191 p. NASCIMENTO, L. P.. Elaboração de projetos de pesquisa: monografia, dissertação, tese e estudo de caso, com base em metodologia científica. São Paulo: Cengage Learning, 2016, 190 p.				

COMPONENTE CURRICULAR: Trabalho de Conclusão de Curso II				
EIXO TEMÁTICO: Integração Curricular				
PERÍODO DE OFERTA: 9º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	0	30	CRÉDITOS:	2
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Trabalho de Conclusão de Curso I.				
EMENTA: Orientações para elaboração, entrega e defesa do Trabalho de Conclusão do Curso - TCC, obedecendo aos padrões de metodologia científica				
BIBLIOGRAFIA BÁSICA: MARCONI, M. A.; LAKATOS, E. M.. Metodologia do trabalho científico: procedimentos básicos, pesquisa bibliográfica, projeto e relatório, publicações e trabalhos científicos. 7. ed. São Paulo: Atlas, 2015. 225 p SEVERINO, A. J. Metodologia do trabalho científico. São Paulo: Cortez, 2016, 317 p. VOLPATO, G. L.. Guia prático para redação científica: publique em revistas internacionais. Botucatu: Ed. Best Writing, 2015, 267 p.				
BIBLIOGRAFIA COMPLEMENTAR: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 10520: informação e documentação – citações em documentos – apresentação. Rio de Janeiro: ABNT, 2002. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 14724: informação e documentação – trabalhos acadêmicos – apresentação. Rio de Janeiro: ABNT, 2011. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6023: informação e documentação – referências – elaboração. Rio de Janeiro, 2002. KOLLER, S.H.; COUTO, M.C.P; VON HOHENDORFF, J. Manual de produção científica. Porto Alegre: Ed. Penso, 2014. 191 p. NASCIMENTO, L. P.. Elaboração de projetos de pesquisa: monografia, dissertação, tese e estudo de caso, com base em metodologia científica. São Paulo: Cengage Learning, 2016, 190 p.				

COMPONENTE CURRICULAR: Visão Computacional				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: 7º Semestre			NÚCLEO DE CONTEÚDO: Específico	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Obrigatório
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial e/ou Ensino a Distância (EaD)				
PRÉ-REQUISITOS: Álgebra Linear; Aprendizado de Máquina.				
EMENTA: Fundamentos da visão computacional aplicada à segurança cibernética: conceitos, histórico e aplicações. Processamento e análise de imagens digitais em contextos de segurança: filtragem, restauração, transformações geométricas e segmentação semântica. Reconhecimento biométrico (faces, íris, impressões digitais) e detecção de falsificações (spoofing). Aplicações de aprendizado profundo para autenticação, monitoramento e prevenção de fraudes. Expressão gráfica, acessibilidade e desenho universal em sistemas visuais: representação e comunicação visual de dados, princípios de design inclusivo e acessibilidade digital em interfaces seguras (WCAG, ISO 9241). Aplicações em tecnologias assistivas e segurança inclusiva. Estudos de caso em sistemas inteligentes de visão computacional.				
BIBLIOGRAFIA BÁSICA: GONZALEZ, Rafael C.; WOODS, Richard E. Digital Image Processing. 4. ed. New York: Pearson, 2018. SZELISKI, Richard. Computer Vision: Algorithms and Applications. 2. ed. Cham: Springer, 2022. GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. Deep Learning. Cambridge: MIT Press, 2016.				
BIBLIOGRAFIA COMPLEMENTAR: BOWYER, Kevin W.; JAIN, Anil K. Biometric Recognition: Fundamentals and Applications. 2. ed. Cham: Springer, 2022. LI, Stan Z.; JAIN, Anil K. (eds.). Handbook of Face Recognition. 2. ed. London: Springer, 2019. REDMON, Joseph; FARHADI, Ali. YOLOv3: An Incremental Improvement. arXiv preprint arXiv:1804.02767, 2018. GOODFELLOW, Ian; SHLENS, Jonathon; SZEGEDY, Christian. Explaining and Harnessing Adversarial Examples. arXiv preprint arXiv:1412.6572, 2015. BHUIYAN, Md Monirul et al. Computer Vision for Cybersecurity: Threat Detection and Prevention. Cham: Springer, 2021.				

15.3 Componentes Curriculares Optativos

COMPONENTE CURRICULAR: Blockchain e Segurança em Criptomoedas				
EIXO TEMÁTICO: Bases da Cibersegurança e Desenvolvimento Seguro				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Criptografia e Segurança de Dados				
EMENTA: Fundamentos de blockchain, mecanismos de segurança e análise de riscos associados a criptomoedas. Trilema da blockchain: segurança, escalabilidade, descentralização. Pagamentos digitais e segurança de dados. Confiança digital. Riscos de segurança na mineração de criptomoedas. Riscos de conformidade relacionados a criptomoedas no Brasil. Riscos em operações envolvendo contratos inteligentes, NFT, DAO, finanças descentralizadas e setoriais.				
BIBLIOGRAFIA BÁSICA: BASHIR, I. Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3. 4. ed. Packt Publishing, 2023. SOHAL, A. Guia Definitivo Para Dominar o Bitcoin e as Criptomoedas. 1. ed. Edições Nosso Conhecimento, 2024. ISBN-13: 978-6207714018. ANTONOPOULOS, Andreas M. Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications. 3. ed. Sebastopol: O'Reilly Media, 2022.				
BIBLIOGRAFIA COMPLEMENTAR: BABICEAN, A. Blockchain e Regulação: Perspectivas de uma Regulação de Valores Mobiliários sob a Forma de Criptoativos. 1. ed. Almedina Brasil, 2024. ISBN-13: 978-9894017745. CHAVES, I. Blockchain e criptomoedas. 1. ed. InterSaberes, 2021. ISBN-13: 978-6589818847. HUBBARD, D. W.; SEIESEN, R. How to Measure Anything in Cybersecurity Risk. 2. ed. Wiley, 2023. ISBN-13: 978-1119892304. REVOREDO, T. Blockchain: Tudo O Que Você Precisa Saber. 1. ed. Independently Published, 2019. ISBN-13: 978-1687405715. TAPSCOTT, Don; TAPSCOTT, Alex. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World. New York: Portfolio/Penguin, 2018.				

COMPONENTE CURRICULAR: Desenvolvimento de Malware Controlado				
EIXO TEMÁTICO: Forense Digital e Defesa de Infraestruturas Críticas				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Sistemas Operacionais; Laboratório de Invasão e Defesa; Análise de Malware e Engenharia Reversa.				
EMENTA: Conceitos fundamentais e tipos de malware. Criação e monitoramento de ambientes seguros: máquina virtual e sandbox. Criptografia e ocultação de código malicioso. Desenvolvimento de backdoors e trojans. Vulnerabilidades para disseminação de malware. Engenharia reversa aplicada ao malware. Injeção de código e escalonamento de privilégios.				
BIBLIOGRAFIA BÁSICA: SEITZ, J.; ARNOLD, T. Black Hat Python: Programação Python para hackers e pentesters. Novatec Editora, 2024. LIGH, M. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac. Wiley, 2014. SIKORSKI, M.; HONIG, A. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press, 2012.				
BIBLIOGRAFIA COMPLEMENTAR: BLUNDEN, B. The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System. Jones & Bartlett Publishers, 2012. SAXE, J.; SANDERS, H. Malware Data Science: Attack Detection and Attribution. No Starch Press, 2018. DANG, B.; GAZET, A.; BACHAALANY, E. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. John Wiley & Sons, 2014. EILAM, E. Reversing: Secrets of Reverse Engineering. Wiley, 2005. YOSIFOVICH, P.; SOLOMON, D.; IONESCU, A.; RUSSINOVICH, M. Windows Internals, Parts 1. Microsoft Press, 2017.				

COMPONENTE CURRICULAR: Segurança em redes Sociais				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Redes de Computadores II; Fundamentos de Cibersegurança.				
EMENTA: Introdução à segurança em redes sociais. Evolução das redes sociais e sua influência na sociedade. Engenharia social e técnicas de persuasão, phishing, malware e ataques direcionados. Configuração de privacidade em redes sociais, gestão de senhas e autenticação multifator. Políticas de segurança para redes sociais corporativas. Monitoramento de ameaças e resposta a incidentes. Gestão de crises e reputação online. Regulamentações e leis sobre privacidade e proteção de dados. Ética no uso de redes sociais e segurança digital.				
BIBLIOGRAFIA BÁSICA: CROSS, M. Social Media Security: Leveraging Social Networking While Mitigating Risk. Syngress, 2013. ÖZYER, S., KAYA, B. Cyber Security and Social Media Applications. Springer, 2023. PROKISCH, C. Cibersegurança: como proteger seus dados no mundo digital. Senac São Paulo, 2023.				
BIBLIOGRAFIA COMPLEMENTAR: MITNICK, K. The Art of Invisibility. Little, Brown and Company, 2017. NUNES, B. Guia Prático de Segurança nas Redes Sociais: Proteja-se!, 2024. MARTINS, G. Segurança Digital: O Guia para a segurança na internet. Brutal Security, 2015. FLYNN, N. The Social Media Handbook: Rules, Policies, and Best Practices to Successfully Manage Your Organization's Social Media Presence, Posts, and Potential. Pfeiffer, 2012. TEIXEIRA, F. Segurança na Era Digital. Clube de Autores, 2023.				

COMPONENTE CURRICULAR: Gerenciamento de Identidade e Acesso				
EIXO TEMÁTICO: Governança, Conformidade e Resiliência Cibernética				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Fundamentos de Cibersegurança; Políticas de Conformidade e Regulação em Segurança.				
EMENTA: Conceitos de autenticação, autorização e auditoria. modelos de controle de acesso (DAC, MAC, RBAC, ABAC). Mecanismos de autenticação Single Sign-On (SSO) e Autenticação Multifator (MFA). Ciclo de vida de identidade. Gestão de identidade. Definição de políticas de controle de identidade.				
BIBLIOGRAFIA BÁSICA: RAWAL, B.; MANOGARAN, G.; PETER, A. Cybersecurity and Identity Access Management. Springer, 2023. ZULEJHIC, A. Identity and Access Management: Fundamentals. 2022. KONTSEVOY, E.; SHAH, S.; CONRAD, P. Identity-Native Infrastructure Access Management: Preventing Breaches by Eliminating Secrets and Adopting Zero Trust. O'Reilly Media, 2023.				
BIBLIOGRAFIA COMPLEMENTAR: WILSON, Y.; HINGNIKAR, A. Solving Identity Management in Modern Applications: Demystifying Oauth 2, Openid Connect, and Saml 2. Apress, 2022. WINDLEY, P. Learning Digital Identity: Design, Deploy, and Manage Identity Architectures. O'Reilly Media, 2023. HABER, M.; ROLLS, D. Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution. Apress, 2019. BLOKDYK, G. Customer Identity And Access Management A Complete Guide. 5STARCooks, 2020. ORONDO, O. Identity & Access Management: A Systems Engineering Approach. IAM Imprints, 2016.				

COMPONENTE CURRICULAR: Segurança em Sistemas Operacionais Abertos				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Sistemas Operacionais.				
EMENTA: Conceito de sistemas operacionais abertos. Comparação entre segurança em sistemas proprietários e de código aberto. Escalonamento de privilégios. Mecanismos de isolamento e proteção no kernel e processos (NX bit, ASLR, etc.). Controle de acesso baseado em papéis (RBAC) e arcabouços de segurança SELinux, AppArmor, jails e contêineres. Mecanismos de autenticação. Permissões de arquivos e diretórios. Configuração e análise de logs.				
BIBLIOGRAFIA BÁSICA: KALSI, T. Practical Linux Security Cookbook. Packt Publishing, 2018. TEVAULT, D. Mastering Linux Security and Hardening. Packt Publishing, 2023. KORFF, Y.; HOPE, P.; POTTER, B. Mastering FreeBSD and OpenBSD Security. O'Reilly Media, 2005.				
BIBLIOGRAFIA COMPLEMENTAR: MCKUSICK, M.; NEVILLE-NEIL, G.; WATSON, R. The Design and Implementation of the Freebsd Operating System. Addison-Wesley, 2014. LUCAS, M. FreeBSD Mastery: Jails. Tilted Windmill Press, 2019. VERMEULEN, S. SELinux System Administration. Packt Publishing, 2020. NIKKEL, B. Practical Linux Forensics. No Starch Press, 2021. DUNKERLEY, M.; TUMBARELLO, M. Mastering Windows Security and Hardening. Packt Publishing, 2022.				

COMPONENTE CURRICULAR: Privacidade e Proteção de Dados Pessoais				
EIXO TEMÁTICO: Governança, Conformidade e Resiliência Cibernética				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: -	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Criptografia e Segurança de Dados; Políticas de Conformidade e Regulação em Segurança.				
EMENTA: Fundamentos de privacidade e proteção de dados. Normas e legislações nacionais e internacionais: LGPD, GDPR e outras. Conceitos de dados pessoais, sensíveis e anonimização. Riscos associados ao tratamento de dados. Técnicas e ferramentas para assegurar privacidade. Impactos da coleta, armazenamento e compartilhamento de dados em organizações públicas e privadas. Estudos de casos aplicados à cibersegurança e à conformidade regulatória.				
BIBLIOGRAFIA BÁSICA: DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. 3. ed. Rio de Janeiro: Forense, 2022. SCHWARTZ, Paul M.; SOLOVE, Daniel J. Information Privacy Law. 7. ed. New York: Wolters Kluwer, 2021. TETTAMANZY, Ana Claudia; PINHEIRO, Patrícia. LGPD comentada: fundamentos e práticas de proteção de dados. São Paulo: Thomson Reuters Brasil, 2022.				
BIBLIOGRAFIA COMPLEMENTAR: CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Toronto: Information & Privacy Commissioner of Ontario, 2011. WESTIN, Alan. Privacy and Freedom. New York: IG Publishing, 2015. ZUBOFF, Shoshana. The Age of Surveillance Capitalism. New York: PublicAffairs, 2019. GREENLEAF, Graham. Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford: Oxford University Press, 2014. CUSTODIO, Mariana. Proteção de Dados Pessoais: Análise Crítica da LGPD. São Paulo: Saraiva, 2021.				

COMPONENTE CURRICULAR: Segurança em Dispositivos IoT e Sistemas Ciberfísicos				
EIXO TEMÁTICO: Forense Digital e Defesa de Infraestruturas Críticas				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Redes de Computadores II; Laboratório de Projeto II				
EMENTA: Fundamentos da Internet das Coisas (IoT) e sistemas ciberfísicos. Arquitetura, protocolos e vulnerabilidades comuns. Segurança em sensores, atuadores e dispositivos inteligentes. Técnicas de mitigação de ataques em IoT. Estratégias de resiliência e defesa em sistemas industriais, smart cities e saúde digital. Normas e frameworks de segurança para IoT e CPS. Estudos de casos reais.				
BIBLIOGRAFIA BÁSICA: ROSE, Karen et al. The Internet of Things: An Overview. Washington: Internet Society, 2015. RAJKUMAR, R.; LEE, I.; SHA, L.; STANKOVIC, J. Cyber-Physical Systems: The Next Computing Revolution. New York: IEEE Press, 2010. KHAN, Shafiullah; ZHOU, Wenye. Security for Cyber-Physical Systems. New York: Springer, 2019.				
BIBLIOGRAFIA COMPLEMENTAR: YANG, Xiaodong; CHEN, Zhi. IoT Security: Advances in Authentication. Cham: Springer, 2020. STANKOVIC, John. Research Directions for the Internet of Things. IEEE Internet of Things Journal, v. 1, n. 1, p. 3–9, 2014. LEE, Edward A. Introduction to Embedded Systems: A Cyber-Physical Systems Approach. Cambridge: MIT Press, 2017. HASSAN, Qusay F. Internet of Things A to Z: Technologies and Applications. Hoboken: Wiley, 2018. BOOCH, Grady. The Future of Software: Cyber-Physical Systems. IEEE Software, v. 36, n. 6, p. 91–95, 2019.				

COMPONENTE CURRICULAR: Cibersegurança em Redes 5G e Futuras Gerações				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Redes de Computadores II; Computação em Nuvem e Segurança em Ambientes Distribuídos				
EMENTA: Conceitos fundamentais de redes móveis 5G. Arquitetura, protocolos e tecnologias habilitadoras (SDN, NFV, edge computing). Vulnerabilidades e desafios de segurança em redes móveis de quinta geração. Estratégias de defesa para ambientes críticos. Políticas de segurança em redes 5G e 6G emergentes. Aplicações em setores estratégicos: saúde, transporte, cidades inteligentes. Estudos de casos.				
BIBLIOGRAFIA BÁSICA: LARSON, Erik et al. 5G NR: The Next Generation Wireless Access Technology. 2. ed. Academic Press, 2021. TANG, Frank. 5G Security: Concepts and Challenges. London: Springer, 2020. AHMED, Imran; HASAN, Zahid. Security in 5G Wireless Networks. Hoboken: Wiley, 2021.				
BIBLIOGRAFIA COMPLEMENTAR: NGUYEN, Phuoc Tran-Gia. 5G and Beyond: Fundamentals and Standards. Cham: Springer, 2020. HU, Huawei et al. Security Issues in 5G and Future Networks. IEEE Communications Surveys & Tutorials, v. 22, n. 3, 2020. BOCQUET, Sylvain. 5G and Future Networks: Performance and Security. London: ISTE Press, 2021. SARI, Ahmet. 5G and 6G Security: Emerging Challenges and Solutions. IEEE Access, v. 10, 2022. MAHMOOD, Nurul; LATVA-AHO, Matti. Security for 6G Communications. Cham: Springer, 2022.				

COMPONENTE CURRICULAR: Segurança Ofensiva e Testes de Intrusão				
EIXO TEMÁTICO: Forense Digital e Defesa de Infraestruturas Críticas				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Laboratório de Invasão e Defesa; Métodos Avançados em Defesa Cibernética				
EMENTA: Fundamentos de segurança ofensiva. Técnicas e metodologias de pentest. Fases do teste de intrusão: reconhecimento, varredura, exploração, pós-exploração e relatório. Ferramentas de testes de intrusão (Metasploit, Nmap, Wireshark, Burp Suite). Simulação de ataques em redes e aplicações. Ética, normas e limitações legais do hacking ético. Estudos de casos e laboratórios práticos.				
BIBLIOGRAFIA BÁSICA: ALLSOPP, Jon Erickson. Hacking: The Art of Exploitation. 2. ed. San Francisco: No Starch Press, 2008. KIM, Seungjin Lee. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press, 2014. SKOUDIS, Ed; LISTON, Tom. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Upper Saddle River: Prentice Hall, 2006.				
BIBLIOGRAFIA COMPLEMENTAR: MESSIER, Ric. Ethical Hacking and Penetration Testing Guide. Boca Raton: CRC Press, 2019. RAMACHANDRAN, Vivek. The Metasploit Penetration Testing Guide. San Francisco: No Starch Press, 2017. GRIMES, Roger A. Hacking Multifactor Authentication. San Francisco: Wiley, 2020. WANG, Xiaofeng. Advanced Penetration Testing: Techniques and Tools. Springer, 2021. ANANTHANARAYANAN, Nithin. Bug Bounty Bootcamp: The Guide to Finding and Reporting Web Vulnerabilities. No Starch Press, 2021.				

COMPONENTE CURRICULAR: Segurança em Aplicações Web e Mobile				
EIXO TEMÁTICO: Bases da Cibersegurança e Desenvolvimento Seguro				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Engenharia de Software Seguro; Programação Orientada a Objetos				
EMENTA: Fundamentos de segurança em aplicações web e mobile. OWASP Top 10. Vulnerabilidades comuns em aplicativos móveis. Ferramentas e técnicas de análise de segurança em aplicações. Princípios de desenvolvimento seguro. Testes de segurança em aplicações web e mobile. Estratégias de mitigação e defesa. Estudos de caso práticos.				
BIBLIOGRAFIA BÁSICA: STUTZMAN, Jeff. The Web Application Hacker's Handbook. 2. ed. Indianapolis: Wiley, 2011. WILLIAMS, Andrew; OWASP Foundation. OWASP Testing Guide. 4. ed. OWASP, 2020. CLARKE, David. Mobile Application Security. New York: McGraw-Hill, 2017.				
BIBLIOGRAFIA COMPLEMENTAR: ENISA. Web Application Security. European Union Agency for Cybersecurity, 2020. SHOSTACK, Adam. Threat Modeling: Designing for Security. Indianapolis: Wiley, 2014. DAFTUAR, Niranjana. Hands-On Mobile Application Security. Packt Publishing, 2020. ANDRESS, Jason. Foundations of Information Security. No Starch Press, 2019. KEARY, Andrew van der Stock. OWASP Cheat Sheet Series. OWASP, 2021.				

COMPONENTE CURRICULAR: Impactos Sociais e Éticos da Privacidade Digital				
EIXO TEMÁTICO: Governança, Conformidade e Resiliência Cibernética				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Questões sociais, éticas e políticas relacionadas à privacidade digital. Vigilância em massa, big data e capitalismo de dados. Redes sociais e privacidade. Aspectos legais, filosóficos e culturais da privacidade na era digital. Direitos fundamentais e proteção contra abusos. Estudos de caso sobre impactos sociais da coleta e uso de dados em diferentes contextos.				
BIBLIOGRAFIA BÁSICA: ZUBOFF, Shoshana. The Age of Surveillance Capitalism. New York: PublicAffairs, 2019. SOLOVÉ, Daniel J. Understanding Privacy. Cambridge: Harvard University Press, 2010. DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2022.				
BIBLIOGRAFIA COMPLEMENTAR: WESTIN, Alan. Privacy and Freedom. New York: IG Publishing, 2015. NISSENBAUM, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press, 2009. TAYLOR, Linnet. Digital Democracy, Social Media and Disinformation. Oxford: Oxford University Press, 2022. DEEPMIND ETHICS & SOCIETY. Ethics and Society in AI. London: DeepMind, 2021. FUCHS, Christian. Social Media: A Critical Introduction. London: Sage, 2021.				

COMPONENTE CURRICULAR:			Engenharia de Privacidade e Tecnologias de Preservação de Dados	
EIXO TEMÁTICO: Governança, Conformidade e Resiliência Cibernética				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Optativo	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS:			Criptografia e Segurança de Dados; Análise e Comunicação de Dados	
EMENTA: Fundamentos da engenharia de privacidade. Princípios de Privacy by Design e Privacy by Default. Técnicas de anonimização e pseudonimização. Tecnologias para preservação de dados (homomorphic encryption, differential privacy, secure multiparty computation). Integração de práticas de privacidade em sistemas e softwares. Estudos de casos de implementação em diferentes setores.				
BIBLIOGRAFIA BÁSICA: CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Toronto: Information & Privacy Commissioner of Ontario, 2011. DWORK, Cynthia; ROTH, Aaron. The Algorithmic Foundations of Differential Privacy. Philadelphia: Now Publishers, 2014. ZHOU, Jianying; DENG, Robert H. Privacy Enhancing Technologies. Cham: Springer, 2020.				
BIBLIOGRAFIA COMPLEMENTAR: GÜRSOY, Mehmet Ercan. Engineering Privacy in Software. New York: Springer, 2019. DOMINGOS, Pedro. The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World. New York: Basic Books, 2018. BERTINO, Elisa. Data Privacy for the Cloud. San Francisco: Morgan & Claypool, 2019. GUPTA, Manish. Handbook of Research on Privacy and Security in the Digital Era. Hershey: IGI Global, 2019. REED, Chris. Making Laws for Cyberspace. Oxford: Oxford University Press, 2012.				

COMPONENTE CURRICULAR: Engenharia de Dados				
EIXO TEMÁTICO: Computação e Infraestruturas de TI				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
30	30	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Banco de Dados; Big Data.				
EMENTA: Fundamentos de engenharia de dados. Arquiteturas de dados modernas. Pipelines de dados: extração, transformação e carga (ETL/ELT). Integração com bancos de dados relacionais e não relacionais. Ferramentas de orquestração e processamento em lote e em fluxo. Armazenamento escalável e gerenciamento de grandes volumes de dados. DataOps e integração com ciência de dados.				
BIBLIOGRAFIA BÁSICA: CRICKARD, P. Data engineering with python: Work with massive datasets to design data models and automate data pipelines using python. Birmingham: Packt Publishing, 2020. 356 p. KLEPPMANN, M. Designing data-intensive applications: The big ideas behind reliable, scalable, and maintainable systems. Boston: O'Reilly Media, 2017. 614 p. REIS, J.; HOUSLEY, M. Fundamentals of data engineering: Plan and build robust data systems. Sebastopol, CA: O'Reilly Media, 2022. 447 p.				
BIBLIOGRAFIA COMPLEMENTAR: AKIDAU, T.; CHERNYAK, S.; LAX, R. Streaming systems: The what, where, when, and how of large-scale data processing. Beijing: O'Reilly Media, 2018. 349 p. KUKREJA, M. Data engineering with apache spark, delta lake, and lakehouse: Create scalable pipelines that ingest, curate, and aggregate complex data in a timely and secure way. Birmingham Mumbai: Packt Publishing, 2021. 480 p. ULLMAN, J. D.; WIDOM, J. First course in database systems, a: Pearson new international edition. [s.l.] Pearson, 2013. 520 p. VEHENT, J. Securing DevOps: Security in the cloud. New York: Manning, 2018. 384 p. WHITE, T. Hadoop: The definitive guide. Beijing Cambridge Farnham Köln Sebastopol Tokyo: O'Reilly, 2015. 1 p.				

COMPONENTE CURRICULAR: Inteligência Artificial e as Redes Neurais				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Aprendizado de Máquina; Inteligência Artificial e Análise de Dados Aplicada à Segurança				
EMENTA: Histórico da inteligência artificial; Características básicas de uma Rede Neural. Aprendizado supervisionado e não supervisionado; As regras de aprendizado; Algoritmo de correção de erros; Neurônio artificial; A regra delta; Rede Feedforward multicamadas e o algoritmo da retropropagação (backpropagation); O problema de regressão em processos estacionários e não estacionários; Problema de classificação; Regressão logística; O classificador softmax; Rede Feedforward em problemas de classificação.				
BIBLIOGRAFIA BÁSICA: GRUS, J.. Data Science do Zero. Editora Alta Books, 2021. E-book. ISBN 9788550816463. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788550816463/. Acesso em: 31 mar. 2023. HAYKIN, S.. Redes neurais princípios e prática. Grupo A, 2001. E-book. ISBN 9788577800865. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788577800865/. Acesso em: 31 mar. 2023. SILVA, F. M.; LENZ, M. L.; FREITAS, P. H C.; et al.. Inteligência artificial. Grupo A, 2018. E-book. ISBN 9788595029392. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595029392/. Acesso em: 31 mar. 2023.				
BIBLIOGRAFIA COMPLEMENTAR: AMARAL, F.. Aprenda Mineração de Dados. Editora Alta Books, 2019. E-book. ISBN 9786555206852. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555206852/. Acesso em: 12 abr. 2023. BROOKSHEAR, J. G.. Ciência da computação. Grupo A, 2013. E-book. ISBN 9788582600313. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582600313/. Acesso em: 12 abr. 2023. FILATRO, A. C. Data science da educação. Editora Saraiva, 2020. E-book. ISBN 9786587958446. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786587958446/. Acesso em: 12 abr. 2023. KAUFMAN, D.. Desmistificando a inteligência artificial. Grupo Autêntica, 2022. E-book. ISBN 9786559281596. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559281596/. Acesso em: 12 abr. 2023. MUELLER, J. P.. Aprendizado profundo para leigos. Editora Alta Books, 2020. E-book. ISBN 9788550816982. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788550816982/. Acesso em: 12 abr. 2023.				

COMPONENTE CURRICULAR: Introdução à Ciência de Dados com Python				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
20	40	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Programação II; Estrutura de Dados II				
EMENTA: Variáveis, tipos e conversão de tipos de dados em Python, listas, dicionários, tuplas; funções; classes; estruturas de dados com pacotes Numpy e Pandas e principais métodos; análise de dados: cálculo de máximo, mínimo, média, mediana, variância, regressão linear ; visualização de dados com pacote Matplotlib; geração de mapas com pacote Folium.				
BIBLIOGRAFIA BÁSICA: GRUS, J.. Data science do zero noções fundamentais com Python, Rio de Janeiro, Alta Books 2016, ISBN 9788550816463 MUELLER, J. P.. Começando a programar em Python para leigos, Rio de Janeiro, Alta Books, 2020, ISBN 9786555202298 SHAW, Z. A.. Aprenda Python 3 do jeito certo uma introdução muito simples ao incrível mundo dos computadores e da codificação, Rio de Janeiro, Alta Books, 2019, ISBN 9788550809205				
BIBLIOGRAFIA COMPLEMENTAR: BEHRMAN, K. R.. Fundamentos de Python para ciência de dados, Porto Alegre, Bookman 2023, ISBN 9788582605974 MENEZES, N. N. C.. Introdução à programação com Python: algoritmos e lógica de programação para iniciantes, São Paulo: Novatec, 2019, ISBN 9788575227183 PERKOVIC, L.. Introdução à computação usando Python um foco no desenvolvimento de aplicações, Rio de Janeiro, LTC 2016, ISBN 9788521630937				

COMPONENTE CURRICULAR: Língua Brasileira de Sinais - Libras				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Introdução aos aspectos históricos e conceituais da educação de surdos, cultura surda e filosofia do bilinguismo. Legislação específica. Conceito de surdez, deficiência auditiva (DA), surdo-mudo, mitos. Processos cognitivos e linguísticos. O cérebro e a língua de sinais. Língua de Sinais Brasileira (LIBRAS) e a modalidade diferenciada para a comunicação (gestual-visual). Ampliação de habilidades expressivas e receptivas em LIBRAS. Aspectos fonológico, morfológico, semântico, sintático e pragmático Libras. Prática em Libras – vocabulário. SignWriting (escrita de sinais).				
BIBLIOGRAFIA BÁSICA: GESSER, A.. Libras: que língua é essa : crenças e preconceitos em torno da língua de sinais e da realidade surda. São Paulo: Parábola, 2009 PLINSKI, R. R. K.. Libras. Porto Alegre SAGAH 2018 QUADROS, R. M.; KARNOPP, L. B.. Língua de sinais brasileira: estudos linguísticos. Porto Alegre: Artmed, 2004				
BIBLIOGRAFIA COMPLEMENTAR: CAPOVILLA, F. C. (Ed.). Dicionário da língua de sinais do Brasil: a Libras em suas mãos. São Paulo: Edusp, 2017 CAPOVILLA, F. C.; RAPHAEL, W. D.. Enciclopédia da língua de sinais brasileira: o mundo do surdo em Libras. São Paulo: Edusp, 2005 LEITE, E. M.. Os papéis do Intérprete na sala de aula inclusiva; Petrópolis: Editora Arara Azul, 2004 THOMAS, A. S.; LOPES, M. C. A.. Invenção da Surdez: Cultura Alteridade Identidades e diferença no campo da Educação; Santa Cruz do Sul: EDUNISC, 2006				

COMPONENTE CURRICULAR: Pesquisa Operacional				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
45	15	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Álgebra Linear; Estatística para Análises de Segurança II.				
EMENTA: Pesquisa Operacional: Criação e Evolução Histórica, Processos de Tomada de Decisão, Ferramentas da Pesquisa Operacional; Programação Linear: Definição de um Problema de Otimização e Modelagem de Problemas de Programação Linear (PPL); Solução de PPLs: Solução Gráfica, Analítica, por Método Simplex e por Computador; Dualidade; Análise de Sensibilidade e Pós-otimização; Problema do Transporte e de Atribuição de Tarefas: Casos Especiais e Algoritmos; Modelos de Otimização de Redes: Caminho Mais Curto, Fluxo Máximo e Árvore Geradora Mínima; Programação Dinâmica; Programação Binária e Inteira.				
BIBLIOGRAFIA BÁSICA: BELFIORE, P.. Pesquisa operacional para cursos de engenharia. Rio de Janeiro GEN LTC 2012 1 recurso online ISBN 9788595155626. GOLDBARG, M. C.; LUNA, H. P. L.. Otimização Combinatória e Programação Linear: Modelos e Algoritmos. 2ª edição. Rio de Janeiro: Ed. Elsevier, 2005, 536 p. HILLIER, F. S. Introdução à pesquisa operacional. 9. Porto Alegre AMGH 2013 1 recurso online ISBN 9788580551198.				
BIBLIOGRAFIA COMPLEMENTAR: BARBOSA, M. A.; ZANARDINI, R. A. D. Iniciação à pesquisa operacional no ambiente de gestão. 3ª Edição. Curitiba: Ed. Intersaberes, 2015, 220 p. COLIN, E. C.. Pesquisa operacional 170 aplicações em estratégia, finanças, logística, produção, marketing e vendas. 2. São Paulo Atlas 2017 1 recurso online ISBN 9788597014488. GOLDBARG, M. M.. Programação Linear e Fluxos em Redes. 1ª edição ed. GEN LTC, 2014. LACHTERMACHER, G.. Pesquisa operacional na tomada de decisões. 5. Rio de Janeiro LTC 2016 1 recurso online ISBN 9788521630494. MOREIRA, D. A.. Pesquisa operacional curso introdutório. 2. São Paulo Cengage Learning 2018 1 recurso online ISBN 9788522128068.				

COMPONENTE CURRICULAR: Tópicos Avançados em Engenharia de Software				
EIXO TEMÁTICO: Bases da Cibersegurança e Desenvolvimento Seguro				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
45	15	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Engenharia de Software Seguro; Projeto e Modelagem de Sistemas Seguros.				
EMENTA: Tópicos avançados em um ou mais temas da Engenharia de Software; estudo de técnicas conforme o estado da arte na área; aprofundamento de métodos, processos e tecnologias emergentes; abordagem flexível para adaptação a novas tendências e demandas.				
BIBLIOGRAFIA BÁSICA: SOMMERVILLE, Ian. Engenharia de Software. 10ª ed. São Paulo: Pearson, 2019. VALENTE, M. T.. Engenharia de Software Moderna: Princípios e Práticas para Desenvolvimento de Software com Produtividade. Editora Independente, 2022. MARTIN, R. C.. Código Limpo: Habilidades Práticas do Agile Software. 1ª ed. Alta Books. 2009				
BIBLIOGRAFIA COMPLEMENTAR: PRIKLADNICKI, R.; WILLI, R.; MILANI, F.. Métodos Ágeis para Desenvolvimento de Software. Bookman, 2014. MARTIN, R. C.. Arquitetura Limpa: o Guia do Artesão Para Estrutura e Design de Software. 1ª ed. Alta Books. 2019 FOWLER, M.. Refatoração: Aperfeiçoando o Design de Códigos Existentes. 2ª ed. Novatec Editora. 2020 PRESSMAN, R. S.; MAXIM, B. R.. Engenharia de Software: Princípios e Práticas para Desenvolvimento de Software com Produtividade. 9ª ed. Porto Alegre: AMGH, 2021. KIM, G.; HUMBLE, J.; WILLIS, J.; DEBOIS, P.. Manual de DevOps: Como Obter Agilidade, Confiabilidade e Segurança em Organizações Tecnológicas. 1ª Ed. Alta Books. 2018.				

COMPONENTE CURRICULAR: Tópicos Avançados em Inteligência Artificial				
EIXO TEMÁTICO: Inteligência Aplicada e Simulação em Cibersegurança				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
45	15	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Aprendizado de Máquina; Aprendizado Profundo.				
EMENTA: Tópicos avançados em um ou mais temas da Inteligência Artificial e Pesquisa Operacional; estudo de técnicas conforme o estado da arte na área; aprofundamento de métodos, algoritmos e aplicações emergentes; abordagem flexível para adaptação a novas tendências e demandas.				
BIBLIOGRAFIA BÁSICA: RUSSELL, S.; NORVIG, P. Inteligência Artificial: Uma Abordagem Moderna. 3ª ed. Rio de Janeiro: Elsevier, 2013. FACELI, K.; LORENA, A. C.; GAMA, J.; CARVALHO, A. C. P. L. F. Inteligência Artificial: Uma Abordagem de Aprendizado de Máquina. 2ª ed. LTC, 2021. GOLDBARG, M. C.; GOLDBARG, E.; LUNA, H. P. L. Otimização Combinatória e Metaheurísticas - Algoritmos e Aplicações. 1ª ed. Rio de Janeiro: LTC, 2016.				
BIBLIOGRAFIA COMPLEMENTAR: ARENALES, M., ARMENTANO, V., MORABITO, R., YANASSE, H. Pesquisa Operacional para Cursos de Engenharia, Rio de Janeiro: Elsevier-Campus, 2007. LUGER, G. F. Inteligência Artificial 6ª ed. Pearson, 2013. WEISS, G. Multiagent Systems. MIT Press, 2013. SILVA, L. A.. Introdução à Mineração de Dados - Com Aplicações em R: com Aplicações em R. 1ª ed. GEN LTC. 2016. GENDREAU, M.; POTVIN, J-Y. Handbook of Metaheuristics. 3rd Ed. Springer, 2019.				

COMPONENTE CURRICULAR: Educação Ambiental e Sustentabilidade Tecnológica				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Optativo	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Educação ambiental e sustentabilidade na era digital. Responsabilidade socioambiental na engenharia e na tecnologia da informação. Poluição eletrônica e descarte sustentável de equipamentos. Green IT e eficiência energética em infraestruturas digitais. O papel da cibersegurança na mitigação de impactos ambientais. Projetos de inovação tecnológica sustentável e economia circular. Princípios éticos e ecológicos aplicados à atuação profissional.				
BIBLIOGRAFIA BÁSICA: DIAS, Genebaldo Freire. Educação Ambiental: princípios e práticas. 9. ed. São Paulo: Gaia, 2022. MURUGESAN, San. Harnessing Green IT: Principles and Practices. Wiley, 2018. VEIGA, José Eli da. Desenvolvimento Sustentável: o desafio do século XXI. 5. ed. Rio de Janeiro: Garamond, 2019.				
BIBLIOGRAFIA COMPLEMENTAR: LANGE, Stephan; GALL, Daniel. Sustainable IT Architecture: The Progressive Approach to Green IT. Springer, 2021. LAYRARGUES, Philippe Pomier (org.). Identidades da Educação Ambiental Brasileira. Brasília: MMA, 2004. CAPRA, Fritjof; LUISI, Pier Luigi. A Visão Sistêmica da Vida. São Paulo: Cultrix, 2014. LEFF, Enrique. Saber Ambiental: Sustentabilidade, Racionalidade, Complexidade, Poder. 7. ed. Petrópolis: Vozes, 2020. SACHS, Ignacy. Caminhos para o Desenvolvimento Sustentável. Rio de Janeiro: Garamond, 2009.				

COMPONENTE CURRICULAR: Direitos Humanos, Ética e Tecnologia				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Optativo	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Fundamentos dos direitos humanos e sua relação com ciência, tecnologia e inovação. Ética e cidadania digital. Privacidade, liberdade e proteção de dados como direitos fundamentais. Diversidade e inclusão na área tecnológica. Violência digital, discurso de ódio e direitos das minorias nas redes. Papel da engenharia e da cibersegurança na promoção de uma sociedade justa, segura e igualitária. Análise de marcos legais e de políticas públicas em direitos humanos digitais.				
BIBLIOGRAFIA BÁSICA: BRASIL. Plano Nacional de Educação em Direitos Humanos. Brasília: SEDH/MEC/UNESCO, 2018. BAUMAN, Zygmunt. Vigilância Líquida. Rio de Janeiro: Zahar, 2014. DONEDA, Danilo; MENDES, Laura Schertel. Tratado de Proteção de Dados Pessoais. São Paulo: Thomson Reuters Brasil, 2021.				
BIBLIOGRAFIA COMPLEMENTAR: UNESCO. Diretrizes para a Educação em Direitos Humanos. Paris: UNESCO, 2012. SEN, Amartya. Desenvolvimento como Liberdade. São Paulo: Companhia das Letras, 2021. CORTINA, Adela. Ética Mínima. São Paulo: Martins Fontes, 2020. CASTELLS, Manuel. Redes de Indignação e Esperança. Rio de Janeiro: Zahar, 2018. RIBEIRO, Djamila. Pequeno Manual Antirracista. São Paulo: Companhia das Letras, 2019.				

COMPONENTE CURRICULAR:			História e Cultura Afro-Brasileira, Africana e Indígena na Sociedade Digital	
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Optativo	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
60	0	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: História e cultura afro-brasileira, africana e indígena no contexto contemporâneo. A presença negra e indígena na ciência e na tecnologia. Tecnologias ancestrais, saberes tradicionais e inovação social. Cidadania digital e representatividade em ambientes tecnológicos. Racismo algorítmico e vieses em sistemas de inteligência artificial. Políticas públicas, legislação e ações afirmativas na educação e na tecnologia. Produção de conteúdos digitais para valorização da diversidade cultural.				
BIBLIOGRAFIA BÁSICA: GOMES, Nilma Lino. O Movimento Negro Educador: saberes construídos nas lutas por emancipação. Petrópolis: Vozes, 2017. MUNANGA, Kabengele. Rediscutindo a mestiçagem no Brasil: identidade nacional versus identidade negra. 5. ed. Petrópolis: Vozes, 2019. BRASIL. Lei nº 10.639/2003 e Lei nº 11.645/2008. Diretrizes Curriculares Nacionais para Educação das Relações Étnico-Raciais. MEC, 2013.				
BIBLIOGRAFIA COMPLEMENTAR: RIBEIRO, Djamila. Quem tem medo do feminismo negro? São Paulo: Companhia das Letras, 2018. NASCIMENTO, Abdias. O Genocídio do Negro Brasileiro. 3. ed. São Paulo: Perspectiva, 2017. KRENAK, Ailton. Ideias para Adiar o Fim do Mundo. São Paulo: Companhia das Letras, 2020. MBEMBE, Achille. Crítica da Razão Negra. Lisboa: Antígona, 2018. SILVA, Petronilha Beatriz Gonçalves e. Educação das Relações Étnico-Raciais: fundamentos teóricos e práticas educativas. Brasília: MEC, 2015.				

15.4 Componentes Curriculares de Extensão

COMPONENTE CURRICULAR: CCEX - Saúde Digital e Proteção de Dados				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Extensão	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
-	-	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Fundamentos de Cibersegurança				
EMENTA: Introdução à saúde digital e seus desafios em privacidade e proteção de dados. Aplicação da LGPD e GDPR em sistemas de saúde. Tecnologias de registro eletrônico em saúde (RES) e riscos associados. Criptografia e anonimização em dados clínicos. Ética e bioética no tratamento de dados de pacientes. Estudos de caso em hospitais, clínicas e telemedicina. Projetos de extensão junto à comunidade para conscientização sobre proteção de dados em saúde.				
BIBLIOGRAFIA BÁSICA: DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2022. MACHADO, Carla. Saúde Digital: Inovação, Regulação e Desafios Éticos. São Paulo: Fiocruz, 2021. TETTAMANZY, Ana Claudia. LGPD comentada: fundamentos e práticas de proteção de dados. São Paulo: Thomson Reuters, 2022.				
BIBLIOGRAFIA COMPLEMENTAR: PIPINO, Leo. Digital Health: Scaling Healthcare to the World. Cham: Springer, 2019. GREENHALGH, Trisha. Digital Health: A Sociotechnical Perspective. Oxford: Oxford University Press, 2022. SHABANI, Mahsa. Genomic Data Sharing and Privacy. Cambridge: Cambridge University Press, 2020. ISO. ISO 27799: Health informatics — Information security management in health. ISO, 2016. TOPOL, Eric. Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again. New York: Basic Books, 2019.				

COMPONENTE CURRICULAR: CCEX - Cibersegurança em Cidades Inteligentes				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Extensão	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
-	-	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Redes de Computadores II				
EMENTA: Conceitos fundamentais de cidades inteligentes e seus desafios de cibersegurança. IoT e sistemas ciberfísicos aplicados ao espaço urbano. Proteção de infraestruturas críticas urbanas (energia, transporte, saneamento, comunicações). Governança digital e políticas públicas para cidades seguras. Análise de riscos e incidentes em ambientes urbanos. Projetos práticos de extensão para conscientização e simulações de segurança em cidades inteligentes.				
BIBLIOGRAFIA BÁSICA: NAM, Taewoo; PARDO, Theresa. Smart City as Urban Innovation. ACM, 2011. HARRISON, Colin; DONNELLY, Ian. A Theory of Smart Cities. Proceedings of the 55th Annual Meeting of the ISSS, 2011. KITCHIN, Rob. The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences. London: Sage, 2014.				
BIBLIOGRAFIA COMPLEMENTAR: ALBINO, Vito; BERARDI, Umberto; DANGELICO, Rosa Maria. Smart Cities: Definitions, Dimensions, Performance, and Initiatives. Journal of Urban Technology, v. 22, n. 1, p. 3–21, 2015. ZANELLA, Andrea et al. Internet of Things for Smart Cities. IEEE IoT Journal, v. 1, n. 1, p. 22–32, 2014. BATAGAN, Lorena. Smart Cities and Sustainability Models. Informatica Economica, v. 16, n. 3, p. 80–87, 2012. PEREIRA, Gabriela et al. Urban Governance and Smart Cities. Cham: Springer, 2020. CAVOUKIAN, Ann. Privacy by Design in Smart Cities. Toronto: IPCO, 2017.				

COMPONENTE CURRICULAR: CCEX - Defesa Digital e Direitos Humanos				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Extensão	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
-	-	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Interseção entre cibersegurança e direitos humanos. Liberdade de expressão, privacidade e vigilância digital. Cibersegurança como direito fundamental. Riscos de exclusão digital e discriminação algorítmica. Marcos regulatórios nacionais e internacionais para defesa digital. Estudos de casos sobre censura, desinformação e ataques digitais contra comunidades vulneráveis. Projetos de extensão voltados para a promoção da cidadania digital e defesa dos direitos humanos no espaço virtual.				
BIBLIOGRAFIA BÁSICA: DONEDA, Danilo. Proteção de Dados como Direito Fundamental. São Paulo: Thomson Reuters, 2022. ZUBOFF, Shoshana. The Age of Surveillance Capitalism. New York: PublicAffairs, 2019. UNESCO. Human Rights in the Digital Age. Paris: UNESCO, 2020.				
BIBLIOGRAFIA COMPLEMENTAR: MOROZOV, Evgeny. The Net Delusion: The Dark Side of Internet Freedom. New York: PublicAffairs, 2012. SCHNEIER, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton, 2015. UNITED NATIONS. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. UN, 2021. DEIBERT, Ronald. Reset: Reclaiming the Internet for Civil Society. Toronto: House of Anansi, 2020. MANTELERO, Alessandro. AI and Human Rights: The Role of Ethics by Design. Computer Law & Security Review, v. 35, n. 2, 2019.				

COMPONENTE CURRICULAR: CCEX - Educação Continuada em Segurança Digital				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO: Extensão	
CARGA HORÁRIA (horas):				
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
-	-	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: -				
EMENTA: Estratégias de educação e capacitação em segurança digital. Alfabetização digital e conscientização em segurança para diferentes públicos (estudantes, empresas, comunidades). Desenvolvimento de cursos, oficinas e campanhas educativas. Gamificação e metodologias ativas em educação para cibersegurança. Análise de programas nacionais e internacionais de capacitação. Projetos de extensão de impacto social em inclusão e segurança digital.				
BIBLIOGRAFIA BÁSICA: SCHNEIER, Bruce. Secrets and Lies: Digital Security in a Networked World. New York: Wiley, 2015. ANDRESS, Jason. Foundations of Information Security. No Starch Press, 2019. SILVA, Tatiana. Educação Digital e Cidadania na Era da Informação. São Paulo: Atlas, 2021.				
BIBLIOGRAFIA COMPLEMENTAR: ENISA. Cybersecurity Training and Awareness. European Union Agency for Cybersecurity, 2020. NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE). Framework for Improving Cybersecurity Workforce. NIST, 2017. JOHNSON, Michael. Cybersecurity Awareness for Dummies. Hoboken: Wiley, 2020. FERREIRA, Patrícia. Inclusão Digital e Cidadania. Porto Alegre: Sulina, 2020. ROSS, John. Teaching Digital Security. Routledge, 2021.				

COMPONENTE CURRICULAR: CCEX - Análise de Incidentes Cibernéticos				
EIXO TEMÁTICO: -				
PERÍODO DE OFERTA: -			NÚCLEO DE CONTEÚDO:	
CARGA HORÁRIA (horas):			Extensão	
TEÓRICA:	PRÁTICA:	TOTAL:	NATUREZA:	Optativo
-	-	60	CRÉDITOS:	4
MODALIDADE DE OFERTA: Presencial				
PRÉ-REQUISITOS: Fundamentos de Cibersegurança; Sistemas Operacionais; Redes de Computadores I.				
EMENTA: Introdução à resposta a incidentes cibernéticos. Tipos de incidentes: malware, phishing, ataques DDoS, ransomware. Estrutura de equipes de resposta a incidentes (CSIRT/CERT). Procedimentos de identificação, contenção, erradicação e recuperação. Ferramentas de análise forense e coleta de evidências digitais. Documentação e comunicação em resposta a incidentes. Estudos de casos práticos. Projetos de extensão voltados para conscientização e resposta comunitária a incidentes de segurança.				
BIBLIOGRAFIA BÁSICA: STALLINGS, William. Network Security Essentials: Applications and Standards. 6. ed. Pearson, 2022. ENISA. Incident Response Planning Guide. European Union Agency for Cybersecurity, 2021. GRIMES, Roger. Ransomware Protection Playbook. Hoboken: Wiley, 2021.				
BIBLIOGRAFIA COMPLEMENTAR: NIST. Computer Security Incident Handling Guide (SP 800-61r2). Gaithersburg: NIST, 2012. BRIAN, Craig. Incident Response Techniques for Ransomware Attacks. Packt Publishing, 2021. WOJTASZEWICZ, Pawel. Incident Management for Operations. Springer, 2019. SANS Institute. Incident Handler's Handbook. SANS, 2020. MANDIANT. M-Trends 2023: Cybersecurity Insights. Mandiant, 2023.				

16. REFERÊNCIAS BIBLIOGRÁFICAS

- FOFONCA, E. et al. (Orgs.). **Metodologias pedagógicas inovadoras: contextos da educação básica e da educação superior**. v. 2. Curitiba: Editora IFPR, 2018. 183 p. Disponível em: https://ifpr.edu.br/wp-content/uploads/2018/08/E-book-Metodologias-Pedagogicas-Inovadoras-V.2_Editora-IFPR-2018.pdf. Acesso em: 10 set. 2025.
- FÓRUM DE PRÓ-REITORES DE EXTENSÃO DAS INSTITUIÇÕES PÚBLICAS DE EDUCAÇÃO SUPERIOR BRASILEIRAS (FORPROEX). **Política Nacional de Extensão Universitária**. Porto Alegre: UFRGS/Pró-Reitoria de Extensão, 2012.
- FÓRUM ECONÔMICO MUNDIAL. **Future of Jobs Report 2025**. 2025. Disponível em: https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf. Acesso em: 10 set. 2025.
- MORIN, André. **Pesquisa-ação Integral e Sistêmica – Uma Antropopedagogia Renovada**. 1. ed. Rio de Janeiro: DP & A, 2024.
- UNIVERSIDADE FEDERAL DO SUL DA BAHIA (UFSB). **Plano de Desenvolvimento Institucional PDI 2025-2031**. Itabuna, BA: UFSB, 2025. Disponível em: https://ufsb.edu.br/proplan/images/CPOR_DIRPLAN/PDI_2025_2031/UFSB_PDI_2025_2031_Aprovado_Consuni_16072025.pdf. Acesso em: 20 ago. 2025.
- UNIVERSIDADE FEDERAL DO SUL DA BAHIA (UFSB). **Plano Orientador da Universidade Federal do Sul da Bahia**. Itabuna / Porto Seguro / Teixeira de Freitas, BA: UFSB, 2014. Disponível em: <https://ufsb.edu.br/wp-content/uploads/Plano-Orientador-UFSB-Final1.pdf>. Acesso em: 20 ago. 2025.