FACULDADE ACADI-TI

ACADI-TI CONSULTORIA EM INFORMÁTICA LTDA-EPP

PROJETO POLÍTICO PEDAGÓGICO DO CURSO SUPERIOR DE TECNOLOGIA EM DEFESA CIBERNÉTICA

São José dos Campos

2022

1. CONTEXTUALIZAÇÃO DA INSTITUIÇÃO

1.1 HISTÓRICO INSTITUCIONAL

A ACADI-TI Consultoria Em Informática - LTDA-EPP, mantenedora da Faculdade ACADI-TI, iniciou suas atividades em 2012, com a Academia Inovadora de TI (ACADIT-TI), idealizado pelo CEO da empresa, Josué Sena Luz.

Em 2015, o Centro de Treinamento Autorizado (ATC), ACADI-TI tornou-se parceira da EC-Council, primeira Brand em cibersegurança. A ACADI-TI faz uso de uma metodologia de *Four Phased InfoSec* para avaliar, bloquear, corrigir e defender a segurança da informação no ambiente em que atua, e com este esforço gradativamente a ACADI-TI foi reunindo atributos e valores necessários para garantir as implementações em segurança cibernética, desenvolvendo assim uma estrutura de segurança cibernética que ajuda na identificação, proteção, detecção, resposta e recuperação a ameaças cibernéticas.

Os serviços da ACADITI foram organizados de acordo com as cinco funções contínuas mencionadas na Estrutura de segurança cibernética do NIST, que foi elaborada pelo Instituto Nacional de Padrões e Tecnologia (NIST) do Departamento de Comércio dos Estados Unidos da América, a saber: identificar, proteger, detectar, responder e recuperar de modo a dar respostas imediatas a quaisquer ameaças cibernéticas.

Com isto as melhores ferramentas foram agregadas, como: Anomali, Darktrace, Aqua, Thucotic, Veracode, Salt, Kenn Security, Sophos e Bitglas de maneira a apoiar os clientes a escolher a melhor solução em cibersegurança. Na análise de segurança avançada, a ACADITI manteve seu entendimento que o valor vem das pessoas, e sendo assim, o software não é o que fornece as respostas; ele fornece as ferramentas e os dados necessários para descobrir as respostas.

Assim, uma série de parcerias, treinamento e certificações foram sendo incorporadas, de modo a tornar a ACADITI, como referência no Sudeste em Ciberseguranca. A parceria com Ec-Council – Lider Mundial em capacitação e certificação em Segurança Cibernetica e criadora da certificação CEH, trouxe o selo de qualidade e certificação internacional aos

cursos de formação da ACADITI. A Offensive Security que definiu um padrão de excelência em treinamento de *penetration testing*, com esta certificação o estudante é considerado um especialista em *penetration testing*. E, a parceira com a CompTIA, consolidou o elo com uma das principais associações comerciais do setor de TI, pois é líder em certificações profissionais para o setor de tecnologia da informação.

Em 2018, com a chegada do ex-diretor da EC-Council, Leandro Mainardi, ocorre uma revolução da empresa, onde muda-se o foco para Cybersecurity. Esse movimento vem acompanhado da 1ª Pós-Graduação em Cibersegurança Ofensiva.

Em 2019, a Pós-Graduação em Cibersegurança Ofensiva, apresenta-se como única e inovadora e recebe o prêmio da EC-Council Global Awards como o melhor Centro de Treinamento Autorizado na América Latina.

Com a segurança cibernética como paixão e foco na ACADITI, tecnologias, ferramentas e pessoas foram sendo mobilizados para alcançar os mais altos níveis de excelência. Em seus 12 anos de atuação, formaram mais de 1500 alunos.

Além de prestarem atendimento na área de segurança cibernética a mais de 150 clientes corporativos no Brasil, Angola, Espanha, Portugal e São Tomé e Príncipe.

Em 2020, o único instrutor eleito como o melhor instrutor da América Latina, Leonardo La Rosa, vem consolidar ainda mais os esforços e estratégias da Pós-graduação em Cibersegurança, já que ele se certificou no Centro de Treinamento Autorizado.

Atualmente a ACADI-TI e a Offensive Security consolidaram a maior parceria em cibersegurança ofensiva no Brasil para elevar a maturidade do mercado brasileiro.

Dessa forma, a ACADI-TI, a partir dos resultados bem-sucedidos em suas certificações e preocupados em proporcionar educação de qualidade aliada à empregabilidade, trouxe a proposta de desenvolvimento da Faculdade ACADI-TI.

Outro vetor motivador da ACADITI, é que cerca de 83% das organizações empresariais no Brasil devem aumentar o investimento em segurança cibernética em 2022, com o intuito de reduzir os frequentes ataques de hackers registrados durante a pandemia de Covid-19.

É o que apontam os números divulgados em 11 de outubro de 2021 pela pesquisa PwC Digital Trust Insights 2022, que contou com 3,6 mil executivos de negócios, tecnologia e segurança, pois o número de empresas que preveem um aumento nos gastos cibernéticos

para o próximo ano é maior entre as companhias brasileiras, quando comparado outras organizações do mundo. O levantamento mostra que o crescimento nas verbas para combate aos hackers em outros países foi de 69%. Já em comparação com o ano passado, os índices eram bem menores: 55% entre empresas brasileiras e 57% para as internacionais.

A força de trabalho em cibersegurança precisa crescer 145%, para atender a demanda por profissionais qualificados em todo o mundo. O que significa dizer que são necessários 4 milhões de profissionais a mais, para manter empresas e organizações mais seguras.

Hoje, o setor emprega 2,8 milhões em dez países, segundo o Cybersecurity Workforce Study, relatório divulgado pelo (ISC)², uma das principais organizações internacionais da área de cibersegurança.

Essas pessoas ocupam funções, principalmente, em segmentos como tecnologia da informação (22%), serviços financeiros (8%) e setor público (7%). Os EUA empregam a maior parte deles: 805 mil. O Brasil está em segundo lugar, com 486 mil.

Somente na América Latina, a demanda por empregados qualificados chega a 600 mil profissionais; a segunda maior, de acordo com o estudo. A primeira é a região da Ásia e Pacífico, com 2,6 milhões de vagas estimadas no setor.

O pedido de credenciamento da Faculdade ACADITI nasce quase que de forma natural, com as demandas requeridas na sociedade da cibercultura em que há a necessidade de preparar profissionais altamente qualificados para atuar em contexto nacional e internacional em Segurança Cibernética.

1.2 INSERÇÃO DA FACULDADE ACADI-TI NA REGIÃO

A seguir serão apresentados os dados referentes a caracterização do território de inserção da instituição.

Figura 1 – São José dos Campos: cidade polo

Fonte: Foto disponível na internet

1.2.1 Caracterização da cidade polo

A ACADITI está localizada em São José dos Campos, município brasileiro do estado de São Paulo. Localizado a cerca de 97 km da capital, São Paulo, trata-se de um polo industrial, com suas várias indústrias instaladas, porém o comércio também representa um relevante parcela de participação na economia da cidade. A cidade é sede da Região Metropolitana do Vale do Paraíba e Litoral Norte.

Em São José dos Campos estão localizados institutos federais de pesquisa científica, universidades, faculdades, centros de formação de mão de obra qualificada, empresas de tecnologia de ponta e prédios de arquitetura arrojada. Em contrapartida, a zona rural concentra quase 70% do território do município, boa parte em áreas de proteção ambiental (SJC, 2021).

É uma cidade que une cultura, tradição e tecnologia, sendo destaque no país devido ao potencial de negócios, agente que impulsiona investimentos na área de hotelaria, comércio e serviços. É possível constatar isso devido ao alto fluxo de pessoas que circulam pela cidade diariamente, devido aos polos industriais e tecnológicos e centros educacionais.

O desenvolvimento industrial de São José dos Campos iniciou-se em 1935, quando Getúlio Vargas investiu no município após o destaque nacional na chamada fase senatorial, em que doentes buscavam o clima da cidade em busca de cura para a tuberculose (SJC, 2021), inaugurando o maior sanatório do país. Com isso, atraiu mais investimentos e pôde avançar em infraestrutura e saneamento básico.

O processo de industrialização do município tomou impulso em 1950, a partir da instalação do Centro Técnico Aeroespacial (CTA) e inauguração da Via Dutra, em 1951. Com a consolidação da economia industrial, a cidade apresentou, nas décadas seguintes, um grande crescimento demográfico que acelerou o processo de urbanização. O município se localiza estrategicamente entre São Paulo e Rio de Janeiro, e hoje é considerado o mais importante polo aeronáutico e aeroespacial da América Latina, possuindo a EMBRAER - terceira maior produtora mundial de jatos civis e uma das maiores companhias exportadoras nacionais. Além de gerar muitos empregos e mão-de-obra especializada, posicionou São José dos Campos numa nova era de desenvolvimento tecnológico.

De acordo com o site da prefeitura de São José dos Campos (2021), nos anos 90 e início do século 21, São José dos Campos passou por um importante incremento no setor terciário. Hoje, a cidade é um centro regional de compras e serviços, com atendimento a aproximadamente 2 milhões de habitantes do Vale do Paraíba e sul de Minas Gerais.

Além das informações acima, existe o Parque Tecnológico São José dos Campos, criado pela prefeitura da cidade, que é pioneiro no Estado de São Paulo – foi o primeiro parque tecnológico criado em território paulista (PQTEC, 2021). É uma parte fundamental para a inovação no empreendedorismo, fomentando a criação de novas tecnologias, produtos e processos, com atuação nas áreas de aeronáutica, energia, saúde, recursos hídricos e saneamento, espacial e ferroviária.

1.2.2 Caracterização da região

A região de São José dos Campos possui vários parques, ruas arborizadas e praças. Sendo o principal município da Região Metropolitana do Vale do Paraíba e Litoral Norte, a população preserva a cultura local e recebe os vários migrantes, que participam do crescimento regional.

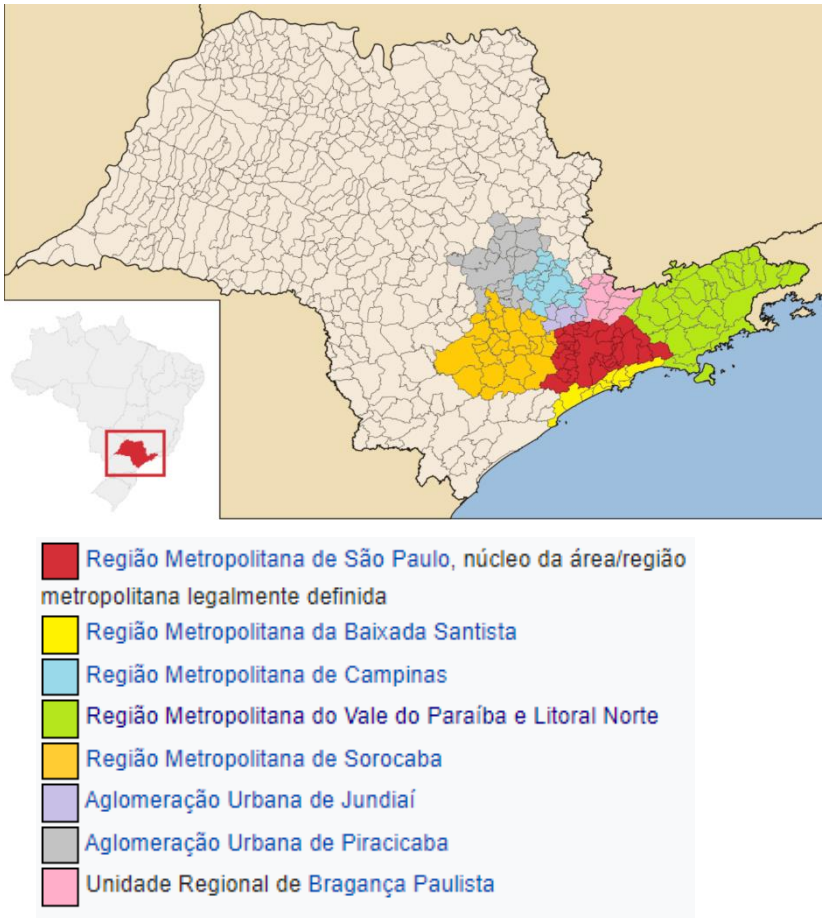
De acordo com o site da prefeitura da cidade, São José dos Campos é ligada por modernas rodovias e pelo aeroporto, estando bem próxima das praias, da região serrana e de outros destinos turísticos do vale. São José dos Campos, segundo o Guia SJC (2021) é um centro de referência no Vale do Paraíba, Sul de Minas, Sul Fluminense e Litoral de São Paulo na área de estudos, trabalho, medicina e serviços diversos.

A região de influência de São José (Ver FIG.2) pode ser compreendida a partir, não de apenas um, mas de vários recortes territoriais. A Região Metropolitana do Vale do Paraíba e Litoral Norte, formada por 39 municípios, é umas das seis regiões metropolitanas do estado de São Paulo e pertence à Macrometrópole de São Paulo (Ver FIG.3). As conexões dessa rede intermunicipal se dão, principalmente, através de rodovias intermunicipais estaduais – SP-50, SP-99, SP-70, SP-65, SP-66, SP-62 – e da rodovia federal BR-116.

Figura 2 – Mapa do Estado de São Paulo

Fonte: Ministério do Interior (1981)

Figura 3 – Macrometrópole



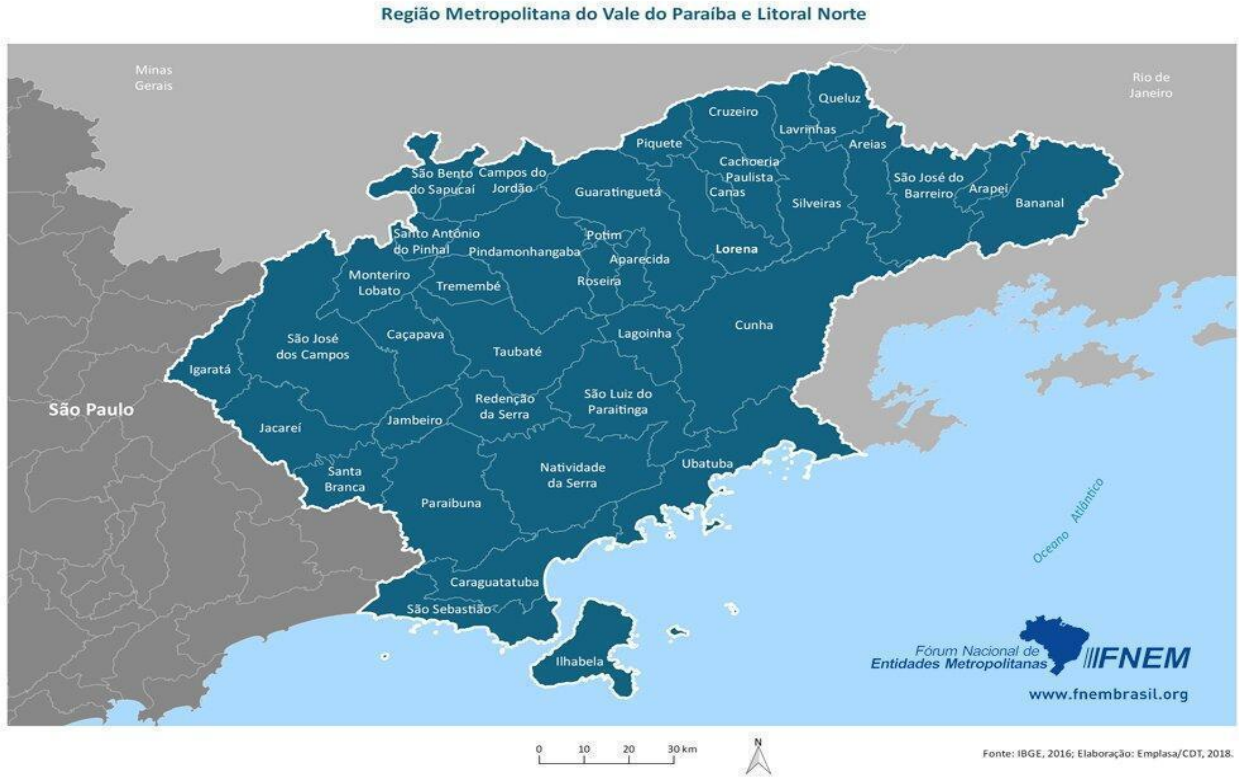
Fonte: Emplasa e Subsecretaria de Desenvolvimento Metropolitano (2020)

O colar metropolitano, do qual São José faz parte, não conforma uma identidade territorial, devido ao crescente processo de conurbação que existe atualmente. As relações da Região Metropolitana do Vale do Paraíba e Litoral Norte ocorrem entre vários municípios, como Taubaté, Aparecida, Caçapava, Guaratinguetá, Caraguatatuba, Campos do Jordão, Pindamonhangaba e Jacareí. A Região Metropolitana pertence ao Complexo Metropolitano Expandido, que compreende também as regiões metropolitanas de São Paulo, Sorocaba, Campinas e Baixada Santista, detendo mais de 75% da população do estado paulista inteiro.

Em síntese, é de se reconhecer que a região de influência de São José, de maneira mais direta, equivale à própria Região Metropolitana do Vale do Paraíba e Litoral Norte (Ver FIG.4).

Adicionalmente, é de se admitir, dependendo da finalidade desejada, por exemplo, na área de inovação e tecnologia, que a região de influência de São José dos Campos não alcança apenas 39 municípios, mas sim o país como um todo.

Figura 4 – Região Metropolitana do Vale do Paraíba e Litoral Norte



Fonte: EMPLASA – Unidade de Dados e Informações Técnicas (2021).

No que diz respeito à Rede Municipal de Serviço de Saúde, São José dos Campos é uma referência em atendimento médico e hospitalar, dispondo de uma rede de hospitais estruturada. É composta por Unidades Básicas de Saúde, Pronto Atendimento (UPA), hospitais com atendimento 24h, e unidades especializadas de saúde, além de outras unidades e hospitais contratados e conveniados. Nas Unidades Básicas de Saúde são estruturados projetos de prevenção a várias doenças e de planejamento e assistência e acompanhamento familiar, incluindo atenção com serviços básicos à população.

São José oferece uma ampla rede de educação básica que conta com instituições públicas e privadas de nível elevado. Além de avançadas incubadoras de base tecnológica, que apoiam projetos e feiras, e manifestações culturais em museus, cinemas, teatros e em inúmeros eventos artísticos. São José percorreu um caminho acelerado onde tem ligação completa com a base de empreendedorismo.

Saúde, qualidade de vida, educação e sustentabilidade. A cidade investe em vida saudável de seus habitantes, mantendo grandes áreas verdes em bairros tranquilos, que garantem qualidade de vida e lazer.

1.2.3 Indicadores econômicos e sociais da região de São José dos Campos

- Indicadores da cidade polo

Tabela 1 – Indicadores Gerais

População	IBGE, Censo 2010	629.921
População	IBGE, Estimada 2021	737.310
PIB municipal	IBGE, 2018	39.697.500,50
PIB per capita	IBGE, 2018	55.603,18
IDHM	PNUD, 2010	0,807 (Muito Alto)

Fonte: IBGE e PNUD-Brasil

Com população, em 2010, de 629.921 habitantes (IBGE, 2010), é estimada, em 2021, com 737.310 habitantes, São José dos Campos ocupa a 5ª posição no ranking populacional estadual é o segundo mais populoso do interior do Brasil, sendo o primeiro em Campinas. Do ponto de vista do PIB. No que diz respeito ao nível de desenvolvimento humano, medido pelo IDHM, com um valor de 0,807, cai para o 12º lugar entre os municípios paulistas.

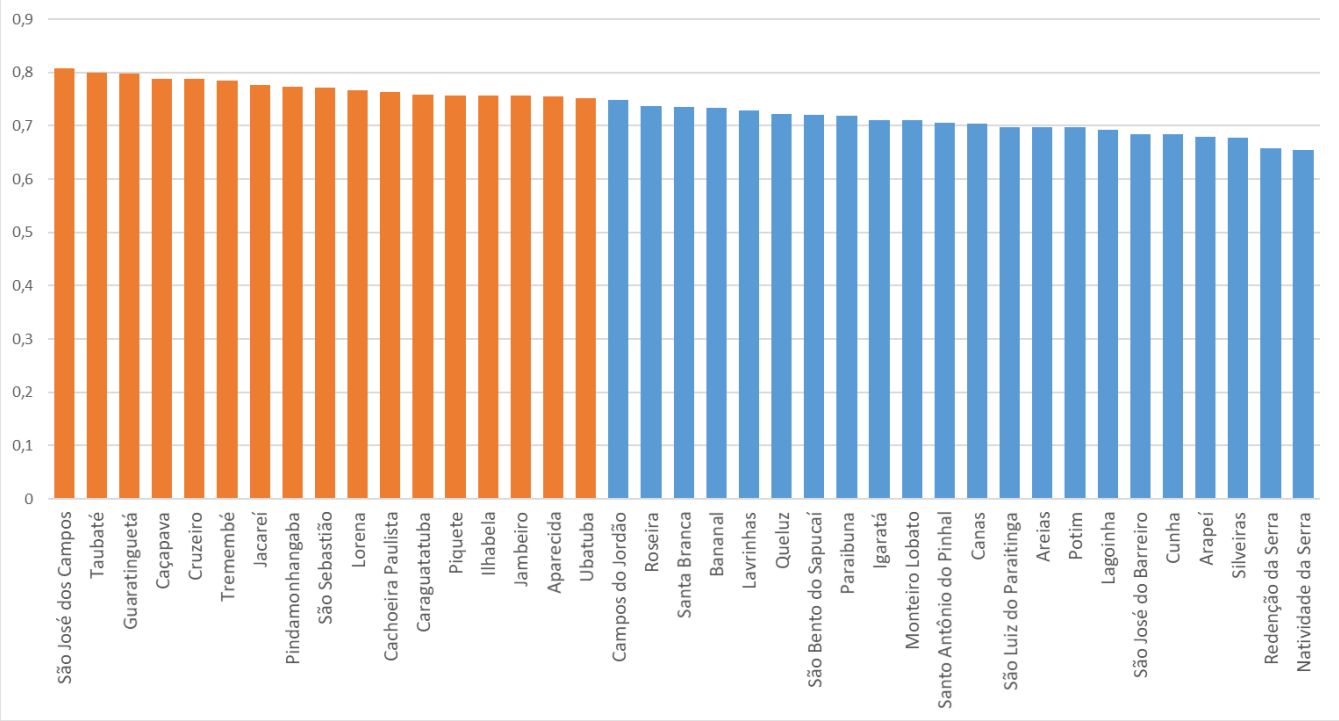
Sobre o IDHM, verifica-se que ele vem tendo um avanço positivo, em todos os seus componentes, na série histórica 2000/2010, respectivamente, de 0,739 a 0,807. De forma estratificada, a expectativa de vida era de 73,39 anos, em 2000, e de 76,27 anos, em 2010 (IBGE, 2010). A propósito do terceiro e último componente, o da educação (Ver TAB.2), com desempenho final de 0,764, é o que teve a maior taxa de crescimento nas últimas décadas.

Algumas observações merecem ser feitas. A primeira, que o IDHM médio regional (0,762) indica que ele se situa numa faixa média (entre 0,680 e 0,807), mas pouco abaixo à média estadual (0,783). A segunda, que 33 dos 39 municípios apresentam IDHM alto (entre 0,721 e 0,798) e 3 muito alto, (entre 0,800 e 0,807). Por fim, que o porte do município parece ter influência no melhor desempenho, uma vez que toda a atenção nas diversas áreas faz com

que a cidade seja reconhecida em todo o país sendo citada como “cidade modelo” e recebendo diversos prêmios em inovação e infraestrutura.

Gráfico 1 – IDHM – Região Ampliada Região Metropolitana do

Vale do Paraíba e Litoral Norte



Fonte: IBGE, 2021

Tabela 2 – IDHM Educação

Componentes	2000	2010
% de 18 anos ou mais com ensino fundamental completo	58,06	70,28
% de 5 a 6 anos frequentando a escola	73,87	93,09
% de 11 a 13 anos frequentando os anos finais do ensino fundamental	85,00	89,77
% de 15 a 17 anos com ensino fundamental completo	71,12	78,58
% de 18 a 20 anos com ensino médio completo	47,92	56,79
IDHM Educação	0,655	0,764

Fonte: PNUD Brasil, 2010

Com relação a indicadores de trabalho e renda, a população economicamente ativa de São José dos Campos passou de 68,91%, em 2000, para 70,71%, em 2010, enquanto a taxa de desocupação reduziu de 17,25% para 7,11%, no mesmo período (Ver TAB.3).

Tabela 3 – Ocupação da população de 18 anos ou mais

Ocupação	2000	2010
Taxa de atividade - 18 anos ou mais	68,91	70,71
Taxa de desocupação - 18 anos ou mais	17,25	7,11
Grau de formalização dos ocupados - 18 anos ou mais	69,56	73,29
Nível educacional dos ocupados		
% dos ocupados com fundamental completo - 18 anos ou mais	67,73	77,20
% dos ocupados com médio completo - 18 anos ou mais	48,21	60,14
Rendimento médio		
% dos ocupados com rendimento de até 1 s.m. - 18 anos ou mais	17,20	9,98
% dos ocupados com rendimento de até 2 s.m. - 18 anos ou mais	51,28	54,82

Fonte: PNUD, 2020

Especialmente quanto à renda, é expressivo o percentual da população que vive com até 2 salários-mínimos (s.m) (Ver TAB.3). Há que se ressaltar, nesse caso, que, embora a renda per capita apresente um aumento considerável e que o percentual de pobres e extremamente pobres tenha caído fortemente, ao longo da última década, o índice GINI (Ver TAB.4), que representa um indicador usado para medir o grau de concentração de renda, diminuiu apenas 0,01 depois de 2000, e permaneceu em patamar pior do que o padrão nacional (0,515). De acordo com PNUD (2013), esse índice varia de 0 a 1, numericamente, sendo que 0 representa a situação de total igualdade, ou seja, todos têm a mesma renda, e o valor 1 significa completa desigualdade de renda, ou seja, se uma só pessoa detém toda a renda do lugar.

Tabela 4 – Pobreza e Desigualdade

Indicadores	**2000**	**2010**
Renda per capita	936,61	1190,96
% de extremamente pobres	2,31	1,01
% de pobres	8,90	3,89
Índice de GINI	0,56	0,55

Fonte: PNUD, 2013

1.2.4 Indicadores da região

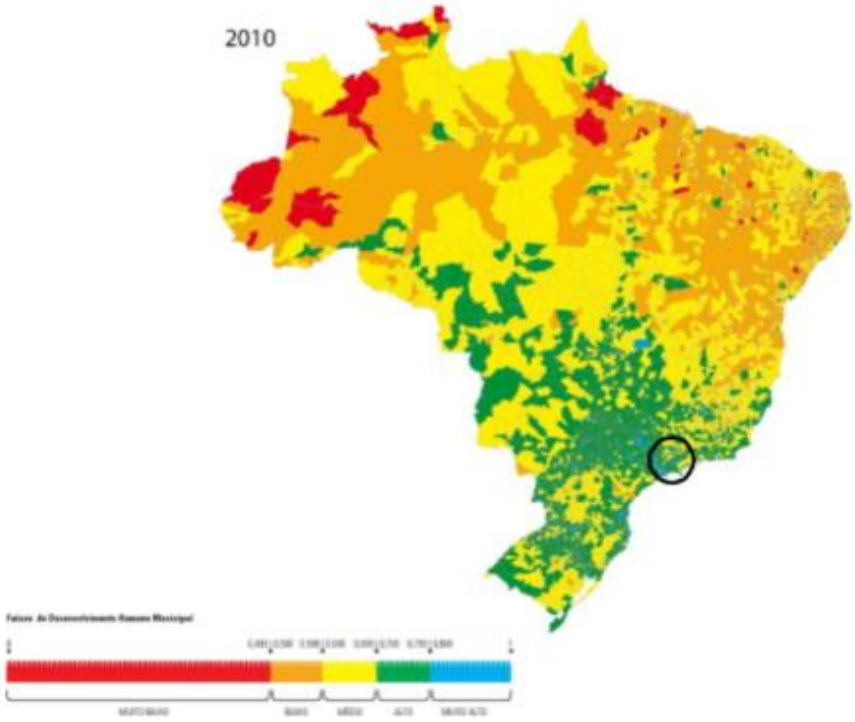
O mapa do IDHM do Brasil (FIG.5) permite uma primeira compreensão da região de influência de São José dos Campos. O IDHM é uma medida composta de indicadores de três dimensões do desenvolvimento humano: longevidade, educação e renda. O índice varia de 0 a 1. Quanto mais próximo de 1, maior o desenvolvimento humano (PNUD, 2010).

São José dos Campos dispõe de um amplo polo industrial, automobilístico e mecânico, o que atrai muitos visitantes com interesse na área tecnológica que se desenvolve. É um grande centro urbano nacional, que se configura como uma área, com nível de desenvolvimento humano alto. Entre as principais instituições e empresas ali sediadas, destacam-se a Embraer, Ambev, General Motors, Ford, Petrobras, Volkswagen, Johnson & Johnson, Instituto de Pesquisa & Desenvolvimento (IPDM), o Instituto Nacional de Pesquisas Espaciais (INPE) e o Departamento de Ciência e Tecnologia Aeroespacial (DCTA).

O Instituto Nacional de Pesquisas Espaciais (INPE), segundo o Portal Brasileiro de Sites Abertos, foi criado em 1961 com o objetivo de capacitar o país nas pesquisas cientificas e nas tecnologias espaciais. Ainda de acordo com o Portal, “ao longo dos anos, suas atividades se ampliaram e a importância dos estudos vão desde assuntos complexos sobre a origem do Universo a aplicações de ciências como nas questões de desflorestamento das nossas matas. O Instituto é centro de excelência, e referência internacional, em pesquisas de ciências espaciais e atmosféricas, engenharia espacial, meteorologia, observação da Terra por imagens de satélite e estudos de mudanças climáticas. O INPE tem como finalidade realizar pesquisas científicas, desenvolvimento tecnológico, atividades operacionais e capacitação de recursos humanos”

A região destaca-se também por abrigar várias instituições de ensino superior com reconhecimento internacional, segundo o site da Prefeitura de São José dos Campos, como ITA (Instituto Tecnológico de Aeronáutica), UNIFESP (Universidade Federal de São Paulo), UNESP (Universidade Estadual de São Paulo), FATEC (Faculdade de Tecnologia de São Paulo), Polo de apoio presencial da UAB (Universidade Aberta do Brasil), Universidade do Vale do Paraíba (Univap), Universidade Paulista (Unip), Etep, Anhanguera, Fundação Armando Álvares Penteado (Faap) e Instituto de Filosofia Santa Teresinha.

Figura 5 – IDH Municipal 2010



Fonte: PNUD-Brasil, 2010

É importante realçar que a área costeira da Região Metropolitana do Vale do Paraíba e Litoral Norte vem se tornando cada vez mais importante nos processos de desenvolvimento no Estado de São Paulo e, também, no Brasil. Isso gera um fluxo de investimentos públicos e corporativos, que acaba atraindo pessoas e aumentando a demanda sobre os recursos naturais, os serviços e os sistemas, assim como sobre a infraestrutura de serviços públicos de acordo com TEIXEIRA, L. (2012).

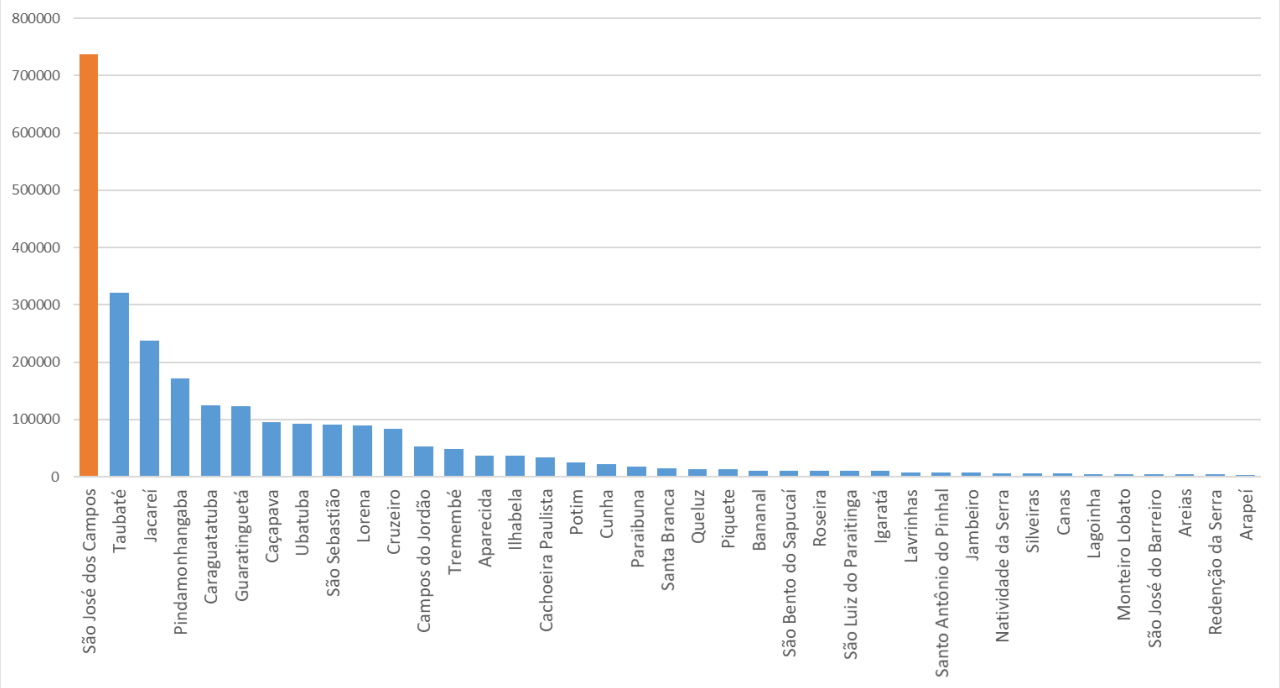
Esse efeito fez com que a região necessitasse de novas políticas sociais, as quais envolvem educação e saúde, fazendo com que a atenção se voltasse para a melhoria do desenvolvimento local, aumentando assim, de uma maneira abrangente, o índice de IDH dos municípios.

O Gráfico 2 mostra a distribuição da população por município da Região Metropolitana do Vale do Paraíba e Litoral Norte, sua região de influência. No primeiro caso, tem-se uma

concentração populacional na cidade polo de 39,6%; ou seja, quase metade da população regional está em São José dos Campos, na sua zona urbana.

Gráfico 2 – População estimada por município

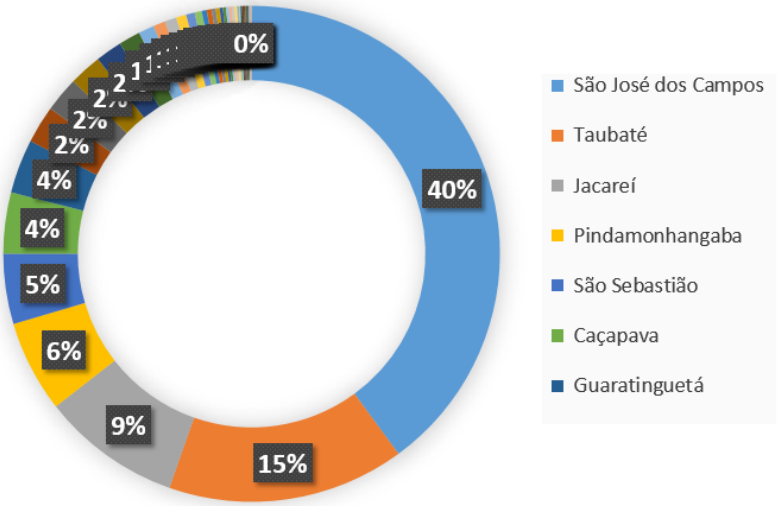
Região Metropolitana do Vale do Paraíba e Litoral Norte



Fonte: IBGE, 2021

Em proporção semelhante, o padrão concentrador de população, que caracteriza a relação intermunicipal regional, replica-se em termos de produção de riqueza. Frente à Região Metropolitana do Vale do Paraíba e Litoral Norte, São José dos Campos é responsável por 40% do PIB Total (GRAF.3), e na sequência, estão os municípios de Taubaté, com 15%, Jacareí, com 9%, e Pindamonhangaba, representando 6%.

Gráfico 3 – PIB Total por município
Região Metropolitana do Vale do Paraíba e Litoral Norte

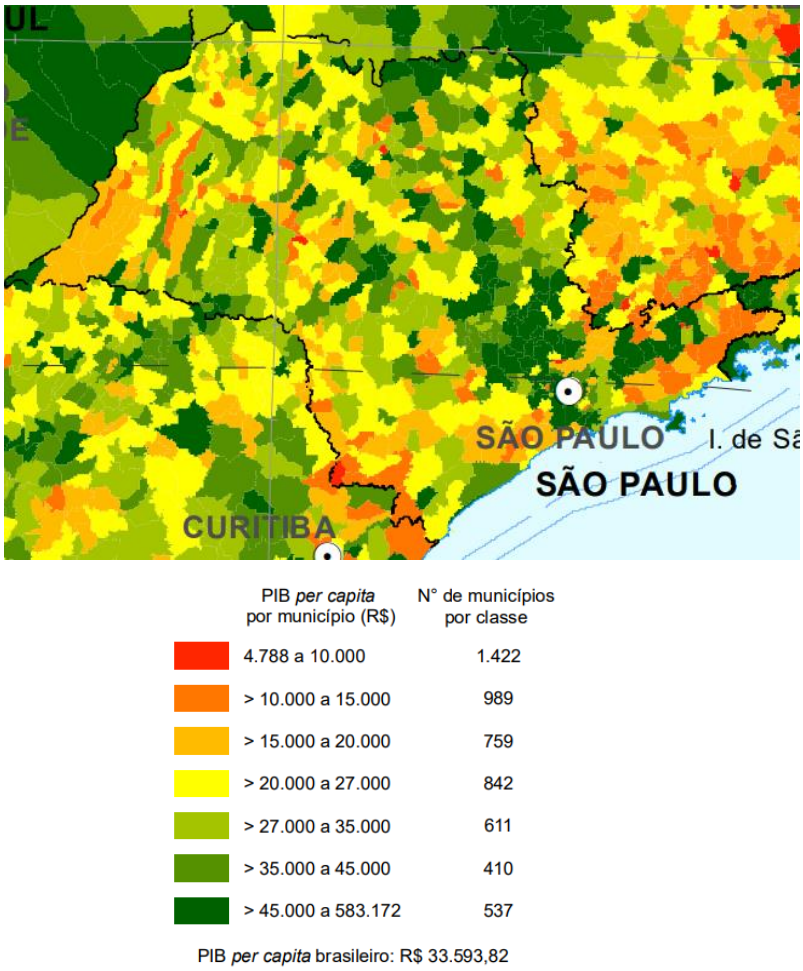


Fonte: Gráfico de autoria própria - dados do IBGE, 2018

A estratificação do PIB Regional possibilita uma observação em relação ao entendimento das características econômicas: São José possui o melhor desempenho em comparação aos outros municípios, representando 40% do total. De acordo com o secretário de Desenvolvimento Econômico e da Ciência e Tecnologia, esses números são condizentes com a realidade de uma cidade que é o maior polo aeroespacial da América Latina e reúne algumas das maiores indústrias do país, líderes nacionais e até mundiais nos respectivos segmentos, de acordo com o site da Prefeitura de São José dos Campos.

Figura 6 – PIB per capita

Região Metropolitana do Vale do Paraíba e Litoral Norte



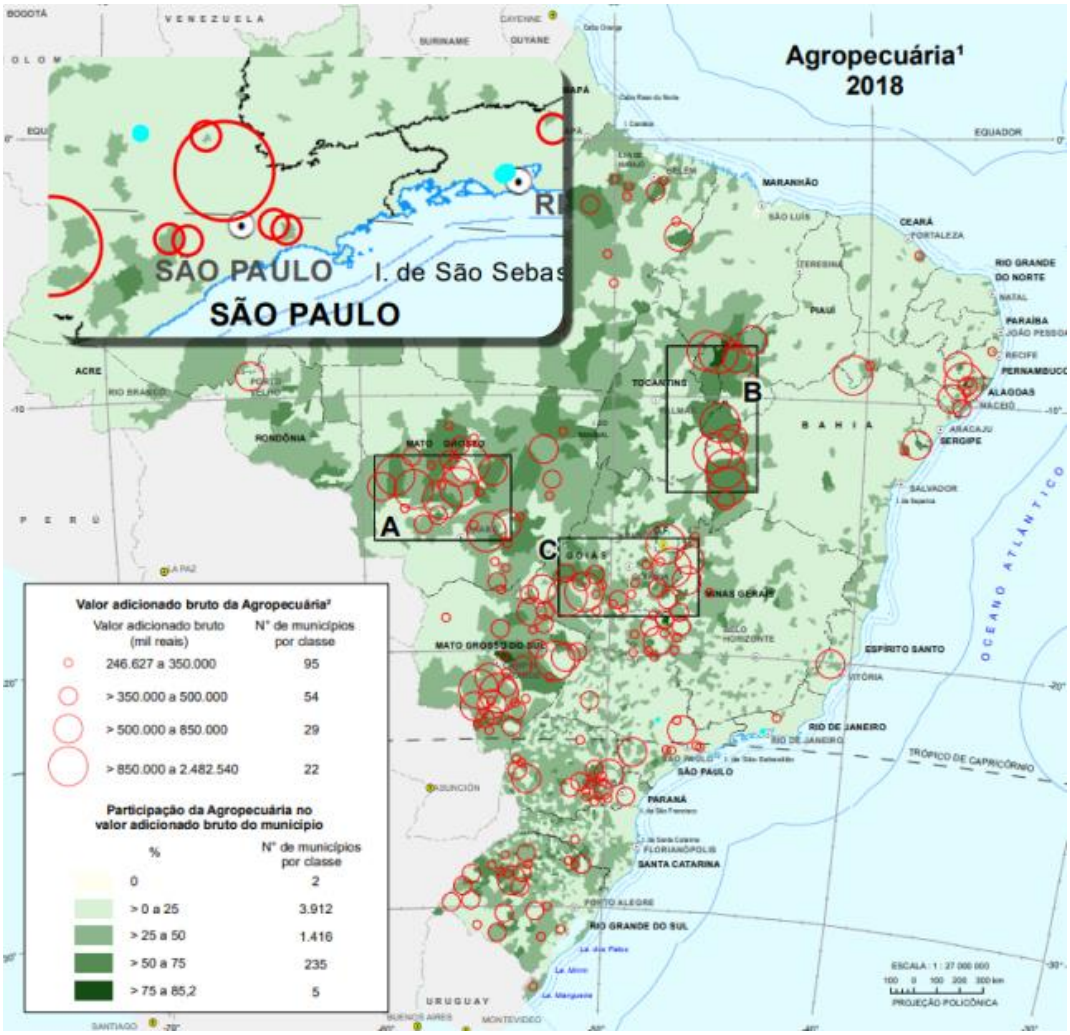
Fonte: IBGE, 2020

https://www.ibge.gov.br/apps/pibmunic

O PIB per capita é um indicador que serve para análise da qualidade de vida de uma região. São José dos Campos, de acordo com o IBGE (2018), se enquadra na categoria que possui um PIB per capita mais alto do Brasil, R$ 55.603,18, estando acima do índice do próprio país, que é de R$ 33.593,82. Considerando a Região Metropolitana do Vale do Paraíba e Litoral Norte, 36% dos municípios possui um PIB per capita acima de R$ 27.000,00, e somente 11 deles, 28%, abaixo de R$ 15.000,00.

A figura 7 mostra que não há rendimento da atividade agropecuária no município de São José dos Campos, com baixíssima participação no valor adicionado bruto municipal total.

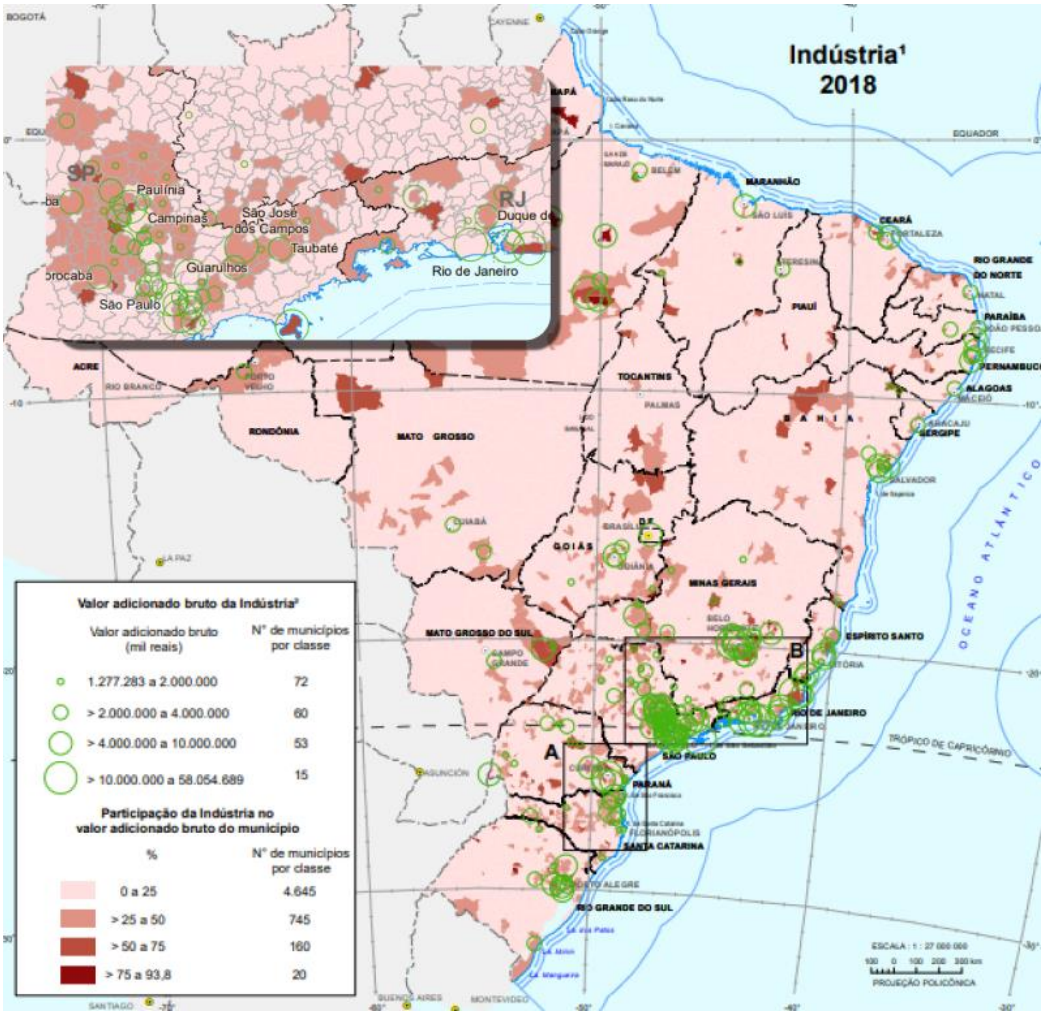
Figura 7 – VAB Agropecuário por município
com foco na Região Metropolitana do Vale do Paraíba e Litoral Norte



Fonte: IBGE, 2018

A figura 8 mostra o total e participação do setor da indústria no valor adicionado bruto municipal. Inclui indústrias extrativas; Indústrias de transformação; eletricidade e gás natural, água, esgoto, gestão de resíduos e atividades de purificação; construção do ciclo anual das contas nacionais IBGE, PIB municipal. Comitê de pesquisa, coordenação de contas nacionais e comitê de ciências da terra, coordenação geográfica.

Figura 8 – VAB da Indústria
com foco na Região Metropolitana do Vale do Paraíba e Litoral Norte



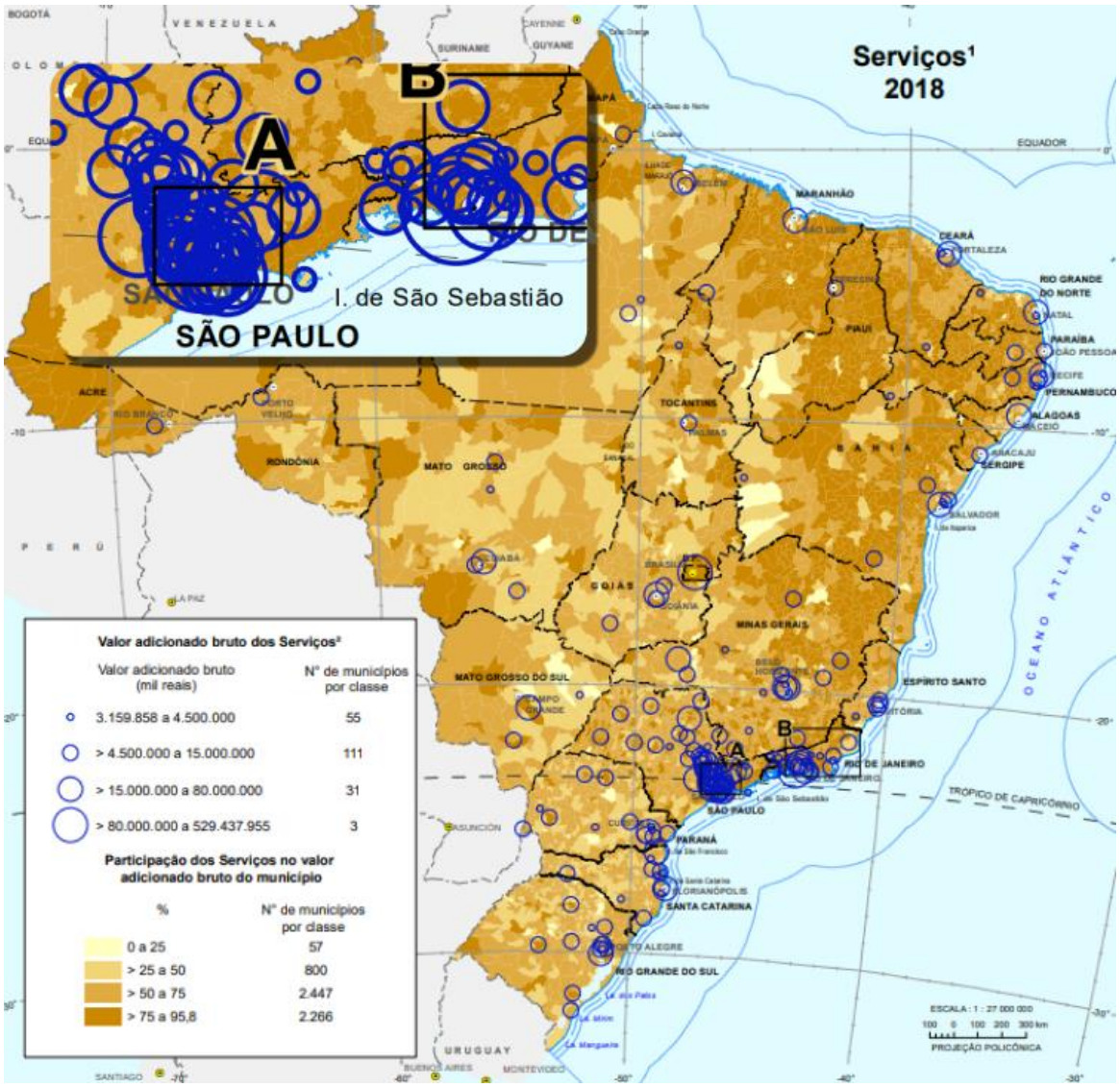
Fonte: IBGE, 2020

Quanto ao rendimento, a atividade industrial ultrapassa todas as outras atividades, que pode ser justificada pelo fato do alto valor adicionado das indústrias instaladas na região, principalmente as voltadas às atividades aeronáuticas e de ciência e tecnologia, que demandam alta qualificação dos funcionários e remuneram melhor.

A figura 9 mostra o valor total e a participação do setor de serviços no valor adicionado municipal, incluindo transporte, armazenamento e correio; alojamento e alimentação; informação e comunicações; finanças, seguros e atividades de serviços relacionados; atividades imobiliárias; atividades profissionais, científicas e técnicas, serviços administrativos e auxiliares; administração, defesa nacional, educação, saúde pública e social segurança;

educação privada e saúde; comércio e reparação de veículos motorizados e motocicletas e outras atividades de serviços.

Figura 9 – VAB de Serviços
com foco na Região Metropolitana do Vale do Paraíba e Litoral Norte



Fonte: IBGE, 2020

Ainda que muito abundante os territórios rurais, a agropecuária representa apenas 0,15%, no tempo em que a indústria por 48,31% e o setor de serviços por 51,54% das atividades realizadas na cidade, conforme IBGE (2011). Apesar do percentual de envolvimento da agropecuária no PIB possa ser baixo considerando os demais setores da economia, é importante

ressaltar que essa participação passou por aumento fundamental (de 0,04% do PIB para 0,15% do PIB) no período entre 1999 e 2010, ainda de acordo com IBGE (2011).

Por último, um dado regional de interesse, diz respeito à população na faixa etária compatível com a educação de nível médio e superior, num cenário de curto prazo, ou seja, a população formada por adolescentes e adultos jovens, na faixa etária de 15 a 29 anos. Ainda que o número disponível remonte ao Censo de 2010 e que, por força da transição demográfica, se saiba que há um envelhecimento persistente da população, ele é considerável, totalizando, naquele ano, quase 588 mil jovens ou mais de ¼ da população total (Ver TAB. 5).

Tabela 5 – População por Agrupamento Etário – 2020

MUNICÍPIOS	15 a 29 anos	População
São José dos Campos	168.655	629.921
Taubaté	72.561	278.686
Jacareí	52.894	211.214
Pindamonhangaba	38.828	146.995
São Sebastião	19.677	73.942
Caçapava	21.864	84.752
Guaratinguetá	28.091	112.072
Caraguatatuba	25.579	100.840
Lorena	21.242	82.537
Cruzeiro	19.400	77.039
Ubatuba	19.780	78.801
Jambeiro	1.380	5.349
Campos do Jordão	12.480	47.789
Tremembé	11.334	40.984
Aparecida	9.240	35.007
Cachoeira Paulista	7.578	30.091
Ilhabela	8.062	28.196

Roseira	2.549	9.599
Santa Branca	3.318	13.763
Paraibuna	4.376	17.388
Cunha	5.293	21.866
Potim	6.307	19.397
Piquete	3.393	14.107
Igaratá	2.144	8.831
São Bento do Sapucaí	2.336	10.468
São Luiz do Paraitinga	2.489	10.397
Bananal	2.417	10.223
Queluz	3.011	11.309
Santo Antônio do Pinhal	1.587	6.486
Lavrinhas	1.781	6.590
Lagoinha	1.090	4.841
Natividade da Serra	1.427	6.678
Silveiras	1.434	5.792
Redenção da Serra	858	3.873
São José do Barreiro	939	4.077
Monteiro Lobato	912	4.120
Canas	1.182	4.385
Areias	895	3.696
Arapeí	592	2.493
TOTAL	**588.975**	**2.264.594**
Percentual	**26%**	**100%**

Fonte: IBGE, 2020

A cidade de São José dos Campos, como relata Medeiros e Perilo (1990), tem projeção internacional e exibe produtos de alto conteúdo tecnológico como aviões, foguetes e satélites. Pode-se afirmar, portanto, que

São José dos Campos constitui um tipo de polo tecnológico que foi implantado sem necessitar de uma estrutura organizacional formal, ainda segundo os autores citados acima. Essa estrutura usualmente é concebida para facilitar a interação entre três parceiros: instituições de ensino e pesquisa, indústrias e governo (nos seus diversos níveis). Essa estrutura existia implicitamente, o que valoriza o caso estudado. (MEDEIROS; PERILO, 1990).

Segundo estimativa da Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação (Brasscom) (2019), até 2024, serão 420 mil novas vagas para absorver a demanda interna, já que milhares de profissionais brasileiros serão contratados por empresas americanas e europeias para trabalhar no programa de home office.

A Brasscom afirmou que em termos de valor móvel os resultados impressionam, pois, o setor de TI já responde por 6,8% do PIB brasileiro, uma média de 90 bilhões de reais por ano.

Com o crescimento da demanda, o foco desse segmento de mercado só é a mão de obra. Ainda segundo a Brasscom (2020) até 2024 a busca por profissionais com habilidades digitais chegará a 70 mil por ano no País, mas o número de formados na área será de 46 mil.

São José dos Campos é um dos exemplos de como o setor de tecnologia se desenvolve e auxilia no desenvolvimento de diferentes regiões. A cidade foi eleita a sexta cidade brasileira mais adequada para empreendedores e sempre foi o centro de inovação do Brasil, baseado no artigo do SPS Consultoria (2021). O Parque Tecnológico de São José dos Campos foi fundado em 2006 e é considerado o maior complexo de inovação e empreendedorismo do Brasil, o que, de acordo com o Diário do Grande ABC (2021) “abre oportunidades para que empresas ofereçam soluções criativas à prefeitura, em áreas como mobilidade, saúde, educação, inteligência de gestão e segurança.”

Segundo ainda o artigo da SPS Consultoria (2021), o Parque cobre uma área de 15 milhões de metros quadrados, com 152 empresas e *startups*, 6 institutos de ciência e tecnologia e 10 instituições de ensino e pesquisa. Cerca de 300 empresas estão conectadas ao parque de alguma forma por meio de programas de inovação e empreendedorismo.

O impacto econômico é enorme. Além de receber altos investimentos públicos e privados, disponibilizou quase 2.000 vagas de emprego, a maioria de alta qualidade, 70% das quais para cargos com ensino superior ou pós-graduação (SPS Consultoria, 2021).

Em matéria no site da Prefeitura de São José dos Campos (2015), foi descrito que mais de 50 empresários se reuniram em São José dos Campos para discutir requisitos, cotações e tendências de tecnologia da informação (TI) na cadeia produtiva do setor aeroespacial.

Na mesma notícia, o secretário de Desenvolvimento Econômico e da Ciência e Tecnologia disse que; "O setor de TI é estratégico para a competitividade da indústria brasileira. Ele exige recursos, mas principalmente criatividade, e o Brasil já possui um nível de conhecimento espetacular nessa área. Ao favorecer a aproximação de dois segmentos tão importantes para a economia de São José dos Campos e do país, o evento contribui para fortalecer nossas empresas no cenário mundial"

O site tiinside, que mostra tendências e inovações em tecnologia e negócios do mundo digital, publicou em abril de 2021, um artigo sobre o investimento de IoT (Internet das Coisas) de São José dos Campos. De acordo com a matéria, o município será o primeiro do Brasil a ser certificado como cidade inteligente (Smart City). O processo de certificação é um movimento inédito no Brasil e traz expectativas de que, no futuro, o conceito de cidade inteligente seja mais bem compreendido e implementado por outras cidades brasileiras. Para obter a certificação, São José investiu em recursos tecnológicos em todas as áreas da gestão pública como saúde, educação, mobilidade urbana e segurança pública, segundo o tiinside (2021).

Desde o início, São José dos Campos tem focado, segundo Medeiros e Perilo (1990), na transferência de tecnologia para a indústria e na superação dos entraves institucionais e burocráticos que ainda hoje existem em vários centros. Assim sendo, a cidade é considerada um dos mais importantes exemplos de desenvolvimento da indústria tecnológica do país (MEDEIROS; PERILO, 1990). Tanto pela relevância de suas instituições de ensino e pesquisa, quanto pelo valor das empresas de base tecnológica, e também pela forte cooperação interativa entre academia e indústria.

1.3 IDENTIDADE INSTITUCIONAL

1.3.1 Missão

A Missão da Faculdade ACADI-TI é

"Ser uma Instituição de Ensino Superior de excelência na formação de profissionais qualificados, éticos e cidadãos. Comprometidos em transformar vidas por meio da educação, ajudando os cidadãos a se manterem seguros no mundo digital".

No âmbito da IES, as prerrogativas que arrolam sua missão inserem-na em um contexto participativo no sentido de proporcionar melhorias significativas ao entorno por meio de suas ações educacionais.

Nesta vertente, o homem é o foco de interesse já que a qualidade de vida depende do desenvolvimento da sociedade na qual ele se insere a partir de ações específicas das organizações do conhecimento. Desse modo, as ações institucionais promulgam o desenvolvimento local e regional, consolidando a razão de ser da Instituição e materializando seus compromissos institucionais com a sociedade a partir do ensino, o qual implica na base para o desenvolvimento sustentável.

Em essência, a ACADITI corrobora sua missão a partir da promoção do Ensino para o desenvolvimento da comunidade, assumindo seu compromisso de ser referência no ensino de cibersegurança, a qual se fundamenta em aspectos de desenvolvimento humano e nas necessidades de diversos segmentos econômicos.

1.3.2 Visão

A visão constitui-se no futuro desejado pela Instituição, com base em um horizonte temporal onde vão ocorrer os esforços individuais, das equipes e o delineamento de recursos aplicados ao desenvolvimento dos objetivos da Instituição. Neste sentido, se apresenta a visão da ACADITI:

"Ser reconhecida, até 2026, como a melhor instituição educacional privada do Estado de São Paulo na área de cibersegurança".

1.3.3 Valores e propósito

Os valores também podem se consolidar em um conjunto de crenças, os quais vão facilitar o compromisso entre os responsáveis pelo desenvolvimento da Instituição e seus stakeholders. Neste sentido, apresenta-se os valores ACADITI da seguinte forma:

- **Acreditar** na educação como forma de construção de uma sociedade mais justa e igualitária;
- **Conceber** a formação profissional pelo princípio da ética, da cidadania e da educação continuada;
- **Buscar**, constantemente, a excelência acadêmica, norteando-se pela responsabilidade social, inclusão e desenvolvimento sustentável;
- **Pensar** a educação como fator decisivo à transformação social e ao progresso científico e tecnológico, de forma a contribuir para o bem comum da sociedade, tornando os cidadãos mais seguros no mundo digital.

1.4 JUSTIFICATIVA PARA O CURSO DE DEFESA CIBERNÉTICA

Barack Obama, quando presidente dos Estados Unidos, já dizia que a próxima guerra seria cibernética, prenunciando um futuro não muito distante. É uma realidade que vai além do universo corporativo, e abala diretamente a rotina e a vida das pessoas no mundo todo.

Hoje já se sabe que boa parte das invasões e sequestro de dados ocorre por falta de cuidado e conhecimento, quando usuários deixam de executar ações básicas de segurança digital. Contudo, vale lembrar, que é também um processo cultural, de hábito doméstico no meio digital.

Assim, no mundo do trabalho, é impossível falarmos de boas práticas de cibersegurança, anteriormente chamada de segurança da informação, sem citarmos a importância da criação de comitês, cartilhas, orientações e treinamento recorrentes de profissionais, porém, apenas isso não basta, se não houver uma conscientização maior de todo um grupo e da sociedade em geral.

É primordial iniciarmos um movimento para a formação de mais profissionais de cibersegurança, os chamados “hackers éticos”, que irão fazer a defesa cibernética das empresas e protegê-las dos hackers mal-intencionados, que, ao contrário dos profissionais éticos, estão à frente e são habilidosos em criar táticas e estratégias para o roubo de dados, ocasionando prejuízo financeiro e de imagem.

Diversas empresas no Brasil, e no mundo todo, já sofreram ataques cibernéticos, até mesmo órgãos públicos tiveram seus sistemas invadidos, como o sofrido pelo Tribunal Federal da 3ª Região, por incrível que pareça.

De acordo com a Cybersecurity Ventures os crimes cibernéticos devem causar um prejuízo na ordem de **US$ 8 trilhões** em 2023, tornando o cibercrime a terceira maior economia do mundo. A previsão é crescer cerca de 15% até 2025.

Por outro lado, as empresas têm dificuldade de contratar profissionais especializados. Levantamento da Cybersecurity estimou que, até o final deste ano, serão abertas mais de **3,5 milhões** de vagas de trabalho na área de segurança cibernética, porém existe um gap de profissionais capacitados e preparados para atuar com cibersegurança, e a escassez é global. Aproximadamente **4 milhões**, de acordo com o International Information System Security Certification Consortium (ISC).

Nesse sentido, o Brasil precisa formar, aproximadamente, **335 mil** profissionais, proporcionalmente. Curiosamente, os salários dos profissionais podem variar entre R$ 5 mil (iniciantes) e ultrapassar R$ 24 mil (profissionais experientes e com alto cargo).

Esses valores são atrativos para as pessoas, principalmente para quem enxerga uma oportunidade profissional em TI. Além disso, para quem já está na área, ter uma formação complementar, como uma pós-graduação em cibersegurança, significa fugir da estagnação e abraçar desafios mais complexos no cotidiano do trabalho.

Em algumas empresas, principalmente fora do Brasil, existe a área de “Blue Team”, que é uma equipe de segurança cibernética que se concentra em defender sistemas e redes contra-ataques maliciosos.

A demanda por esse perfil profissional tem aumentado nos últimos anos, devido ao crescente número de ameaças cibernéticas como ransomware e phishing, além do surgimento de novas ameaças, como deep fakes.

Nesse caso, é utilizado a Inteligência Artificial para criar vídeos ou imagens falsas que parecem ser reais. Essa tecnologia pode ser utilizada para criar conteúdo enganoso, difamatório ou mesmo para fraudes financeiras, é imprescindível a necessidade de proteger seus sistemas.

A IA está sendo cada vez mais sendo utilizada na área de cibersegurança para ajudar a detectar ameaças nas corporações.

Algumas das aplicações de IA na cibersegurança incluem a análise de comportamento, e pode ser usada para analisar o perfil dos usuários e identificar atividades suspeitas, como tentativas de acesso não autorizado ou uso indevido de informações confidenciais.

Além disso, a Inteligência Artificial, pode detectar ameaças usando técnicas de análise de dados e aprendizado de máquina para identificar padrões de comportamento malicioso, como o malware e o phishing.

A IA pode ser usada para responder rapidamente a incidentes de segurança, automatizando tarefas de resposta e mitigação, como a remoção de malware e a restauração de sistemas comprometidos, bem como prevenção de fraudes financeiras, identificando transações suspeitas e comportamentos fraudulentos em tempo real.

Diante de tudo isso, a pergunta que devemos responder é: por que instalar um curso de Defesa Cibernetica em São José dos Campos? E respondemos:

A instalação de um curso de Defesa Cibernética em São José dos Campos é uma medida essencial e estratégica por várias razões. Primeiro, como anteviu Barack Obama, o cenário global está cada vez mais voltado para conflitos cibernéticos, tornando a cibersegurança uma área crítica para a defesa nacional e corporativa. São José dos Campos, sendo um polo tecnológico e industrial de referência no Brasil, possui uma infraestrutura tecnológica avançada que necessita de proteção constante contra ameaças cibernéticas. A formação de profissionais capacitados em defesa cibernética é, portanto, imperativa para salvaguardar os interesses nacionais e empresariais.

Em segundo lugar, a crescente digitalização das atividades cotidianas e corporativas eleva o risco de ataques cibernéticos, como demonstram os prejuízos estimados em US$ 8 trilhões por crimes cibernéticos até 2023. São José dos Campos, com seu ecossistema tecnológico, não está imune a tais riscos. Um curso de Defesa Cibernética na região

contribuirá para mitigar essas ameaças, capacitando indivíduos a implementar práticas de segurança eficazes e a desenvolver soluções inovadoras para combater o cibercrime.

Terceiro, a lacuna global de profissionais qualificados em cibersegurança, estimada em 3,5 milhões de vagas até o final do ano, representa uma oportunidade para São José dos Campos. Ao oferecer formação especializada na área, a cidade pode se tornar um centro de excelência em cibersegurança, atraindo investimentos e criando oportunidades de emprego de alta qualidade para seus cidadãos.

Quarto, a integração da Inteligência Artificial (IA) na cibersegurança, conforme destacado, é uma tendência crescente que exige um novo conjunto de habilidades e conhecimentos. Um curso em São José dos Campos que aborde esses aspectos inovadores prepararia profissionais não apenas para enfrentar desafios atuais, mas também para liderar o desenvolvimento de soluções avançadas em cibersegurança, mantendo a cidade e o país na vanguarda da tecnologia.

Por fim, a instalação de um curso de Defesa Cibernética em São José dos Campos reforçaria o compromisso da cidade com a segurança e inovação tecnológica, alinhando-se com as necessidades globais e nacionais de proteção cibernética. Isso beneficiaria a economia local, através da criação de empregos e atração de investimentos, e contribuiria para a segurança nacional, fortalecendo as capacidades do Brasil de defender suas infraestruturas críticas contra ameaças cibernéticas cada vez mais sofisticadas.

2. ORGANIZAÇÃO DIDÁTICO-PEDAGÓGICA

A Faculdade ACADI-TI, em processo de credenciamento institucional e autorização do curso de Defesa Cibernética, quer se comprometer com a promoção de uma educação superior de qualidade. Amparada por sua missão, a instituição desenvolverá programas de graduação alinhados ao pressuposto da democratização do acesso, amplamente difundido nos documentos oficiais que regem a educação superior no Brasil.

Neste contexto, a ACADI-TI desenvolverá uma proposta pedagógica que busca o desenvolvimento sustentável dos locais onde atua, neste momento em seu polo sede, localizado na Cidade de São José dos Campos. Essa proposta converge para o cumprimento dos objetivos institucionais da instituição e para uma contribuição significativa ao entorno.

De acordo com as informações disponíveis nos órgãos reguladores da educação superior brasileira, o curso da ACADI-TI buscará êxito no momento em que os gestores institucionais assumirem a preocupação de manter a qualidade do curso. Essa preocupação deve se pautar pela observância de critérios prescritos no momento da avaliação institucional e que estão concretizados nos demais cursos da instituição.

A partir de uma integração entre a gestão institucional da ACADI-TI, a Coordenação de Curso, o Colegiado, o Núcleo Docente Estruturante e a Equipe Multidisciplinar, busca-se o desenvolvimento de diferenciais competitivos que permitam a formação de egressos alinhados com este Projeto Pedagógico.

Identificação do Curso	
Mantida	Faculdade ACADITI
Endereço de Funcionamento do Curso	Avenida Barão do Rio Branco, 882, Jardim Esplanada, São José dos Campos/SP.
Vagas a serem autorizadas	800
Carga Horária Total	2080
Tempo mínimo de integralização	2,5 anos (5 semestres)
Tempo máximo de integralização	5 anos (10 semestres)
Modalidade	A distância
Coordenador	Fábio Sena da Luz

Para gerenciar o escopo do curso, a Mantenedora da ACADITI, por meio de seu Presidente, instituiu uma equipe de coordenação e gestão, por intermédio do Núcleo Docente Estruturante (NDE). Essa equipe atuará, em conjunto com a Comissão Própria de Avaliação (CPA) e com a Equipe Multidisciplinar, no desenvolvimento de ações para a consolidação do curso.

Dentre os requisitos propostos, a coordenação do curso passa a assumir a função de acompanhar as demandas institucionais, sociais e da comunidade. Essa função é fundamental para que o perfil do egresso esteja alinhado de modo direto com os direcionamentos estratégicos da Instituição.

2.1 POLÍTICAS INSTITUCIONAIS NO ÂMBITO DO CURSO

As políticas de ensino, iniciação científica e extensão da Faculdade ACADI-TI, traçadas no Plano de Desenvolvimento Institucional (PDI) e detalhadas no Projeto Pedagógico Institucional (PPI), são as bases e pressupostos para o ensino da graduação do curso de Defesa Cibernética.

As ações desenvolvidas pela Coordenação do Curso, integradas às demais instâncias institucionais e aos objetivos do curso, servem como instrumento norteador à construção de reflexões que visem à consolidação das competências e habilidades inerentes à formação do egresso do curso de Defesa Cibernética.

Desta forma, em consonância com PDI, o curso adota as seguintes políticas:

2.1.1 Políticas de ensino

Na Faculdade ACADI-TI, o curso de Defesa Cibernética, atualmente em processo de autorização, incorpora as diretrizes do Projeto Pedagógico Institucional (PDI) com foco em um ensino inovador e estratégico. A coordenação do curso está comprometida com a criação de métodos de aprendizagem dinâmicos, promovendo a interação entre alunos, professores, tutores e as demandas específicas da região de São José dos Campos. Isso inclui a prática da interdisciplinaridade pelos docentes, integrando teoria e prática em suas disciplinas da matriz curricular para formar profissionais conforme o perfil delineado neste projeto pedagógico.

Os professores da ACADITI são altamente qualificados, com larga experiência em Cyber defesa e dedicados a combinar ensino teórico e prático, enriquecendo o conhecimento acadêmico e profissional dos alunos. O curso resposta às demandas Institucionais (PPI) de um ensino contextualizado com o desenvolvimento de práticas profissionais, apoiadas por metodologias que refletem a identidade e os objetivos de formação deste curso.

Um aspecto fundamental do ensino do curso é a inclusão de parte da carga horária das disciplinas serem voltadas às práticas, as quais têm a intenção de imergir os estudantes em ambientes profissionais reais e simulados, inseri-los no trabalho colaborativo em equipe para reforçar o processo educativo. O curso visa formar um profissional da área de Tecnologia com visão holística, capaz de entender a essência dos desafios da cibersegurança nas organizações modernas e as características do seu campo de atuação da área.

Além disso, o curso de Tecnologia em Defesa Cibernética da ACADI-TI vai além do convencional, propondo uma formação abrangente em tecnologia. O objetivo é preparar os alunos não só para compreender, mas também para desenvolver soluções completas em segurança cibernética, equipando-os com uma perspectiva abrangente e prática para enfrentar os desafios contemporâneos na área.

Enquanto políticas de ensino institucional, no curso Tecnologia em Defesa Cibernética na Faculdade ACADI-TI, o NDE definiu cinco princípios fundamentais:

1. **Interatividade e Engajamento Colaborativo**: O curso prioriza métodos de aprendizagem que fomentam a interação ativa entre estudantes, professores. Isso promove um ambiente de aprendizado colaborativo e engajado.
2. **Interdisciplinaridade e Integração Prática-Teórica**: Com a presença dos projetos multidisciplinares em todos os semestres, há um forte enfoque na interdisciplinaridade. Os alunos, e naturalmente professores, são incentivados a integrar teoria e prática nas e entre as disciplinas, e dialogar o conteúdo com o projeto pedagógico.
3. **Qualificação Docente e Desenvolvimento Profissional**: A qualificação do corpo docente no *Programa de Qualificação Docente* é destacada como um elemento chave. Acreditamos que professores altamente qualificados trazem um equilíbrio entre o ensino teórico e prático, contribuindo para o desenvolvimento profissional dos alunos.
4. **Imersão em Contextos Profissionais Reais**: A inclusão de parte da carga horaria das disciplinas com práticas, além dos projetos multidisciplinares extensionistas e o uso de

técnica de simulação e outras abordagens imersivas, visam a inserção dos alunos em ambientes profissionais reais. Esse é um princípio fundamental no PPI da ACADI e que é concretizado no curso de Defesa Cibernética em sua carga horária prática. Isso prepara os estudantes para os desafios reais do campo de segurança cibernética.

5. **Formação Holística e Visão Ampliada**: O curso visa desenvolver nos alunos uma visão holística, preparando-os para compreender e resolver os problemas complexos das organizações modernas. A formação visa ser abrangente, cobrindo não apenas aspectos técnicos, mas também o desenvolvimento de uma compreensão ampla das implicações da tecnologia na sociedade e nos negócios.

2.1.2 Políticas de Iniciação Científica

No âmbito do curso Defesa Cibernética da Faculdade ACADI-TI, a iniciação científica é valorizada como um elemento essencial na formação dos alunos de Tecnologia. Esta abordagem é vista como uma forma de promover o conhecimento teórico, além de ser uma forma de integrar a instituição com o setor organizacional e produtivo da região de São José dos Campos. As atividades de iniciação científica são alinhadas às disciplinas de formação profissional, com um foco particular no desenvolvimento de competências práticas através de projetos e pesquisas.

As práticas de iniciação científica são projetadas para complementar e enriquecer o currículo de graduação tecnológica em Defesa Cibernética, incentivando os alunos a se engajarem na investigação e na produção de conhecimento. Isso inclui a realização de atividades práticas, leitura crítica e a produção de materiais acadêmicos, como *papers* e artigos, que são adaptados conforme as necessidades específicas de cada linha de pesquisa.

A Faculdade ACADI-TI se empenha em desenvolver metodologias que facilitem a inserção dos alunos de Defesa Cibernética em contextos científicos, fomentando a formação de um estudante autônomo e crítico. A Instituição entende a educação superior como um veículo de emancipação e consolidação de valores fundamentais, por isso, previu em seu orçamento uma dotação orçamentária para investir na iniciação cientifica e incentivar professores e alunos para participarem de congresso nacionais e internacionais.

As práticas de iniciação científica na Faculdade ACADI-TI serão propostas pelo Colegiado do Curso e implementadas com o suporte do Núcleo Docente Estruturante (NDE).

Estas atividades serão constantemente reavaliadas para garantir sua relevância, assegurando que os alunos estejam sempre engajados em aprendizagens significativas e alinhadas com as demandas contemporâneas do campo de Defesa Cibernética e demandas específicas de São José dos Campos e Vale do Paraíba.

A iniciação científica no curso de Tecnologia em Defesa Cibernética na Faculdade ACADI-TI centra-se em cinco princípios fundamentais, amplamente discutido pelo NDE:

1. **Integração da pesquisa com o mercado**: A iniciação científica é vista como uma ponte entre a instituição e o mercado (setor produtivo) de São José dos Campos e Região do Vale do Paraíba. Com isso, enfatizamos a importância de conectar a pesquisa acadêmica com as necessidades e os desafios do mundo real, especialmente no contexto da defesa cibernética.
2. **Alinhamento com a Formação Profissional**: As atividades de iniciação científica são alinhadas às disciplinas profissionalizantes do curso. Isso assegura que a investigação científica esteja diretamente relacionada às competências e habilidades requeridas no campo profissional na área de Defesa Cibernética.
3. **Desenvolvimento de Competências Práticas e Teóricas**: A iniciação científica na ACADI-TI é projetada para desenvolver tanto as competências teóricas quanto as práticas. Isso inclui atividades como a produção de *papers* e artigos científicos, bem como a participação em projetos de pesquisa aplicada.
4. **Fomento à Autonomia e Pensamento Crítico**: Um dos objetivos centrais é promover a autonomia e o pensamento crítico entre os estudantes. A instituição busca cultivar estudantes que são não apenas consumidores de conhecimento, mas também produtores ativos e críticos de novas ideias e soluções.
5. **Reavaliação e Adaptação Contínua**: As práticas de iniciação científica são constantemente reavaliadas e adaptadas para garantir sua relevância e eficácia. Isso demonstra um compromisso contínuo com a melhoria e a adaptação às mudanças nas demandas acadêmicas e profissionais, especialmente em um campo dinâmico como a defesa cibernética.

2.1.3 Políticas de Extensão

Na Faculdade ACADI-TI a extensão será valorizada como um elemento fundamental para o desenvolvimento de interações sociais e a relação da IES com a sociedade, contribuindo para a consolidação das políticas sociais e dos objetivos institucionais. Da forma como está compreendida, a Extensão permite uma participação ativa da comunidade na vida acadêmica, fortalecendo o compromisso da instituição com o desenvolvimento social, técnico e estrutural da região em que atua.

Reconhecendo a relevância social do curso de Tecnologia em Defesa Cibernética, pois trata da segurança online de todos nós, a ACADI-TI buscará desenvolver políticas que impulsionem uma contribuição para a sociedade. As atividades de extensão originadas do curso serão vistas como oportunidades para uma construção social duradoura, envolvendo profissionais dedicados à valorização das características e necessidades da comunidade regional.

As ações da Coordenação do Curso, apoiadas pelos órgãos responsáveis pelo desenvolvimento do Projeto Pedagógico, são direcionadas para fomentar eventos e programas que devolvam à sociedade o que é produzido no curso de Defesa Cibernética, em particular, e a área de tecnologia em geral. Estas iniciativas visam engajar a comunidade em questões relacionadas à transformação social, técnica e estrutural promovida por estes profissionais de T.I.

A Faculdade ACADI-TI buscará integrar ensino e extensão através de projetos e ações que transportem o conhecimento acadêmico para fora das paredes da instituição, beneficiando a comunidade mais ampla. Esta abordagem reforça a identidade institucional e contribui para o alcance dos objetivos propostos ao curso. Como hoje a ACADI-TI já faz com a Live de quinta feira aberta ao público, não será diferente quando da operação do curso.

As práticas extensionistas na ACADI-TI serão constantemente reavaliadas pelo Núcleo Docente Estruturante (NDE), com base em dados coletados pela Comissão Própria de Avaliação (CPA) e nas reuniões da coordenação de curso com os líderes de turma. Qualquer necessidade de adequação será aprovada junto ao Colegiado de Curso, garantindo a implementação das melhorias necessárias.

Na Faculdade ACADI-TI, as atividades de extensão do curso de Tecnologia em Defesa Cibernética são baseadas em cinco princípios, propostos e debatidos pelo NDE:

1. **Interação social e comunitária**: As atividades extensionistas são desenvolvidas para fortalecer os laços entre a instituição e a comunidade. Elas promoverão interações sociais que beneficiam tanto os estudantes quanto a sociedade local.
2. **Desenvolvimento regional**: A extensão da ACADI-TI está voltada para o desenvolvimento social, técnico e estrutural de São José dos Campos e região. As atividades são alinhadas com as necessidades locais, contribuindo para o crescimento e aprimoramento da área.
3. **Integração de ensino, iniciação científica e extensão**: As atividades extensionistas são integradas com o ensino e a iniciação científica do curso. Essa abordagem holística permite que o conhecimento acadêmico seja compartilhado com a comunidade externa.
4. **Valorização profissional e engajamento comunitário**: As ações extensionistas valorizam o papel do profissional de Defesa Cibernética e engajam a comunidade em questões relevantes. Elas incluem eventos, palestras e programas que destacam a importância desses profissionais na transformação social e técnica.
5. **Reavaliação contínua e melhoria de práticas:** As atividades extensionistas são continuamente reavaliadas e aprimoradas. Isso é feito com base no feedback da CPA e de reuniões regulares de coordenação. As atividades extensionistas devem ser eficazes, relevantes e alinhadas com os objetivos do curso e as necessidades da comunidade.

2.1.4 Promoção de oportunidades de aprendizagem alinhadas ao perfil do egresso

As políticas institucionais de ensino, iniciação científica e extensão – que acabamos de apresentar – têm um papel fundamental na formação dos estudantes de Defesa Cibernética. Elas estão voltadas para a promoção de oportunidades de aprendizagem que preparem os estudantes para o mercado de trabalho e para a vida cidadã.

Para isso, alinhamos essas políticas ao perfil do egresso, que será tratada página a frente. No perfil do egresso definimos as competências e habilidades que os estudantes devem desenvolver ao longo do curso. Ele foi elaborado com base nas demandas do mercado de Defesa Cibernética em São José dos Campos e Vale do Paraíba.

Quando as políticas institucionais estão alinhadas ao perfil do egresso, elas garantem que os estudantes tenham acesso a uma formação que os prepare para o sucesso na carreira profissional e na vida pessoal.

Para garantir que as políticas institucionais estivessem alinhadas ao perfil do egresso preocupamo-nos em adotar algumas ações que serão realizadas para promover oportunidades de deste alinhamento:

- **Elaboração de currículos flexíveis e atualizados**: Os currículos é flexíveis, em especial no componente Projeto Multidisciplinar Extensionista e nas disciplinas optativas, para permitir que os estudantes personalizem sua formação de acordo com seus interesses e objetivos. Eles também são atualizados periodicamente para acompanhar as mudanças no mercado de trabalho e na sociedade.
- **Oferta de atividades de extensão e pesquisa**: As atividades de extensão e pesquisa são oportunidades valiosas para os estudantes desenvolverem competências e habilidades práticas. Em respeito a Resolução Nº 7, de 18 de dezembro de 2018, ao menos 10% da carga horária, e destinada às ações extensionistas. Os alunos podem envolver projetos de pesquisa, estágios, atividades de voluntariado e participação em eventos e competições.
- **Integração entre ensino, extensão e iniciação científica**: A integração entre ensino, extensão e pesquisa permite que os estudantes tenham uma formação mais completa e interdisciplinar. Ela também contribui para a geração de conhecimento e para o desenvolvimento social.

A promoção de oportunidades de aprendizagem alinhadas ao perfil do egresso é essencial para que a Faculdade ACADI-TI cumpra sua missão de formar profissionais qualificados e cidadãos responsáveis.

2.1.5 Avaliação e revisão as políticas com base em práticas inovadoras

A avaliação e revisão das políticas institucionais de ensino, pesquisa e extensão no curso de Defesa Cibernética são fundamentais para garantir que o curso se mantenha relevante ao logo do tempo, dada a dinamicidade na área de tecnologia. Dissemos há pouco tempo que o objetivo central dessas políticas é formar profissionais com competências técnicas e socioemocionais, contribuir para o avanço da ciência, tecnologia e inovação na área de tecnologia em geral, e da defesa cibernética em particular, e promover a extensão universitária e o envolvimento comunitário.

Para alcançar esses objetivos, a avaliação das políticas incorporão práticas inovadoras, como: a aplicação de tecnologias digitais para facilitar a coleta e análise de dados e fomenta a colaboração; o uso de ferramentas de gestão do conhecimento para organizar e compartilhar informações, apoiando decisões informadas; e a intensificação das avaliações da CPA, tratada como um comitê de qualidade para avaliar o impacto das políticas sobre o curso.

No curso de Defesa Cibernética, algumas práticas específicas serão adotadas, como a criação de um conselho consultivo de avaliação, composto por membros da comunidade acadêmica, para auxiliar na definição de objetivos, elaboração de instrumentos de coleta de dados e análise de resultados. A utilização de métodos de avaliação mistos, que combinam abordagens quantitativas, qualitativas e autoavaliativas, oferece uma visão mais abrangente do desempenho do curso e das políticas institucionais. Além disso, é essencial manter um foco na melhoria contínua, estabelecendo metas claras e utilizando os resultados para aprimorar as práticas educacionais.

Entre os indicadores que serão utilizados na avaliação, destacam-se a satisfação dos alunos, avaliada por meio de questionários; o desempenho dos alunos, medido através de provas, trabalhos, estágios e atividades extracurriculares; a produção de trabalhos científicos, participação em eventos e transferência de tecnologia por parte de professores e alunos; e a realização de atividades de extensão que impactem positivamente a sociedade.

A avaliação das políticas institucionais será um processo periódico, adaptado às necessidades do curso de Defesa Cibernética, e seus resultados devem ser compartilhados com a comunidade acadêmica para fomentar a melhoria contínua. Adotar práticas inovadoras na avaliação e revisão das políticas institucionais não apenas aprimora a qualidade do ensino e da aprendizagem no curso, mas também assegura um processo mais eficiente e participativo, envolvendo todos os stakeholders da comunidade acadêmica.

2.2 OBJETIVOS DO CURSO

Faculdade ACADI-TI ofertará do Curso Superior de Tecnologia em Defesa Cibernética, fruto do trabalho dedicado e comprometido de sua equipe de professores. O curso tem por objetivo formar profissionais excepcionalmente talentosos e bem-preparados para enfrentar os desafios do mundo contemporâneo da segurança da informação.

A missão da ACADI-TI transcende a mera transmissão de conhecimento técnico. Inspiramos cada estudante a conectar suas habilidades únicas e aspirações pessoais com os valores e objetivos estratégicos do curso. Essa abordagem, além de assegurar um padrão educacional de excelência, também capacita nossos alunos a se destacarem e a exercerem um impacto significativo no competitivo mercado de trabalho.

2.2.1 Objetivos gerais

- Formar profissionais na qualidade de tecnólogos em Defesa Cibernética com uma forte base conceitual e habilidades práticas, no âmbito das ciências relativas às suas atividades, capacitados a atuarem efetivamente no mercado de trabalho, bem como prosseguirem seus estudos em níveis superiores tanto em lato sensu e stricto sensu.
- Formar profissionais qualificados para o desenvolvimento de atividades técnico-científicas, gerenciais e administrativas na área de Defesa Cibernética, capazes de intervir nos processos de gestão e planejamento de defesa cibernética, contribuindo para segurança da informação e no planejamento contra os ataques cibernéticos, considerando seus aspectos políticos, econômicos, sociais, ambientais e culturais, com visão holística, ética e humanística.

2.2.2 Objetivos específicos

No Curso Superior de Tecnologia em Defesa Cibernética da Faculdade ACADI-TI, temos um propósito claro e dedicado: formar profissionais excepcionais em defesa cibernética.

Nosso foco está em nutrir talentos que sejam proficientes nas tecnologias na segurança (hard skill) e ao mesmo tempo possuem maturidade emocional e de relacionamento interpessoal (soft skills). Isso significa que, além de dominar as habilidades técnicas necessárias para o setor, nossos alunos também desenvolvem competências únicas, como pensamento crítico, resolução de problemas e comunicação eficaz. Neste sentido, nossos objetivos específicos se apresentam desta forma:

- Oferecer formação global, apoiada em conhecimento disciplinar, multidisciplinar e interdisciplinar, que proporcione uma visão abrangente das atividades de segurança da informação e cibersegurança, prevendo o domínio

sobre a técnica, os instrumentos, as estratégias e práticas inerentes à respectiva área, preparando o tecnólogo para os grandes desafios das situações exigidas no desempenho de suas funções;

- Produzir e difundir conhecimento na área de Defesa Cibernética, através do desenvolvimento de atividades de ensino, pesquisa e extensão, em uma contínua interação entre a Instituição e a Sociedade;
- Proporcionar aos alunos informações e procedimentos indispensáveis à análise, estudo, estratégia, interpretações, planejamento, implantação, coordenação, pesquisa e controle de atividades relacionadas ao seu campo de atuação, bem como em outros campos com os quais tenha conexão;
- Conhecer e disseminar os fundamentos e técnicas de segurança da informação;
- Oferecer formação crítica e analítica ao acadêmico em consonância com as necessidades do ser e do saber;
- Capacitar o egresso para identificar e propor soluções técnicas aos problemas da sociedade, através do domínio e utilização de conhecimentos tecnológicos aplicados na área da defesa cibernética.
- Absorver e desenvolver novas tecnologias, dentro de uma postura de permanente busca da atualização profissional.

2.2.3 Organização curricular

A organização curricular, ou estrutura curricular, do Curso Superior de Tecnologia em Defesa Cibernética da Faculdade ACADI-TI foi planejada para atender aos objetivos gerais e específicos do curso, bem como atingir o perfil do egresso desenhado este PPC.

A matriz curricular apresentada revela uma lógica de progressão pedagógica estruturada e bem definida, focada em preparar o estudante para carreiras na área de tecnologia da informação e cibersegurança. Esta progressão é feita da seguinte forma:

1. **Fundamentação Básica no 1º Período:** O currículo inicia com disciplinas fundamentais como Matemática para Computação, Introdução à Informática, Lógica de Programação e Algoritmos, Fundamentos de Redes de Computadores, e Princípios de Segurança da Informação. Essas disciplinas fornecem uma base sólida em computação e cibersegurança, essenciais para o entendimento de conceitos mais avançados.

2. **Especialização Progressiva:** À medida que o estudante avança, o currículo se aprofunda em áreas específicas de segurança da informação e administração de sistemas. No 2º período, as disciplinas focam na segurança cibernética e administração segura de sistemas operacionais (Linux e Windows), introduzindo também a ética e direitos humanos na tecnologia da informação.
3. **Aprofundamento em Cibersegurança e Redes no 3º Período:** Neste momento, as disciplinas tornam-se mais específicas em relação à segurança cibernética, com foco em inteligência de ameaças cibernéticas, tratamento e resposta a incidentes, hacking ético, defesa de rede, e planejamento e política de segurança cibernética. A inclusão de uma disciplina optativa permite a personalização do aprendizado conforme os interesses do aluno.
4. **Avanço e Consolidação no 4º e 5º Período:** No 4º período, o estudante é exposto a disciplinas avançadas como Segurança de Sistemas Operacionais, Segurança em Nuvem e Virtualização, Defesa de Rede Avançada, e Digital Forense, além de educação para relações Étnico-Raciais e Sociodiversidade. No 5º período, o foco está em gerenciamento avançado de redes e sistemas, segurança aplicada a IoT, análise avançada de malware, gestão de crises e continuidade de negócios, e desenvolvimento seguro de aplicações, preparando o estudante para enfrentar desafios complexos e atuais no campo da segurança da informação.
5. **Projetos Multidisciplinares Extensionistas:** Através de todos os períodos, há um claro foco na aplicação prática do conhecimento através de projetos multidisciplinares. Estes projetos permitem que os estudantes apliquem o conhecimento teórico em situações reais, incentivando a inovação, trabalho em equipe e solução de problemas complexos.
6. **Disciplinas Optativas:** As disciplinas optativas oferecem a oportunidade de explorar áreas de interesse específicas, permitindo que os estudantes personalizem parte de sua formação de acordo com suas preferências e objetivos de carreira. As opções incluem tópicos emergentes e de alta relevância como segurança cibernética para dispositivos móveis, infraestrutura crítica, inteligência artificial aplicada à segurança, inovação e empreendedorismo, e design thinking.
7. **Equilíbrio entre Teoria e Prática:** A matriz curricular apresenta um equilíbrio entre teoria (37,5% da carga horária total) e prática (43,3% da carga horária total), além dos

projetos multidisciplinares extensionista (19,2%), garantindo que os estudantes obtenham uma compreensão abrangente dos conceitos teóricos enquanto desenvolvem habilidades práticas essenciais para sua futura carreira.

Esta progressão pedagógica reflete um cuidadoso planejamento para desenvolver profissionais qualificados e adaptáveis, capazes de enfrentar os desafios contemporâneos no campo da tecnologia da informação e cibersegurança.

2.2.4 Contexto educacional e características locais e regionais

São José dos Campos, cidade do polo sede da Faculdade ACADI-TI, é uma cidade com um forte contexto educacional, com várias instituições de ensino superior, incluindo a Universidade Estadual Paulista (UNESP), a UNIFESP (Universidade Federal de São Paulo) e o Instituto Tecnológico de Aeronáutica (ITA). No Vale do Paraíba, marco região, também existem várias instituições de ensino superior, como a Universidade do Vale do Paraíba (UNIVAP), a Universidade de Taubaté (UNITAU) e a Faculdade de Tecnologia de São José dos Campos (FATEC SJC). Há, contudo, uma carência na oferta e formação de profissionais na área de tecnologia e mais na área de defesa cibernética.

O Vale do Paraíba é uma região com uma economia forte, baseada na indústria, tecnologia e serviços. A região abriga várias empresas de tecnologia, como a Embraer, a Siemens e a IBM. Essas empresas demandam profissionais qualificados em defesa cibernética para proteger suas redes e sistemas de ataques cibernéticos.

A demanda por profissionais de defesa cibernética é crescente em todo o mundo, como apresentamos no tópico sobre a Justificativa do curso, e não seria diferente no Vale do Paraíba. De acordo com um estudo da consultoria Frost & Sullivan, a demanda por profissionais de defesa cibernética na América Latina deve crescer 20% ao ano até 2025.

O curso de Defesa Cibernética da ACADI-TI pode atender a essa demanda de profissionais na região, preparando os alunos para as habilidades e conhecimentos necessários para trabalhar na área.

Além disso, o curso deve oferecer oportunidades de estágio e emprego para os alunos, para que eles possam colocar em prática os conhecimentos adquiridos.

Diante deste cenário, fica evidente que o curso de Defesa Cibernética da Faculdade ACADI-TI, em seus objetivos, considera o contexto educacional de São José dos Campos e

Vale do Paraíba, e sua demanda local, além de atender a essa demanda de profissionais na região, o curso oferece uma formação completa, que abrange os principais temas da área, como segurança de redes e sistemas, análise de vulnerabilidades, detecção e resposta a incidentes, testes de invasão, segurança de aplicações e segurança de dados.

2.2.5 Novas práticas emergentes em T.I

O cenário de ameaças cibernéticas está em constante evolução, com novos ataques sendo desenvolvidos a todo momento. Para se manterem protegidas, as organizações precisam adotar novas práticas de defesa cibernética que sejam capazes de enfrentar essas ameaças.

A Faculdade ACADI-TI está atenta a essas tendências e, por isso, a matriz curricular do curso de defesa cibernética está bem alinhada com as práticas emergentes no campo. Algumas das novas práticas emergentes na defesa cibernética que estão contempladas no curso são::

Inteligência Artificial e Machine Learning:

- **3º Período:** Introdução ao Hacking Ético (abordagem de machine learning para ataques e defesa)
- **5º Período:** Optativa - Inteligência Artificial Aplicada à Segurança Cibernética (aplicação de IA para detectar e prevenir ameaças)

Segurança em Nuvem e IoT:

- **4º Período:** Segurança em Nuvem e Virtualização (abordagem de conceitos e ferramentas de segurança em ambientes de nuvem)
- **5º Período:** Segurança Aplicada a IoT (estudo de vulnerabilidades e medidas de segurança em dispositivos IoT)

Cibersegurança e Forense Digital:

- **3º Período:** Inteligência de Ameaças Cibernéticas (análise de dados para identificar e prever ataques)
- **4º Período:** Defesa de Rede Avançada (técnicas avançadas de proteção de redes)
- **4º Período:** Digital Forense em Defesa Cibernética (investigação de crimes cibernéticos e coleta de provas digitais)

Gestão de Crises e Continuidade de Negócios:

- **5º Período:** Gestão de Crises e Continuidade de Negócios (planejamento para lidar com incidentes de segurança e garantir a continuidade das operações)

Soft Skills e Ética:

- **2º Período:** Ética, Moral e Direitos Humanos em Tecnologia da Informação (conscientização sobre os impactos éticos da tecnologia)
- **4º Período:** Educação para relações Étnico-Raciais e Sociodiversidade (promoção da diversidade e inclusão no ambiente de trabalho)

A matriz curricular está em constante atualização para acompanhar as novas tendências do mercado. As disciplinas optativas permitem que os alunos se aprofundem em temas específicos de seu interesse. Os projetos multidisciplinares incentivam a pesquisa e a aplicação prática dos conhecimentos adquiridos.

Em resumo, os objetivos do curso estão alinhados com a missão de preparar os alunos para os desafios atuais e emergentes no campo da defesa cibernética, abrangendo desde o entendimento teórico e prático de tecnologias chave até a conscientização ética e legal necessária para a prática profissional na área.

Os alunos que se formarem no curso estarão preparados para enfrentar os desafios de segurança cibernética do futuro, utilizando as tecnologias e práticas mais avançadas do setor.

2.3 PERFIL PROFISSIONAL DO EGRESSO

O perfil profissional do egresso de um curso de Tecnologia em Defesa Cibernética é definido de acordo com as determinações do Catálogo Nacional de Cursos Superiores de Tecnologia e com as demandas do mercado de trabalho.

2.3.1 Competências e habilidades do egresso

O egresso terá competências e conhecimentos técnicos sólidos em:

- **Redes de computadores**: Entender como as redes de computadores funcionam, incluindo as tecnologias, protocolos e segurança envolvidos.
- **Sistemas operacionais**: Ser capaz de identificar e mitigar ameaças em sistemas operacionais, incluindo Windows, macOS e Linux.
- **Segurança da informação**: Ter um conhecimento profundo dos princípios e práticas de segurança da informação, incluindo segurança de rede, segurança de aplicativos e segurança de dados.
- **Criptografia**: Ser capaz de usar a criptografia para proteger dados e sistemas contra-ataques.
- **Análise de vulnerabilidades**: Ser capaz de identificar e avaliar vulnerabilidades em sistemas e redes.
- **Forense digital**: Ser capaz de coletar, analisar e preservar evidências digitais para investigar crimes cibernéticos.
- **Inteligência artificial**: Ter um entendimento básico de inteligência artificial (IA) e machine learning, pois essas tecnologias estão sendo cada vez mais utilizadas para fins de segurança cibernética.
- **Machine learning**: Ter um entendimento básico de machine learning, pois essa tecnologia está sendo cada vez mais utilizada para fins de segurança cibernética.
- **Cloud computing**: Ter um entendimento básico de cloud computing, pois essa tecnologia está se tornando cada vez mais popular e representa um novo conjunto de desafios de segurança.

Habilidades

Além das competências e dos conhecimentos técnicos, o egresso também desenvolverá as seguintes habilidades:

- **Capacidade de análise e resolução de problemas**: Será capaz de identificar e resolver problemas complexos de segurança cibernética.
- **Raciocínio lógico e crítico**: Será capaz de pensar de forma lógica e crítica para identificar e mitigar ameaças cibernéticas.

- **Habilidades de comunicação e trabalho em equipe**: Será capaz de se comunicar de forma eficaz com uma variedade de públicos e trabalhar em equipe com outras pessoas para resolver problemas.
- **Capacidade de aprendizagem contínua**: Será capaz de aprender e se adaptar às novas tecnologias e ameaças.
- **Liderança**: Será capaz de liderar equipes de segurança cibernética, portanto, terá habilidades de liderança.
- **Ética e conformidade legal**: O profissional de segurança cibernética estará ciente das leis e regulamentos de segurança cibernética e agir de forma ética.

Áreas de atuação

O egresso de um curso de Tecnologia em Defesa Cibernética poderá atuar em diversas áreas, como:

- **Segurança de redes e sistemas**: Análise de segurança, implementação de sistemas de segurança, gerenciamento de sistemas de segurança.
- **Forense digital**: Investigação de crimes cibernéticos, análise de evidências digitais.
- **Execução de projetos de segurança da informação**: Planejamento e execução de projetos de segurança da informação, avaliação de riscos cibernéticos, implementação de medidas de segurança.
- **Centro de Operação de Segurança (SOC):** Análise de vulnerabilidades, controle de acesso, operação de tecnologia de segurança, monitoramento de indicadores de segurança.

2.3.2 Conformidade com o Catálogo

O curso de Defesa Cibernética foi cuidadosamente projetado não apenas para atender ao desejo de excelência e inovação, mas também em conformidade com as diretrizes estabelecidas pelo Catálogo Nacional de Cursos Superiores de Tecnologia. Este documento, em sua página 53, delineia o perfil esperado do egresso, oferecendo uma base sólida para a estruturação de nosso programa educacional. A nossa matriz curricular foi minuciosamente elaborada para refletir essas expectativas, assegurando que os alunos adquiram conhecimentos

e habilidades relevantes para enfrentar os desafios do campo da defesa cibernética. Ao integrar os requisitos do catálogo ao nosso planejamento, conseguimos criar um curso que não só atende às necessidades do mercado, mas também prepara os estudantes para serem profissionais capacitados, prontos para contribuir de forma significativa na área de segurança da informação e defesa cibernética. Esta abordagem evidencia nosso compromisso com a qualidade e a relevância acadêmica, alinhando nosso curso às melhores práticas e expectativas do setor:

Obrigatoriedade do Catálogo	Disciplina do Curso	Justificativa
Avaliação de Ameaças de Invasão	Inteligência de Ameaças Cibernéticas, Análise Avançada de Malware	Oferecem conhecimento para compreender, avaliar e responder a ameaças cibernéticas.
Planejamento de Sistemas de Proteção	Planejamento e Política de Segurança Cibernética, Gestão de Crises e Continuidade de Negócios	Preparam os alunos para desenvolver e implementar planos e estratégias de proteção cibernética.
Desenvolvimento de Sistemas de Proteção	Arquitetura de Segurança de Sistemas para Segurança Cibernética, Desenvolvimento Seguro de Aplicações	Ensinam o design e o desenvolvimento de sistemas seguros contra ataques cibernéticos.
Investigação e Monitoramento de Ataques	Tratamento e Resposta a Incidentes, Digital Forense em Defesa Cibernética	Capacitam os alunos a investigar incidentes de segurança e monitorar ataques continuamente.
Estabelecimento de Procedimentos Contra Invasão e Guerra Eletrônica	Defesa de Rede, Defesa de Rede Avançada	Fornecem estratégias e tecnologias para proteger redes e sistemas contra invasões e ataques.
Coordenação de Equipes de Trabalho	Gerenciamento de Projetos para Segurança Cibernética	Aborda habilidades de liderança e coordenação de equipes em projetos de segurança cibernética.
Vistoria e Perícia Técnica	Digital Forense em Defesa Cibernética	Prepara os alunos para realizar perícias técnicas em incidentes de segurança cibernética.
Avaliação e Emissão de Laudos e Pareceres Técnicos	Diversas disciplinas, incluindo projetos multidisciplinares e digital forense	Desenvolvem habilidades para avaliar, investigar e documentar incidentes de segurança.

2.3.3 Articulação com necessidades locais e regionais

A cidade de São José dos Campos e o Vale do Paraíba são regiões importantes para o desenvolvimento tecnológico do Brasil. A região, como já apresentamos página atrás, abriga diversas empresas importantes para o país e algumas de alta tecnologia, como a Embraer, Petrobras, Usiminas, Cherry, Hyundai entre outras. Além disso, a região é um importante polo de pesquisa e desenvolvimento, com instituições como o Instituto Tecnológico de Aeronáutica

(ITA), o Instituto Nacional de Pesquisas Espaciais (Inpe), o Centro de Desenvolvimento em Tecnologias Aeronáuticas (CDTA), Centro de Desenvolvimento de Tecnologias em Energia (CDTE), o Departamento de Ciência e Tecnologia Aeroespacial (DCTA), Serviço Nacional de Aprendizagem Industrial (SENAI) e o Serviço Nacional de Aprendizagem Comercial (SENAC).

Essa forte presença de empresas de tecnologia e de instituições de pesquisa e desenvolvimento cria uma demanda significativa por profissionais formados na área de Defesa Cibernética. Essas empresas e instituições precisam de profissionais qualificados para proteger seus sistemas e dados contra-ataques cibernéticos.

O perfil do egresso do curso de Tecnologia em Defesa Cibernética da Faculdade ACADI-TI é compatível com as necessidades locais e regionais. O curso oferece uma formação completa na área de segurança cibernética, preparando os alunos para atuar em diversas áreas. Esses conhecimentos e habilidades, como apresentados há algumas páginas, são essenciais para que os profissionais de Defesa Cibernética irão atuar na região de São José dos Campos e Vale do Paraíba.

2.3.4 Planejamento para ampliação de competências

A Faculdade ACADI-TI está preocupada em ampliar cada vez mais as competências dos egressos do curso de Defesa Cibernética para atender à demanda do mercado de trabalho e se manter atualizada com as novas demandas do setor. Para isso, a instituição implementará uma série de estratégias, que incluirão, mas não se limitarão:

- **Avaliação contínua das tendências do mercado**: A Faculdade ACADI-TI estabelecerá parcerias com empresas e organizações de TI para obter insights sobre as últimas tendências e necessidades em segurança cibernética. A instituição também realizará pesquisas e análises de mercado para identificar novas habilidades e tecnologias emergentes no campo da defesa cibernética.
- **Atualização curricular dinâmica**: O currículo do curso de Defesa Cibernética da Faculdade ACADI-TI será revisado e atualizado anualmente para incorporar novas tecnologias, ferramentas e práticas. A instituição também oferecerá módulos de ensino flexíveis que podem ser rapidamente atualizados ou substituídos para refletir as mudanças no setor.

- **Integração de tecnologias avançadas**: A Faculdade ACADI-TI investirá cada vez mais em laboratórios equipados com as mais recentes tecnologias e softwares de defesa cibernética. A instituição também implementará simulações de ataques cibernéticos e cenários de guerra cibernética para treinamento prático.
- **Parcerias para pesquisa e desenvolvimento**: A Faculdade ACADI-TI estabelecerá colaborações para projetos de pesquisa e desenvolvimento em segurança cibernética. A instituição também apoiará pesquisas focadas em soluções inovadoras e emergentes no campo da cibersegurança.
- **Desenvolvimento de competências transversais**: O curso de Defesa Cibernética da Faculdade ACADI-TI incluirá componentes curriculares sobre gestão de equipes e liderança em projetos de segurança cibernética. A instituição também enfatizará a importância da ética e do cumprimento de regulamentos em defesa cibernética.
- **Programas de educação continuada**: A Faculdade ACADI-TI oferecerá workshops e cursos de curta duração sobre novas ameaças, tecnologias e estratégias de defesa cibernética. A instituição também oferecerá parcerias com organizações certificadoras para oferecer cursos que levem a certificações profissionais reconhecidas.
- **Estágios e experiência prática**: A Faculdade ACADI-TI oferecerá programas de estágio com empresas de tecnologia e organizações de segurança cibernética. A instituição também incluirá projetos em parceria com empresas para resolver problemas reais de defesa cibernética.
- **Feedback de egressos e empregadores**: A Faculdade ACADI-TI realizará enquetes regulares com ex-alunos e empregadores para obter feedback sobre o curso e áreas de melhoria.

A implementação dessas estratégias permitirá à Faculdade ACADI-TI manter seu curso de Defesa Cibernética atualizado com as demandas do mercado e assegurar que seus egressos estejam bem equipados para enfrentar os desafios emergentes no campo da cibersegurança.

2.4 ESTRUTURA CURRICULAR

O Currículo do Curso de Defesa Cibernética, conforme estabelecido pelo Catálogo Nacional de Cursos Superiores de Tecnologia e de acordo com sua concepção teórico-metodológica, com a missão, com os objetivos e com o perfil do egresso traçados neste Projeto Pedagógico, é composto pelo conjunto de unidades curriculares e atividades agrupadas em conteúdos de formação geral e de formação específica.

Os pressupostos formativos para o egresso da Faculdade ACADI-TI visam assegurar uma formação que contemple as áreas do conhecimento do Tecnólogo em Defesa Cibernética. Por meio de uma abordagem sistêmica, o curso encontra-se estruturado de modo a respeitar a evolução lógica dos conceitos e sua respectiva interdisciplinaridade.

Em sintonia com o Catálogo Nacional de Cursos Superiores de Tecnologia, o curso Tecnólogo em Defesa Cibernética promove uma organização curricular que contempla conteúdos apoiados em seus princípios de flexibilização curricular e proporcionando a relevância ao processo de organização da matriz, no que se referem às abordagens metodológicas adotadas. Por meio da interdisciplinaridade a relação entre os conteúdos curriculares e o campo de atuação profissional permite a operacionalização de práticas acadêmicas, pedagógicas e profissionais permeadas com toda a proposta curricular.

Uma inovação do curso faz referência ao uso dos laboratórios virtuais, os quais simulam o ambiente real e proporcionam ao aluno a execução de experimentos mesmo à distância .

2.4.1 Flexibilidade e interdisciplinaridade curricular

A segurança cibernética é uma área de conhecimento, por natureza, interdisciplinar, vez que exige o domínio de uma ampla gama de conhecimentos e habilidades, e princípio flexível, por conta de sua amplitude de área. Nesse sentido, o curso de Defesa Cibernética da Faculdade ACADI-TI respeita a interdisciplinaridade e flexibilidade curricular em sua matriz.

A interdisciplinaridade é atributo fundamental para um curso de Segurança, pois permite que os alunos entendam a segurança cibernética como um sistema complexo, que envolve uma ampla gama de fatores. No curso de Defesa Cibernética da Faculdade ACADI-TI, a interdisciplinaridade é proporcionada por meio de três mecanismos:

1. **Estrutura curricular**: a estrutura curricular do curso é dividida em cinco módulos, cada um com foco em um conjunto específico de conhecimentos e habilidades. Essa divisão permite que os alunos

desenvolvam uma base sólida em diferentes áreas da segurança cibernética, como redes, sistemas operacionais, segurança de dados e inteligência de ameaças.

2. **Integração das disciplinas**: as disciplinas do curso são desenvolvidas de forma interdisciplinar, promovendo a integração de conhecimentos de diferentes áreas. Essa integração é realizada por meio de projetos, atividades práticas e discussões em sala de aula.
3. **Corpo docente**: os professores do curso são especialistas em diferentes áreas da segurança cibernética, o que permite que eles promovam a discussão e a reflexão interdisciplinares.

A interdisciplinaridade é essencial para que os profissionais de segurança cibernética possam resolver problemas complexos e emergentes. O curso de Defesa Cibernética da Faculdade ACADI-TI oferece aos alunos uma formação interdisciplinar abrangente, preparando-os para os desafios da área.

Quando da flexibilidade curricular o vemos como um atributo indispensável para um curso de Defesa Cibernética ofertado na modalidade à distância, vez que a flexibilidade permite que os alunos personalizem seu aprendizado de acordo com seus interesses e objetivos profissionais.

No curso de Defesa Cibernética da Faculdade ACADI-TI, a flexibilidade curricular é proporcionada por meio de dois mecanismos:

1. **Disciplinas Optativas** A oferta de disciplinas optativas nos semestres 3, 4 e 5 é um dos pilares da personalização da aprendizagem neste curso. Permitindo aos alunos escolher entre uma variedade de tópicos avançados em tecnologia da informação e segurança cibernética, tais como inteligência artificial, análise de dados, blockchain, e computação em nuvem, esta estrutura flexível possibilita que cada estudante direcione sua formação para áreas de interesse específico. Este enfoque enriquece o currículo ao mesmo tempo que permite que os alunos moldem suas carreiras de acordo com seus objetivos profissionais.
2. **Projetos Multidisciplinares Extensionistas**: Os cinco projetos multidisciplinares extensionistas, integrados em todos os semestres do curso, reforçam a aplicação prática dos conhecimentos adquiridos. Estes projetos são desenhados para fomentar habilidades como trabalho em equipe, criatividade, resolução de problemas e comunicação eficaz. A flexibilidade para escolher temas que se alinham com seus interesses e

objetivos permite aos alunos uma personalização ainda maior da sua aprendizagem, garantindo uma experiência educacional rica e relevante.

Em resposta às rápidas mudanças no campo da Defesa Cibernética, o curso mantém sua matriz curricular constantemente atualizada. A inclusão de disciplinas optativas e projetos multidisciplinares facilita a incorporação de novas tecnologias e tendências emergentes. Esta abordagem assegura que os alunos estejam sempre à frente, equipados com conhecimentos atualizados e prontos para atender às demandas futuras do mercado de trabalho.

Além de conhecimentos técnicos específicos acima apresentados, o curso enfatiza o desenvolvimento de habilidades essenciais para o futuro da área de Tecnologia, incluindo pensamento crítico e analítico, resolução de problemas, habilidades de comunicação e trabalho em equipe, adaptabilidade e flexibilidade, bem como criatividade e inovação. Essas competências são fundamentais para formar profissionais completos e versáteis, capazes de navegar pelos desafios e oportunidades do mercado de trabalho na área de tecnologia e segurança cibernética.

2.4.2 Acessibilidade metodológica da estrutura curricular

No contexto da educação superior, a acessibilidade metodológica refere-se à adoção de estratégias e práticas pedagógicas que promovam a inclusão de estudantes com deficiência ou com necessidades especiais. No nosso caso, no curso de Defesa Cibernética, a acessibilidade metodológica é particularmente importante, pois este curso envolve o uso de tecnologias digitais. As tecnologias digitais podem ser uma ferramenta poderosa para promover a inclusão, mas também podem representar uma barreira para estudantes com deficiência. Por isso, estamos atentos às questões de acessibilidade metodológica e adotamos estratégias para garantir que todos os estudantes tenham acesso ao conteúdo e às atividades do curso de defesa cibernética.

A Faculdade ACADI-TI, que está em fase de credenciamento e autorização do curso de Tecnólogo em Defesa Cibernética, considera a acessibilidade metodológica como uma prioridade. Para isso, o curso prevê as seguintes estratégias:

- Inclusão de conteúdos sobre acessibilidade nos currículos: O currículo do curso prevê a inclusão de conteúdos sobre acessibilidade, de forma a preparar os estudantes para atuarem em um ambiente inclusivo. Esses conteúdos, que serão ministrados em workshop e programas extensionistas, abordarão temas como as diferentes deficiências, as tecnologias de acessibilidade e as estratégias para promover a inclusão.

- Oferta de recursos e materiais acessíveis: O curso oferece recursos e materiais acessíveis aos estudantes com deficiência, como textos em braile, legendas em Libras, recursos audiovisuais e softwares de acessibilidade.
- Adaptação de atividades e avaliações: O curso prevê a adaptação de atividades e avaliações para atender às necessidades específicas dos estudantes com deficiência. Essas adaptações incluem a concessão de mais tempo para a realização das atividades, a utilização de recursos de acessibilidade ou a substituição de atividades por outras que sejam mais adequadas às necessidades do estudante. As questões específicas da avaliação são tratadas no documento sobre esse tomo.
- Oferta de apoio pedagógico especializado: O curso oferecerá apoio pedagógico especializado aos estudantes com deficiência. Esse apoio será oferecido por meio de profissionais especializados, como professores de educação especial, intérpretes de Libras ou assistentes de alunos. Importante mencionar que a Faculdade a implantação do Núcleo de Orientação Psicopedagógico (NAP) sob a supervisão de uma psicopedagoga.
- Promoção de uma cultura inclusiva na ACADI-TI: A Instituição promoverá uma cultura inclusiva. Isso será feito por meio de ações como a realização de campanhas de conscientização sobre a importância da acessibilidade, a capacitação dos docentes e funcionários para atuarem em um ambiente inclusivo e a criação de espaços de convivência inclusivos.

A adoção dessas estratégias garantirá que o curso de Tecnólogo em Defesa Cibernética da Faculdade ACADI-TI seja acessível a todos os estudantes, independentemente de suas deficiências ou necessidades especiais.

2.4.3 Compatibilidade da carga horária total

A carga horária total do curso de Tecnologia em Defesa Cibernética é de **2080 horas**, organizada de forma a oferecer uma formação abrangente e equilibrada entre teoria e prática. Esta carga horária é distribuída entre:

- 780 horas de componentes curriculares teóricos;
- 900 horas dedicadas à prática;
- 400 horas destinadas a projetos multidisciplinares extensionistas.

Essa estrutura cuidadosamente planejada assegura que os alunos adquiram conhecimentos fundamentais através das aulas teóricas, ao mesmo tempo que oferece amplas oportunidades para aplicar esses conhecimentos em situações práticas e projetos reais. Os projetos multidisciplinares, em particular, são essenciais para a integração do conhecimento, permitindo que os alunos trabalhem em equipe para solucionar problemas complexos, uma habilidade crítica no campo da defesa cibernética. Essa combinação de teoria, prática e aplicação prática prepara os alunos de forma eficaz para as demandas do mercado de trabalho, enfatizando a importância da experiência prática ao lado do aprendizado teórico.

A carga horária total do curso está de acordo com o Catálogo Nacional dos Cursos Superiores de Tecnologia (p. 53), que estabelece 2.000 horas como carga horária mínima para os cursos de tecnologia.

A carga horária total do curso de Defesa Cibernética da Faculdade ACADI-TI está de acordo com o CNCST e é suficiente para garantir a formação de profissionais qualificados para atuar na área de segurança cibernética. O curso oferece uma base sólida de conhecimentos teóricos e práticos, que capacita os alunos para enfrentar os desafios da profissão.

2.4.4 Articulação entre teoria e prática

A matriz curricular do curso demonstra uma forte articulação entre teoria e prática, fundamental para a formação de profissionais eficazes. As disciplinas teóricas fornecem a base conceitual sólida, enquanto as atividades práticas permitem que os alunos apliquem seus conhecimentos em situações reais, consolidando o aprendizado e desenvolvendo habilidades essenciais.

A carga horária dedicada à prática, equivalente a 43,3% do total, demonstra o compromisso do curso com a formação prática dos alunos. Laboratórios, simulações, estudos de caso e projetos práticos proporcionam um ambiente de aprendizado dinâmico e relevante, onde os alunos podem desenvolver as habilidades e competências necessárias para atuar na área.

Os Projetos Multidisciplinares Extensionistas, realizados ao longo do curso, representam uma oportunidade ímpar para os alunos integrarem conhecimentos de diferentes disciplinas e os aplicarem a problemas reais de segurança cibernética. Essa experiência

promove o trabalho colaborativo, a comunicação eficaz e a resolução de problemas, habilidades essenciais para o mercado de trabalho.

As disciplinas optativas permitem que os alunos personalizem sua formação de acordo com seus interesses específicos. A escolha entre Segurança cibernética para dispositivos móveis, Segurança cibernética para infraestrutura crítica, Inteligência Artificial Aplicada à Segurança Cibernética, Inovação e Empreendedorismo em Segurança Cibernética e Design Thinking e Inovação em Cibersegurança garante que os alunos possam aprofundar seus conhecimentos em áreas de maior interesse e potencial profissional.

O corpo docente experiente, composto por profissionais que atuam na academia e no mercado de trabalho, garante que os alunos estejam aprendendo com os melhores da área. Essa experiência prática e conhecimento das últimas tendências e desafios do mercado são transmitidos aos alunos, preparando-os para os desafios que encontrarão em suas carreiras.

A infraestrutura moderna, com laboratórios equipados com as últimas tecnologias em segurança cibernética, permite que os alunos pratiquem em um ambiente real e simulem situações que podem encontrar no mercado de trabalho. Essa experiência prática é essencial para que os alunos se sintam confiantes e preparados para atuar na área.

O Curso Superior de Tecnologia em Defesa Cibernética oferece uma formação completa e abrangente, preparando os alunos para as demandas do mercado de trabalho em constante evolução. A articulação entre teoria e prática, a ênfase em atividades práticas, as optativas, o corpo docente experiente e a infraestrutura moderna garantem que os alunos estejam aptos a atuar com sucesso na defesa das fronteiras digitais do futuro.

2.4.5 Oferta da disciplina de LIBRAS (Língua Brasileira de Sinais).

A Língua Brasileira de Sinais (LIBRAS) é a língua natural das pessoas surdas e é reconhecida como meio legal de comunicação e expressão no Brasil. A importância da LIBRAS é cada vez mais reconhecida, pois ela permite que as pessoas surdas tenham acesso à informação e à comunicação de forma plena.

A disciplina de LIBRAS é ofertada no 4º semestre do curso de Defesa Cibernética, com carga horária de 80 horas. A disciplina é optativa, o que significa que os alunos podem escolher se querem ou não cursar.

2.4.6 Mecanismos de familiarização com a modalidade a distância

Na ACADI-TI sabemos que o Ensino a Distância é uma modalidade de ensino que vem crescendo cada vez mais no Brasil e no mundo. Entendemos também que essa modalidade oferece uma série de vantagens, como flexibilidade de horário, autonomia de aprendizagem e custo reduzido. No entanto, temos consciência de que o EAD também apresenta alguns desafios, como a necessidade de disciplina e organização do tempo, o desenvolvimento de habilidades de aprendizagem autônoma e a interação com os colegas e tutores.

É por isso que a Faculdade ACADI-TI se preocupa com a aproximação e a naturalização dos alunos à modalidade a distância. Acreditamos que é nesta preocupação que estará o sucesso da Faculdade. Para isso, a IES prevê uma série de ações inovadoras para familiarizar os alunos com a modalidade a distância. Entre estas ações, destacam-se:

- Oferta de uma disciplina introdutória à educação a distância. Essa disciplina abordará temas como a história da EAD, os fundamentos pedagógicos da modalidade, as tecnologias educacionais utilizadas e as estratégias de aprendizagem autônoma.
- Realização de atividades online antes do início do curso. Essas atividades serão realizadas na plataforma de aprendizagem da Faculdade e abordarão temas como a apresentação do curso, a plataforma de aprendizagem e as diretrizes pedagógicas.
- Oferta de orientação e suporte aos estudantes. Os estudantes terão acesso a informações e recursos que os auxiliem na adaptação à modalidade a distância.

Acreditamos que essas ações inovadoras contribuirão para que os alunos da ACADI-TI tenham uma experiência de aprendizagem positiva na modalidade a distância

2.4.7 Articulação entre os componentes curriculares no percurso de formação.

A matriz curricular do curso de Defesa Cibernética da Faculdade ACADI-TI articula os componentes curriculares de forma equilibrada, proporcionando aos alunos uma formação completa e atualizada na área de segurança cibernética. A articulação entre os componentes curriculares é realizada de forma horizontal e vertical.

- **Horizontalmente**, os componentes curriculares estão agrupados em módulos, que abordam temas relacionados. Essa organização permite que os alunos aprendam os conceitos básicos antes de avançar para temas mais avançados. Neste sentido, vemos que: Módulo 1 aborda os fundamentos de tecnologias básicas, como redes de

computadores, sistemas operacionais e dados. O Módulo 2 aborda a administração segura de sistemas, com foco em Linux e Windows. O Módulo 3 aborda áreas específicas da segurança cibernética, como auditoria, inteligência de ameaças, tratamento de incidentes, hacking ético e defesa de redes. O Módulo 4 aborda áreas de especialização, como segurança de sistemas operacionais, dispositivos móveis, nuvem e virtualização.

- **Verticalmente**, os componentes curriculares estão organizados em uma sequência lógica, que permite aos alunos construir seu conhecimento gradualmente. Por exemplo, a disciplina Introdução à Segurança Cibernética apresenta os conceitos fundamentais da segurança cibernética, que são desenvolvidos nas disciplinas subsequentes, como Auditoria e Avaliações de Segurança e Tratamento e Resposta a Incidentes.

Alguns exemplos específicos de como a articulação entre os componentes curriculares é realizada na matriz curricular apresentada:

- A disciplina "Introdução à Redes de Computadores" fornece uma base para as disciplinas "Defesa de Redes" e "Inteligência de Ameaças Cibernéticas".
- A disciplina "Fundamentos de Sistemas Operacionais" fornece uma base para as disciplinas "Administração Segura de Sistema Linux" e "Administração Segura de Sistema Windows".
- A disciplina "Fundamentos de Dados para Segurança Cibernética" fornece uma base para as disciplinas "Criptografia" e "Segurança de Aplicações".

A articulação entre os componentes curriculares é essencial para que os alunos desenvolvam uma formação completa e atualizada na área de segurança cibernética. Essa articulação permite que os alunos aprendam os conceitos básicos antes de avançar para temas mais avançados, e que construam seu conhecimento gradualmente.

2.4.8 Elementos inovadores na estrutura curricular.

A segurança cibernética é uma área em constante evolução, com novos desafios surgindo a cada dia. Para atender a essas demandas, a Defesa Cibernética oferece uma formação inovadora, que prepara os alunos para os desafios presente e futuros da área de segurança.

A estrutura curricular do curso de Defesa Cibernética da Faculdade ACADI-TI apresenta alguns aspectos inovadores que a tornam alinhada às tendências da área.

Abordagem multidisciplinar

A segurança cibernética é uma área complexa que envolve diferentes tecnologias e conceitos. Por isso, o curso de Defesa Cibernética oferece uma abordagem multidisciplinar, que permita aos alunos compreender como as diferentes áreas se relacionam entre si. Neste sentido, a matriz curricular do curso da ACADI-TI inclui disciplinas de diferentes áreas, como:

- Redes de computadores: Esta disciplina aborda os fundamentos de redes de computadores, incluindo arquitetura, protocolos, segurança e aplicações.
- Sistemas operacionais: Esta disciplina aborda os fundamentos de sistemas operacionais, incluindo arquitetura, gerenciamento de processos, memória, arquivos e segurança.
- Dados: Esta disciplina aborda os fundamentos de dados, incluindo análise de dados, mineração de dados e segurança de dados.
- Virtualização e Computação em Nuvem: Esta disciplina aborda os fundamentos de virtualização e computação em nuvem, incluindo arquitetura, segurança e aplicações.
- Programação: Esta disciplina aborda os fundamentos da programação, incluindo linguagens de programação, algoritmos e estruturas de dados.

Essa abordagem multidisciplinar permite que os alunos adquiram uma compreensão holística da área de segurança cibernética e sejam capazes de lidar com diferentes desafios de segurança cibernética.

Ênfase na prática

Além da teoria, a Defesa Cibernética oferece uma ênfase na prática, que permita aos alunos aplicar os conceitos aprendidos na teoria. A matriz curricular do curso da ACADI-TI inclui um grande número de disciplinas e carga horária prática, como:

- Laboratório de redes de computadores: Esta disciplina permite aos alunos praticar os fundamentos de redes de computadores, incluindo configuração de redes, gerenciamento de redes e segurança de redes.
- Laboratório de sistemas operacionais: Esta disciplina permite aos alunos praticar os fundamentos de sistemas operacionais, incluindo gerenciamento de processos, memória, arquivos e segurança de sistemas operacionais.

- Laboratório de dados: Esta disciplina permite aos alunos praticar os fundamentos de dados, incluindo análise de dados, mineração de dados e segurança de dados.
- Laboratório de virtualização e computação em nuvem: Esta disciplina permite aos alunos praticar os fundamentos de virtualização e computação em nuvem, incluindo configuração de ambientes virtuais, gerenciamento de ambientes virtuais e segurança de ambientes virtuais.
- Laboratório de programação: Esta disciplina permite aos alunos praticar os fundamentos da programação, incluindo desenvolvimento de software, testes de software e segurança de software.

Essa ênfase na prática permite que os alunos desenvolvam as habilidades necessárias para identificar, analisar e responder a ameaças cibernéticas.

Atenção à ética

A ética é um aspecto importante da segurança cibernética. Os profissionais de segurança cibernética devem estar cientes dos princípios éticos que devem ser seguidos na área e estar preparados para lidar com os desafios éticos que podem surgir. A matriz curricular do curso da ACADI-TI inclui uma disciplina específica sobre ética, moral e valores humanos. Essa disciplina aborda temas como:

- Ética profissional: Os alunos aprendem sobre os princípios éticos que devem ser seguidos por profissionais de segurança cibernética.
- Ética na segurança cibernética: Os alunos aprendem sobre os desafios éticos que podem surgir na área de segurança cibernética.
- Legislação e regulamentação em segurança cibernética: Os alunos aprendem sobre as leis e regulamentações que regem a área de segurança cibernética.

Essa atenção à ética é importante para que os alunos se tornem profissionais responsáveis e éticos.

A estrutura curricular do curso de Defesa Cibernética da Faculdade ACADI-TI apresenta aspectos inovadores que a tornam alinhada às tendências da área de segurança cibernética. A abordagem multidisciplinar, a ênfase na prática e a atenção à ética são elementos que permitem que os alunos adquiram uma formação sólida e abrangente, preparando-os para o mercado de trabalho e para os desafios futuros da área de segurança cibernética.

2.4.9 Certificações intermediárias - CBO

Como a matriz curricular do Curso Superior de Tecnologia em Defesa Cibernética demonstra uma forte articulação entre as disciplinas ofertadas em cada semestre e as CBOs (Classificações Brasileiras de Ocupações) para as quais o curso prepara os alunos. Essa relação garante que os alunos estejam adquirindo os conhecimentos e habilidades necessárias para atuar com sucesso nas áreas de maior demanda do mercado de trabalho em segurança cibernética.

1º Semestre:

- **CBO 2124-10 - Analistas de tecnologia da informação:**
  - **Matemática para Computação:** Fornece a base matemática necessária para o desenvolvimento de algoritmos e lógica de programação, habilidades essenciais para analistas de TI.
  - **Introdução à Informática:** Introduz os alunos aos principais conceitos da informática, como hardware, software, sistemas operacionais e redes, preparando-os para o estudo de áreas específicas como segurança da informação.
  - **Lógica de Programação e Algoritmos:** Ensina os fundamentos da lógica de programação e a construção de algoritmos, habilidades básicas para a análise e desenvolvimento de sistemas.
  - **Fundamentos de Redes de Computadores:** Aborda os conceitos básicos de redes de computadores, como protocolos, modelos de referência e tipos de redes, conhecimento essencial para a análise e segurança de redes.
  - **Princípios de Segurança da Informação:** Introduz os principais conceitos de segurança da informação, como confidencialidade, integridade e disponibilidade, conscientizando os alunos sobre os riscos e medidas de proteção.

2º Semestre:

- **CBO 2123-15 - Administradores de sistemas operacionais:**
  - **Gerenciamento de Projetos para Segurança Cibernética:** Ensina as melhores práticas para gerenciar projetos com foco em segurança cibernética, incluindo metodologias ágeis e tradicionais, preparando os alunos para coordenar e executar projetos na área.

- **Administração Segura de Sistema Linux:** Fornece conhecimentos e habilidades para administrar sistemas Linux de forma segura, incluindo instalação, configuração, gerenciamento de usuários e segurança de rede.
- **Administração Segura de Sistema Windows:** Aborda os principais aspectos da administração segura de sistemas Windows, incluindo configuração de segurança, políticas de grupo, gerenciamento de usuários e gerenciamento de patches de correção de vulnerabilidades .
- **Arquitetura de Segurança de Sistemas para Segurança Cibernética:** Ensina os princípios das arquiteturas de segurança de sistemas, para que com base em uma modelagem de ameaças, coloque em prática os princípios design seguro, minimizando as superfície de ataque , preparando os alunos para projetar sistemas mais seguros.
- **Ética, Moral e Direitos Humanos em Tecnologia da Informação:** Discute questões éticas e morais relacionadas à tecnologia da informação, como privacidade, responsabilidade social e profissional, conscientizando os alunos sobre o uso responsável da tecnologia.

3º Semestre:

- **CBO 2124-10 - Analista de redes e de comunicação de dados:**
  - **Inteligência de Ameaças Cibernéticas:** Aprofunda os conhecimentos sobre inteligência de ameaças cibernéticas, incluindo coleta, análise e aplicação de dados para identificar e prevenir ataques.
  - **Tratamento e Resposta a Incidentes:** Ensina as melhores práticas para lidar com incidentes de segurança cibernética, desde a detecção e investigação até a contenção e recuperação.
  - **Introdução ao Hacking Ético:** Aborda os princípios e técnicas do hacking ético, permitindo que os alunos utilizem seus conhecimentos para identificar e corrigir vulnerabilidades em sistemas.
  - **Defesa de Rede:** Oferece uma visão abrangente das técnicas e estratégias de defesa de rede, capacitando os alunos para proteger redes contra ataques cibernéticos.

- **Planejamento e Política de Segurança Cibernética:** Ensina a desenvolver, implementar e gerenciar políticas e planos de segurança cibernética eficazes, alinhados com os objetivos da organização.
- **Optativa:** Permite que os alunos explorem áreas de interesse dentro da segurança cibernética, como segurança em nuvem, forense digital ou criptografia.

4º Semestre:

- **CBO 2123 - Administradores de tecnologia da informação:**
  - **Segurança de Sistemas Operacionais:** Aprofunda os conhecimentos sobre segurança em sistemas operacionais Windows, Linux e outros, capacitando os alunos para proteger sistemas contra diferentes tipos de ameaças.
  - **Segurança em Nuvem e Virtualização:** Aborda os desafios e estratégias de segurança específicos para ambientes de nuvem e virtualizados, preparando os alunos para proteger dados e infraestruturas em nuvem.
  - **Defesa de Rede Avançada:** Expande as habilidades de defesa de rede com técnicas de ponta para detectar, prevenir e responder a ataques sofisticados.
  - **Digital Forense em Defesa Cibernética:** Introduz o campo da forense digital, ensinando as técnicas e ferramentas utilizadas para investigar incidentes de segurança cibernética e crimes digitais.
  - **Educação Étnico-Raciais e Sociodiversidade:** Sensibiliza os alunos quanto à diversidade e inclusão na tecnologia, promovendo a compreensão sobre respeito às diferenças e o combate ao preconceito.
  - **Optativa:** Garante a possibilidade de aprimoramento em áreas mais avançadas específicas, como segurança para IoT ou gestão de crises.

5º Semestre

- **CBO 2123-20 Especialista em segurança da informação**
  - **Gerenciamento Avançado de Redes e Sistemas:** Aborda técnicas avançadas para otimização, segurança e alta disponibilidade de redes e sistemas, permitindo que os alunos desenvolvam soluções para problemas complexos da área.

- **Segurança Aplicada a IoT:** Mergulha na segurança de dispositivos e redes IoT (Internet das Coisas), um campo crítico na atualidade e que demandará cada vez mais especialistas.
- **Análise Avançada de Malware:** Ensina técnicas aprofundadas de identificação, engenharia reversa e neutralização de malware, preparando os alunos para o combate a ameaças avançadas.
- **Gestão de Crises e Continuidade de Negócios:** Abrange os processos e práticas essenciais para elaborar e executar planos de continuidade de negócios e resposta a crises cibernéticas.
- **Desenvolvimento Seguro de Aplicações:** Ensina a incorporar segurança desde o início do ciclo de vida de desenvolvimento de software, reduzindo vulnerabilidades e gerando aplicações mais robustas.
- **Optativa:** Permite escolha entre tópicos emergentes ou correlatos, tais como Inteligência Artificial aplicada à segurança, inovação, ou outras áreas de grande relevância.

A análise da matriz curricular do Curso Superior de Tecnologia em Defesa Cibernética demonstra uma clara correlação entre as disciplinas oferecidas e as CBOs visadas. A cada semestre, os alunos aprofundam seus conhecimentos e habilidades em áreas específicas da segurança cibernética, recebendo a preparação necessária para atuar em diferentes funções ligadas à proteção de sistemas, redes e dados. Essa abordagem integrada é crucial para a formação de profissionais completos e adaptados às demandas do mercado de trabalho

Essas CBOs foram escolhidas por serem ocupações relevantes na área de segurança cibernética e por abranger um amplo espectro de atividades.

Para obter o certificado CBO, o aluno deve ser aprovado em todas as disciplinas do semestre. As disciplinas de cada semestre somam 480 horas, o que atende às condições de certificação da CBO, que exige um curso com no mínimo 360 horas.

A emissão do Certificado de Competência será realizada pela Faculdade ACADI-TI, após a aprovação do aluno em todas as disciplinas do semestre. O certificado é válido em todo o território nacional e pode ser utilizado para fins de contratação, promoção ou qualificação profissional.

A oferta de certificados Certificado de Competência, relacionado a CBO ao final de cada semestre é uma iniciativa da Faculdade ACADI-TI para contribuir com a inserção de seus alunos no mercado de trabalho. Os certificados CBO são uma forma de demonstrar que o aluno possui as competências e habilidades necessárias para atuar na ocupação correspondente.

2.4.10 Projetos Multidisciplinares e curricularização da extensão

A Resolução nº 7, de 18 de dezembro de 2018, determina que os cursos de graduação no Brasil devem destinar pelo menos 10% da carga horária total para atividades extensionistas. Essas atividades devem promover a integração entre a formação acadêmica e a atuação profissional, além de contribuir para o desenvolvimento social e cultural do país.

O curso de Defesa Cibernética da Faculdade ACADI-TI atende a essa exigência por meio de seus Projetos Multidisciplinares Extensionistas, presentes em todos os semestres. Destinamos 16% da carga horária do curso a estes projetos, os quais serão desenvolvidos em parceria com instituições públicas e privadas, e abordam temas relacionados à segurança cibernética.

Alguns exemplos de projetos multidisciplinares que serão desenvolvidos pelo curso de Defesa Cibernética, assim que ele receber a autorização de funcionamento:

- Projeto "Educação Cibernética nas Escolas": O projeto tem como objetivo promover a educação e conscientização sobre segurança cibernética em escolas públicas. Os estudantes desenvolvem materiais educativos e realizam palestras e workshops para alunos e professores.
- Projeto "Segurança Cibernética na Saúde": O projeto tem como objetivo desenvolver soluções de segurança cibernética para proteger infraestruturas críticas de saúde. Os estudantes trabalham em parceria com hospitais e laboratórios para identificar e mitigar riscos cibernéticos.
- Projeto "Defesa Cibernética de Cidades Inteligentes": O projeto tem como objetivo desenvolver soluções de segurança cibernética para proteger cidades inteligentes. Os estudantes trabalham em parceria com prefeituras e empresas para identificar e mitigar riscos cibernéticos relacionados a tecnologias emergentes, como internet das coisas (IoT).

Os Projetos Multidisciplinares Extensionistas da Faculdade ACADI-TI são uma importante ferramenta para o cumprimento da Resolução nº 7, de 18 de dezembro de 2018. Eles contribuem para a formação integral dos estudantes e para o desenvolvimento social e cultural do país.

Especificamente, os Projetos Multidisciplinares Extensionistas da ACADI-TI articulam teoria e prática integrando as disciplinas do semestre e dando sentido a Certificação de Competência que o aluno fará jus ao final do curso.

Isso ocorre porque os projetos são desenvolvidos com base nos conteúdos das disciplinas do semestre. Os estudantes têm a oportunidade de aplicar os conhecimentos teóricos adquiridos nas disciplinas para resolver problemas reais da comunidade.

Além disso, os projetos contribuem para o desenvolvimento das competências e habilidades necessárias para a obtenção da Certificação de Competência (CBO). Essa certificação é concedida pela ACADI-TI aos alunos que concluem o curso com aproveitamento.

Assim, os Projetos Multidisciplinares Extensionistas da ACADI-TI são uma importante contribuição para a formação de profissionais de segurança cibernética qualificados e competentes.

2.4.11 Matriz curricular

Diante do exposto, a estrutura do curso está disposta conforme apresentado a seguir:

FACULDADE ACADI-TI							
	Curso:	**CURSO SUPERIOR DE TECNOLOGIA EM DEFESA CIBERNÉTICA**	**Semestre**	*5 semestres*			
	Modalidade:	*A distância*	**Grau:**	*Tecnólogo*			
Período	**Código**	**Componentes Curriculares**	**Modalidade**	**Hora Relógio**			**Total Hora /Relógio**
				Teórica	**Prática**	**Projetos multidisciplinar**	
CBO 2124-10 - Analistas de tecnologia da informação							
1º	DC01.01	Matemática para Computação	DC	30	30	0	**60**
1º	DC01.02	Introdução à Informática	DC	30	30	0	**60**
1º	DC01.03	Lógica de Programação e Algoritmos	DC	30	30	0	**60**
1º	DC01.04	Fundamentos de Redes de Computadores	DC	30	30	0	**60**
1º	DC01.05	Princípios de Segurança da Informação	DC	30	30	0	**60**
1º	DC01.06	Projeto Multidisciplinar Extensionista I	PI	0	0	80	**80**
1º		**Total**		**150**	**150**	**80**	**380**
CBO 2123-15 - Administrador de sistemas operacionais							
2º	DC02.01	Gerenciamento de Projetos para Segurança Cibernética	DC	30	30	0	**60**
2º	DC02.02	Administração Segura de Sistema Linux	DC	30	30	0	**60**

2º	DC02.03	Administração Segura de Sistema Windows	DC	30	30	0	**60**
2º	DC02.04	Arquitetura de Segurança de Sistemas para Segurança Cibernética	DC	30	30	0	**60**
2º	DC02.05	Ética, Moral e Direitos Humanos em Tecnologia da Informação	DC	30	30	0	**60**
2º	DC02.06	Projeto Multidisciplinar Extensionista II	PI	0	0	80	**80**
2º		**Total**		**150**	**150**	**80**	**380**
CBO 2124-10 - Analista de redes e de comunicação de dados							
3º	DC03.01	Inteligência de Ameaças Cibernéticas	DC	30	30	0	**60**
3º	DC03.02	Tratamento e Resposta a Incidentes	DC	30	30	0	**60**
3º	DC03.03	Introdução ao Hacking Ético	DC	30	30	0	**60**
3º	DC03.04	Defesa de Rede	DC	30	30	0	**60**
3º	DC03.05	Planejamento e Política de Segurança Cibernética	DC	30	30	0	**60**
3º	DC03.06	Optativa (OPT)	OPT	30	30	0	**60**
3º	DC03.07	Projeto Multidisciplinar Extensionista III	PI	0	0	80	**80**
3º		**Total**		**180**	**180**	**80**	**440**
CBO 2123 - Administradores de tecnologia da informação							
4º	DC04.01	Segurança de Sistemas Operacionais	DC	30	30	0	**60**
4º	DC04.02	Segurança em Nuvem e Virtualização	DC	30	30	0	**60**
4º	DC04.03	Defesa de Rede Avançada	DC	30	30	0	**60**
4º	DC04.04	Digital Forense em Defesa Cibernética	DC	30	30	0	**60**

4º	DC04.06	Educação para relações Étnico-Raciais e Sociodiversidade	DC	30	30	0	**60**
4º	DC04.05	Projeto Multidisciplinar Extensionista IV	PI	0	0	80	**80**
4º	DC04.07	Optativa (OPT)	OPT	0	60	0	**60**
4º		**Total**		**150**	**210**	**80**	**440**
CBO 2123-20 Especialista em segurança da informação							
5º	DC05.01	Gerenciamento Avançado de Redes e Sistemas	DC	30	30	0	**60**
5º	DC05.02	Segurança Aplicada a IoT	DC	30	30	0	**60**
5º	DC05.03	Análise Avançada de Malware	DC	30	30	0	**60**
5º	DC05.04	Gestão de Crises e Continuidade de Negócios	DC	30	30	0	**60**
5º	DC05.05	Desenvolvimento Seguro de Aplicações	DC	30	30	0	**60**
5º	DC05.06	Projeto Multidisciplinar Extensionista V	PI	0	0	80	**80**
5º	DC05.07	Optativa (OPT)	OPT	0	60	0	**60**
				150	**210**	**80**	**440**
Resumo	**100,00%**	**Total**		780	900	400	2.080
Resumo Geral							
Resumo	**36,10%**	**Disciplinas curriculares**	**DC**	750		--	**750**
Resumo	**19,20%**	**Projetos Multidisciplinares Extensionistas**	**PI**	--	--	400	**400**
Resumo	**37,50%**	**Carga horária teórica**	**Teórica**	780	--	--	**780**

Resumo	**43,30%**	**Carga horária prática**	**Prática**		900	--	**900**
Rol Opt	**2,90%**	Optativa 1 - Língua Brasileira de Sinais (Libras)	OPT	60	--	--	60
Rol Opt	**2,90%**	Optativa 2 - Segurança cibernética para dispositivos móveis	OPT	60	--	--	60
Rol Opt	**2,90%**	Optativa 3 - Segurança cibernética para infraestrutura crítica	OPT	60	--	--	60
Rol Opt	**2,90%**	Optativa 4 - Inteligência Artificial Aplicada à Segurança Cibernética	OPT	60	--	--	60
Rol Opt	**2,90%**	Optativa 5 - Inovação e Empreendedorismo em Segurança Cibernética	OPT	60	--	--	60
Rol Opt	**2,90%**	Optativa 6 - Design Thinking e Inovação em Cibersegurança	OPT	60	--	--	60

2.4.12 Ementas

Apresentamos a seguir a descrição das unidades curriculares que compõe o curso:

PLANO DE ENSINO
I. IDENTIFICAÇÃO DA DISCIPLINA
CURSO: Defesa Cibernética **DISCIPLINA**: Matemática para Computação **SÉRIE: 1º** **CARGA TEÓRIA:** 30 **CARGA HORÁRIA PRÁTICA:** 30 **CARGA HORÁRIA TOTAL: 60** **CBO ASSOCIADA:** CBO 2124-10 - Analistas de tecnologia da informação **COD_DISCIPLINA:** DC01.01
II. DOCENTE RESPONSÁVEL
PROFESSOR: **TITULAÇÃO:**
III. EMENTA
Conceitos básicos de matemática discreta e de lógica matemática para computação e estratégias de provas, indução matemática, relações e conceitos de teoria de grafos
IV. OBJETIVOS
1. Capacitar os alunos a compreender e aplicar conceitos de lógica matemática relevantes para a segurança cibernética 2. Desenvolver habilidades de resolução de problemas relacionados à segurança cibernética por meio de técnicas matemáticas e lógicas. 3. Promover a compreensão dos princípios matemáticos subjacentes aos sistemas de segurança cibernética, incluindo algoritmos
V. COMPETÊNCIA/HABILIDADES
Competências: 1. Capacidade de aplicar conceitos matemáticos na resolução de problemas de segurança cibernética 2. Habilidade para avaliar e analisar algoritmos e técnicas criptográficas 3. Capacidade de compreender e implementar modelos matemáticos de ameaças cibernéticas 4. Habilidade para interpretar e analisar dados estatísticos relacionados à segurança cibernética 5. Capacidade de colaborar em equipes interdisciplinares para resolver desafios de segurança cibernética Habilidades: 1. Habilidade para programação em linguagens de alto nível para implementação de soluções de segurança cibernética 2. Capacidade de comunicação eficaz para apresentar e discutir resultados e recomendações relacionados à segurança cibernética.

VI. CONTEÚDO PROGRAMÁTICO

1. Introdução à Matemática para Computação
- Conceitos básicos de matemática e sua aplicação na computação
- Operações matemáticas e algoritmos
2. Álgebra Linear e Geometria Analítica
- Vetores e operações vetoriais
- Matrizes e suas aplicações na computação
- Geometria analítica e suas aplicações em problemas de cibernética
3. Cálculo Diferencial e Integral
- Limites, derivadas e integrais
- Aplicações na análise de algoritmos e otimização de sistemas cibernéticos
4. Teoria dos Números e Criptografia
- Princípios da teoria dos números e suas aplicações em criptografia
- Algoritmos de criptografia e segurança em sistemas cibernéticos
5. Probabilidade e Estatística
- Conceitos de probabilidade e estatística aplicados à segurança cibernética
- Análise de dados e detecção de anomalias em sistemas de defesa cibernética
6. Lógica e Teoria da Computação
- Conceitos de lógica matemática e sua aplicação em problemas de computação
- Teoria da computação e suas aplicações em segurança cibernética

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam

informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

DA SILVA, Mario Olivero; ... [et al.]. Cálculo III. Volume único. Rio de Janeiro : Fundação CECIERJ, 2016.
POMBO JÚNIOR, Dinamérico P. Cálculo 2. v.1. Rio de Janeiro: Fundação CECIERJ, 2010.
MAGALHÃES, Celius Antonio. Navegue por belas paisagens do cálculo. Brasília: Editora Universidade de Brasília, 2019.

BIBLIOGRAFIA COMPLEMENTAR

POMBO JÚNIOR, Dinamérico P. Cálculo 1. v.1. Rio de Janeiro: Fundação CECIERJ, 2010.
OLIVERO, Mário. Cálculo 1. Rio de Janeiro: Fundação CECIERJ, 2010.
VELLOSO JUNIOR, Walter Ferreira. Cálculo é fácil. Pirassununga: Faculdade de Zootecnia e Engenharia de Alimentos da Universidade de São Paulo, 2020.
PATRÃO, Mauro. Cálculo 1: derivada e integral em uma variável. Brasília: Editora Universidade de Brasília, 2011.
CARNEIRO, Carlos E. I. Prado; ... [et al.]. Introdução elementar as técnicas do cálculo diferencial e integral. São Paulo, USP-Instituto de Física, 2018.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Introdução à Informática
SÉRIE: 1º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2124-10 - Analistas de tecnologia da informação
COD_DISCIPLINA: DC01.02

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

O curso de Tecnologia em Defesa Cibernética tem como objetivo fornecer aos alunos uma base sólida em informática e segurança cibernética. A disciplina "Introdução à Informática" abordará os fundamentos da computação, incluindo hardware, software, sistemas operacionais e redes. Além disso, fornecerá uma visão geral das principais aplicações e tendências da área, preparando os estudantes para compreenderem as tecnologias e os

desafios que enfrentarão ao longo do curso. Serão discutidos temas como algoritmos, estruturas de dados, segurança da informação, entre outros, fornecendo uma base sólida para as disciplinas subsequentes. A ênfase será na aplicação prática dos conceitos, visando preparar os alunos para atuarem de forma eficaz na Defesa Cibernética. Ao final da disciplina, os alunos terão adquirido o conhecimento necessário para compreender os princípios fundamentais da informática e estarão aptos a aplicá-los em ambientes cibernéticos.

IV. OBJETIVOS

1. Capacitar os alunos para compreender e analisar as ameaças cibernéticas atuais e futuras, visando identificar vulnerabilidades e propor soluções eficazes de defesa.
2. Desenvolver as habilidades necessárias para implementar e gerenciar estratégias de segurança cibernética em ambientes corporativos, governamentais e militares.
3. Formar profissionais aptos a investigar e responder a incidentes cibernéticos, incluindo a coleta e análise de evidências digitais para identificar e responsabilizar os responsáveis.
4. Promover o pensamento crítico e a ética profissional, incentivando a atuação responsável e legalmente conforme os princípios da defesa cibernética.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Compreensão avançada de conceitos de segurança cibernética
2. Habilidade para identificar e remediar vulnerabilidades de segurança
3. Capacidade de análise de ataques cibernéticos e tomada de ações defensivas
4. Conhecimento em legislação e ética em segurança da informação
5. Habilidade para implementar e gerenciar sistemas de segurança cibernética

Habilidades:
1. Proficiência em ferramentas de segurança cibernética
2. Capacidade de comunicação eficaz sobre questões de segurança cibernética e ameaças em potencial

VI. CONTEÚDO PROGRAMÁTICO

1. Unidade 1: Fundamentos da Defesa Cibernética
- Introdução à segurança cibernética
- Princípios de proteção de dados
- Ameaças e vulnerabilidades cibernéticas
- Legislação e ética em segurança da informação

2. Unidade 2: Tecnologias e Ferramentas de Defesa Cibernética
- Criptografia e criptologia
- Firewall e sistemas de detecção de intrusão
- Análise de malware e antivírus
- Segurança em redes e sistemas

3. Unidade 3: Gestão de Riscos e Incidentes Cibernéticos
- Avaliação de riscos cibernéticos
- Planos de continuidade de negócios
- Resposta a incidentes cibernéticos
- Auditoria e conformidade em segurança da informação

4. Unidade 4: Desenvolvimento e Implementação de Estratégias de Defesa Cibernética
- Modelos de segurança cibernética
- Testes de segurança e avaliação de vulnerabilidades
- Políticas de segurança e governança de TI
- Estratégias de resposta a incidentes e gestão de crises cibernéticas

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

MASCARENHAS NETO, Pedro Tenório;...[et al.]. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: UFPB, 2019.
GROSS, Christian Meinecke. Segurança em tecnologia da informação. Indaial: Uniasselvi, 2013.
FERNANDES, Nélia O. Campo. Segurança da Informação. Cuiabá: UFMT, 2013.

BIBLIOGRAFIA COMPLEMENTAR

BARROS, Otávio Santana Rêgo;...[et al.]. Desafios estratégicos para segurança e defesa

cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2019.

WENDT, Emerson. Inteligência cibernética: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil. São Paulo: Editora Delfos, 2018.

BARBOSA, Alexandre;...[et al.]. Segurança digital : uma análise da gestão de riscos em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

NOVO, Jorge Procópio da Costa. Softwares de segurança da informação. Florianópolis: UFSC, 2010.

SANTOS, Nádia Mendes dos. Estrutura de dados. Teresina: IFPI, 2013.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Lógica de Programação e Algoritmos
SÉRIE: 1º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2124-10 - Analistas de tecnologia da informação
COD_DISCIPLINA: DC01.03

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Lógica de Programação e Algoritmos no curso de Tecnologia em Defesa Cibernética aborda os fundamentos teóricos e práticos para a resolução de problemas computacionais utilizando algoritmos e estruturas de dados. Com enfoque na segurança cibernética, os alunos serão capacitados para desenvolver habilidades de análise, pensamento crítico e raciocínio lógico na criação e implementação de algoritmos, visando a proteção de sistemas e informações sensíveis. A disciplina também abrange a compreensão e aplicação de lógica de programação em linguagens específicas utilizadas na defesa cibernética, contribuindo para a formação de profissionais qualificados e preparados para os desafios do campo da segurança da informação.

IV. OBJETIVOS

1. Compreender os princípios de lógica de programação e algoritmos para aplicação na defesa cibernética.
2. Desenvolver habilidades para a identificação e resolução de problemas relacionados à segurança cibernética por meio da lógica de programação e algoritmos.

3. Capacitar os alunos a utilizar a lógica de programação e algoritmos para a implementação de soluções de defesa cibernética eficazes.
4. Promover a aplicação prática dos conhecimentos adquiridos em lógica de programação e algoritmos para a proteção e segurança de sistemas e dados digitais.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Raciocínio lógico
2. Análise de algoritmos
3. Resolução de problemas
4. Segurança cibernética
5. Programação defensiva

Habilidades:
1. Desenvolvimento de algoritmos seguros
2. Análise e identificação de vulnerabilidades em sistemas de computadores

VI. CONTEÚDO PROGRAMÁTICO

1. Introdução à Defesa Cibernética
- Conceitos básicos de segurança cibernética
- Principais ameaças e vulnerabilidades
- Princípios de defesa cibernética
2. Fundamentos de Programação em Defesa Cibernética
- Linguagens de programação utilizadas em segurança cibernética
- Desenvolvimento de algoritmos para detecção e prevenção de ataques
- Práticas de programação segura
3. Algoritmos de Segurança Cibernética
- Tipos de algoritmos utilizados em segurança cibernética (criptografia, autenticação, etc.)
- Aplicações de algoritmos na defesa cibernética
- Análise de algoritmos de segurança cibernética
4. Aplicações Práticas em Defesa Cibernética
- Estudos de casos reais de ataques cibernéticos e suas defesas
- Utilização de ferramentas e tecnologias em defesa cibernética
- Desenvolvimento de estratégias de defesa cibernética.

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:
  - Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Situações de Reprovação:
  - Nota final inferior a 3,0.
  - Falta em mais de 25% das aulas.
  - Não entrega de mais de 25% das atividades avaliativas.

Observações:
- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

ALÉSSIO, Simone Cristina. Lógica e técnicas de Programação. Indaial: Uniasselvi, 2017.

GOMES, Bruno Emerson Gurgel. Fundamentos de Lógica e Algoritmos. Natal: IFRN, 2015.

LACERDA, Liluyoud Cury de; ... [et al.]. Lógica de programação. Cuiabá: Ed.UFMT, 2014.

BIBLIOGRAFIA COMPLEMENTAR

CASTILHO, Marcos Alexandre. Algoritmos e estruturas de dados 1. Curitiba: UFPR, 2020.

BATISTA, Rogério da Silva. Lógica de programação. Teresina: IFPI, 2013

RAMOS, José Marcio Benite. Estrutura de dados. Cuiabá: UFMT, 2013.

RIBEIRO, Maria Ivanilse Calderon; ... [et al.]. Projeto de Sistemas WEB. Cuiabá: UFMT, 2015.

CUNHA, Luiz Egidio Costa. Análise de sistemas. Colatina: CEAD / Ifes, 2011.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Fundamentos de Redes de Computadores
SÉRIE: 1º

CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2124-10 - Analistas de tecnologia da informação
COD_DISCIPLINA: DC01.04

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Fundamentos de Redes de Computadores no curso de Tecnologia em Defesa Cibernética tem como objetivo fornecer aos alunos uma compreensão abrangente e aprofundada dos conceitos fundamentais de redes de computadores, incluindo modelos de redes, protocolos de comunicação, topologias de redes, arquiteturas de redes e tecnologias de rede. Os alunos também irão explorar questões de segurança e defesa cibernética relacionadas a redes de computadores, incluindo ameaças e vulnerabilidades comuns, estratégias de mitigação de riscos e técnicas de monitoramento e proteção de redes. Através de estudos de caso e projetos práticos, os alunos desenvolverão habilidades práticas para projetar, implementar e gerenciar redes de computadores seguras e robustas, fundamentais para atuar com sucesso na área de defesa cibernética. A disciplina também abordará aspectos éticos e legais relacionados à segurança de redes, preparando os alunos para agir de acordo com as melhores práticas e regulações vigentes. Ao final do curso, os alunos estarão aptos a aplicar os conhecimentos adquiridos na disciplina para enfrentar os desafios reais enfrentados por profissionais de defesa cibernética atuantes no mercado de trabalho.

IV. OBJETIVOS

1. Compreender os fundamentos de redes de computadores, incluindo conceitos de protocolos, endereçamento e roteamento, de forma a aplicar esse conhecimento na defesa cibernética.
2. Desenvolver habilidades práticas em configuração, manutenção e monitoramento de redes de computadores, visando a identificação e prevenção de ameaças cibernéticas.
3. Analisar e avaliar as vulnerabilidades de sistemas de redes de computadores, a fim de propor e implementar soluções de segurança eficazes.
4. Integrar os conhecimentos adquiridos na disciplina com as estratégias de defesa cibernética, visando a proteção de informações e sistemas de maneira eficiente e eficaz.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Compreensão dos princípios fundamentais de redes de computadores
2. Capacidade para analisar e diagnosticar problemas em redes
3. Conhecimento em segurança de redes e defesa cibernética
4. Habilidade para configurar e gerenciar redes de computadores
5. Capacidade para implementar soluções de segurança em redes de computadores

Habilidades:
1. Habilidade para identificar e corrigir vulnerabilidades em redes de computadores

2. Habilidade para utilizar ferramentas de monitoramento e análise de tráfego de rede

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Introdução à Defesa Cibernética
- Conceitos fundamentais de defesa cibernética
- Evolução das ameaças cibernéticas
- Importância da segurança cibernética para as organizações
- Legislação e regulamentação em defesa cibernética

Unidade de Aprendizagem 2: Arquiteturas de Segurança
- Firewalls e IDS/IPS
- Segurança em redes de computadores
- Controle de acesso e autenticação
- Criptografia e segurança em redes sem fio

Unidade de Aprendizagem 3: Gerenciamento de Incidentes
- Identificação, classificação e resposta a incidentes
- Procedimentos de resposta a incidentes
- Análise forense em segurança cibernética
- Ferramentas e técnicas para detecção e resposta a incidentes

Unidade de Aprendizagem 4: Aspectos Éticos e Legais em Defesa Cibernética
- Ética profissional em segurança cibernética
- Responsabilidades legais e regulatórias
- Privacidade e proteção de dados
- Aspectos éticos em testes de segurança e hacking ético

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.

- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

BAY, Edemilson;...[et al.]. Fundamentos de redes de computadores. Indaial: Uniasselvi, 2021.

MACEDO, Ricardo Tombesi;...[et al.]. Redes de computadores. Santa Maria: UFSM, 2018.

FERNANDEZ, Marcial Porto. Rede de computadores. Fortaleza: EdUECE, 2019.

BIBLIOGRAFIA COMPLEMENTAR

LATZKE, Carlos Alberto;...[et al.]. Infraestrutura e redes de computadores. Indaial: Uniasselvi, 2019.

AMARAL, Marcos Prado; ... [et al.]. Redes de computadores I. Belo Horizonte: CEFET-MG, 2013.

GUEDES, Jackes Ridan da Silva; ... [et al.]. Redes de computadores. Brasília : Escola Técnica de Brasília, 2014.

PINTO NETO, João Batista. Redes de Computadores. Cuiabá: UFMT, 2014.

SAMPAIO, Leobino Nascimento. Redes de computadores. Rio de Janeiro: UFRJ, 2018

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Princípios de Segurança da Informação
SÉRIE: 1º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2124-10 - Analistas de tecnologia da informação
COD_DISCIPLINA: DC01.05

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Princípios de Segurança da Informação no curso de Tecnologia em Defesa Cibernética abordará os fundamentos e metodologias para proteção de dados, sistemas e redes contra ameaças cibernéticas. Serão estudados conceitos de confidencialidade, integridade e disponibilidade da informação, além de técnicas de criptografia, autenticação, controle de acesso e gerenciamento de riscos. Também serão exploradas legislações e normas de segurança da informação, bem como estratégias de prevenção e resposta a incidentes de segurança. A disciplina terá enfoque prático, com atividades de simulação de ataques e defesa, visando preparar os alunos para atuarem de forma eficiente na proteção do ambiente cibernético.

IV. OBJETIVOS

1. Compreender os princípios fundamentais da segurança da informação e sua aplicação prática no contexto da defesa cibernética.
2. Desenvolver habilidades para identificar e analisar potenciais ameaças cibernéticas, visando a proteção de sistemas e dados.
3. Aprender a aplicar técnicas e ferramentas de segurança da informação para mitigar riscos e garantir a integridade, confidencialidade e disponibilidade de informações em ambientes cibernéticos.
4. Adquirir conhecimentos sobre as principais regulamentações e boas práticas relacionadas à segurança da informação, a fim de atuar de forma ética e responsável na defesa cibernética.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Identificar e mitigar vulnerabilidades em sistemas e redes.
2. Aplicar técnicas avançadas de criptografia para proteger informações sensíveis.
3. Desenvolver e implementar políticas de segurança da informação.
4. Realizar análise de riscos e ameaças cibernéticas.
5. Atuar de forma ética e responsável na defesa cibernética.

Habilidades:
1. Pensamento analítico e resolução de problemas em ambientes cibernéticos.
2. Comunicação eficaz para atuar em equipes multidisciplinares e apresentar soluções de segurança da informação.

VI. CONTEÚDO PROGRAMÁTICO

1. Unidade 1: Introdução à Segurança da Informação
- Conceitos básicos de segurança da informação
- Importância da segurança da informação na defesa cibernética
- Princípios de segurança da informação aplicados à defesa cibernética
2. Unidade 2: Gerenciamento de Riscos e Vulnerabilidades
- Identificação de riscos e vulnerabilidades em ambientes cibernéticos
- Técnicas de avaliação de riscos
- Estratégias de mitigação de riscos e vulnerabilidades

3. Unidade 3: Criptografia e Segurança de Redes
- Princípios de criptografia e sua aplicação na defesa cibernética
- Protocolos de segurança para redes cibernéticas
- Técnicas de proteção de dados em redes cibernéticas
4. Unidade 4: Gestão de Incidentes e Resposta a Ataques
- Procedimentos de gestão de incidentes em ambientes cibernéticos
- Análise de ataques cibernéticos e técnicas de resposta
- Planejamento de continuidade de negócios em caso de incidentes de segurança da informação

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:
- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:
- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:
  - Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Situações de Reprovação:
  - Nota final inferior a 3,0.
  - Falta em mais de 25% das aulas.
  - Não entrega de mais de 25% das atividades avaliativas.

Observações:
- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

MASCARENHAS NETO, Pedro Tenório;...[et al.]. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: UFPB, 2019.

GROSS, Christian Meinecke. Segurança em tecnologia da informação. Indaial: Uniasselvi, 2013.

FERNANDES, Nélia O. Campo. Segurança da Informação. Cuiabá: UFMT, 2013.

BIBLIOGRAFIA COMPLEMENTAR

BARROS, Otávio Santana Rêgo;...[et al.]. Desafios estratégicos para segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2019.

WENDT, Emerson. Inteligência cibernética: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil. São Paulo: Editora Delfos, 2018.

BARBOSA, Alexandre;...[et al.]. Segurança digital : uma análise da gestão de riscos em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

NOVO, Jorge Procópio da Costa. Softwares de segurança da informação. Florianópolis: UFSC, 2010.

SANTOS, Nádia Mendes dos. Estrutura de dados. Teresina: IFPI, 2013.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Projeto Multidisciplinar Extensionista I
SÉRIE: 1º
CARGA TEÓRIA: 0
CARGA HORÁRIA PRÁTICA: 80
CARGA HORÁRIA TOTAL: 80
CBO ASSOCIADA: CBO 2124-10 - Analistas de tecnologia da informação
COD_DISCIPLINA: DC01.06

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Projeto Multidisciplinar Extensionista I oferece aos estudantes do curso de Tecnologia em Defesa Cibernética a oportunidade de aplicar os conhecimentos teóricos adquiridos ao longo do curso em um projeto prático e interdisciplinar. A ementa abordará temas como segurança de redes, análise de vulnerabilidades, estratégias de defesa cibernética, entre outros, com o objetivo de desenvolver habilidades de trabalho em equipe, comunicação e resolução de problemas reais. Além disso, os alunos terão a oportunidade de se envolver com a comunidade local e contribuir para a conscientização sobre a importância da segurança cibernética. Ao final do curso, os estudantes estarão aptos a aplicar seus

conhecimentos de forma eficaz e ética em situações do mundo real, preparando-os para futuras carreiras na área de defesa cibernética.

IV. OBJETIVOS

1. Capacitar os alunos para identificar e analisar ameaças cibernéticas, desenvolvendo habilidades de detecção e prevenção de ataques.
2. Desenvolver competências de gerenciamento de riscos cibernéticos, incluindo a avaliação de vulnerabilidades e a implementação de medidas de segurança.
3. Promover a colaboração e o trabalho em equipe entre os alunos, visando a prática de resolução de problemas e a tomada de decisões em situações de segurança cibernética.
4. Estimular a criatividade e inovação dos alunos na proposição de soluções para desafios e problemas relacionados à defesa cibernética.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Capacidade de identificar e analisar ameaças cibernéticas.
2. Habilidade para desenvolver e implementar estratégias de defesa cibernética.
3. Conhecimento em tecnologias de segurança da informação.
4. Capacidade de realizar avaliações de vulnerabilidade em sistemas.
5. Habilidade para gerenciar incidentes de segurança cibernética.

Habilidades:
1. Codificação de script para automação de processos de segurança.
2. Análise forense digital para investigação de incidentes.

VI. DESCRIÇÃO DO PROJETO

Este projeto visa criar um sistema acessível e de fácil utilização que permita a pequenas e médias empresas monitorar suas redes e sistemas em busca de potenciais ameaças à segurança da informação. Considerando que PMEs muitas vezes não possuem os recursos necessários para manter uma equipe de segurança cibernética dedicada, esse sistema serviria como uma ferramenta crucial para a proteção de seus dados e infraestrutura tecnológica.

VII. INTEGRAÇÃO DAS DISCIPLINAS

- **Matemática para Computação:** Utilização de conceitos estatísticos para analisar padrões de tráfego na rede que possam indicar comportamentos suspeitos. Além disso, técnicas de criptografia para a segurança dos dados coletados e transmitidos pelo sistema.
- **Introdução à Informática:** Conhecimento sobre hardware e software será fundamental para o desenvolvimento do sistema, garantindo que ele possa ser implementado em diferentes configurações de infraestrutura de TI.
- **Lógica de Programação e Algoritmos:** Desenvolvimento do núcleo lógico do sistema, incluindo algoritmos para detecção de ameaças, análise de vulnerabilidades e geração de alertas.
- **Fundamentos de Redes de Computadores:** Entendimento profundo sobre o funcionamento das redes será necessário para monitorar efetivamente o tráfego e identificar possíveis invasões ou anomalias.
- **Princípios de Segurança da Informação:** Aplicação de conceitos de

confidencialidade, integridade e disponibilidade no design do sistema, assegurando que as PMEs possam confiar na proteção oferecida.

VII. CONTRIBUIÇÃO À COMUNIDADE

Este projeto não apenas integra conhecimentos fundamentais das disciplinas iniciais do curso, mas também oferece uma solução prática e extremamente relevante para um problema real enfrentado por muitas empresas. Ao disponibilizar o sistema para PMEs, os estudantes estarão contribuindo diretamente para a melhoria da segurança cibernética na comunidade empresarial, um passo importante para a construção de uma sociedade digital mais segura.

VII. AVALIAÇÃO

Para avaliar o projeto de "Sistema de Monitoramento e Alerta de Segurança Cibernética para Pequenas e Médias Empresas (PMEs)", estruturamos um sistema de avaliação baseado em entregas parciais, cada uma focando em aspectos diferentes do desenvolvimento do projeto. A nota final será calculada com base no desempenho em cada entrega, considerando uma nota mínima de aprovação de 7,0.

Estrutura de Avaliação:

1. Proposta do Projeto (15% da nota final)
   - **Descrição detalhada do projeto:** objetivo, justificativa, impacto esperado.
   - **Revisão bibliográfica:** referências sobre segurança da informação, estatísticas aplicadas à segurança, lógica de programação aplicada à detecção de ameaças.
   - **Critérios de avaliação:** clareza, relevância, aplicabilidade.

2. Design e Planejamento (20% da nota final)
   - **Arquitetura do sistema:** diagramas de componentes, fluxo de dados.
   - **Plano de desenvolvimento:** metodologia, ferramentas, linguagens de programação escolhidas, cronograma de execução.
   - **Critérios de avaliação:** coerência, viabilidade técnica, organização.

3. Desenvolvimento de Algoritmos (20% da nota final)
   - **Implementação de algoritmos:** detecção de ameaças, análise de vulnerabilidades, criptografia para segurança de dados.
   - **Testes unitários:** comprovação da funcionalidade dos algoritmos.
   - **Critérios de avaliação:** eficácia, eficiência, inovação.

4. Implementação e Testes de Rede (20% da nota final)
   - **Simulação de rede:** configuração de um ambiente de rede controlado para testes.
   - **Testes de penetração:** verificação da capacidade do sistema em detectar e alertar sobre tentativas de intrusão.
   - **Critérios de avaliação:** realismo, abrangência, resultados obtidos.

5. Segurança e Confiabilidade (15% da nota final)
   - **Análise de segurança:** avaliação de vulnerabilidades no próprio sistema de

monitoramento.
- **Mecanismos de segurança implementados:** autenticação, controle de acesso, criptografia.
- **Critérios de avaliação:** robustez, confiabilidade, aderência aos princípios de segurança da informação.

6. Apresentação Final e Documentação (10% da nota final)
- **Apresentação do sistema:** demonstração prática das funcionalidades e dos testes.
- **Documentação técnica e de usuário:** guias de instalação, uso e manutenção.
- **Critérios de avaliação:** clareza, completude, profissionalismo.

Nota Final:
A nota final será a soma ponderada das notas obtidas em cada entrega, conforme os percentuais atribuídos. Para ser aprovado, o grupo deve atingir uma nota mínima de 7,0 na soma das entregas. Feedbacks detalhados serão fornecidos em cada etapa para permitir melhorias contínuas.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA
1. Todas as bibliografias básicas estudadas até o momento

BIBLIOGRAFIA COMPLEMENTAR
1. Todas as bibliografias complementares estudadas até o momento

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Gerenciamento de Projetos para Segurança Cibernética
SÉRIE: 2º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123-15 - Administrador de sistemas operacionais
COD_DISCIPLINA: DC02.01

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Gerenciamento de Projetos para Segurança Cibernética tem como objetivo fornecer aos estudantes do curso de Tecnologia em Defesa Cibernética as habilidades necessárias para planejar, executar e controlar projetos de segurança cibernética de forma

eficiente e eficaz. Durante o curso, os alunos irão aprender sobre os princípios e práticas de gerenciamento de projetos, incluindo a definição de objetivos, o estabelecimento de metas, a identificação de recursos necessários e a elaboração de cronogramas. Eles também serão introduzidos às ferramentas e técnicas utilizadas no gerenciamento de projetos, com ênfase nas particularidades da segurança cibernética. Além disso, os estudantes serão incentivados a desenvolver habilidades de liderança e trabalho em equipe, fundamentais para o sucesso na gestão de projetos de segurança cibernética. Ao final do curso, espera-se que os alunos sejam capazes de aplicar os conhecimentos adquiridos para gerenciar com sucesso projetos de segurança cibernética em ambientes reais.

IV. OBJETIVOS

1. Capacitar os alunos para compreender e aplicar os conceitos de gerenciamento de projetos específicos para segurança cibernética.
2. Desenvolver as habilidades necessárias para liderar e gerenciar projetos em ambientes de segurança cibernética, incluindo planificação, execução e controle.
3. Promover a compreensão das melhores práticas e ferramentas utilizadas no gerenciamento de projetos de segurança cibernética, incluindo a identificação de riscos e caminhos críticos .
4. Preparar os alunos para a certificação em gerenciamento de projetos na área de segurança cibernética, aumentando suas oportunidades no mercado de trabalho.

V. COMPETÊNCIA/HABILIDADES

Competências:

1. Compreensão dos princípios de Gerenciamento de Projetos voltados para Segurança Cibernética
2. Gestão de projetos focados em Segurança Cibernética
3. Utilização de ferramentas e práticas de Gerenciamento de Projetos
4. Embasamento técnico para realizar certificações em gerenciamento de projetos de segurança cibernética

Habilidades:
1. Elaboração de planos de segurança cibernética
2. Utilização de ferramentas e tecnologias para gestão de projetos.

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Introdução ao Gerenciamento de Projetos de Segurança Cibernética

Visão geral da segurança cibernética e sua importância
Princípios fundamentais do gerenciamento de projetos
Diferenças entre gerenciamento de projetos tradicional e gerenciamento de projetos de segurança cibernética
Estruturas e metodologias de gerenciamento de projetos (PMBOK, Agile, Scrum) aplicadas à segurança cibernética

Unidade de Aprendizagem 2: Planejamento de Projetos de Segurança Cibernética

Definição de escopo e objetivos de segurança
Identificação de stakeholders e comunicação eficaz
Planejamento de recursos, tempo e custos
Desenvolvimento de planos de segurança cibernética integrados

Unidade de Aprendizagem 3: Liderança e Gerenciamento de Equipes em Segurança Cibernética

Estratégias para liderança eficaz de equipes de segurança cibernética
Gestão de conflitos e motivação de equipe
Comunicação eficaz e gerenciamento de stakeholders
Diversidade e inclusão em equipes de segurança cibernética

Unidade de Aprendizagem 4: Execução e Controle de Projetos de Segurança Cibernética

Implementação de planos de segurança cibernética
Monitoramento e controle de progresso do projeto
Gestão de mudanças e comunicação de alterações
Avaliação de desempenho e garantia de qualidade em segurança cibernética

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.

- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

FRANÇA, Cesar Moises;...[et al.]. Gestão de serviços e projetos de TI. Indaial: Uniasselvi, 2019.

CARDOSO, Rodrigo dos Santos. Gestão de projetos e processos. Indaial: Uniasselvi, 2020.

CARVALHO, Claudinê Jordão de. Elaboração e Gestão de Projetos. Florianópolis : UFSC, 2011

BIBLIOGRAFIA COMPLEMENTAR

ESMERALDO, Jorge Ney. Gestão de Projetos. Cuiabá: UFMT, 2013.

CAMPOS, Luiz Fernando Rodrigues. Gestão de Projetos. Curitiba: IFPR, 2011.

LA TORRE, José Alfredo Pareja Gomez. Gestão de projetos públicos. Indaial: Uniasselvi, 2015.

SANTOS, Carla Marilia dos; ... [et al.]. Fundamentos de Gestão de Projetos de Tecnologia da Informação. v. 1. Rio de Janeiro: Fundação CECIERJ, 2010.

GRANJA, Sandra Inês Baraglio. Elaboração e avaliação de projetos. Florianópolis : UFSC, 2010

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Administração Segura de Sistema Linux
SÉRIE: 2º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123-15 - Administrador de sistemas operacionais
COD_DISCIPLINA: DC02.02

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Administração Segura de Sistema Linux do curso de Tecnologia em Defesa Cibernética tem como objetivo capacitar os estudantes para administrar de forma eficiente e segura os sistemas operacionais baseados em Linux, abordando temas como configuração de permissões, gerenciamento de usuários, atualizações de segurança, monitoramento de atividades suspeitas, prevenção de ataques cibernéticos e resposta a incidentes. Ao longo do curso, os alunos aprenderão técnicas avançadas de administração de sistemas Linux, utilizando ferramentas e práticas recomendadas para garantir a integridade, confidencialidade e disponibilidade das informações, preparando-os para atuar no mercado de segurança cibernética com sólidos conhecimentos em administração de sistemas operacionais de código aberto.

IV. OBJETIVOS

1. Desenvolver habilidades para administrar sistemas Linux de forma segura, visando a proteção contra ameaças cibernéticas.
2. Compreender e aplicar as boas práticas de segurança em sistemas Linux, incluindo a configuração de firewalls, controle de acessos e detecção de intrusões.
3. Capacitar os alunos a analisar e responder a incidentes de segurança em sistemas Linux, incluindo a investigação e mitigação de possíveis brechas de segurança.
4. Promover a conscientização sobre a importância da administração segura de sistemas Linux para a defesa cibernética, incluindo a ética e responsabilidade na utilização dessas ferramentas.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Gerenciamento seguro de sistemas Linux
2. Identificação de vulnerabilidades em sistemas Linux
3. Implementação de medidas de segurança em sistemas Linux
4. Análise de logs e monitoramento de atividades em sistemas Linux
5. Resolução de incidentes de segurança em sistemas Linux

Habilidades:
1. Configuração avançada de sistemas Linux
2. Corrigir falhas de segurança em sistemas Linux

VI. CONTEÚDO PROGRAMÁTICO

Unidade de aprendizagem 1: Conceitos básicos de administração segura de sistemas Linux
- Introdução aos princípios de administração de sistemas Linux
- Importância da segurança em ambientes de tecnologia em defesa cibernética
- Aplicação de medidas de segurança em sistemas Linux

Unidade de aprendizagem 2: Gerenciamento de usuários e permissões no Linux
- Criação e gerenciamento de contas de usuários
- Controle de acesso e permissões de arquivos e diretórios
- Implementação de políticas de segurança para usuários no Linux

Unidade de aprendizagem 3: Segurança de redes e servidores Linux
- Configuração de firewalls e filtros de pacotes
- Análise de tráfego de rede e detecção de intrusos
- Proteção contra ataques externos e internos em servidores Linux

Unidade de aprendizagem 4: Auditoria e monitoramento de sistemas Linux
- Implementação de ferramentas de monitoramento e análise de logs
- Melhores práticas de auditoria de segurança em sistemas Linux
- Resposta a incidentes de segurança e elaboração de políticas de resposta rápida.

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

ANDRADE, Alessandro Vivas;...[et al.]. Linux: comandos básicos e avançados. Diamantina: Ed. do autor, 2019.

NEGUS, Christopher. Linux – a Bíblia. São Paulo: Smartbooks, 2018.

LINUX INSTITUTE. Linux Essentials. São Paulo: Linux Professional Institute, 2023.

BIBLIOGRAFIA COMPLEMENTAR

SILVA JÚNIOR, Edson Nascimento. Introdução ao Ambiente Linux. Manaus: UFAM, 2009.

JUCA, Sandro;...[et al.]. Aplicações Práticas de sistemas embarcados Linux utilizando Raspberry Pi. Rio de Janeiro: PoD, 2018.

VALLE, Odilson Tadeu. Linux básico, gerência, segurança e monitoramento de redes. São José: IFSC, 2019.

FRANÇA, Cícero Tadeu Pereira Lima. Banco de dados. Fortaleza, CE : EdUECE, 2015.

SILVA, Thiago Alves Elias da; ... [et al.]. Prática de banco de dados. Teresina : Instituto Federal de Educação, Ciência e Tecnologia do Piauí, 2013.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Administração Segura de Sistema Windows
SÉRIE: 2º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123-15 - Administrador de sistemas operacionais
COD_DISCIPLINA: DC02.03

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Administração Segura de Sistema Windows, oferecida no curso de Tecnologia em Defesa Cibernética, tem como objetivo fornecer aos alunos os conhecimentos necessários para a gestão e manutenção segura de sistemas operacionais Windows. A ementa abordará tópicos como configuração de políticas de segurança, gerenciamento de contas de usuário, implementação de firewalls e antivírus, monitoramento de ameaças e vulnerabilidades, e resposta a incidentes de segurança. Os estudantes aprenderão a aplicar práticas de administração segura em ambientes corporativos, visando proteger a integridade e confidencialidade dos dados, garantindo a disponibilidade dos recursos de TI. Além disso, serão apresentadas as melhores estratégias para a prevenção e detecção de ataques cibernéticos, preparando os alunos para atuarem de forma proativa na defesa dos sistemas

Windows contra ameaças digitais.

IV. OBJETIVOS

1. Desenvolver habilidades de configuração e administração segura de sistemas Windows para garantir a proteção de redes e sistemas contra ameaças cibernéticas.
2. Capacitar os estudantes a identificar vulnerabilidades em sistemas Windows e implementar medidas de segurança eficazes para mitigar riscos de ataques cibernéticos.
3. Fomentar a compreensão dos princípios de segurança da informação e a importância da administração segura de sistemas Windows no contexto da defesa cibernética.
4. Preparar os estudantes para lidar com desafios reais em ambientes de tecnologia da informação, promovendo a aplicação prática dos conhecimentos adquiridos na administração segura de sistemas Windows.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Identificar e avaliar potenciais ameaças à segurança dos sistemas Windows
2. Implementar estratégias para proteger sistemas Windows contra invasões e ataques cibernéticos
3. Analisar e interpretar relatórios de segurança do sistema Windows
4. Desenvolver planos de contingência para lidar com possíveis incidentes de segurança
5. Manter-se atualizado sobre as mais recentes ferramentas e práticas de segurança cibernética para sistemas Windows

Habilidades:
1. Habilidade para configurar e administrar com eficácia a segurança de sistemas Windows
2. Habilidade para corrigir falhas de segurança

VI. CONTEÚDO PROGRAMÁTICO

Unidade de aprendizagem 1: Conceitos básicos de administração segura de sistemas Windows
- Introdução aos princípios de administração de sistemas Windows
- Importância da segurança em ambientes de tecnologia em defesa cibernética
- Aplicação de medidas de segurança em sistemas Windows

Unidade de aprendizagem 2: Gerenciamento de usuários e permissões no Windows
- Criação e gerenciamento de contas de usuários
- Controle de acesso e permissões de arquivos e diretórios
- Implementação de políticas de segurança para usuários no Windows

Unidade de aprendizagem 3: Segurança de redes e servidores Windows
- Configuração de firewalls e filtros de pacotes
- Análise de tráfego de rede e detecção de intrusos
- Proteção contra ataques externos e internos em servidores Linux

Unidade de aprendizagem 4: Auditoria e monitoramento de sistemas Windows
- Implementação de ferramentas de monitoramento e análise de logs
- Melhores práticas de auditoria de segurança em sistemas Linux
- Resposta a incidentes de segurança e elaboração de políticas de resposta rápida.

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

MAZIERO, Carlos Alberto. Sistemas operacionais: conceitos e mecanismos. Curitiba: DINF - UFPR, 2019.

PINTO NETO, João Batista. Sistemas operacionais. Cuiabá : UFMT, 2014.

PEREIRA, Adriana Soares. Sistemas operacionais. Frederico Westphalen: UFSM, 2015

BIBLIOGRAFIA COMPLEMENTAR

RIBEIRO, Maria Ivanilse Calderon; ... [et al.]. Projeto de Sistemas WEB. Cuiabá: UFMT, 2015.

FRAGA, Marcelo Caramuru Pimentel; ... [et al.]. Sistemas operacionais II. Belo Horizonte: CEFET/MG, 2012.

COUTINHO, Bruno Cardoso. Sistemas operacionais. Colatina: CEAD / Ifes, 2010.

NOVO, Jorge Procópio da Costa. Softwares de segurança da informação. Florianópolis: UFSC, 2010.

FERNANDES, Nélia O. Campo. Segurança da Informação. Cuiabá: UFMT, 20131.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Arquitetura de Segurança de Sistemas para Segurança Cibernética
SÉRIE: 2º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123-15 - Administrador de sistemas operacionais
COD_DISCIPLINA: DC02.04

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Arquitetura de Segurança de Sistemas para Segurança Cibernética no curso de Tecnologia em Defesa Cibernética abordará os princípios fundamentais da arquitetura de sistemas de segurança, incluindo redes, servidores, bancos de dados e aplicativos. Serão exploradas as melhores práticas para o planejamento, implementação e gestão de sistemas de segurança, considerando as ameaças e vulnerabilidades presentes no ambiente cibernético. Também será enfatizada a importância da integração de tecnologias de segurança, tais como firewalls, criptografia, autenticação e detecção de intrusos, visando a proteção efetiva das informações e a prevenção de ataques cibernéticos. Ao longo da disciplina, os estudantes serão desafiados a aplicar os conhecimentos teóricos em estudos de caso e laboratórios práticos, a fim de desenvolver habilidades para projetar e implementar arquiteturas de segurança robustas e eficientes.

IV. OBJETIVOS

1. Fundamentar os alunos nos Princípios da Arquitetura de Segurança de Sistemas
2. Desenvolver Competências para o Planejamento e Implementação de Sistemas de Segurança
3. Promover a Compreensão das Ameaças e Vulnerabilidades Cibernéticas
4. Fomentar a Aplicação Prática Através de Laboratórios e Estudos de Caso

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Compreensão avançada dos princípios de arquitetura de segurança de sistemas.
2. Capacidade de analisar e identificar vulnerabilidades em ambientes cibernéticos.
3. Aptidão para desenvolver e implementar estratégias de defesa cibernética.
4. Conhecimento aprofundado sobre as melhores práticas de segurança em sistemas.
5. Habilidade para gerenciar e mitigar incidentes de segurança cibernética.

Habilidades:
1. Análise Crítica e Solução de Problemas
2. Aplicação Prática de Conhecimentos Teóricos .

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Fundamentos da Arquitetura de Segurança de Sistemas
Princípios da Arquitetura de Segurança de Sistemas
Ameaças, Vulnerabilidades e Riscos Cibernéticos
Unidade 2: Tecnologias de Proteção e Estratégias de Segurança
Firewalls e Sistemas de Prevenção de Intrusão
Fundamentos de Criptografia e Autenticação
Fundamentos Detecção de Intrusos e Resposta a Incidentes
Unidade 3: Design e Implementação de Arquiteturas de Segurança
Fundamentos de Design de Sistemas Seguros
Implementação de Sistemas de Segurança
Gestão de Configuração de Segurança e Políticas de Segurança
Unidade 4: Práticas Avançadas e Tendências em Segurança Cibernética
Integração de Tecnologias Emergentes em Segurança
Análise de Casos de Uso e Estudos de Caso
Preparação para o Futuro da Segurança Cibernética

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**

- Prova escrita com questões sobre os conteúdos da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

MACHADO, Vinicius Ponte. Arquitetura e organização de computadores. Teresina: EDUFPI, 2019.

FERNANDEZ, Marcial Porto. Arquitetura de Computadores. Fortaleza : EdUECE, 2015.

BADALOTTI; Greisse Moser . Lógica e organização de computadores. Indaial : Uniasselvi, 2016.

BIBLIOGRAFIA COMPLEMENTAR

CRISTO, Fernando de; ... [et al.]. Arquitetura de computadores. Frederico Westphalen: UFSM, 2018.

WANDERLEY NETTO, Eduardo Bráulio. Arquitetura de Computadores: A visão do software. Natal: Editora do CEFET-RN, 2005.

CUNHA, Judson Michael; ... [et al.]. Arquitetura de computadores. Indaial : Uniasselvi, 2012.

FÁVERO, Eliane Maria de Bortoli. Organização e arquitetura de computadores. Pato Branco: Universidade Tecnológica Federal do Paraná, 2011.

POLLI, Marco. Organização de computadores. Rio de Janeiro: SESES, 2014

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Ética, Moral e Direitos Humanos em Tecnologia da Informação
SÉRIE: 2º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123-15 - Administrador de sistemas operacionais
COD_DISCIPLINA: DC02.05

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Ética, Moral e Direitos Humanos em Tecnologia da Informação no curso de Tecnologia em Defesa Cibernética tem como objetivo introduzir os estudantes aos principais conceitos e debates éticos, morais e de direitos humanos relacionados à segurança cibernética. Serão abordados temas como privacidade, responsabilidade social, impactos da tecnologia na sociedade, dilemas éticos em ataques cibernéticos, políticas de segurança e direitos individuais. Além disso, a disciplina estimulará a reflexão crítica dos alunos sobre o papel dos profissionais de defesa cibernética na promoção de uma cultura ética e moralmente responsável no uso da tecnologia da informação.

IV. OBJETIVOS

1. Compreender os princípios éticos e morais relacionados à tecnologia da informação e sua aplicação na defesa cibernética.
2. Analisar as implicações dos direitos humanos no contexto da segurança da informação e da defesa cibernética.
3. Desenvolver habilidades para identificar e resolver dilemas éticos e morais relacionados à tecnologia da informação na área de defesa cibernética.
4. Aplicar os conhecimentos de ética, moral e direitos humanos na tomada de decisões éticas e responsáveis em situações de segurança cibernética.

V. COMPETÊNCIA/HABILIDADES

1. Competências:
- Compreensão ética e moral na tomada de decisões em tecnologia da informação
- Capacidade de analisar e avaliar as implicações éticas e morais nas práticas de defesa cibernética
- Conhecimento de legislação e direitos humanos relacionados à segurança cibernética
- Habilidade em identificar e solucionar dilemas éticos e morais na área de Tecnologia da Informação
- Capacidade de aplicar princípios éticos na prática de defesa cibernética
2. Habilidades:
- Habilidade em comunicar e defender decisões éticas e morais em Tecnologia da Informação
- Capacidade de integrar conceitos éticos e morais na implementação de estratégias de defesa cibernética.

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Ética na Defesa Cibernética
- Introdução à ética na tecnologia da informação
- Ética profissional e responsabilidade social na defesa cibernética
- Ética no uso de dados e informações na área de segurança cibernética

Unidade 2: Moral na Defesa Cibernética
- Fundamentos da moral e sua aplicação na defesa cibernética
- Tomada de decisão moral em situações de segurança cibernética
- Ética hacker e sua relação com a moral na defesa cibernética

Unidade 3: Direitos Humanos na Defesa Cibernética
- Visão geral dos direitos humanos na era digital
- Proteção dos direitos humanos em ambientes digitais
- Impacto dos direitos humanos na prática da defesa cibernética

Unidade 4: Aplicações éticas, morais e direitos humanos na prática da Defesa Cibernética
- Estudos de casos práticos de dilemas éticos na defesa cibernética
- Desenvolvimento de políticas éticas e morais em ambientes de segurança cibernética
- Implementação de direitos humanos na prática da defesa cibernética

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:
- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:
- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:
  - Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Situações de Reprovação:
  - Nota final inferior a 3,0.
  - Falta em mais de 25% das aulas.
  - Não entrega de mais de 25% das atividades avaliativas.

Observações:
- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e

serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

ASSUNÇÃO, Marcos Flávio Araújo. Segredos do hacker ético. São Paulo: Smartbook, 2019.

FERREIRA, Nicholas. O guia do hacker. São Paulo: Smartbook, 2018.

FRAGA, Bruno. Técnicas de invasão: aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Labrador, 2019.

BIBLIOGRAFIA COMPLEMENTAR

MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº13.709/18). Goiânia: RM Digital Education, 2019.

GROSSI, Bernardo Menicucci;...[et al.]. Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Editora Fi, 2020.

SOUSA, Nadya Rodrigues Gomes de. Guia rápido da LGPD. Brasília: ESMPU, 2021.

ANDRADE, Inacilma Rita Silva. Ética geral e profissional. Salvador: UFBA, 2017.

GUIMARÃES, Bruno Almeida. A ética desde Lacan: implicações filosóficas da crítica ao sujeito autoconsciente. Ouro Preto: UFOP, 2015

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Projeto Multidisciplinar Extensionista II
SÉRIE: 2º
CARGA TEÓRIA: 0
CARGA HORÁRIA PRÁTICA: 80
CARGA HORÁRIA TOTAL: 80
CBO ASSOCIADA: CBO 2123-15 - Administrador de sistemas operacionais
COD_DISCIPLINA: DC02.06

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Projeto Multidisciplinar Extensionista II do curso de Tecnologia em Defesa

Cibernética tem como objetivo proporcionar aos alunos a oportunidade de aplicar de forma prática os conhecimentos adquiridos ao longo do curso. A ementa abordará temas como análise de ameaças cibernéticas, implementação de estratégias de defesa, gestão de crises em segurança da informação, elaboração de projetos de segurança cibernética, além de promover a integração de conhecimentos das diversas disciplinas do curso. Através de atividades práticas e trabalhos de campo, os alunos terão a oportunidade de desenvolver habilidades de resolução de problemas reais e de trabalho em equipe, preparando-os para os desafios do mercado de trabalho na área de segurança cibernética.

IV. OBJETIVOS

1. Aprofundar o conhecimento técnico dos alunos em segurança cibernética, abordando temas como criptografia, detecção de ameaças e segurança de redes.
2. Promover a integração multidisciplinar dos conhecimentos adquiridos no curso, aplicando técnicas de defesa cibernética em cenários práticos e reais.
3. Desenvolver habilidades de análise e resolução de problemas em segurança cibernética, através de estudos de caso e simulações de ataques cibernéticos.
4. Fomentar o espírito empreendedor e inovador dos alunos, incentivando a criação de soluções e ferramentas de defesa cibernética para atender às demandas atuais do mercado.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Análise de vulnerabilidades cibernéticas
2. Implementação de medidas de segurança cibernética
3. Gerenciamento de projetos de segurança cibernética
4. Conformidade com regulamentos e padrões de segurança cibernética
5. Comunicação eficaz sobre questões de segurança cibernética

Habilidades:
1. Utilização de ferramentas de varredura de vulnerabilidades
2. Elaboração de relatórios técnicos sobre segurança cibernética

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Análise de Ameaças Cibernéticas e Inteligência de Segurança

- Fundamentos da Análise de Ameaças Cibernéticas
- Ferramentas e Técnicas de Inteligência de Segurança
- Estudos de Caso em Análise de Ameaças

Unidade 2: Estratégias de Defesa e Implementação de Segurança

- Design e Implementação de Arquiteturas de Defesa
- Desenvolvimento de Políticas de Segurança e Procedimentos Operacionais
- Laboratório de Implementação de Estratégias de Defesa

Unidade 3: Gestão de Crises em Segurança da Informação

Preparação e Resposta a Incidentes de Segurança
Comunicação e Gestão de Stakeholders durante Crises
Simulações de Gestão de Crises

Unidade 4: Projeto Integrador em Segurança Cibernética

Integração de Conhecimentos e Desenvolvimento de Projeto
Trabalho em Equipe e Liderança
Apresentação de Projetos

VII. INTEGRAÇÃO ENTRE AS DISCIPLINAS

A integração entre as disciplinas do segundo semestre do curso de Defesa Cibernética e o projeto multidisciplinar "Laboratório Virtual de Treinamento em Segurança Cibernética" é um exemplo claro de como a abordagem prática e a aplicação de conhecimentos teóricos podem ser efetivamente realizadas. Cada disciplina contribui para o desenvolvimento e a realização deste projeto:

1. Gerenciamento de Projetos para Segurança Cibernética
   - Integração: Essa disciplina fornece as ferramentas e metodologias necessárias para o planejamento, execução e gerenciamento do projeto. Os alunos aplicam práticas de gerenciamento de projetos para definir escopo, cronograma, recursos e riscos, garantindo que o laboratório virtual seja desenvolvido de forma eficiente e eficaz.
   - Aplicação prática: A utilização de metodologias ágeis ou tradicionais adaptadas ao contexto de TI ajuda a equipe do projeto a responder rapidamente às mudanças e a priorizar tarefas críticas para a segurança.

2. Administração Segura de Sistema Linux e Administração Segura de Sistema Windows
   - Integração: Estas disciplinas oferecem conhecimentos essenciais sobre a configuração segura e administração dos sistemas operacionais Linux e Windows, respectivamente. Os alunos aplicam esses conhecimentos ao configurar o ambiente do laboratório virtual, garantindo que ele seja robusto contra ataques cibernéticos e simule com precisão os ambientes reais.
   - Aplicação prática: A implementação de políticas de segurança, gerenciamento de usuários, e configurações seguras em ambos os sistemas operacionais são fundamentais para o projeto, proporcionando uma base segura para a simulação de ameaças e práticas defensivas.

3. Arquitetura de Segurança de Sistemas para Segurança Cibernética
   - Integração: Esta disciplina contribui com princípios de design seguro e arquitetura de sistemas focados em minimizar a superfície de ataque. Os conhecimentos adquiridos são aplicados na estruturação do laboratório virtual, desde a modelagem de ameaças até a implementação de mecanismos de segurança que protejam o ambiente virtual.
   - Aplicação prática: O entendimento de como construir sistemas com arquitetura segura é diretamente aplicado no desenvolvimento do laboratório, garantindo que os cenários de treinamento sejam não apenas educativos, mas também seguros.

4. Ética, Moral e Direitos Humanos em Tecnologia da Informação
   - Integração: Esta disciplina aborda a importância da conduta ética e da responsabilidade social na área de TI. No contexto do projeto, estimula-se a reflexão sobre o impacto das ações de segurança cibernética na sociedade, incluindo questões de privacidade, direitos humanos e o papel dos profissionais de TI como defensores éticos da informação.
   - Aplicação prática: A integração de cenários que envolvam dilemas éticos no laboratório virtual serve como uma ferramenta valiosa para ensinar aos alunos como navegar por questões complexas e tomar decisões responsáveis no mundo real da segurança cibernética.

Portanto, o projeto "Laboratório Virtual de Treinamento em Segurança Cibernética" serve como uma ponte entre a teoria e a prática, permitindo que os alunos apliquem conhecimentos interdisciplinares de forma sinérgica para resolver problemas complexos e prepará-los para os desafios do mundo real na área de segurança cibernética.

VIII. CONTRUIBUIÇÃO À COMUNIDADE

O projeto "Laboratório Virtual de Treinamento em Segurança Cibernética" contribui para a comunidade ao:

1. Educar: Oferece treinamento prático em segurança cibernética para estudantes e profissionais, aumentando o número de especialistas qualificados na área.
2. Conscientizar: Melhora a compreensão sobre a importância da segurança cibernética e promove práticas seguras entre indivíduos e organizações.
3. Apoiar PMEs: Fornece às pequenas e médias empresas ferramentas para treinar seus funcionários em segurança, ajudando a proteger seus negócios contra ataques cibernéticos sem custo elevado.
4. Incentivar Ética: Estimula discussões sobre ética e responsabilidade social na tecnologia, destacando a importância de proteger os direitos e a privacidade das pessoas.

XIX. AVALIAÇÃO

Este projeto visa desenvolver um ambiente virtual onde os alunos e profissionais possam simular ataques e defesas em sistemas operacionais tanto Linux quanto Windows, com o objetivo de aprender e aplicar práticas seguras de administração de sistemas, arquitetura de segurança e ética profissional em tecnologia da informação. Este laboratório virtual também servirá como uma ferramenta para treinamentos e conscientização sobre segurança cibernética, oferecendo cenários reais e atualizados de ameaças.

Estrutura de Avaliação:

1. Proposta de Projeto (15% da nota final)
   - **Descrição do projeto:** objetivos, relevância para a segurança cibernética, benefícios educacionais e comunitários.
   - **Revisão teórica:** práticas de segurança em sistemas operacionais, importância da

ética na tecnologia.
- **Critérios de avaliação:** clareza, relevância, aplicabilidade.

2. Planejamento e Gerenciamento (20% da nota final)
- **Estratégia de projeto:** uso de metodologias ágeis ou tradicionais adaptadas para o contexto.
- **Plano de execução:** fases, tarefas, responsabilidades, cronograma.
- **Critérios de avaliação:** viabilidade, organização, adaptabilidade.

3. Configuração e Segurança de Sistemas (20% da nota final)
- **Implementação de práticas seguras:** em sistemas Linux e Windows, documentação das configurações.
- **Simulação de ameaças e defesas:** cenários práticos no laboratório virtual.
- **Critérios de avaliação:** profundidade técnica, eficácia das práticas de segurança.

4. Arquitetura de Segurança (20% da nota final)
- **Design do laboratório:** considerações sobre arquitetura de segurança, minimização da superfície de ataque.
- **Modelagem de ameaças:** identificação e simulação no ambiente virtual.
- **Critérios de avaliação:** inovação, coerência com princípios de segurança.

5. Ética e Responsabilidade Social (15% da nota final)
- **Integração de questões éticas:** cenários que envolvam dilemas éticos e morais, discussão e reflexão.
- **Documentação sobre ética e direitos humanos:** aplicação prática no desenvolvimento e uso do laboratório.
- **Critérios de avaliação:** profundidade da discussão, aplicabilidade, consciência social.

6. Apresentação Final e Documentação (10% da nota final)
- **Demonstração do laboratório:** usabilidade, funcionalidades, cenários de teste.
- **Documentação completa:** guias de configuração segura, uso do laboratório, considerações éticas.
- **Critérios de avaliação:** clareza, completude, profissionalismo.

Nota Final:
A nota final será composta pela soma ponderada das notas de cada entrega, com a aprovação sendo alcançada por uma nota mínima de 7,0. Este sistema de avaliação não só incentiva a integração e aplicação dos conhecimentos adquiridos nas disciplinas, como também promove o desenvolvimento de competências relevantes para a carreira em segurança cibernética. Feedbacks construtivos serão fornecidos em cada etapa para orientar a melhoria contínua do projeto.

X BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA
Todas as bibliografias básicas estudadas até o momento

BIBLIOGRAFIA COMPLEMENTAR
Todas as bibliografias complementares estudadas até o momento

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Inteligência de Ameaças Cibernéticas
SÉRIE: 3º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2124-10 - Analista de redes e de comunicação de dados
COD_DISCIPLINA: DC03.01

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Inteligência de Ameaças Cibernéticas no curso de Tecnologia em Defesa Cibernética aborda as estratégias, técnicas e ferramentas utilizadas para identificar, analisar e prevenir ameaças cibernéticas. O conteúdo programático inclui estudos de casos reais, análise de tendências de ataques, métodos de coleta e análise de informações, utilização de ferramentas de inteligência cibernética e elaboração de relatórios de ameaças. Os alunos irão desenvolver habilidades para detectar padrões e comportamentos suspeitos, compreender a dinâmica do cibercrime e contribuir para a proteção de infraestruturas e sistemas de informação. A disciplina também aborda aspectos éticos e legais relacionados à coleta e uso de dados, visando formar profissionais capacitados para atuar na defesa cibernética de organizações públicas e privadas.

IV. OBJETIVOS

1. Compreender as principais ameaças cibernéticas e as técnicas de ataque mais utilizadas, a fim de identificar e prevenir possíveis vulnerabilidades nos sistemas de defesa cibernética.
2. Desenvolver habilidades de análise de dados e investigação forense digital para detectar e responder a incidentes de segurança cibernética de forma eficaz.
3. Aprender a utilizar ferramentas e técnicas avançadas de segurança cibernética para proteger redes, sistemas e dados sensíveis contra ataques cibernéticos.
4. Dominar a aplicação de políticas e procedimentos de segurança cibernética para garantir a conformidade com regulamentações e padrões de segurança.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Identificar e analisar ameaças cibernéticas.
2. Compreender as características e mecanismos de ataques cibernéticos.
3. Desenvolver estratégias de defesa cibernética.
4. Implementar medidas preventivas e proativas para proteção de sistemas e redes.
5. Avaliar e gerenciar riscos de segurança cibernética.
Habilidades:
1. Análise de dados para identificação de ameaças cibernéticas.
2. Implementação de ferramentas e técnicas de segurança cibernética.

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Introdução à Defesa Cibernética
- Conceitos básicos de segurança cibernética
- História e evolução das ameaças cibernéticas
- Principais desafios e ameaças atuais na área de segurança cibernética

Unidade de Aprendizagem 2: Técnicas de Proteção e Prevenção
- Criptografia e técnicas de encriptação
- Firewall e sistemas de detecção de intrusão
- Políticas de segurança e boas práticas de proteção cibernética

Unidade de Aprendizagem 3: Análise e Investigação de Ameaças
- Identificação de ameaças cibernéticas
- Análise forense digital
- Técnicas de investigação de incidentes de segurança cibernética

Unidade de Aprendizagem 4: Estratégias de Defesa Cibernética
- Estratégias de resiliência cibernética
- Planejamento e gestão de crises cibernéticas
- Aplicação de políticas de segurança em ambientes cibernéticos complexos

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.

- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

BARROS, Otávio Santana Rêgo;...[et al.]. Desafios estratégicos para segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2019.

WENDT, Emerson. Inteligência cibernética: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil. São Paulo: Editora Delfos, 2018.

OLIVEIRA, Marcos Aurélio Guedes de;...[et al]. Guia de defesa cibernética na América do Sul. Recife: UFPE, 2017.

BIBLIOGRAFIA COMPLEMENTAR

MASCARENHAS NETO, Pedro Tenório;...[et al.]. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: UFPB, 2019.

BARBOSA, Alexandre;...[et al.]. Segurança digital : uma análise da gestão de riscos em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

FERNANDES, Nélia O. Campo. Segurança da Informação. Cuiabá: UFMT, 2013.

COSTA, Celso;...[et al.]. Introdução à criptografia. v. 1. Rio de Janeiro: UFF, 2010.

FIGUEIREDO, Luiz Manoel. Introdução à Criptografia. v. 2. Rio de Janeiro: UFF, 2010.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Tratamento e Resposta a Incidentes
SÉRIE: 3º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30

CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2124-10 - Analista de redes e de comunicação de dados
COD_DISCIPLINA: DC03.02

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Tratamento e Resposta a Incidentes no curso de Tecnologia em Defesa Cibernética abordará os principais conceitos e técnicas para identificação, análise e resposta a incidentes de segurança da informação. Serão discutidas as melhores práticas em planejamento e estratégias de resposta, incluindo a preparação de planos de contingência e a coordenação de equipes multidisciplinares. Além disso, serão abordadas as ferramentas e tecnologias utilizadas para investigar e mitigar incidentes, bem como a legislação e regulamentação relacionadas à segurança cibernética. Ao final da disciplina, os alunos estarão aptos a atuar de forma eficaz na prevenção e na resposta a incidentes de segurança, contribuindo para a proteção e a defesa de sistemas e redes cibernéticas.

IV. OBJETIVOS

1. Capacitar os alunos para identificar e analisar incidentes de segurança cibernética, visando a resposta eficiente e eficaz.
2. Desenvolver habilidades para atuar na prevenção, detecção e correção de vulnerabilidades e ameaças cibernéticas.
3. Promover o entendimento e a aplicação de frameworks e melhores práticas de resposta a incidentes cibernéticos, alinhados com as normas e regulamentações vigentes.
4. Estimular a colaboração e o trabalho em equipe para lidar com incidentes cibernéticos complexos, garantindo a continuidade das operações e a proteção dos ativos digitais.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Identificar e analisar incidentes de segurança cibernética.
2. Responder de forma eficaz a incidentes de segurança cibernética.
3. Gerenciar e mitigar os efeitos de incidentes cibernéticos.
4. Compreender e aplicar boas práticas de resposta a incidentes.
5. Colaborar e coordenar com equipes de segurança cibernética para tratar incidentes.

Habilidades:
1. Análise forense digital para investigação de incidentes.
2. Comunicação eficaz em situações de crise cibernética.

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Introdução à Defesa Cibernética
- Fundamentos de segurança cibernética
- Conceitos básicos de incidentes de segurança
- Normas e regulamentações de segurança cibernética

Unidade de Aprendizagem 2: Identificação e Classificação de Incidentes

- Métodos de identificação de incidentes de segurança
- Classificação de incidentes por gravidade e impacto
- Análise de tendências de incidentes

Unidade de Aprendizagem 3: Resposta a Incidentes

- Processos de resposta a incidentes
- Estratégias de mitigação de riscos
- Desenvolvimento de planos de contingência

Unidade de Aprendizagem 4: Gerenciamento de Incidentes

- Monitoramento e controle de incidentes
- Análise pós-incidente e lições aprendidas
- Melhoria contínua em segurança cibernética

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0

Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA
BARROS, Otávio Santana Rêgo;...[et al.]. Desafios estratégicos para segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2019.

WENDT, Emerson. Inteligência cibernética: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil. São Paulo: Editora Delfos, 2018.

OLIVEIRA, Marcos Aurélio Guedes de;...[et al]. Guia de defesa cibernética na América do Sul. Recife: UFPE, 2017.

BIBLIOGRAFIA COMPLEMENTAR
MASCARENHAS NETO, Pedro Tenório;...[et al.]. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: UFPB, 2019.

BARBOSA, Alexandre;...[et al.]. Segurança digital : uma análise da gestão de riscos em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

FERNANDES, Nélia O. Campo. Segurança da Informação. Cuiabá: UFMT, 2013.

COSTA, Celso;...[et al.]. Introdução à criptografia. v. 1. Rio de Janeiro: UFF, 2010.

FIGUEIREDO, Luiz Manoel. Introdução à Criptografia. v. 2. Rio de Janeiro: UFF, 2010.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Introdução ao Hacking Ético
SÉRIE: 3º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2124-10 - Analista de redes e de comunicação de dados
COD_DISCIPLINA: DC03.03

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Introdução ao Hacking Ético tem como objetivo fornecer aos alunos do curso de Tecnologia em Defesa Cibernética um entendimento abrangente dos princípios e práticas do hacking ético, capacitando-os a identificar e explorar vulnerabilidades em sistemas computacionais de forma ética e legal. Durante o curso, os alunos irão aprender sobre as técnicas de hacking mais comuns, as ferramentas e metodologias utilizadas pelos hackers

éticos, bem como as medidas de segurança e prevenção de ataques cibernéticos. Além disso, serão abordados temas como engenharia social, forense digital, políticas de segurança e conformidade, preparando os alunos para atuarem de forma proativa na proteção da informação e na defesa contra ameaças cibernéticas. Ao final do curso, espera-se que os alunos estejam aptos a aplicar seus conhecimentos na prática, contribuindo para a segurança e integridade de sistemas e redes computacionais.

IV. OBJETIVOS

1. Compreender os princípios e conceitos fundamentais do hacking ético, incluindo as técnicas e ferramentas utilizadas para identificar e corrigir vulnerabilidades em sistemas de informação.
2. Desenvolver habilidades práticas de hacking ético, através de simulações de ataques e exercícios de resolução de problemas em ambientes controlados.
3. Analisar e avaliar as ameaças à segurança cibernética, incluindo a identificação de vulnerabilidades, a análise de riscos e a elaboração de estratégias de defesa e mitigação.
4. Aplicar os conhecimentos adquiridos para desenvolver políticas e procedimentos de segurança cibernética, visando proteger efetivamente os ativos de informação das organizações contra ataques e invasões.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Identificação e análise de vulnerabilidades em sistemas de informação.
2. Aplicação de métodos de ataque e defesa cibernética.
3. Gestão de riscos em ambientes cibernéticos.
4. Implementação de medidas de segurança para prevenir ataques cibernéticos.
5. Conformidade com regulamentações e padrões de segurança cibernética.

Habilidades:
1. Análise crítica de sistemas de informação para identificação de vulnerabilidades.
2. Comunicação efetiva para relatar incidentes de segurança e propor soluções.

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Fundamentos de Defesa Cibernética
- Introdução aos conceitos básicos de defesa cibernética
- Princípios de segurança da informação
- Ética e legalidade no contexto da defesa cibernética

Unidade 2: Gerenciamento de Riscos e Ameaças Cibernéticas
- Identificação e avaliação de riscos cibernéticos
- Tipos de ameaças cibernéticas e como se proteger
- Estratégias de mitigação de riscos e ameaças

Unidade 3: Técnicas de Investigação e Análise Forense
- Uso de ferramentas para investigação forense
- Coleta e análise de evidências digitais
- Procedimentos legais e éticos na análise forense

Unidade 4: Práticas de Hacking Ético e Teste de Vulnerabilidades
- Conceitos de hacking ético e sua importância na defesa cibernética
- Teste de vulnerabilidades em sistemas e redes

- Estratégias para lidar com incidentes de segurança e resposta a incidentes

Espero que essas sugestões sejam úteis para sua disciplina de Tecnologia em Defesa Cibernética!

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0

Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

ASSUNÇÃO, Marcos Flávio Araújo. Segredos do hacker ético. São Paulo: Smartbook, 2019.

FERREIRA, Nicholas. O guia do hacker. São Paulo: Smartbook, 2018.

FRAGA, Bruno. Técnicas de invasão: aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Labrador, 2019.

BIBLIOGRAFIA COMPLEMENTAR

MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados

Pessoais (Lei nº13.709/18). Goiânia: RM Digital Education, 2019.

GROSSI, Bernardo Menicucci;...[et al.]. Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Editora Fi, 2020.

SOUSA, Nadya Rodrigues Gomes de. Guia rápido da LGPD. Brasília: ESMPU, 2021.

ANDRADE, Inacilma Rita Silva. Ética geral e profissional. Salvador: UFBA, 2017.

GUIMARÃES, Bruno Almeida. A ética desde Lacan: implicações filosóficas da crítica ao sujeito autoconsciente. Ouro Preto: UFOP, 2015.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Defesa de Rede
SÉRIE: 3º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2124-10 - Analista de redes e de comunicação de dados
COD_DISCIPLINA: DC03.04

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Defesa de Rede no curso de Tecnologia em Defesa Cibernética abordará os princípios e práticas de proteção e segurança de redes de computadores. Serão estudados os fundamentos da segurança da informação, incluindo criptografia, autenticação e controle de acesso. Além disso, serão exploradas técnicas de detecção e prevenção de ataques cibernéticos, como firewalls, IDS/IPS e controle de tráfego. Também serão discutidas estratégias de monitoramento e resposta a incidentes, com ênfase na análise forense digital. A disciplina incluirá estudos de casos e práticas de laboratório para a aplicação dos conceitos teóricos na proteção efetiva de redes.

IV. OBJETIVOS

1. Compreender os princípios da segurança cibernética e sua relevância na proteção de redes de computadores.
2. Desenvolver habilidades para identificar e mitigar possíveis vulnerabilidades em sistemas de rede.
3. Aplicar técnicas avançadas de defesa cibernética para proteger as informações e dados

confidenciais da empresa.
4. Estar apto a responder a incidentes cibernéticos e implementar procedimentos eficazes de recuperação de dados após um ataque.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Identificação de vulnerabilidades e ameaças em redes.
2. Implementação de medidas de proteção e prevenção de ataques cibernéticos.
3. Análise de dados e detecção de atividades suspeitas na rede.
4. Desenvolvimento de estratégias de defesa cibernética.
5. Resolução de incidentes de segurança cibernética.
Habilidades:
1. Proficiência em ferramentas de segurança cibernética.
2. Capacidade de trabalhar sob pressão e tomar decisões rápidas em situações de emergência.

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Introdução à Defesa Cibernética
- Conceitos básicos de segurança da informação
- Principais ameaças cibernéticas
- Importância da defesa cibernética para organizações e governos
Unidade 2: Estratégias de Defesa Cibernética
- Métodos de prevenção de ataques cibernéticos
- Análise de riscos e vulnerabilidades
- Políticas de segurança da informação
Unidade 3: Tecnologias de Defesa Cibernética
- Firewall, antivírus e outras ferramentas de segurança
- Criptografia e autenticação de dados
- Monitoramento e detecção de intrusos
Unidade 4: Aplicações Práticas em Defesa Cibernética
- Estudos de caso de ataques cibernéticos famosos
- Simulações de ataques e respostas
- Desenvolvimento de planos de contingência e recuperação após ataques cibernéticos

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:
- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:
- **Exame de Recuperação:**

- Prova escrita com questões sobre os conteúdos da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

MACEDO, Ricardo Tombesi;...[et al.]. Redes de computadores. Santa Maria: UFSM, 2018.

FERNANDEZ, Marcial Porto. Rede de computadores. Fortaleza: EdUECE, 2019.

LATZKE, Carlos Alberto;...[et al.]. Infraestrutura e redes de computadores. Indaial: Uniasselvi, 2019.

BIBLIOGRAFIA COMPLEMENTAR

AMARAL, Marcos Prado; ... [et al.]. Redes de computadores I. Belo Horizonte: CEFET-MG, 2013.

GUEDES, Jackes Ridan da Silva; ... [et al.]. Redes de computadores. Brasília : Escola Técnica de Brasília, 2014.

PINTO NETO, João Batista. Redes de Computadores. Cuiabá: UFMT, 2014.

SAMPAIO, Leobino Nascimento. Redes de computadores. Rio de Janeiro: UFRJ, 2018.

BAY, Edemilson;...[et al.]. Fundamentos de redes de computadores. Indaial: Uniasselvi, 2021.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética

DISCIPLINA: Planejamento e Política de Segurança Cibernética
SÉRIE: 3º
CARGA TEÓRICA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2124-10 - Analista de redes e de comunicação de dados
COD DISCIPLINA: DC03.05

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Planejamento e Política de Segurança Cibernética no curso de Tecnologia em Defesa Cibernética abordará os fundamentos e princípios da segurança cibernética, incluindo a análise de riscos e ameaças, a elaboração e implementação de políticas de segurança, a gestão de incidentes, a conformidade com regulamentações e normas, e a importância da educação e conscientização dos usuários. Serão discutidos também os aspectos éticos e legais relacionados à segurança cibernética, visando preparar os alunos para atuarem de forma ética e responsável na defesa dos sistemas de informação e na proteção de dados. A disciplina promoverá ainda a compreensão da interação entre o planejamento estratégico e a segurança cibernética, capacitando os alunos a desenvolverem políticas e procedimentos eficazes para garantir a integridade, confidencialidade e disponibilidade das informações em ambientes digitais.

IV. OBJETIVOS

1. Desenvolver habilidades práticas em planejamento e implementação de estratégias de segurança cibernética para proteger sistemas de informação e redes.
2. Capacitar os alunos para identificar e analisar ameaças cibernéticas, como malware, ataques de phishing e invasões de rede, e aplicar medidas preventivas e corretivas.
3. Promover a compreensão das leis, regulamentações e melhores práticas relacionadas à segurança cibernética, preparando os alunos para atuar em conformidade com os padrões internacionais de proteção de dados.
4. Estimular a colaboração e o trabalho em equipe na resolução de desafios e incidentes de segurança cibernética, preparando os alunos para atuar de forma eficiente em ambientes de defesa cibernética.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Conhecimento em estratégias de defesa cibernética
2. Capacidade de analisar e identificar possíveis vulnerabilidades em sistemas
3. Habilidade para desenvolver e implementar políticas de segurança cibernética
4. Competência em responder a incidentes de segurança cibernética
5. Conhecimento em legislação e regulamentação relacionada à segurança cibernética

Habilidades:
1. Habilidade para programação e desenvolvimento de ferramentas de defesa cibernética

2. Capacidade de comunicação e colaboração eficaz em equipes de segurança cibernética

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Fundamentos de Segurança Cibernética
- Introdução à segurança cibernética
- Princípios básicos de defesa cibernética
- Ameaças e ataques cibernéticos
- Conceitos de criptografia

Unidade 2: Tecnologias de Defesa Cibernética
- Firewall e antivírus
- Detecção e prevenção de intrusões
- Segurança em redes de computadores
- Forense digital

Unidade 3: Políticas e Estratégias de Segurança Cibernética
- Legislação e normas de segurança cibernética
- Gestão de riscos em segurança cibernética
- Planejamento estratégico de segurança cibernética
- Ética e responsabilidade em defesa cibernética

Unidade 4: Aplicações Práticas em Defesa Cibernética
- Análise de casos reais de ataques cibernéticos
- Simulações e exercícios de defesa cibernética
- Proteção de sistemas e dados sensíveis
- Gestão de incidentes em segurança cibernética

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.

- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

MOURA, Adriano de Andrade;...[et al.]. Guia de Framework de Privacidade e Segurança da Informação. Brasília: Ministério da Gestão e da Inovação, 2023.

BARROS, Otávio Santana Rêgo;...[et al.]. Desafios estratégicos para segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2019.

WENDT, Emerson. Inteligência cibernética: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil. São Paulo: Editora Delfos, 2018

BIBLIOGRAFIA COMPLEMENTAR

MASCARENHAS NETO, Pedro Tenório;...[et al.]. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: UFPB, 2019.

BARBOSA, Alexandre;...[et al.]. Segurança digital : uma análise da gestão de riscos em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

FERNANDES, Nélia O. Campo. Segurança da Informação. Cuiabá: UFMT, 2013.

COSTA, Celso;...[et al.]. Introdução à criptografia. v. 1. Rio de Janeiro: UFF, 2010.

FIGUEIREDO, Luiz Manoel. Introdução à Criptografia. v. 2. Rio de Janeiro: UFF, 2010

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Projeto Multidisciplinar Extensionista III
SÉRIE: 3º
CARGA TEÓRIA: 0
CARGA HORÁRIA PRÁTICA: 0
CARGA HORÁRIA TOTAL: 80
CBO ASSOCIADA: CBO 2124-10 - Analista de redes e de comunicação de dados

COD_DISCIPLINA: DC03.07

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina Projeto Multidisciplinar Extensionista III do curso de Tecnologia em Defesa Cibernética abordará a integração de conhecimentos adquiridos ao longo do curso para a resolução de desafios reais de segurança cibernética. Os alunos serão desafiados a aplicar técnicas de análise, prevenção e investigação de ameaças cibernéticas, utilizando ferramentas avançadas e estratégias de defesa para proteção de sistemas e redes. Além disso, serão incentivados a desenvolver soluções inovadoras e eficazes para mitigar riscos e enfrentar situações emergenciais no contexto da segurança cibernética. Ao final da disciplina, os estudantes estarão aptos a atuar de forma colaborativa, ética e proativa na identificação e resolução de problemas complexos relacionados à defesa cibernética, preparando-os para o mercado de trabalho e para a constante evolução do cenário de ameaças digitais.

IV. OBJETIVOS

1. Desenvolver habilidades práticas em defesa cibernética, incluindo detecção e resposta a ameaças cibernéticas.
2. Promover a compreensão e aplicação de estratégias de proteção de dados e sistemas de informação em ambientes cibernéticos.
3. Fomentar a colaboração e comunicação efetiva entre profissionais de defesa cibernética para enfrentar desafios e ameaças emergentes.
4. Capacitar os alunos a analisar e avaliar cenários de segurança cibernética, identificando vulnerabilidades e propondo soluções eficazes.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Análise de ameaças cibernéticas
2. Gerenciamento de riscos de segurança cibernética
3. Desenvolvimento de estratégias de defesa cibernética
4. Investigação forense digital
5. Implementação de políticas de segurança cibernética

Habilidades:
1. Conhecimento avançado em tecnologias de segurança cibernética
2. Capacidade de tomar decisões estratégicas em situações de segurança cibernética

VI. DESCRIÇÃO DO PROJETO

O objetivo é criar um SOC virtual que ofereça, de forma prática e acessível, serviços de monitoramento, detecção, análise e resposta a ameaças cibernéticas para organizações comunitárias que geralmente não têm recursos para manter suas próprias operações de segurança cibernética. Este projeto permitiria aos alunos aplicar conhecimentos teóricos e técnicos em um ambiente realista, preparando-os para enfrentar ameaças cibernéticas contemporâneas

VII. CONTRIBUIÇÃO À COMUNIDADE

O projeto funcionaria como uma ponte entre a academia e a comunidade, aplicando conhecimentos teóricos para resolver problemas reais. Isso não apenas proporcionaria aos alunos uma valiosa experiência prática, mas também contribuiria positivamente para a sociedade, reforçando a segurança cibernética em um nível comunitário. Além disso, ao trabalhar em conjunto com organizações locais, o projeto fomentaria uma cultura de segurança cibernética e colaboração entre diferentes setores da sociedade.

- Aumento da Segurança Cibernética para Organizações Comunitárias: O projeto ofereceria proteção vital contra ataques cibernéticos para pequenas organizações que desempenham funções críticas na comunidade mas que não possuem a infraestrutura de segurança necessária.
- Educação e Sensibilização: Além de fornecer serviços de segurança, o projeto atuaria como um centro de educação para a comunidade sobre a importância da segurança cibernética, promovendo melhores práticas e aumentando a conscientização sobre ameaças digitais.
- Desenvolvimento de Habilidades Locais: Ao envolver membros da comunidade no projeto, seja por meio de workshops, seminários ou treinamentos, haveria uma transferência de conhecimento, capacitando as pessoas localmente com habilidades básicas em segurança cibernética.

VIII. INTEGRAÇÃO DAS DISCIPLINAS

Para o projeto "Centro de Operações de Segurança (SOC) Virtual para Organizações Comunitárias" no terceiro semestre do curso de Defesa Cibernética, a relação entre as disciplinas e o projeto é detalhada da seguinte forma:

1. Inteligência de Ameaças Cibernéticas

- **Relação:** Os alunos aplicarão técnicas de coleta e análise de inteligência para identificar ameaças potenciais e emergentes. Isso é essencial para o funcionamento do SOC, permitindo antecipar e preparar defesas contra ataques cibernéticos.
- **Aplicação no Projeto:** Monitoramento contínuo de fontes abertas, fóruns na dark web e feeds de inteligência para atualizar o banco de dados de ameaças do SOC e informar estratégias de defesa.

2. Tratamento e Resposta a Incidentes

- **Relação:** Esta disciplina fornece conhecimento sobre como gerenciar e responder a incidentes de segurança, um componente crítico do SOC.
- **Aplicação no Projeto:** Desenvolvimento de planos de resposta a incidentes, realização de exercícios de simulação e implementação de processos para lidar com incidentes em tempo real para as organizações comunitárias.

3. Introdução ao Hacking Ético

- **Relação:** Ensina técnicas de teste de penetração para identificar vulnerabilidades em sistemas e redes.
- **Aplicação no Projeto:** Realização de avaliações de vulnerabilidade e testes de penetração nos sistemas das organizações comunitárias para identificar e corrigir falhas de segurança antes que sejam exploradas.

4. Defesa de Rede

- **Relação:** Aborda estratégias e tecnologias para proteger redes contra ataques

cibernéticos.

- **Aplicação no Projeto:** Implementação de soluções de defesa em camadas, incluindo firewalls, sistemas de detecção/prevenção de intrusões e outras tecnologias de segurança para fortalecer a infraestrutura de rede das organizações comunitárias.

5. Planejamento e Política de Segurança Cibernética

- **Relação:** Capacita os alunos a criar políticas de segurança e planos que alinham segurança cibernética com objetivos de negócios e regulamentações.
- **Aplicação no Projeto:** Desenvolvimento de políticas de segurança personalizadas para cada organização comunitária, garantindo que suas práticas de segurança estejam alinhadas com suas necessidades específicas e conformidade legal.

VII. AVALIAÇÃO

Para avaliar o projeto "Centro de Operações de Segurança (SOC) Virtual para Organizações Comunitárias", a estrutura de avaliação poderá ser dividida em entregas parciais focadas em diferentes aspectos do desenvolvimento do projeto. Cada entrega contribuirá para a nota final, com uma nota mínima de aprovação estabelecida em 7,0. A seguir, detalhamos as entregas e os critérios de avaliação para cada uma delas:

1. Planejamento e Desenho do Projeto (15% da nota final)

- **Descrição detalhada do SOC:** Objetivos, serviços a serem oferecidos, tecnologias utilizadas.
- **Plano de Implementação:** Estratégias, cronograma, definição de equipe e responsabilidades.
- **Critérios de Avaliação:** Clareza, viabilidade, detalhamento do planejamento.

2. Desenvolvimento de Inteligência de Ameaças (20% da nota final)

- **Metodologia de Coleta de Inteligência:** Fontes de dados, ferramentas de análise.
- **Aplicação de Inteligência:** Como a inteligência coletada é usada para melhorar a segurança das organizações comunitárias.
- **Critérios de Avaliação:** Relevância das informações coletadas, eficácia na aplicação da inteligência.

3. Implementação e Testes de Segurança (20% da nota final)

- **Configurações de Segurança:** Implementação de medidas de segurança baseadas nas disciplinas de defesa de rede e hacking ético.
- **Testes de Penetração:** Relatório de vulnerabilidades encontradas e corrigidas.
- **Critérios de Avaliação:** Abrangência das configurações de segurança, eficácia na identificação e correção de vulnerabilidades.

4. Resposta a Incidentes e Recuperação (20% da nota final)

- **Plano de Resposta a Incidentes:** Desenvolvimento, implementação e simulação de um plano de resposta a incidentes.
- **Estratégias de Recuperação:** Procedimentos para restaurar serviços e dados após um incidente de segurança.
- **Critérios de Avaliação:** Completude e realismo do plano de resposta, eficiência

nas estratégias de recuperação.

5. Políticas de Segurança e Conformidade (15% da nota final)

- **Desenvolvimento de Políticas:** Criação de políticas de segurança cibernética customizadas para organizações comunitárias.
- **Avaliação de Conformidade:** Verificação da aderência às normas regulatórias e melhores práticas.
- **Critérios de Avaliação:** Adequação e detalhamento das políticas, eficácia na promoção da conformidade.

6. Apresentação Final e Relatório (10% da nota final)

- **Demonstração do SOC:** Apresentação das funcionalidades, serviços oferecidos e tecnologias implementadas.
- **Relatório Final:** Documentação completa do projeto, incluindo análise de desempenho e lições aprendidas.
- **Critérios de Avaliação:** Clareza e profissionalismo da apresentação, completude e profundidade do relatório.

Cada entrega parcial será rigorosamente avaliada, e o feedback será fornecido para orientar melhorias contínuas. A nota final será calculada com base no desempenho acumulado em todas as entregas, com a exigência de atingir uma média mínima de 7,0 para aprovação no projeto. Esta abordagem incentiva o progresso constante e o engajamento dos alunos e garante que o projeto atenda a altos padrões de qualidade e relevância para a comunidade.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA
Todas as bibliografias básicas estudadas até o momento

BIBLIOGRAFIA COMPLEMENTAR
Todas as bibliografias complementares estudadas até o momento.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Segurança de Sistemas Operacionais
SÉRIE: 4º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123 - Administradores de tecnologia da informação
COD_DISCIPLINA: DC04.01

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Segurança de Sistemas Operacionais no curso de Tecnologia em Defesa Cibernética abordará os principais conceitos e práticas relacionadas à proteção e defesa de sistemas operacionais. Os alunos irão aprender sobre os diferentes tipos de ameaças cibernéticas que podem afetar os sistemas operacionais, incluindo vírus, malware, ataques de negação de serviço e engenharia social. Além disso, serão apresentadas técnicas de mitigação de riscos e controle de acesso, bem como a implementação de políticas de segurança para garantir a integridade, confidencialidade e disponibilidade dos sistemas operacionais. A disciplina também abordará aspectos relacionados à conformidade regulatória e ética em segurança de sistemas operacionais, preparando os alunos para atuar de forma responsável e ética no contexto da defesa cibernética.

IV. OBJETIVOS

1. Compreender os princípios de segurança de sistemas operacionais e sua aplicação na defesa cibernética.
2. Desenvolver habilidades para identificar vulnerabilidades em sistemas operacionais e implementar medidas de segurança eficazes.
3. Capacitar os alunos a projetar e implementar estratégias de proteção de sistemas operacionais contra ameaças cibernéticas.
4. Promover a conscientização sobre a importância da segurança de sistemas operacionais e seu papel na defesa cibernética.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Identificar e avaliar possíveis vulnerabilidades em sistemas operacionais.
2. Desenvolver estratégias de segurança para prevenir ataques cibernéticos em sistemas operacionais.
3. Utilizar ferramentas de monitoramento e detecção de ameaças em sistemas operacionais.
4. Implementar medidas de segurança proativas para proteger sistemas operacionais.
5. Avaliar e responder a incidentes de segurança em sistemas operacionais.

Habilidades:
1. Capacidade de análise e resolução de problemas relacionados à segurança de sistemas operacionais.
2. Comunicação eficaz para relatar e lidar com incidentes de segurança em sistemas operacionais.

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Introdução à Segurança de Sistemas Operacionais
- Conceitos fundamentais de segurança de sistemas operacionais
- Principais ameaças e vulnerabilidades
- Práticas de segurança para sistemas operacionais

Unidade 2: Gerenciamento de Acesso e Identidade
- Controle de acesso e autenticação

- Políticas de segurança de acesso
- Gestão de identidades e privilégios

Unidade 3: Proteção de Dados e Comunicações
- Criptografia e segurança de dados
- Segurança em redes de comunicação
- Proteção de informações sensíveis

Unidade 4: Monitoramento e Resposta a Incidentes
- Ferramentas de monitoramento e detecção de ameaças
- Resposta a incidentes e planos de contingência
- Contramedidas para neutralizar ameaças e ataques.

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:
  - Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Situações de Reprovação:
  - Nota final inferior a 3,0.
  - Falta em mais de 25% das aulas.
  - Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

NEGUS, Christopher. Linux – a Bíblia. São Paulo: Smartbooks, 2018.

MAZIERO, Carlos Alberto. Sistemas operacionais: conceitos e mecanismos. Curitiba: DINF - UFPR, 2019.

VALLE, Odilson Tadeu. Linux básico, gerência, segurança e monitoramento de redes. São José: IFSC, 2019.

BIBLIOGRAFIA COMPLEMENTAR

SILVA JÚNIOR, Edson Nascimento. Introdução ao Ambiente Linux. Manaus: UFAM, 2009.

PINTO NETO, João Batista. Sistemas operacionais. Cuiabá : UFMT, 2014.

PEREIRA, Adriana Soares. Sistemas operacionais. Frederico Westphalen: UFSM, 2015.

LINUX INSTITUTE. Linux Essentials. São Paulo: Linux Professional Institute, 2023.

ANDRADE, Alessandro Vivas;...[et al.]. Linux: comandos básicos e avançados. Diamantina: Ed. do autor, 2019.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Segurança em Nuvem e Virtualização
SÉRIE: 4º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123 - Administradores de tecnologia da informação
COD_DISCIPLINA: DC04.02

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Segurança em Nuvem e Virtualização no curso de Tecnologia em Defesa Cibernética abordará os princípios e práticas para proteção de dados e sistemas em ambientes virtuais e em nuvem. Serão estudados conceitos de virtualização, políticas de segurança, criptografia, monitoramento de ameaças, gestão de identidade, e ferramentas de segurança específicas para ambientes em nuvem. Os alunos aprenderão a configurar e gerenciar ambientes virtualizados de forma segura, identificar e mitigar riscos de segurança em nuvem, e aplicar técnicas avançadas de proteção para garantir a integridade, confidencialidade e disponibilidade das informações. Além disso, serão discutidos aspectos regulatórios e compliance relacionados à segurança em nuvem, preparando os estudantes para atuar de

forma ética e responsável na defesa cibernética em ambientes cada vez mais virtualizados e em nuvem.

IV. OBJETIVOS

1. Compreender os conceitos de segurança em nuvem e virtualização e sua aplicação na defesa cibernética.
2. Desenvolver habilidades para identificar e analisar ameaças e vulnerabilidades em ambientes de nuvem e virtualização.
3. Aprender a implementar estratégias de proteção e mitigação de riscos em ambientes de nuvem e virtualização.
4. Adquirir conhecimentos avançados sobre ferramentas e técnicas de defesa cibernética específicas para ambientes de nuvem e virtualização.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Compreensão dos princípios e práticas de segurança em nuvem.
2. Habilidade para identificar e avaliar ameaças cibernéticas em ambientes virtuais.
3. Capacidade de implementar medidas de segurança adequadas em ambientes de virtualização.
4. Conhecimento avançado em técnicas de criptografia e autenticação em nuvem.
5. Habilidade para desenvolver estratégias de defesa cibernética em ambientes de nuvem e virtualização.
Habilidades:
1. Pensamento crítico para analisar e resolver problemas de segurança em nuvem e virtualização.
2. Comunicação eficaz para apresentar e justificar decisões relacionadas à defesa cibernética em ambientes virtuais.

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Fundamentos de Segurança em Nuvem e Virtualização
- Conceitos básicos de segurança em nuvem
- Principais desafios de segurança em ambientes virtualizados
- Estratégias de proteção de dados em ambientes de nuvem

Unidade de Aprendizagem 2: Arquitetura e Implementação de Segurança em Nuvem
- Arquitetura de segurança para ambientes de nuvem
- Ferramentas e tecnologias para implementação de segurança em nuvem
- Políticas de segurança e conformidade em ambientes de nuvem

Unidade de Aprendizagem 3: Gestão de Riscos e Compliance em Ambientes Virtuais
- Avaliação de riscos e ameaças em ambientes virtualizados
- Frameworks de compliance para segurança em nuvem
- Estratégias de gestão de riscos em ambientes virtuais

Unidade de Aprendizagem 4: Práticas Avançadas de Defesa Cibernética em Ambientes Virtualizados
- Análise de incidentes de segurança em nuvem
- Implementação de estratégias avançadas de proteção e detecção
- Tendências e desafios futuros em defesa cibernética em ambientes virtualizados

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

OPUS. O que você realmente precisa saber sobre computação em nuvem. São Paulo: Opus Software, 2015.

VERAS, Manoel. Virtualização - Componente Central do Datacenter. Rio de Janeiro: Brasport, 2017.

VERAS, Manoel. Cloud computing: nova arquitetura da TI. Rio de Janeiro: Brasport, 2018.

BIBLIOGRAFIA COMPLEMENTAR

ZANCHETT, Pedro Sidnei. Engenharia e projeto de software. Indaial: Uniasselvi, 2015.

GUDWIN, Ricardo R. Engenharia de software: uma visão prática. Campinas: Unicamp, 2015.

ALÉSSIO; Simone Cristina; ... [et al.]. Processos de software. Indaial: Uniasselvi, 2017.

FRAGA, Marcelo Caramuru Pimentel; ... [et al.]. Sistemas operacionais II. Belo Horizonte: CEFET/MG, 2012.

CUNHA, Luiz Egidio Costa. Análise de sistemas. Colatina: CEAD / Ifes, 2011

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Defesa de Rede Avançada
SÉRIE: 4º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123 - Administradores de tecnologia da informação
COD_DISCIPLINA: DC04.03

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Defesa de Rede Avançada no curso de Tecnologia em Defesa Cibernética visa fornecer aos alunos os conhecimentos avançados necessários para proteger e fortalecer as redes de computadores contra ameaças cibernéticas. Através de estudos aprofundados sobre técnicas de criptografia, firewalls avançados, detecção e prevenção de intrusões, os alunos serão capazes de desenvolver estratégias eficazes para garantir a segurança e integridade das informações que trafegam pelas redes. Além disso, a disciplina abordará a importância da análise de tráfego e a gestão de incidentes, proporcionando aos estudantes a capacidade de identificar e responder rapidamente a possíveis ataques. Com uma abordagem prática e atualizada, os alunos serão preparados para atuar no mercado de defesa cibernética, contribuindo para a proteção das redes em um mundo digital cada vez mais ameaçador.

IV. OBJETIVOS

1. Desenvolver habilidades avançadas em identificação e resposta a ameaças cibernéticas.
2. Aprofundar o conhecimento em técnicas de defesa de rede, incluindo firewalls, detecção de intrusos e criptografia.
3. Capacitar os estudantes a implementar estratégias de defesa proativa para prevenir ataques cibernéticos.
4. Proporcionar experiência prática em simulações de ataques cibernéticos e exercícios de resposta a incidentes.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Análise avançada de ameaças cibernéticas
2. Implementação de estratégias de defesa de rede
3. Resposta rápida a incidentes de segurança
4. Conhecimento avançado em técnicas de criptografia
5. Gerenciamento eficiente de recursos de segurança cibernética

Habilidades:
1. Capacidade de identificar e analisar vulnerabilidades em redes avançadas
2. Dominar ferramentas de segurança cibernética para defesa de rede

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Fundamentos de Defesa Cibernética
- Introdução à segurança cibernética
- Conceitos de defesa de rede avançada
- Principais ameaças cibernéticas
- Estratégias de proteção de dados

Unidade de Aprendizagem 2: Ferramentas e Tecnologias de Defesa
- Firewall e sistemas de detecção de intrusos
- Criptografia e técnicas de proteção de dados
- Análise de vulnerabilidades e testes de segurança
- Gerenciamento de acessos e identidades

Unidade de Aprendizagem 3: Resposta a Incidentes Cibernéticos
- Procedimentos de resposta a incidentes
- Identificação e análise de ataques cibernéticos
- Recuperação de sistemas e dados
- Legislação e ética em segurança cibernética

Unidade de Aprendizagem 4: Estratégias Avançadas de Defesa
- Pensamento estratégico em segurança cibernética
- Gestão de riscos e conformidade regulatória
- Tendências e inovações em defesa cibernética
- Simulações e exercícios práticos de defesa de rede avançada

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:
  - Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Situações de Reprovação:
  - Nota final inferior a 3,0.
  - Falta em mais de 25% das aulas.
  - Não entrega de mais de 25% das atividades avaliativas.

Observações:
- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

OPUS. O que você realmente precisa saber sobre computação em nuvem. São Paulo: Opus Software, 2015.

VERAS, Manoel. Virtualização - Componente Central do Datacenter. Rio de Janeiro: Brasport, 2017.

VERAS, Manoel. Cloud computing: nova arquitetura da TI. Rio de Janeiro: Brasport, 2018

BIBLIOGRAFIA COMPLEMENTAR

ZANCHETT, Pedro Sidnei. Engenharia e projeto de software. Indaial: Uniasselvi, 2015.

GUDWIN, Ricardo R. Engenharia de software: uma visão prática. Campinas: Unicamp, 2015.

ALÉSSIO; Simone Cristina; ... [et al.]. Processos de software. Indaial: Uniasselvi, 2017.
FRAGA, Marcelo Caramuru Pimentel; ... [et al.]. Sistemas operacionais II. Belo Horizonte: CEFET/MG, 2012.

CUNHA, Luiz Egidio Costa. Análise de sistemas. Colatina: CEAD / Ifes, 2011.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética

DISCIPLINA: Digital Forense em Defesa Cibernética
SÉRIE: 4º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123 - Administradores de tecnologia da informação
COD_DISCIPLINA: DC04.04

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

O curso de Tecnologia em Defesa Cibernética abordará a disciplina de Digital Forense, que tem como objetivo capacitar os alunos para atuarem na investigação de crimes cibernéticos e na coleta de evidências digitais. Serão abordados temas como análise de dispositivos de armazenamento, recuperação de dados, técnicas de identificação e preservação de evidências, utilização de ferramentas forenses, procedimentos legais e éticos, além de estudos de casos reais. A disciplina também enfatizará a importância da conformidade com leis e regulamentações relacionadas à privacidade e proteção de dados, preparando os alunos para atuarem de forma ética e responsável no campo da defesa cibernética.

IV. OBJETIVOS

1. Desenvolver habilidades de análise forense digital para identificar e investigar possíveis incidentes de segurança cibernética.
2. Capacitar os alunos a utilizar ferramentas e técnicas avançadas de defesa cibernética para proteger organizações e sistemas de ataques virtuais.
3. Promover o entendimento das leis e regulamentações relacionadas à segurança cibernética, para garantir a conformidade e a responsabilidade legal no ambiente digital.
4. Fomentar a colaboração e o trabalho em equipe na resolução de problemas de segurança cibernética, visando a proteção efetiva de dados e informações sensíveis.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Análise forense digital
2. Investigação de crimes cibernéticos
3. Proteção e defesa de sistemas e redes
4. Perícia digital
5. Análise de evidências digitais

Habilidades:
1. Utilização de ferramentas forenses digitais
2. Compreensão das técnicas de ataque e defesa cibernética

VI. CONTEÚDO PROGRAMÁTICO

1. Introdução à Tecnologia em Defesa Cibernética
- Conceitos básicos de cibersegurança

- História e evolução da defesa cibernética
- Legislação e ética em segurança da informação

2. Fundamentos de Segurança da Informação
- Princípios de criptografia
- Protocolos de segurança
- Identificação e autenticação de usuários

3. Gerenciamento de Riscos e Incidentes Cibernéticos
- Análise de riscos em ambientes digitais
- Ferramentas e técnicas para detecção de ameaças e ataques cibernéticos
- Estratégias de resposta a incidentes

4. Proteção em Ambientes Digitais
- Segurança em redes e sistemas operacionais
- Segurança em dispositivos móveis e computação em nuvem
- Políticas e práticas de segurança em organizações digitais

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

NASCIMENTO, Claudio Joel Brito Lóssio Luciano;...[et al.]. Cibernética jurídica: estudo sobre o direito digital. Campina Grande: EDUEPB, 2020.

MOZETIC, Vinícius Almada. Direito e Novas tecnologias: Perspectivas na Sociedade da Informação e Cibercultura. Joaçaba: Editora Unoesc, 2017.

BRASIL, Ministério Público do Distrito Federal e Territórios – MPDFT. Fundamentos do Direito Digital para Atuação Judicial e Extrajudicial. Brasília, MPDFT: 2015

BIBLIOGRAFIA COMPLEMENTAR

OPICE BLUM, Renato M.S.; Coletânea Direito Digital. São Paulo: LCT, 2017.

ALMEIDA, Daniel Evangelista Vasconcelos. Shadow profiles e a Privacidade na Internet: a coleta de dados pessoais de usuários e não usuários das redes sociais. Porto Alegre, RS: Editora Fi, 2019.

SOUSA, Rosilene Paiva Marinho de. A informação e a proteção da propriedade intelectual. João Pessoa: Editora da UFPB, 2017.

LEMOS. Ronaldo. Direito, Tecnologia e Cultura. Rio de Janeiro: FGV, 2015.

SARLET, Gabrielle Bezerra Sales;...[et al.]. Inteligência artificial e direito. Porto Alegre : Editora Fundação Fênix, 2023

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Educação para relações Étnico-Raciais e Sociodiversidade
SÉRIE: 4º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123 - Administradores de tecnologia da informação
COD_DISCIPLINA: DC04.06

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Educação para relações Étnico-Raciais e Sociodiversidade tem como objetivo fornecer aos alunos do curso de Tecnologia em Defesa Cibernética uma compreensão aprofundada das questões étnico-raciais e da diversidade sociocultural, com foco na atuação

profissional responsável e inclusiva. Serão abordados temas como as relações étnico-raciais no Brasil, a construção social da identidade e as políticas de inclusão e igualdade. Além disso, serão discutidos os desafios e oportunidades inerentes à diversidade cultural e étnica no contexto da defesa cibernética, preparando os estudantes para atuar de forma ética e sensível às diferenças em sua futura carreira. Ao final do curso, os alunos estarão aptos a reconhecer e lidar com as questões étnico-raciais e socioculturais de forma consciente e comprometida, contribuindo para a construção de um ambiente profissional mais inclusivo e justo.

IV. OBJETIVOS

1. Compreender a relação entre a educação para relações étnico-raciais e a diversidade sociocultural, a fim de promover um ambiente inclusivo e equitativo na defesa cibernética.
2. Reconhecer a importância da diversidade étnico-racial e sociocultural na formação de equipes de defesa cibernética, buscando promover a integração e o respeito mútuo entre os membros.
3. Desenvolver habilidades para identificar potenciais desafios e ameaças cibernéticas que possam afetar grupos étnico-raciais e minorias, visando garantir a segurança digital de todos os cidadãos.
4. Promover a conscientização sobre a importância da diversidade e inclusão na área de defesa cibernética, incentivando a criação de estratégias e políticas que reflitam a realidade sociocultural e étnico-racial da sociedade.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Compreensão das relações étnico-raciais e sociodiversidade no contexto da segurança cibernética.
2. Capacidade de identificar e combater discriminação e preconceito no ambiente cibernético.
3. Conhecimento sobre as políticas e legislação relacionadas à segurança cibernética e diversidade.
4. Habilidade de promover um ambiente inclusivo e diversificado dentro de equipes de defesa cibernética.
5. Capacidade de analisar e propor soluções para desafios relacionados à diversidade e segurança cibernética.
Habilidades:
1. Comunicação eficaz e sensível em relação a questões étnico-raciais e de diversidade.
2. Utilização de tecnologias e estratégias específicas para defesa cibernética que considerem a diversidade e inclusão.

VI. CONTEÚDO PROGRAMÁTICO

1. Unidade 1: Introdução à diversidade étnico-racial e sociodiversidade
- Conceitos e definições de diversidade étnico-racial e sociodiversidade
- Importância da inclusão e representatividade na área de defesa cibernética
- Desafios e oportunidades da diversidade na área de tecnologia
2. Unidade 2: Impacto da diversidade na segurança cibernética
- Análise do impacto de preconceitos e discriminação na segurança cibernética
- Estudos de casos de ataques cibernéticos motivados por questões étnico-raciais
- Melhores práticas para promover a diversidade e minimizar vulnerabilidades na segurança

cibernética
3. Unidade 3: Políticas e práticas inclusivas em defesa cibernética
- Legislações e políticas relacionadas à diversidade e inclusão na área de tecnologia
- Estratégias para promover a diversidade e inclusão no ambiente de trabalho em defesa cibernética
- Desenvolvimento de programas e iniciativas para a promoção da diversidade e inclusão na área de segurança cibernética
4. Unidade 4: Desafios e oportunidades para profissionais diversos em defesa cibernética
- Discussão sobre barreiras e dificuldades enfrentadas por profissionais diversos na área de defesa cibernética
- Políticas de recrutamento e retenção de talentos diversos na área de tecnologia
- Oportunidades de carreira e impacto positivo da diversidade na inovação em segurança cibernética

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

NEGREIROS, Dalila Fernandes de Educação das relações étnico-raciais: avaliação da formação de docentes. São Bernardo do Campo, SP : EdUFABC, 2017.

BAEZ, Narciso Leandro Xavier. Teorias da justiça e direitos indígenas. Joaçaba: Editora Unoesc, 2017.

REIS, Cristiane de Souza. Políticas públicas e grupos em situação de vulnerabilidade: volume único. Rio de Janeiro: Fundação Cecierj, 2019

BIBLIOGRAFIA COMPLEMENTAR

AGUIAR, Rodrigo Luiz Simas de. Antropologia sociocultural. Dourados, MS: Ed. UFGD, 2015.

LIMONCIC, Flávio; GRIN, Mônica. História e sociologia. Rio de Janeiro: Fundação CECIERJ, 2010. V. 1.

QUEIROZ, Pedro Fernandes de; ... [et al.]. Antropologia Geral. Sobral: Inta, 2016.

DUTRA, Cristiane Feldmann; PEREIRA, Gustavo de Lima... [et al.]. Direitos Humanos e Migrações Forçadas: migrações, xenofobia e transnacionalidade. Porto Alegre, RS: Editora Fi, 2020.

ALVES, Verena Holanda de Mendonça; NEVES, Rafaela Teixeira Sena; RESQUE, João Daniel Daibes... [et al.]. Direitos Humanos e(m) tempos de crise. Porto Alegre, RS: Editora Fi, 2019.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Projeto Multidisciplinar Extensionista IV
SÉRIE: 4º
CARGA TEÓRIA: 0
CARGA HORÁRIA PRÁTICA: 80
CARGA HORÁRIA TOTAL: 80
CBO ASSOCIADA: CBO 2123 - Administradores de tecnologia da informação
COD_DISCIPLINA: DC04.05

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Projeto Multidisciplinar Extensionista IV para o curso de Tecnologia em

Defesa Cibernética tem como objetivo proporcionar aos alunos a oportunidade de aplicar os conhecimentos adquiridos ao longo do curso de forma prática e interdisciplinar. A ementa abordará temas como segurança da informação, análise de vulnerabilidades, estratégias de defesa cibernética, gestão de incidentes, ética e legislação, promovendo uma visão integrada das diversas áreas de atuação do profissional de defesa cibernética. Além disso, os alunos terão a oportunidade de desenvolver projetos de extensão, aplicando seus conhecimentos em situações reais e contribuindo para a comunidade acadêmica e/ou sociedade em geral. A disciplina também contemplará a apresentação e defesa dos projetos desenvolvidos, fomentando o desenvolvimento de habilidades de comunicação e trabalho em equipe.

IV. OBJETIVOS

1. Desenvolver habilidades práticas em segurança cibernética, incluindo a identificação e correção de vulnerabilidades em sistemas e redes.
2. Promover o entendimento das ameaças cibernéticas atuais e emergentes, e as estratégias para mitigá-las.
3. Capacitar os alunos a aplicar técnicas avançadas de defesa cibernética em ambientes reais, como simulações de ataques e defesa.
4. Fomentar a consciência ética e responsabilidade social na atuação profissional em defesa cibernética, enfatizando a importância da privacidade e conformidade com regulamentações.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Análise de segurança cibernética
2. Avaliação de riscos em ambientes digitais
3. Implementação de medidas de proteção cibernética
4. Investigação de incidentes de segurança
5. Desenvolvimento de estratégias para prevenção de ataques cibernéticos

Habilidades:
1. Conhecimento avançado em sistemas de segurança cibernética
2. Capacidade de análise crítica e resolução de problemas em ambientes cibernéticos

VI. DESCRIÇÃO DO PROJETO

O projeto consistiria na criação de uma plataforma educacional online acessível, destinada a oferecer recursos de treinamento, workshops e ferramentas práticas para melhorar a conscientização sobre segurança cibernética em comunidades diversificadas. A plataforma abordaria temas como segurança de sistemas operacionais, segurança em ambientes de nuvem e virtualização, defesa de rede avançada, e introdução à forense digital. Além disso, incorporaria conteúdos que enfatizam a importância das relações étnico-raciais e da sociodiversidade, promovendo um espaço inclusivo de aprendizado.

VII. INTEGRAÇÃO ENTRE AS DISCIPLINAS

- **Segurança de Sistemas Operacionais:** Criação de módulos educacionais que ensinam técnicas para proteger sistemas operacionais contra ameaças cibernéticas, utilizando exemplos práticos e acessíveis para um público amplo.
- **Segurança em Nuvem e Virtualização:** Desenvolvimento de conteúdo focado em estratégias de segurança para ambientes de nuvem, visando pequenas organizações e

usuários individuais, destacando a importância da proteção de dados e gerenciamento de acesso.

- **Defesa de Rede Avançada:** Oferecimento de workshops interativos online sobre como implementar técnicas avançadas de defesa de rede para detectar e mitigar ataques cibernéticos.
- **Digital Forense em Defesa Cibernética:** Inclusão de cursos que introduzem conceitos básicos de forense digital, ensinando a comunidade a entender e reagir a incidentes de segurança de forma informada.
- **Educação para relações Étnico-Raciais e Sociodiversidade:** Incorporação de materiais que promovem a diversidade e inclusão no setor de tecnologia, visando criar um ambiente mais acolhedor e equitativo

VIII. CONTRIBUIÇÃO À COMUNIDADE

- **Educação e Capacitação:** Aumento da conscientização e compreensão sobre segurança cibernética nas comunidades, capacitando indivíduos com conhecimentos para proteger suas informações e dispositivos.
- **Inclusão e Diversidade:** Promoção da inclusão digital e do respeito pela diversidade, criando um espaço seguro para aprendizado e discussão sobre temas tecnológicos e sociais.
- **Empoderamento de Comunidades Vulneráveis:** Oferecimento de recursos educacionais que empoderam comunidades historicamente marginalizadas, promovendo a igualdade de acesso a informações críticas de segurança cibernética.

VII. AVALIAÇÃO

Para avaliar o projeto "Plataforma de Conscientização e Resiliência Cibernética para Comunidades Diversificadas", o sistema de avaliação é baseado em entregas parciais, focando em diferentes aspectos do desenvolvimento do projeto. A nota final será calculada com base no desempenho em cada entrega, sendo a nota mínima para aprovação de 7,0.

1. Planejamento do Projeto e Pesquisa Inicial (15% da nota final)

- **Entrega:** Um documento detalhando o plano do projeto, incluindo objetivos, público-alvo, metodologia de pesquisa para conteúdo e estratégias de inclusão e diversidade.
- **Critérios de Avaliação:** Clareza dos objetivos, relevância da pesquisa, abrangência da estratégia de inclusão.

2. Desenvolvimento de Conteúdo Educativo (20% da nota final)

- **Entrega:** Módulos de aprendizado sobre segurança de sistemas operacionais, segurança em nuvem, defesa de rede e forense digital, além de conteúdo sobre ética e diversidade.
- **Critérios de Avaliação:** Qualidade educativa, precisão técnica, acessibilidade do conteúdo, integração de perspectivas de diversidade.

3. Implementação da Plataforma (20% da nota final)

- **Entrega:** Protótipo funcional da plataforma online, incluindo interface do usuário,

acessibilidade e funcionalidades básicas para a interação com o conteúdo educativo.
- **Critérios de Avaliação:** Funcionalidade, usabilidade, design inclusivo.

4. Estratégias de Engajamento e Marketing (15% da nota final)
- **Entrega:** Plano de engajamento da comunidade, incluindo estratégias de marketing digital para promover a plataforma e atrair o público-alvo.
- **Critérios de Avaliação:** Criatividade das estratégias, potencial de engajamento, inclusão de táticas para alcançar comunidades diversas.

5. Feedback e Melhorias (10% da nota final)
- **Entrega:** Coleta de feedback de usuários beta, análise dos comentários recebidos e implementação de melhorias na plataforma.
- **Critérios de Avaliação:** Efetividade na coleta de feedback, qualidade das melhorias realizadas, responsividade às necessidades dos usuários.

6. Apresentação Final e Relatório de Projeto (20% da nota final)
- **Entrega:** Apresentação da versão final da plataforma, incluindo uma demonstração das funcionalidades e um relatório detalhado do projeto, cobrindo desde a pesquisa inicial até as etapas de implementação e feedback.
- **Critérios de Avaliação:** Clareza e profissionalismo da apresentação, completude e profundidade do relatório, demonstração do impacto potencial na comunidade.

Cada entrega parcial será rigorosamente avaliada, e feedback detalhado será fornecido para possibilitar a melhoria contínua do projeto. A nota final será a soma ponderada das notas obtidas em cada entrega, exigindo-se uma média mínima de 7,0 para aprovação. Esta estrutura de avaliação visa não apenas medir o desempenho técnico e educativo do projeto, mas também seu impacto social e capacidade de promover inclusão e diversidade

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA
Todas as bibliografias básicas estudadas até o momento

BIBLIOGRAFIA COMPLEMENTAR
Todas as bibliografias complementares estudadas até o momento

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Gerenciamento Avançado de Redes e Sistemas
SÉRIE: 5º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60

CBO ASSOCIADA: CBO 2123-20 Especialista em segurança da informação
COD_DISCIPLINA: DC04.01

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Gerenciamento Avançado de Redes e Sistemas para o curso de Tecnologia em Defesa Cibernética abordará tópicos avançados relacionados à administração e monitoramento de redes e sistemas, com foco na segurança cibernética. Os alunos irão estudar métodos avançados de gerenciamento de redes, incluindo configuração, manutenção e otimização de sistemas, bem como estratégias de prevenção e detecção de ameaças cibernéticas. Também serão abordados temas como virtualização, nuvem computacional, ferramentas de monitoramento e análise de desempenho, visando fornecer aos estudantes as habilidades necessárias para atuar na proteção e defesa de sistemas de informação em ambientes cibernéticos complexos.

IV. OBJETIVOS

1. Capacitar os estudantes para reconhecer e analisar possíveis ameaças cibernéticas em redes e sistemas avançados.
2. Desenvolver habilidades avançadas de gerenciamento de redes e sistemas, visando a proteção e defesa contra ataques cibernéticos.
3. Promover a compreensão e aplicação de técnicas avançadas de segurança cibernética, incluindo a detecção e resposta a incidentes de segurança.
4. Preparar os alunos para atuar como profissionais qualificados no campo da defesa cibernética, com conhecimento avançado em gerenciamento de redes e sistemas.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Identificar e analisar vulnerabilidades em redes e sistemas.
2. Implementar e configurar soluções avançadas de segurança cibernética.
3. Gerenciar incidentes e responder a ataques cibernéticos.
4. Avaliar e propor melhorias em políticas de segurança da informação.
5. Compreender e aplicar técnicas avançadas de criptografia.

Habilidades:
1. Análise avançada de dados para detecção de ameaças cibernéticas.
2. Comunicação eficaz para relatar e criar planos de ação em situações de segurança cibernética.

VI. CONTEÚDO PROGRAMÁTICO

1. Introdução à Defesa Cibernética
- Conceitos básicos de defesa cibernética
- A importância da segurança cibernética na atualidade
- Principais ameaças e vulnerabilidades em ambientes cibernéticos
- Legislação e regulamentação relacionada à defesa cibernética

2. Gerenciamento de Riscos em Ambientes Cibernéticos
- Identificação e análise de riscos cibernéticos
- Estratégias e técnicas de mitigação de riscos
- Avaliação de impacto de segurança cibernética
- Planejamento e implementação de políticas de segurança cibernética
3. Monitoramento e Detecção de Ameaças Cibernéticas
- Ferramentas e técnicas de monitoramento de segurança cibernética
- Identificação e classificação de ameaças cibernéticas
- Análise de padrões e comportamentos suspeitos
- Resposta a incidentes cibernéticos
4. Implementação de Medidas de Defesa Cibernética
- Estratégias de defesa em profundidade
- Proteção de dados e informações sensíveis
- Segurança de redes e sistemas
- Controle de acesso e autenticação em ambientes cibernéticos

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:
- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:
- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:
  - Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Situações de Reprovação:
  - Nota final inferior a 3,0.
  - Falta em mais de 25% das aulas.
  - Não entrega de mais de 25% das atividades avaliativas.

Observações:
- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA
MACEDO, Ricardo Tombesi;...[et al.]. Redes de computadores. Santa Maria: UFSM, 2018.

FERNANDEZ, Marcial Porto. Rede de computadores. Fortaleza: EdUECE, 2019.

LATZKE, Carlos Alberto;...[et al.]. Infraestrutura e redes de computadores. Indaial: Uniasselvi, 2019

BIBLIOGRAFIA COMPLEMENTAR
AMARAL, Marcos Prado; ... [et al.]. Redes de computadores I. Belo Horizonte: CEFET-MG, 2013.

GUEDES, Jackes Ridan da Silva; ... [et al.]. Redes de computadores. Brasília: Escola Técnica de Brasília, 2014.

PINTO NETO, João Batista. Redes de Computadores. Cuiabá: UFMT, 2014.

SAMPAIO, Leobino Nascimento. Redes de computadores. Rio de Janeiro: UFRJ, 2018.

BAY, Edemilson;...[et al.]. Fundamentos de redes de computadores. Indaial: Uniasselvi, 2021..

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Segurança Aplicada a IoT
SÉRIE: 5º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123-20 Especialista em segurança da informação
COD_DISCIPLINA: DC04.02

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Segurança Aplicada a IoT no curso de Tecnologia em Defesa Cibernética tem como objetivo fornecer aos alunos os conhecimentos necessários para compreender os desafios e as soluções relacionadas à segurança da Internet das Coisas. A ementa abordará conceitos fundamentais de segurança cibernética, ameaças e vulnerabilidades específicas da

IoT, práticas de segurança e criptografia aplicadas a dispositivos conectados, padrões de segurança e conformidade regulatória, além de estratégias de detecção e resposta a incidentes. Os alunos também serão capacitados para avaliar riscos de segurança, desenvolver e implementar políticas de segurança para ambientes IoT, e participar de atividades práticas que simulem cenários reais de ataque e defesa. Ao final da disciplina, espera-se que os estudantes estejam aptos a contribuir proativamente para a proteção de sistemas e dispositivos IoT em ambientes corporativos e industriais.

IV. OBJETIVOS

1. Capacitar os estudantes para compreender e aplicar práticas de segurança especificamente voltadas para dispositivos de Internet das Coisas (IoT).
2. Desenvolver habilidades de identificação e avaliação de vulnerabilidades em sistemas IoT, e propor estratégias de mitigação de riscos.
3. Promover o entendimento das regulamentações e padrões de segurança relacionados a dispositivos IoT, e a capacidade de aplicá-los na prática.
4. Preparar os alunos para atuarem de forma proativa na proteção de sistemas IoT em ambientes corporativos, governamentais e industriais.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Identificar e analisar vulnerabilidades em dispositivos IoT.
2. Aplicar medidas de segurança em ambientes IoT.
3. Criar estratégias de defesa cibernética específicas para dispositivos IoT.
4. Avaliar e selecionar ferramentas de segurança adequadas para ambientes IoT.
5. Desenvolver soluções inovadoras para proteger dispositivos IoT contra ameaças cibernéticas.

Habilidades:
1. Capacidade de identificar e interpretar padrões de tráfego de dados em dispositivos IoT.
2. Competência em implementar protocolos de segurança específicos para dispositivos IoT.

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Introdução à Internet das Coisas (IoT)
- Conceitos básicos de IoT
- História e evolução da IoT
- Aplicações e impactos da IoT na sociedade

Unidade 2: Segurança na Internet das Coisas
- Vulnerabilidades e ameaças em dispositivos IoT
- Protocolos de segurança para dispositivos IoT
- Políticas de segurança para ambientes IoT

Unidade 3: Defesa Cibernética aplicada à IoT
- Estratégias de defesa cibernética para dispositivos IoT
- Análise de riscos e ameaças em ambientes IoT
- Monitoramento e resposta a incidentes de segurança em dispositivos IoT

Unidade 4: Tendências e desafios em Segurança Aplicada a IoT
- Novas tecnologias e sua influência na segurança de dispositivos IoT
- Desafios emergentes em segurança para dispositivos IoT

- Perspectivas futuras e desenvolvimentos na área de Segurança Aplicada a IoT

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

HOMEM, William Ludovico. Machine Learning. Vitória: UFES, 2020.

ZANIN, Aline. Fundamentos de Internet of Things (IoT). São Paulo: Smartbook, 2022.

MANAGEMENT SOLUTIONS. Machine Learning: transformação dos modelos de negócio. São Paulo: Management Solutions, 2018

BIBLIOGRAFIA COMPLEMENTAR

FRANCO; Cristiano Roberto. Inteligência artificial. Indaial: Uniasselvi, 2017.

COZMAN, Fabio G. Inteligência artificial: avanços e tendências. São Paulo : Instituto de

Estudos Avançados, 2021.

WACHOWICZ, Marcos; ... [et al.]. Inteligência artificial e criatividade: novos conceitos na propriedade intelectual. Curitiba: Gedai, 2019.

ALVES, Isabella Fonseca; ... [et al.]. Inteligência Artificial e Processo. Belo Horizonte: Editora D'Plácido, 2019.

TOFFOLI, José Antônio Dias; ... [et al.]. Inteligência artificial na Justiça. Brasília: CNJ, 2019.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Análise Avançada de Malware
SÉRIE: 5º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123-20 Especialista em segurança da informação
COD_DISCIPLINA: DC04.03

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

O curso de Tecnologia em Defesa Cibernética abordará a disciplina de Análise Avançada de Malware, oferecendo aos alunos conhecimentos aprofundados sobre a identificação, análise e resposta a ameaças virtuais avançadas. O conteúdo programático incluirá técnicas de engenharia reversa, análise de comportamento de códigos maliciosos, desmontagem de programas e identificação de técnicas de evasão. Além disso, os estudantes explorarão estudos de caso reais, laboratórios práticos e simulações de ataques, proporcionando uma visão prática e atualizada das táticas utilizadas por cibercriminosos. Ao final do curso, os alunos estarão aptos a atuar na linha de frente da defesa cibernética, contribuindo para a proteção de sistemas e informações vitais em um ambiente digital cada vez mais complexo e desafiador.

IV. OBJETIVOS

1. Compreender as técnicas avançadas de análise de malware e sua aplicação na defesa cibernética.
2. Desenvolver habilidades para identificar e classificar ameaças de malware de forma avançada.
3. Aplicar técnicas avançadas para a análise de códigos maliciosos e sua mitigação em

ambientes cibernéticos.
4. Avaliar e propor soluções avançadas para a prevenção e detecção de ameaças de malware em ambientes de defesa cibernética.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Capacidade de identificar e analisar diferentes tipos de malware
2. Conhecimento avançado em técnicas de defesa cibernética
3. Habilidade para realizar análises avançadas de ameaças cibernéticas
4. Competência para elaborar estratégias de prevenção e combate a malware
5. Capacidade de realizar relatórios detalhados sobre incidentes de segurança cibernética
Habilidades:
1. Análise avançada de códigos maliciosos
2. Utilização de ferramentas especializadas em segurança cibernética

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Introdução à Análise Avançada de Malware
- Conceitos básicos de malware
- Tipos de malware
- Métodos de propagação
- Principais ameaças atuais
Unidade 2: Análise Estática de Malware
- Ferramentas e técnicas de análise estática
- Análise de código e comportamento
- Identificação de assinaturas e padrões
Unidade 3: Análise Dinâmica de Malware
- Ambientes de sandbox
- Monitoramento de comportamento
- Análise de redes de comunicação
Unidade 4: Mitigação e Resposta a Ataques de Malware
- Estratégias de prevenção e detecção
- Procedimentos de resposta a incidentes
- Estudo de casos e práticas recomendadas

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:
- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:
  - Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Situações de Reprovação:
  - Nota final inferior a 3,0.
  - Falta em mais de 25% das aulas.
  - Não entrega de mais de 25% das atividades avaliativas.

Observações:
- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

MOURA, Adriano de Andrade;...[et al.]. Guia de Framework de Privacidade e Segurança da Informação. Brasília: Ministério da Gestão e da Inovação, 2023.

BARROS, Otávio Santana Rêgo;...[et al.]. Desafios estratégicos para segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2019.

WENDT, Emerson. Inteligência cibernética: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil. São Paulo: Editora Delfos, 2018.

OLIVEIRA, Marcos Aurélio Guedes de;...[et al]. Guia de defesa cibernética na América do Sul. Recife: UFPE, 2017.

BIBLIOGRAFIA COMPLEMENTAR

MASCARENHAS NETO, Pedro Tenório;...[et al.]. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: UFPB, 2019.

BARBOSA, Alexandre;...[et al.]. Segurança digital : uma análise da gestão de riscos em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

FERNANDES, Nélia O. Campo. Segurança da Informação. Cuiabá: UFMT, 2013.

COSTA, Celso;...[et al.]. Introdução à criptografia. v. 1. Rio de Janeiro: UFF, 2010.

FIGUEIREDO, Luiz Manoel. Introdução à Criptografia. v. 2. Rio de Janeiro: UFF, 2010..

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Gestão de Crises e Continuidade de Negócios
SÉRIE: 5º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123-20 Especialista em segurança da informação
COD_DISCIPLINA: DC04.04

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Gestão de Crises e Continuidade de Negócios no curso de Tecnologia em Defesa Cibernética abordará conceitos e estratégias para identificar, avaliar e gerir situações de crise, especialmente as relacionadas à segurança cibernética. Serão discutidos temas como plano de contingência, recuperação de desastres, comunicação de crise e aspectos legais e éticos. Além disso, a disciplina abordará a importância da continuidade de negócios em ambientes cibernéticos, incluindo a análise de riscos, planos de mitigação e estratégias para manter a operação em cenários de crise. Ao final do curso, os alunos estarão aptos a desenvolver e implementar planos eficazes de gestão de crises e continuidade de negócios em ambientes de defesa cibernética, visando a proteção e a segurança das organizações.

IV. OBJETIVOS

1. Desenvolver habilidades de prevenção e detecção de possíveis crises cibernéticas.
2. Capacitar os alunos para a tomada de decisões rápidas e eficientes em situações de crise cibernética.
3. Ensinar estratégias de continuidade de negócios em caso de ataques cibernéticos.
4. Promover o entendimento e a aplicação de melhores práticas em gestão de crises e continuidade de negócios no contexto da defesa cibernética.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Capacidade de identificar e avaliar potenciais vulnerabilidades e ameaças cibernéticas.
2. Conhecimento em estratégias de prevenção e resposta a incidentes cibernéticos.
3. Habilidade de analisar e interpretar dados para identificar atividades suspeitas.
4. Compreensão de normas e regulamentos relacionados à segurança cibernética.
5. Capacidade de elaborar planos de continuidade de negócios e recuperação de desastres em ambiente cibernético.

Habilidades:
1. Utilização de ferramentas de segurança cibernética para monitoramento e detecção de ameaças.

2. Capacidade de comunicação eficaz para relatar incidentes cibernéticos e propor soluções.

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Introdução à Defesa Cibernética
- Conceitos básicos de defesa cibernética
- Ciberataques mais comuns e suas consequências
- Legislação e normas relacionadas à segurança cibernética

Unidade de Aprendizagem 2: Métodos de Proteção em Defesa Cibernética
- Estratégias de segurança cibernética
- Criptografia e sua importância na proteção de dados
- Firewalls, antivírus e outras ferramentas de proteção cibernética

Unidade de Aprendizagem 3: Gestão de Crises em Defesa Cibernética
- Planejamento de contingência em caso de ciberataques
- Resposta a incidentes de segurança cibernética
- Comunicação em situações de crise em segurança cibernética

Unidade de Aprendizagem 4: Continuidade de Negócios em Defesa Cibernética
- Estratégias de recuperação de dados e sistemas após ciberataques
- Plano de continuidade de negócios em caso de incidentes de segurança cibernética
- Treinamento e conscientização em segurança cibernética para manter a continuidade dos negócios.

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

MOURA, Adriano de Andrade;...[et al.]. Guia de Framework de Privacidade e Segurança da Informação. Brasília: Ministério da Gestão e da Inovação, 2023.

BARROS, Otávio Santana Rêgo;...[et al.]. Desafios estratégicos para segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2019.

WENDT, Emerson. Inteligência cibernética: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil. São Paulo: Editora Delfos, 2018.

BIBLIOGRAFIA COMPLEMENTAR

MASCARENHAS NETO, Pedro Tenório;...[et al.]. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: UFPB, 2019.

BARBOSA, Alexandre;...[et al.]. Segurança digital : uma análise da gestão de riscos em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

FERNANDES, Nélia O. Campo. Segurança da Informação. Cuiabá: UFMT, 2013.

COSTA, Celso;...[et al.]. Introdução à criptografia. v. 1. Rio de Janeiro: UFF, 2010.

FIGUEIREDO, Luiz Manoel. Introdução à Criptografia. v. 2. Rio de Janeiro: UFF, 2010.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Desenvolvimento Seguro de Aplicações
SÉRIE: 5º
CARGA TEÓRIA: 30
CARGA HORÁRIA PRÁTICA: 30
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA: CBO 2123-20 Especialista em segurança da informação
COD_DISCIPLINA: DC04.05

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

O curso de Tecnologia em Defesa Cibernética abordará, entre suas disciplinas, o Desenvolvimento Seguro de Aplicações, visando capacitar os estudantes para identificar e corrigir vulnerabilidades em software. Nesta disciplina, serão estudadas técnicas de codificação segura, boas práticas de desenvolvimento, além de análise de ameaças e testes de penetração. Com enfoque na prevenção de ataques cibernéticos, os alunos aprenderão a implementar medidas de segurança desde a fase inicial do desenvolvimento, promovendo a proteção dos sistemas e dados contra potenciais brechas de segurança.

IV. OBJETIVOS

1. Capacitar os alunos a identificar e analisar vulnerabilidades em aplicações e sistemas para garantir o desenvolvimento seguro de aplicações.
2. Promover a compreensão dos princípios de segurança cibernética e sua aplicação no desenvolvimento de aplicações.
3. Desenvolver habilidades para implementar práticas de segurança cibernética em todas as fases do ciclo de vida das aplicações.
4. Preparar os alunos para enfrentar desafios reais de segurança cibernética e proteger aplicações contra ameaças internas e externas.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Gerenciamento de riscos em segurança de aplicações
2. Análise de vulnerabilidades e ameaças em aplicações
3. Implementação de práticas de segurança de dados
4. Compreensão dos princípios de segurança da informação
5. Desenvolvimento de estratégias de defesa cibernética

Habilidades:
1. Identificação e correção de falhas de segurança em aplicações
2. Utilização de ferramentas e técnicas de segurança cibernética para proteção de aplicações.

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Introdução à Segurança de Aplicações
- Conceitos fundamentais de segurança de aplicações
- A importância da segurança de aplicações na Defesa Cibernética
- Principais ameaças e vulnerabilidades em aplicações

Unidade de Aprendizagem 2: Práticas de Desenvolvimento Seguro
- Boas práticas de codificação segura
- Uso de ferramentas de segurança durante o desenvolvimento
- Testes de segurança e revisões de código

Unidade de Aprendizagem 3: Proteção de Dados e Privacidade
- Regulamentações de proteção de dados
- Criptografia e segurança de dados em aplicações
- Privacidade e ética no desenvolvimento de aplicações

Unidade de Aprendizagem 4: Gerenciamento de Incidentes de Segurança em Aplicações
- Identificação e resposta a incidentes de segurança

- Recuperação de aplicações após incidentes
- Plano de contingência e continuidade de negócios em caso de violação de segurança

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

ANDRADE, Mayb. Qualidade de software. Rio de Janeiro: Seses, 2015.

PÁDUA, Clarindo Isaías Pereira da Silva e. Engenharia de Usabilidade. Belo Horizonte: UFMG, 2016

SALLUM, William Geraldo. Aplicativos para a WEB II. Belo Horizonte : CEFET- MG, 2012.

BIBLIOGRAFIA COMPLEMENTAR

RIBEIRO, Maria Ivanilse Calderon; ... [et al.]. Projeto de Sistemas WEB. Cuiabá: UFMT,

2015.

MARINHO, Carlos Fábio Rocha. Fundamentos de Web Design e formatação de imagem. Manaus: CETAM, 2012.

SCHÜTZ, Fernando. Web design. Curitiba: Ed. UTFPR, 2013.

FERNANDES, Nélia O. Campo. Segurança da Informação. Cuiabá: UFMT, 2013.

FREITAS, Romualdo Rubens de. Análise e Projeto de Software. Cuiabá: UFMT, 2015.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Projeto Multidisciplinar Extensionista V
SÉRIE: 5º
CARGA TEÓRIA: 0
CARGA HORÁRIA PRÁTICA: 80
CARGA HORÁRIA TOTAL: 80
CBO ASSOCIADA: CBO 2123-20 Especialista em segurança da informação
COD_DISCIPLINA: DC04.06

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina Projeto Multidisciplinar Extensionista V para o curso de Tecnologia em Defesa Cibernética visa capacitar os estudantes para aplicarem de forma prática os conhecimentos adquiridos ao longo do curso, desenvolvendo projetos que integrem diversas áreas da tecnologia em defesa cibernética. A ementa abordará temas como análise de vulnerabilidades, implementação de soluções de segurança, gerenciamento de incidentes, políticas de segurança da informação, ética e aspectos legais, visando preparar os alunos para atuarem de forma eficiente e ética no mercado de trabalho na área de defesa cibernética. A disciplina buscará promover a integração entre as diferentes disciplinas do curso, estimulando a colaboração e o trabalho em equipe, e incentivando a busca por soluções inovadoras e eficazes para os desafios enfrentados na área de segurança cibernética.

IV. OBJETIVOS

1. Desenvolver habilidades práticas em defesa cibernética, através da análise de vulnerabilidades e elaboração de estratégias de segurança da informação.
2. Promover o entendimento das ameaças cibernéticas atuais e futuras, bem como as melhores práticas de proteção e prevenção.
3. Incentivar o trabalho em equipe e a colaboração na resolução de desafios relacionados à

defesa cibernética.
4. Capacitar os estudantes a aplicar conceitos teóricos em situações reais de segurança cibernética, por meio de estudos de caso e simulações de ataques.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Conhecimento avançado em segurança da informação
2. Habilidade em identificar e mitigar vulnerabilidades cibernéticas
3. Capacidade de desenvolver estratégias de defesa cibernética
4. Compreensão de técnicas de análise forense digital
5. Domínio em gestão de riscos de segurança cibernética
Habilidades:
1. Implementar soluções de segurança cibernética eficazes
2. Colaborar em equipe para lidar com incidentes de segurança cibernética

VI. DESCRIÇÃO DO PROJETO

O objetivo é criar um sistema abrangente que forneça às comunidades vulneráveis ferramentas e conhecimentos para proteger suas infraestruturas digitais e dados contra ameaças cibernéticas, com um foco particular na segurança da Internet das Coisas (IoT), crucial para muitas soluções de tecnologia assistiva e infraestrutura crítica. O projeto incluiria o desenvolvimento de um framework de desenvolvimento seguro para aplicações locais, workshops de treinamento para a comunidade, e um plano de resposta a crises e continuidade de negócios personalizado para as necessidades específicas da comunidade

VII. INTEGRAÇÃO ENTRE AS DISCIPLINAS

- **Fortalecimento da Infraestrutura Tecnológica:** Ao aumentar a segurança dos sistemas e dispositivos, o projeto diretamente beneficia a infraestrutura tecnológica das comunidades vulneráveis, protegendo-as contra ameaças cibernéticas.
- **Capacitação e Educação:** Workshops e treinamentos sobre segurança cibernética, especialmente focados em IoT, malware e desenvolvimento seguro, capacitarão os membros da comunidade com o conhecimento necessário para proteger suas informações e tecnologias.
- **Resiliência e Recuperação:** O plano de gestão de crises e continuidade de negócios garantirá que a comunidade possa responder eficazmente a incidentes de segurança, minimizando o impacto sobre suas operações críticas.

VIII. AVALIAÇÃO

Para avaliar o projeto "Sistema Integrado de Resiliência Cibernética para Comunidades Vulneráveis", o sistema de avaliação é baseado em entregas parciais será estabelecido, com cada componente focando em aspectos críticos do desenvolvimento do projeto. A nota final será determinada pelo desempenho acumulado nas entregas, com uma nota mínima para aprovação de 7,0.

1. Planejamento e Análise Inicial (15% da nota final)

- **Entrega:** Documento de projeto detalhando o escopo, objetivos específicos para a comunidade, análise de riscos, e estratégias preliminares de implementação.

- **Critérios de Avaliação:** Clareza dos objetivos, relevância e aplicabilidade das estratégias de segurança propostas, profundidade da análise de riscos.

2. Desenvolvimento de Framework de Segurança IoT (20% da nota final)
- **Entrega:** Framework desenvolvido para a segurança de dispositivos e redes IoT, incluindo diretrizes e padrões de segurança específicos.
- **Critérios de Avaliação:** Completude do framework, adequação às necessidades específicas de segurança IoT, praticidade e aplicabilidade.

3. Criação de Material de Treinamento e Workshop (20% da nota final)
- **Entrega:** Material educativo e workshops projetados para treinar membros da comunidade em práticas de segurança cibernética, focando em gerenciamento de redes, segurança IoT, e análise de malware.
- **Critérios de Avaliação:** Qualidade educativa do material, engajamento e feedback dos participantes dos workshops, abrangência dos tópicos de segurança cobertos.

4. Implementação do Plano de Gestão de Crises (15% da nota final)
- **Entrega:** Plano detalhado de resposta a crises e continuidade de negócios, adaptado às necessidades da comunidade.
- **Critérios de Avaliação:** Realismo e viabilidade do plano, clareza na comunicação das etapas de resposta, eficácia dos procedimentos de continuidade de negócios.

5. Desenvolvimento e Teste de Aplicações Seguras (20% da nota final)
- **Entrega:** Aplicações desenvolvidas utilizando práticas de desenvolvimento seguro, juntamente com a documentação de testes de segurança realizados.
- **Critérios de Avaliação:** Integração de práticas de segurança no desenvolvimento, ausência de vulnerabilidades conhecidas, documentação completa de testes e correções.

6. Apresentação Final e Relatório de Projeto (10% da nota final)
- **Entrega:** Apresentação abrangente do projeto, incluindo demonstrações de tecnologia implementada, resultados dos workshops, e análise de impacto na comunidade.
- **Critérios de Avaliação:** Clareza e profissionalismo da apresentação, abrangência do relatório final, evidências de impacto positivo na comunidade.

Cada entrega será cuidadosamente avaliada, e feedback construtivo será fornecido para promover a melhoria contínua do projeto. A soma ponderada das notas das entregas determinará a nota final, exigindo-se uma média mínima de 7,0 para aprovação. Este sistema de avaliação visa assegurar a qualidade e eficácia do projeto em aumentar a resiliência cibernética das comunidades vulneráveis, além de estimular o desenvolvimento contínuo de habilidades práticas e conhecimento teórico dos alunos.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA
Todas as bibliografias básicas estudadas até o momento

BIBLIOGRAFIA COMPLEMENTAR
Todas as bibliografias complementares estudadas até o momento

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Optativa 1 - Língua Brasileira de Sinais (Libras)
SÉRIE: Optativa
CARGA TEÓRIA: 60
CARGA HORÁRIA PRÁTICA: 0
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA:
COD_DISCIPLINA: DFOPT1

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina Optativa 1 - Língua Brasileira de Sinais (Libras) no curso de Tecnologia em Defesa Cibernética abordará os fundamentos da comunicação em Libras, visando capacitar os alunos a interagir de forma eficiente com a comunidade surda. Serão estudados aspectos linguísticos, culturais e práticos da Libras, com ênfase na aplicação desses conhecimentos no contexto da defesa cibernética, incluindo a comunicação e colaboração com colegas e profissionais surdos, bem como a análise de possíveis vulnerabilidades e ameaças relacionadas à segurança da informação nesse contexto. A disciplina proporcionará aos alunos uma base sólida para compreender e utilizar Libras de forma apropriada e eficaz, contribuindo para uma atuação profissional mais inclusiva e consciente.

IV. OBJETIVOS

1. Compreender a estrutura e o funcionamento da Língua Brasileira de Sinais (Libras) para promover a inclusão e comunicação eficaz com pessoas surdas ou com deficiência auditiva no contexto da segurança cibernética.
2. Desenvolver habilidades de comunicação em Libras para facilitar a interação e colaboração com profissionais surdos ou com deficiência auditiva na área da defesa cibernética.
3. Reconhecer a importância da inclusão e acessibilidade na área da tecnologia e segurança cibernética, e promover práticas inclusivas e acessíveis no ambiente de trabalho.
4. Integrar a Língua Brasileira de Sinais (Libras) como uma competência complementar na formação de profissionais de defesa cibernética, visando a construção de um ambiente de trabalho mais diversificado e inclusivo.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Compreender e se comunicar em Língua Brasileira de Sinais (Libras) de forma fluente e eficaz.
2. Aplicar os conhecimentos adquiridos em Libras para a inclusão de pessoas surdas na sociedade e no ambiente de trabalho.
3. Reconhecer e respeitar a cultura surda, bem como suas particularidades e desafios.
4. Utilizar a Língua Brasileira de Sinais (Libras) como ferramenta de comunicação em situações cotidianas e profissionais.
5. Colaborar ativamente na construção de um ambiente mais inclusivo e acessível para pessoas surdas.
Habilidades:
1. Ser capaz de interpretar e traduzir informações entre Libras e Português de forma precisa e eficiente.
2. Demonstrar fluência e expressividade ao se comunicar em Língua Brasileira de Sinais (Libras) em diferentes contextos e situações.

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Introdução à Língua Brasileira de Sinais (Libras) e sua importância na Defesa Cibernética
- História e origem da Libras
- Comparação entre a Libras e outras línguas de sinais do mundo
- Aplicações da Libras na área de Defesa Cibernética
Unidade de Aprendizagem 2: Compreensão e comunicação em Libras na Defesa Cibernética
- Fundamentos da gramática e estrutura da Libras
- Vocabulário relacionado à Defesa Cibernética em Libras
- Desenvolvimento de habilidades de comunicação em Libras para situações específicas na área de Defesa Cibernética
Unidade de Aprendizagem 3: Libras e Segurança da Informação
- Uso da Libras na comunicação de conceitos e práticas de segurança da informação
- Estratégias de segurança para pessoas surdas na era digital
- Desafios e soluções para a segurança da informação em ambientes onde a comunicação é feita em Libras
Unidade de Aprendizagem 4: Desenvolvimento de projetos em Defesa Cibernética com enfoque na inclusão de surdos
- Análise de casos de sucesso e desafios em projetos de Defesa Cibernética voltados para a comunidade surda
- Desenvolvimento de um projeto de Defesa Cibernética com estratégias de inclusão da comunidade surda
- Apresentação e avaliação dos projetos desenvolvidos pelos alunos, com foco na aplicação da Libras e inclusão de surdos na área de Defesa Cibernética

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0

Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

FERRAZ, Charles Lary Marques. Dicionário de configurações das mãos em libras. Cruz das Almas: UFRB, 2019.

ALBRES, Neiva de Aquino;...[et al.]. Libras e sua tradução em pesquisa: interfaces, reflexões e metodologias. Florianópolis: UFSC, 2017.

SOUZA, Mariana da Cunha Teixeira de. Curso de Libras on-line. Niterói: UFF, 2013

BIBLIOGRAFIA COMPLEMENTAR

LIMA, José Willen Brasil;...[et al.]. A surdez em múltiplos (con)textos: educação, tecnologia e saúde. Porto Alegre: Editora Fi, 2019.

LIMA, Eliamar Godoi;...[et al.]. Língua Brasileira de Sinais - Libras: a formação continuada de professores. Uberlândia: EDUFU, 2016.

MENEZES, Adriane Melo de Castro;...[et al.]. Introdução aos Estudos sobre Surdez e Libras.

Boa Vista: UFRR, 2018.

VIÇOSI, Paulo Willian Brunelli. Libras como instrumento de inclusão político-social na educação infantil. Goiânia: Editora Phillos, 2020.

SOFIATO, Cássia Geciauskas;...[et al.]. Língua Brasileira de Sinais - Libras: aspectos linguísticos e históricos. São Carlos: UNESP ,2012.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Optativa 2 - Segurança cibernética para dispositivos móveis
SÉRIE: Optativa
CARGA TEÓRIA: 60
CARGA HORÁRIA PRÁTICA: 0
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA:
COD_DISCIPLINA: DFOPT2

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina "Segurança cibernética para dispositivos móveis" abordará os principais desafios e estratégias para proteção de informações e dados em ambientes móveis. Serão estudados temas como criptografia, autenticação, prevenção de ataques e vulnerabilidades específicas de dispositivos móveis, bem como técnicas de investigação forense para dispositivos móveis. Além disso, serão discutidas as melhores práticas para mitigar riscos de segurança em aplicativos e redes móveis, visando capacitar os alunos a atuarem de forma proativa na defesa cibernética em ambientes móveis.

IV. OBJETIVOS

1. Capacitar os alunos a compreender e aplicar técnicas de segurança cibernética específicas para dispositivos móveis, como smartphones e tablets.
2. Desenvolver habilidades para identificar e mitigar ameaças e vulnerabilidades em dispositivos móveis, garantindo a proteção de informações confidenciais e dados pessoais.
3. Fomentar a capacidade dos alunos de projetar e implementar estratégias de segurança cibernética eficazes para dispositivos móveis, levando em consideração as tendências e desafios atuais nesse campo.
4. Preparar os alunos para atuarem como profissionais qualificados e atualizados no mercado de defesa cibernética, com especialização em segurança para dispositivos móveis.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Capacidade de identificar e analisar vulnerabilidades em dispositivos móveis.
2. Conhecimento avançado em técnicas de proteção e segurança cibernética.
3. Habilidade para desenvolver e implementar estratégias de proteção para dispositivos móveis.
4. Capacidade de realizar testes de segurança e avaliar a eficácia das medidas adotadas.
5. Habilidade para gerenciar incidentes de segurança em dispositivos móveis.
Habilidades:
1. Proficiência em utilização de ferramentas de segurança cibernética para dispositivos móveis.
2. Capacidade de comunicação e trabalho em equipe para lidar com situações de segurança cibernética em dispositivos móveis.

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Introdução à Segurança Cibernética
- Fundamentos de segurança cibernética
- Principais ameaças em dispositivos móveis
- Importância da segurança cibernética para dispositivos móveis

Unidade 2: Vulnerabilidades em Dispositivos Móveis
- Análise de vulnerabilidades em sistemas operacionais móveis
- Riscos de segurança em aplicativos móveis
- Métodos de detecção e exploração de vulnerabilidades

Unidade 3: Estratégias de Proteção e Prevenção em Dispositivos Móveis
- Criptografia e segurança de dados em dispositivos móveis
- Autenticação e controle de acesso em dispositivos móveis
- Políticas de segurança em dispositivos móveis

Unidade 4: Gestão de Incidentes em Dispositivos Móveis
- Monitoramento e detecção de incidentes de segurança
- Resposta a incidentes em dispositivos móveis
- Prevenção de futuros incidentes e melhoria contínua da segurança cibernética em dispositivos móveis

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:
- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:
- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.

- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

METZNER, Laercio. Programação Web I. Indaial :UNIASSELVI, 2021.

FRANCO, Cristiano Roberto. Programação Web II. Indaial :UNIASSELVI, 2022.

GOMES, Bruno Emerson Gurgel. Fundamentos de Lógica e Algoritmos. Natal: IFRN, 2015.

BIBLIOGRAFIA COMPLEMENTAR

CASTILHO, Marcos Alexandre. Algoritmos e estruturas de dados 1. Curitiba: UFPR, 2020.

BATISTA, Rogério da Silva. Lógica de programação. Teresina: IFPI, 2013

RAMOS, José Marcio Benite. Estrutura de dados. Cuiabá: UFMT, 2013.

ALÉSSIO, Simone Cristina. Lógica e técnicas de Programação. Indaial: Uniasselvi, 2017.

LACERDA, Liluyoud Cury de; ... [et al.]. Lógica de programação. Cuiabá: Ed.UFMT, 2014.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Optativa 3 - Segurança cibernética para infraestrutura crítica
SÉRIE: Optativa
CARGA TEÓRIA: 60
CARGA HORÁRIA PRÁTICA: 0
CARGA HORÁRIA TOTAL: 60

CBO ASSOCIADA:
COD_DISCIPLINA: DFOPT3

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina "Segurança cibernética para infraestrutura crítica" do curso de Tecnologia em Defesa Cibernética abordará os principais conceitos e práticas relacionadas à proteção de sistemas de informação que suportam infraestruturas críticas. Serão discutidos temas como ameaças cibernéticas, vulnerabilidades em sistemas de controle e monitoramento, técnicas de criptografia e prevenção de ataques, com ênfase na aplicação desses conhecimentos para garantir a disponibilidade, integridade e confidencialidade das informações em ambientes críticos. Além disso, serão apresentados estudos de casos reais e exercícios práticos para a compreensão e aplicação dos conceitos apresentados. Ao final do curso, os alunos deverão estar aptos a implementar medidas de segurança cibernética eficazes para proteger infraestruturas críticas contra ameaças internas e externas.

IV. OBJETIVOS

1. Compreender os princípios fundamentais de segurança cibernética para proteger a infraestrutura crítica contra ameaças e ataques cibernéticos.
2. Desenvolver habilidades para identificar vulnerabilidades em sistemas de infraestrutura crítica e implementar medidas de segurança eficazes para mitigar essas vulnerabilidades.
3. Capacitar os alunos para avaliar e analisar possíveis cenários de ataques cibernéticos contra infraestrutura crítica, e desenvolver estratégias de defesa e resposta a esses ataques.
4. Promover a compreensão dos regulamentos e diretrizes relacionados à segurança cibernética para infraestrutura crítica, e capacitá-los para garantir conformidade com essas normas.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Capacidade de identificar vulnerabilidades em sistemas de infraestrutura crítica.
2. Habilidade para elaborar estratégias de defesa cibernética específicas para ambientes de infraestrutura crítica.
3. Conhecimento em regulamentações e normas de segurança cibernética aplicáveis à infraestrutura crítica.
4. Habilidade para realizar análise de riscos e impactos em caso de ataques cibernéticos.
5. Capacidade de elaborar planos de contingência e recuperação de sistemas em infraestrutura crítica.

Habilidades:
1. Boa comunicação e colaboração em equipe para implementar medidas de segurança cibernética.
2. Domínio de ferramentas e técnicas de segurança cibernética específicas para proteger infraestrutura crítica.

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Fundamentos de Segurança Cibernética para Infraestrutura Crítica
- Introdução à segurança cibernética
- Conceitos e princípios de infraestrutura crítica
- Ameaças e vulnerabilidades específicas para infraestrutura crítica
- Estratégias de defesa cibernética para infraestrutura crítica

Unidade de Aprendizagem 2: Gestão de Riscos e Compliance em Segurança Cibernética para Infraestrutura Crítica
- Avaliação de riscos em infraestrutura crítica
- Normas e regulamentações de segurança cibernética para infraestrutura crítica
- Implementação de políticas de compliance em segurança cibernética
- Auditorias e monitoramento em segurança cibernética para infraestrutura crítica

Unidade de Aprendizagem 3: Tecnologias e Ferramentas em Segurança Cibernética para Infraestrutura Crítica
- Software e hardware específicos para segurança cibernética em infraestrutura crítica
- Análise de dados e detecção de ameaças em tempo real
- Simulação de ataques e testes de segurança em infraestrutura crítica
- Gerenciamento de incidentes em segurança cibernética para infraestrutura crítica

Unidade de Aprendizagem 4: Estratégias Avançadas em Segurança Cibernética para Infraestrutura Crítica
- Inteligência cibernética e análise de ameaças específicas para infraestrutura crítica
- Resposta a incidentes e plano de continuidade de negócios em infraestrutura crítica
- Parcerias público-privadas em segurança cibernética para infraestrutura crítica
- Tendências e desafios futuros em segurança cibernética para infraestrutura crítica.

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

LATZKE, Carlos Alberto;...[et al.]. Infraestrutura e redes de computadores. Indaial: Uniasselvi, 2019.

MASCARENHAS NETO, Pedro Tenório;...[et al.]. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: UFPB, 2019.

GROSS, Christian Meinecke. Segurança em tecnologia da informação. Indaial: Uniasselvi, 2013.

BIBLIOGRAFIA COMPLEMENTAR

MACEDO, Ricardo Tombesi;...[et al.]. Redes de computadores. Santa Maria: UFSM, 2018.

FERNANDEZ, Marcial Porto. Rede de computadores. Fortaleza: EdUECE, 2019.

PINTO NETO, João Batista. Redes de Computadores. Cuiabá: UFMT, 2014.

SAMPAIO, Leobino Nascimento. Redes de computadores. Rio de Janeiro: UFRJ, 2018.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Optativa 4 - Inteligência Artificial Aplicada à Segurança Cibernética
SÉRIE: Optativa
CARGA TEÓRIA: 60
CARGA HORÁRIA PRÁTICA: 0
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA:
COD_DISCIPLINA: DFOPT4

II. DOCENTE RESPONSÁVEL

PROFESSOR:

TITULAÇÃO:

III. EMENTA

A disciplina de Optativa 4 - Inteligência Artificial Aplicada à Segurança Cibernética do curso de Tecnologia em Defesa Cibernética tem como objetivo oferecer aos alunos conhecimentos avançados sobre a aplicação da inteligência artificial na proteção de sistemas cibernéticos. Serão abordados temas como algoritmos de machine learning, redes neurais, detecção de ameaças, análise de comportamento e prevenção de ataques cibernéticos. A ementa inclui estudos de casos reais, simulações de ataques e defesas, além do desenvolvimento de soluções inovadoras para garantir a segurança da informação em ambientes virtuais. Ao final da disciplina, os alunos estarão aptos a utilizar ferramentas de inteligência artificial para enfrentar os desafios atuais e futuros da segurança cibernética.

IV. OBJETIVOS

1. Compreender os princípios e técnicas de Inteligência Artificial aplicados à Segurança Cibernética para a identificação e prevenção de ataques cibernéticos.
2. Desenvolver habilidades práticas na aplicação de algoritmos e técnicas de Inteligência Artificial para detecção e resposta a ameaças cibernéticas.
3. Explorar e analisar casos de uso de Inteligência Artificial em Segurança Cibernética, identificando possíveis aplicações e benefícios para a defesa cibernética.
4. Integrar conhecimentos teóricos e práticos da Inteligência Artificial com as estratégias e táticas de defesa cibernética, visando fortalecer a capacidade de proteção de sistemas e dados contra ataques virtuais.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Análise de ameaças cibernéticas
2. Implementação de técnicas de segurança cibernética
3. Avaliação de vulnerabilidades em sistemas de informação
4. Desenvolvimento de estratégias de defesa cibernética
5. Resolução de incidentes de segurança cibernética

Habilidades:
1. Uso de ferramentas de análise de segurança cibernética
2. Compreensão de técnicas avançadas de inteligência artificial aplicadas à segurança cibernética

VI. CONTEÚDO PROGRAMÁTICO

Unidade de Aprendizagem 1: Introdução à Segurança Cibernética
- Conceitos básicos de segurança cibernética
- Principais ameaças e vulnerabilidades em ambientes cibernéticos
- História e evolução da segurança cibernética

Unidade de Aprendizagem 2: Princípios de Inteligência Artificial
- Noções básicas de inteligência artificial
- Algoritmos e técnicas de aprendizado de máquina aplicados à segurança cibernética
- Uso de IA para detecção e prevenção de ataques cibernéticos

Unidade de Aprendizagem 3: Aplicações da Inteligência Artificial em Segurança Cibernética

- Análise de dados de segurança cibernética com IA
- Implementação de sistemas de detecção de anomalias com IA
- Desenvolvimento de sistemas de segurança cibernética autônomos

Unidade de Aprendizagem 4: Desafios e Tendências em Segurança Cibernética com IA
- Ética e regulamentação no uso de IA em segurança cibernética
- Novas tecnologias e tendências em segurança cibernética com IA
- Aplicações práticas e estudos de caso em defesa cibernética com IA

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

FRANCO; Cristiano Roberto. Inteligência artificial. Indaial: Uniasselvi, 2017.

COZMAN, Fabio G. Inteligência artificial: avanços e tendências. São Paulo : Instituto de Estudos Avançados, 2021.

WACHOWICZ, Marcos; ... [et al.]. Inteligência artificial e criatividade: novos conceitos na propriedade intelectual. Curitiba: Gedai, 2019

BIBLIOGRAFIA COMPLEMENTAR

HOMEM, William Ludovico. Machine Learning. Vitória: UFES, 2020.

RODRIGUES, Ricardo Batista. Novas Tecnologias da Informação e da Comunicação. Recife: IFPE, 2016.

MANAGEMENT SOLUTIONS. Machine Learning: transformação dos modelos de negócio. São Paulo: Management Solutions, 2018.

ALVES, Isabella Fonseca; ... [et al.]. Inteligência Artificial e Processo. Belo Horizonte: Editora D'Plácido, 2019.

TOFFOLI, José Antônio Dias; ... [et al.]. Inteligência artificial na Justiça. Brasília: CNJ, 2019..

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Optativa 5 - Inovação e Empreendedorismo em Segurança Cibernética
SÉRIE: Optativa
CARGA TEÓRIA: 60
CARGA HORÁRIA PRÁTICA: 0
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA:
COD_DISCIPLINA: DFOPT5

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Inovação e Empreendedorismo em Segurança Cibernética proposta para o curso de Tecnologia em Defesa Cibernética tem como objetivo fornecer aos alunos conhecimentos teóricos e práticos sobre as tendências e inovações no campo da segurança cibernética, com foco no empreendedorismo e nas estratégias de inovação. Durante o curso, os alunos serão introduzidos aos principais conceitos e metodologias relacionados à inovação em segurança cibernética, compreendendo as necessidades do mercado e as oportunidades de negócio na área. Além disso, serão abordados temas como identificação de problemas, desenvolvimento de soluções inovadoras, gestão de projetos e empreendedorismo em segurança cibernética, preparando os estudantes para atuarem de forma empreendedora e inovadora no mercado de defesa cibernética. Ao final da disciplina, os alunos estarão aptos

a identificar oportunidades de inovação, desenvolver projetos inovadores e empreender no setor de segurança cibernética, contribuindo para o avanço e aprimoramento dessa área estratégica.

IV. OBJETIVOS

1. Compreender as mais recentes inovações em segurança cibernética, incluindo novas técnicas de ataque e defesa, para estar preparado para lidar com ameaças emergentes.
2. Desenvolver habilidades empreendedoras para identificar oportunidades de negócios na área de segurança cibernética e criar soluções inovadoras para proteger a infraestrutura de TI das organizações.
3. Analisar os desafios éticos e legais relacionados à segurança cibernética, e desenvolver estratégias para lidar com essas questões de forma responsável e eficaz.
4. Aplicar conhecimentos teóricos e práticos em projetos reais de segurança cibernética, com foco na inovação e no empreendedorismo, para desenvolver soluções eficazes e inovadoras para proteger sistemas e dados.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Conhecimento avançado em inovação tecnológica na área de segurança cibernética;
2. Capacidade de identificar e avaliar novas ameaças cibernéticas;
3. Habilidade para desenvolver estratégias inovadoras de defesa cibernética;
4. Conhecimento empreendedor para identificar oportunidades de negócio na área de segurança cibernética;
5. Capacidade de liderança e trabalho em equipe para implementar soluções inovadoras em segurança cibernética.

Habilidades:
1. Habilidade técnica para implementar sistemas de segurança cibernética inovadores;
2. Capacidade de análise crítica e tomada de decisões em situações emergenciais relacionadas à segurança cibernética.

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Fundamentos de Segurança Cibernética
- Introdução à segurança cibernética
- Princípios básicos de defesa cibernética
- Conceitos de ameaças e ataques cibernéticos
- Práticas recomendadas para prevenção de ataques cibernéticos

Unidade 2: Tecnologias e Ferramentas de Defesa Cibernética
- Firewall e segurança de redes
- Criptografia e segurança de dados
- Software de detecção de intrusos
- Segurança em ambientes de nuvem

Unidade 3: Estratégias de Defesa Cibernética
- Políticas de segurança cibernética
- Análise de riscos e vulnerabilidades
- Resposta a incidentes cibernéticos
- Educação e conscientização em segurança cibernética

Unidade 4: Tópicos Avançados em Defesa Cibernética
- Análise forense digital
- Segurança de dispositivos móveis
- Internet das coisas e segurança cibernética
- Tendências e desafios futuros em segurança cibernética

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:

- **Avaliações Formativas (50%)**
  - Participação em fóruns e debates online (10%)
  - Atividades individuais e em grupo (20%)
  - Portfólio digital (20%)
- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

GIOVANELA, Adriana;... [et al.]. Empreendedorismo. Indaial: Uniasselvi, 2017.

MENDONÇA, Rosângela Míriam L. O. Economia criativa: práticas para inovação e desenvolvimento. Belo Horizonte: EdUEMG,2019.

SANTOS, Renato Lima dos; SOUZA, Lady Day Pereira de. Empreendedorismo. Cuiabá: Instituto Federal do Rondônia, 2015.

BIBLIOGRAFIA COMPLEMENTAR

RUSSO, Suzana Leitão;... [et al.]. Propriedade intelectual, tecnologias e empreendedorismo. Aracaju: Associação Acadêmica de Propriedade Intelectual, 2017.

MARCOVITCH, Jacques;... [et al.]. Pioneirismo e educação empreendedora: projetos e iniciativas. São Paulo: Com-Arte, 2018.

GITMAN, Lawrence J. ... [et al.]. Introdução ao negócios. Texas: OpenStax, 2018.

ABREU, Antonio Jorlan Soares de;... [et al.]. Mulheres empreendedoras: entre o batom ao planejamento estratégico. São Luís: IFMA, 2019.

MASSENSINI, Ariana Ramos. Empreendedorismo. Cuiabá: UFMT, 2011.

PLANO DE ENSINO

I. IDENTIFICAÇÃO DA DISCIPLINA

CURSO: Defesa Cibernética
DISCIPLINA: Optativa 6 - Design Thinking e Inovação em Cibersegurança
SÉRIE: Optativa
CARGA TEÓRIA: 60
CARGA HORÁRIA PRÁTICA: 0
CARGA HORÁRIA TOTAL: 60
CBO ASSOCIADA:
COD_DISCIPLINA: DFOPT6

II. DOCENTE RESPONSÁVEL

PROFESSOR:
TITULAÇÃO:

III. EMENTA

A disciplina de Design Thinking e Inovação em Cibersegurança no curso de Tecnologia em Defesa Cibernética aborda as metodologias e práticas de design thinking aplicadas à segurança cibernética, com foco na inovação e resolução de problemas complexos. Os estudantes irão aprender a utilizar abordagens criativas para identificar ameaças, desenvolver soluções inovadoras e projetar estratégias eficazes de defesa cibernética. Além disso, serão exploradas técnicas de prototipagem, colaboração interdisciplinar e pensamento crítico para aprimorar a segurança de sistemas e redes, preparando os alunos para enfrentar os desafios emergentes no campo da cibersegurança.

IV. OBJETIVOS

1. Compreender as metodologias de pensamento de design e sua aplicação na inovação em cibersegurança.
2. Desenvolver habilidades para identificar e resolver problemas complexos relacionados à

defesa cibernética por meio de abordagens criativas e inovadoras.
3. Adquirir conhecimentos práticos em técnicas de design thinking aplicadas à segurança cibernética, visando aprimorar a capacidade de antecipar e responder a ameaças cibernéticas.
4. Integrar os princípios do design thinking com as estratégias de inovação em cibersegurança, a fim de promover a criação de soluções eficazes e adaptáveis para proteger sistemas e redes de informações.

V. COMPETÊNCIA/HABILIDADES

Competências:
1. Capacidade de identificar e analisar vulnerabilidades em sistemas e redes de computadores.
2. Habilidade para propor soluções inovadoras para proteger informações e dados confidenciais.
3. Conhecimento avançado em técnicas de design thinking aplicadas à segurança cibernética.
4. Habilidade para trabalhar em equipe na resolução de problemas complexos relacionados à cibersegurança.
5. Capacidade de acompanhar as tendências e inovações do mercado de cibersegurança.
Habilidades:
1. Domínio em ferramentas de análise e detecção de ameaças cibernéticas.
2. Capacidade de comunicação eficaz para apresentar e defender soluções de segurança cibernética para diferentes públicos.

VI. CONTEÚDO PROGRAMÁTICO

Unidade 1: Introdução à Defesa Cibernética
- Conceitos fundamentais de defesa cibernética
- Panorama atual da segurança cibernética
- Desafios e ameaças em cibersegurança

Unidade 2: Princípios de Design Thinking
- Fundamentos do Design Thinking
- Metodologias e ferramentas de Design Thinking aplicadas à segurança cibernética
- Exercícios práticos de aplicação do Design Thinking em cenários de defesa cibernética

Unidade 3: Inovação em Cibersegurança
- Tendências e inovações em segurança cibernética
- Novas tecnologias e abordagens para a defesa cibernética
- Estudos de caso de inovações em cibersegurança

Unidade 4: Aplicação do Design Thinking e Inovação em Defesa Cibernética
- Desenvolvimento de projetos e soluções utilizando Design Thinking
- Implementação de inovações em cibersegurança
- Avaliação de impacto e eficácia das estratégias de defesa cibernética baseadas em Design Thinking e inovação

VII. AVALIAÇÃO

Nota mínima de aprovação: 7,0
Composição da Nota:
- **Avaliações Formativas (50%)**

- Participação em fóruns e debates online (10%)
- Atividades individuais e em grupo (20%)
- Portfólio digital (20%)

- **Avaliações Somativas (50%)**
  - Projetos práticos e desafios (30%)
  - Exame prático (20%)

Exames para alunos com nota entre 3,0 e 5,9:

- **Exame de Recuperação:**
  - Prova escrita com questões sobre os conteúdos da disciplina.
  - Data a ser definida pelo professor.
  - Nota mínima para aprovação: 7,0.

Exame Final:

- Prova escrita e/ou prática abrangendo todo o conteúdo da disciplina.
- Data a ser definida pelo professor.
- Nota mínima para aprovação: 7,0.

Situações de Reprovação:

- Nota final inferior a 3,0.
- Falta em mais de 25% das aulas.
- Não entrega de mais de 25% das atividades avaliativas.

Observações:

- O professor poderá realizar outras atividades avaliativas, desde que sejam informadas aos alunos no início da disciplina.
- A frequência e participação nas aulas online são importantes para o aprendizado e serão consideradas na avaliação final.
- O aluno que reprovar na disciplina poderá cursá-la novamente em outro semestre.

VIII. BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA

ARRUDA, Amilton J. V.; ... [et al.]. Design & Complexidade. São Paulo : Blucher Open Access, 2017.

VIANNA, Maurício.; ... [et al.]. Design thinking: inovação em negócios. Rio de Janeiro : MJV Press, 2012.

CARVALHO, Marco Aurélio de. Inovação em produtos: IDEATRIZ: uma aplicação da Triz: inovação sistemática na ideação de produtos. São Paulo: Blucher Open Access, 2017.

BIBLIOGRAFIA COMPLEMENTAR

ROMEIRO FILHO, Eduardo. Projeto de Produto. Belo Horizonte, Edição do autor, 2006.

RIBEIRO, Rafael Dias; ... [et al.]. Métodos Ágeis em Gerenciamento de Projetos. Rio de Janeiro: Edição dos autores, 2015.

BUAINAIN, Antônio Márcio.; ... [et al.]. Propriedade intelectual e desenvolvimento no Brasil. Rio de Janeiro : Ideia D; ABPI , 2019.

NOGUEIRA, Heloisa. Gestão de Marketing I. Rio de Janeiro: Fundação CECIERJ, 2009.

NOGUEIRA, Heloisa. Gestão de marketing II. Rio de Janeiro: Fundação CECIERJ, 2009.

2.5 CONTEÚDOS CURRICULARES

O curso de Defesa Cibernética, que será oferecido pela Faculdade ACADI-TI após seu credenciamento, será um tecnólogo com duração de dois anos e meio (5 semestres), focado em preparar profissionais altamente qualificados em segurança cibernética. Este curso abrange desde os fundamentos básicos até as mais avançadas tecnologias em proteção de sistemas e redes contra-ataques cibernéticos, garantindo uma formação completa e atualizada. A estrutura curricular está alinhada às exigências atuais do mercado, incluindo atualizações constantes do conteúdo, ajuste de carga horária e seleção criteriosa de bibliografias.

Além de sua forte ênfase na prática, o curso adota uma metodologia de ensino inclusiva e multidisciplinar, abarcando temas como educação ambiental, direitos humanos e questões étnico-raciais, promovendo uma formação mais holística. O curso também se destaca pela sua abordagem inovadora, encorajando os alunos a se engajarem com as mais recentes descobertas e inovações na área. Analisemos com mais detalhes esses conteúdos curriculares.

2.5.1 Desenvolvimento do perfil profissional

O perfil profissional do egresso do curso de Defesa Cibernética respeita o Catálogo Nacional de Cursos Superiores de Tecnologia e atende as demandas específicas de São José dos Campos e Região do Vale do Paraíba, em geral. Esse perfil é composto por competências técnicas e habilidades gerais, como já tratado neste PPC no subcapítulo PERFIL DO EGRESSO.

Sinteticamente, para rememorarmos algumas premissas básicas, sabemos que as competências técnicas do egresso de um curso de defesa cibernética são essenciais para que ele possa atuar na área. Essas competências incluem, como já vimos, conhecimentos e habilidades em:

- Redes de computadores
- Sistemas operacionais
- Segurança da informação
- Criptografia

- Análise de vulnerabilidades
- Forense digital
- Inteligência artificial
- Machine learning
- Cloud computing

Os conteúdos curriculares do curso abordam todos esses tópicos, fornecendo aos alunos os conhecimentos e habilidades necessários para atuar na área de defesa cibernética.

Para citar um caso, há uma relação entre os tópicos acima e a disciplina Introdução à Redes de Computadores, ofertada no primeiro semestre do curso, que aborda os conceitos básicos de redes de computadores, incluindo tecnologias, protocolos e segurança envolvidos. Na mesma linha, a disciplina Fundamentos de Sistemas Operacionais aborda os conceitos básicos de sistemas operacionais, incluindo segurança de sistemas operacionais. Completando, a disciplina Introdução à Segurança Cibernética aborda os conceitos básicos de segurança da informação, incluindo princípios e práticas de segurança da informação, segurança de rede, segurança de aplicativos e segurança de dados. Ao contruir a matriz curricular o perfil do egresso foi um dos critérios para seleção dos conteúdos.

Além das competências técnicas, sabemos que o egresso de um curso de Defesa Cibernética também deve desenvolver habilidades gerais, que são essenciais para o sucesso profissional. Essas habilidades incluem:

- Capacidade de análise e resolução de problemas
- Raciocínio lógico e crítico
- Habilidades de comunicação e trabalho em equipe
- Capacidade de aprendizagem contínua
- Liderança
- Ética e conformidade legal

Os conteúdos curriculares do curso também abordam essas habilidades, fornecendo aos alunos a possibilidade de desenvolverem essas competências. De forma ilustrativa, a disciplina Avaliação de Ameaças de Invasão exige que os alunos desenvolvam habilidades de análise e resolução de problemas para identificar e avaliar vulnerabilidades em sistemas e redes. Já a disciplina Planejamento e Política de Segurança Cibernética exige que os alunos desenvolvam habilidades de raciocínio lógico e crítico para planejar e implementar políticas de segurança da

informação. De modo análogo, a disciplina Digital Forense em Defesa Cibernética exige que os alunos desenvolvam habilidades de comunicação e trabalho em equipe para coletar, analisar e preservar evidências digitais.

O egresso de um curso de defesa cibernética poderá atuar em diversas áreas, como:

- Segurança de redes e sistemas
- Forense digital
- Execução de projetos de segurança da informação
- Centro de Operação de Segurança (SOC)

Os conteúdos curriculares do curso também abordam essas áreas, fornecendo aos alunos os conhecimentos e habilidades necessários para atuar em cada uma delas. Para exemplificar, a disciplina Segurança de Redes e Sistemas fornece aos alunos os conhecimentos e habilidades necessários para atuar na área de segurança de redes e sistemas. A disciplina Forense Digital, também pensando no campo de atuação, fornece aos alunos os conhecimentos e habilidades necessários para atuar na área de forense digital. A disciplina Execução de Projetos de Segurança da Informação, por sua vez, fornece aos alunos os conhecimentos e habilidades necessários para atuar na área de execução de projetos de segurança da informação. Na mesma linha, a disciplina Centro de Operação de Segurança (SOC) fornece aos alunos os conhecimentos e habilidades necessários para atuar na área de Centro de Operação de Segurança (SOC).

Como se quer demonstrar, o perfil do egresso do curso de Defesa Cibernética é abordado nos conteúdos curriculares por meio de uma abordagem holística, que inclui competências técnicas, habilidades gerais e áreas de atuação. Os conteúdos curriculares garantem que os egressos terão os conhecimentos e habilidades necessários para atuar com sucesso na área na área de Tecnologia em geral, e na Defesa Cibernética em particular.

2.5.2 Atualização dos conteúdos em relação à área

O curso de Defesa Cibernética da Faculdade ACADI-TI apresenta uma estrutura curricular que está alinhada com as diretrizes e frameworks mais recentes no campo da cibersegurança. A abordagem da faculdade cobre uma variedade de tópicos essenciais que são consistentes com as orientações do Cyber2yr2020 da *Association for Computing Machinery*

(ACM), um guia desenvolvido para ajudar instituições a criar currículos alinhados com frameworks reconhecidos de cibersegurança.

O currículo inclui componentes como fundamentos de redes de computadores, sistemas operacionais, segurança cibernética, virtualização e computação em nuvem, além de programação específica para segurança cibernética. Essa amplitude de tópicos é importante, pois o Cyber2yr2020 enfatiza competências em oito domínios de segurança, que incluem segurança de dados, segurança de software, segurança de componentes e segurança de conexão, entre outros.

A Faculdade ACADI-TI também valorizar uma abordagem prática, oferecendo um equilíbrio entre horas teóricas e práticas. Essa metodologia está em sintonia com as práticas educacionais atuais que enfatizam a importância da experiência prática, algo fundamental na área de tecnologia e especialmente relevante no campo dinâmico da cibersegurança.

Além disso, a inclusão de tópicos como ética, moral e direitos humanos reflete uma consciência da importância das questões sociais e humanas na tecnologia, alinhando-se com a tendência atual de enfatizar não apenas as habilidades técnicas, mas também a compreensão do impacto mais amplo da tecnologia na sociedade.

Neste sentido, o curso da Faculdade ACADI-TI mostra um comprometimento com a educação em cibersegurança que é relevante, abrangente e atualizada, preparando os alunos com as competências necessárias para enfrentar as ameaças cibernéticas modernas e adaptar-se às rápidas mudanças na tecnologia.

2.5.3 Adequação das cargas horárias dos conteúdos

A matriz curricular do curso aborda uma ampla gama de tópicos relevantes para a área de defesa cibernética, incluindo os fundamentos da segurança cibernética, bem como tópicos mais avançados, como segurança em nuvem, segurança de dispositivos móveis e defesa de rede avançada.

Além disso, o curso oferece uma abordagem prática, com disciplinas que envolvem atividades práticas, como laboratórios de segurança e exercícios de hacking ético. Isso permite que os alunos adquiram as habilidades e o conhecimento necessários para aplicar os conceitos aprendidos na prática.

A matriz curricular do curso também será constantemente revisada para garantir que os alunos estejam preparados para enfrentar as ameaças e vulnerabilidades cibernéticas que estão em constante evolução. Mais a frente, vamos tratar das formas periódicas de avaliação do curso para mantê-lo sempre atualizado

Especificamente, as disciplinas do curso possuem carga horária adequada para o componente curricular, pois as disciplinas teóricas têm carga horária suficiente para permitir que os alunos compreendam os conceitos abordados. A título de exemplo, a disciplina "Introdução à Segurança Cibernética" tem 50 horas teóricas, o que é suficiente para que os alunos aprendam os fundamentos da segurança cibernética, como os conceitos de confidencialidade, integridade e disponibilidade.

As disciplinas práticas também têm carga horária suficiente para permitir que os alunos apliquem os conceitos aprendidos na prática. Exemplificando, a disciplina "Administração Segura de Sistema Linux" tem 30 horas práticas, o que é suficiente para que os alunos aprendam a implementar e avaliar medidas de segurança em sistemas operacionais Linux.

No entanto, é importante ressaltar que a carga horária do curso pode ser ajustada de acordo com as necessidades dos alunos e do mercado de trabalho.

A carga horária dos componentes curriculares do curso de defesa cibernética da ACADI-TI está adequada, pois atende aos seguintes critérios:

- Aborda uma ampla gama de tópicos relevantes para a área de defesa cibernética.
- Oferece uma abordagem prática.
- É atualizado.

Essa carga horária permite que os alunos adquiram os conhecimentos e habilidades necessários para se tornarem profissionais de defesa cibernética qualificados.

2.5.4 Adequação da bibliografia aos conteúdos curriculares

A bibliografia dos componentes curriculares do foi pensada e discutida pelo Núcleo Docente Estruturante (NDE). A elaboração da bibliografia foi realizada com extrema atenção e cuidado, que se empenhou em selecionar materiais que atendessem aos seguintes critérios:

- Relevância: os livros devem abordar os tópicos relevantes para a área de defesa cibernética.
- Atualidade: os livros devem estar atualizados com as últimas tendências da área.

- Qualidade: os livros devem ser de qualidade acadêmica e técnica.

A decisão de disponibilizar todos os livros em formato virtual é um reflexo do compromisso do curso com a acessibilidade e a inovação. Este formato digital oferece várias vantagens para os alunos:

- Acesso imediato: os alunos podem acessar os livros de qualquer lugar, a qualquer hora, removendo barreiras físicas que, muitas vezes, impedem o acesso a recursos educacionais de qualidade.
- Interatividade: a natureza digital dos livros permite uma interatividade maior, com recursos como busca de palavras-chave, anotações digitais e links para recursos adicionais, enriquecendo a experiência de aprendizagem.
- Atualização: os livros virtuais podem ser atualizados com mais facilidade e rapidez, garantindo que os alunos estejam sempre aprendendo com as informações mais atuais e relevantes.
- Sustentabilidade: a escolha por livros virtuais também reflete uma consciência ambiental, alinhando-se com práticas sustentáveis ao reduzir a necessidade de impressão de materiais.

A seleção da bibliografia referendada em ata pelos membros do NDE, aliada à decisão estratégica de adotar livros em formato virtual, reafirma o carater inovador e o zelo com a qualidade educacional, a acessibilidade dos alunos e a sustentabilidade.

2.5.5 Acessibilidade metodológica aos conteúdos curriculares

A Faculdade ACADI-TI está comprometida com a inclusão de todos os alunos, independentemente de suas características ou necessidades específicas. Para garantir o acesso e a participação de todos os alunos aos conteúdos curriculares do curso de Defesa Cibernética, a faculdade adota uma série de estratégias e recursos de acessibilidade metodológica, parte dos quais já foram explicado no contexto da acessibilidade quanto tratamos sobre a ESTRUTURA CURRICULAR.

Como já discutirmos, uma das estratégias adotadas pela ACADI-TI é a adaptação curricular. As adaptações curriculares incluem modificações no conteúdo, nos materiais didáticos, nas atividades ou nas avaliações. Exemplificando, um aluno com deficiência visual pode ter acesso a materiais didáticos em formato acessível, como Braille ou áudio.

A ACADI-TI também disponibiliza tecnologias assistivas aos alunos com deficiência. As tecnologias assistivas são ferramentas ajudam os alunos com deficiência a acessar e participar da aprendizagem. Em um caso prático, para um aluno com deficiência física disponibilizamos um computador com teclado e mouse adaptados.

Além disso, a ACADI-TI oferecerá serviços de apoio aos alunos com deficiência. Os serviços de apoio incluirão atendimento psicológico.

A ACADI-TI acredita que a acessibilidade metodológica é essencial para garantir que todos os alunos tenham a oportunidade de aprender e se desenvolver no curso de Defesa Cibernética. A faculdade, em fase de credenciamento, firma com a Sociedade e o Ministério da Educação o compromisso de implementação de estratégias e recursos de acessibilidade metodológica que permitam que todos os alunos tenham acesso e participem do processo de ensino-aprendizagem.

Detalhemos, para tornar mais claro o nosso compromisso. As estratégias de acessibilidade metodológica que serão usadas para beneficiar os alunos com deficiência no curso de Defesa Cibernética:

- Alunos com deficiência visual: os materiais didáticos em formato acessível, como Braille ou áudio, permitirão que os alunos com deficiência visual tenham acesso ao conteúdo das disciplinas curriculares. As tecnologias assistivas, como leitores de tela, também podem ajudar os alunos com deficiência visual a acessar e participar da aprendizagem.
- Alunos com deficiência física: as tecnologias assistivas, como computadores com teclado e mouse adaptados, ajudarão os alunos com deficiência física a realizar as atividades e avaliações das disciplinas curriculares.
- Alunos com deficiência auditiva: as legendas e as transcrições das aulas ajudarão os alunos com deficiência auditiva a acompanhar as atividades e avaliações das disciplinas curriculares.

A acessibilidade metodológica é um processo contínuo, que requer um compromisso da faculdade com a inclusão de todos os alunos. A ACADI-TI está comprometida com a avaliação periódica das estratégias e recursos de acessibilidade metodológica utilizados, para garantir que todos os alunos tenham a oportunidade de aprender e se desenvolver no curso de Defesa Cibernética. Tais avaliações serão incluídas no projeto de Avaliação da CPA

2.5.6 Abordagem de conteúdos relacionados à educação ambiental.

A Educação Ambiental (EA) é um processo de aprendizagem que visa a conscientização e a sensibilização das pessoas para a importância da conservação do meio ambiente. A EA tem um papel fundamental na formação de profissionais de Tecnologia, pois os capacita para compreenderem os impactos ambientais das tecnologias da informação e para adotarem práticas sustentáveis no exercício de suas atividades profissionais. Sabemos que hoje, nesta área, há pouca discussão ou conscientização das questões ambientais. Por isso, torna-se mais urgentes termos clareza e abordar esse tema em nossa matriz curricular, visto que estamos trabalhando num curso que é o estado da arte em Defesa Cibernética.

A matriz curricular do curso de Defesa Cibernética da Faculdade ACADI-TI, muito além da obrigação trazida pela Resolução CNE/CP nº 2, de 15 de junho de 2012 – que estabelece as Diretrizes Curriculares Nacionais para a Educação Ambiental – contempla o conteúdo de EA em diversas disciplinas, incluindo:

- Introdução à Redes de Computadores: aborda os impactos ambientais do uso de redes de computadores, como o consumo de energia e a geração de emissões de gases de efeito estufa.
- Fundamentos de Sistemas Operacionais: aborda as melhores práticas para o uso eficiente de recursos computacionais, como a otimização de processos e a redução do uso de memória.
- Introdução à Segurança Cibernética: aborda os riscos ambientais associados ao uso de tecnologias da informação, como o uso de dados pessoais para fins de marketing ou o uso de tecnologias da informação para controlar sistemas críticos de infraestrutura.
- Fundamentos de Dados para Segurança Cibernética: aborda as aplicações de tecnologias da informação para a análise de dados ambientais, como o uso de técnicas de inteligência artificial para detectar mudanças climáticas ou o uso de técnicas de análise de big data para monitorar a qualidade do ar.
- Fundamentos de Virtualização e Computação em Nuvem: aborda as melhores práticas para o uso sustentável de recursos computacionais em nuvem, como o uso de máquinas virtuais de menor tamanho e o uso de recursos compartilhados.

A abordagem do conteúdo de EA nessas disciplinas será contextualizada e relevante para a formação dos alunos em T.I. Os professores serão preparados dentro do Programa de

qualificação docente para discutir esses temas de forma crítica e reflexiva, incentivando os alunos a pensar sobre o papel da tecnologia na proteção do meio ambiente.

A abordagem do conteúdo de EA nas disciplinas do curso de defesa cibernética será contínua e progressiva, de modo que os alunos possam desenvolver uma compreensão cada vez mais aprofundada sobre o papel da tecnologia na proteção do meio ambiente.

A ACADI-TI formará profissionais de defesa cibernética que sejam conscientes e responsáveis com o meio ambiente. A inclusão do conteúdo de EA na matriz curricular do curso é uma demonstração desse compromisso.

2.5.7 Educação em direitos humanos

A segurança cibernética é um campo de atuação em constante evolução, que exige dos profissionais da área um conhecimento profundo das tecnologias e das ameaças existentes. No entanto, além dos conhecimentos técnicos, os profissionais de segurança cibernética também devem ter um entendimento claro dos princípios e valores que devem orientar suas ações.

Nesse sentido, a abordagem da temática de direitos humanos na matriz curricular do curso de Defesa Cibernética da Faculdade ACADI-TI, muito além de uma obrigação trazida pela Resolução CNE/CP nº 1, de 30 de maio de 2012 – que estabelece Diretrizes Nacionais para a Educação em Direitos Humanos – é importante para garantir que os profissionais formados pela instituição sejam capazes de proteger os direitos humanos na prática.

A abordagem da temática de direitos humanos na matriz curricular da ACADI-TI ocorre de forma direta e indireta.

Diretamente, o tema é abordado na disciplina "Ética, moral e direitos humanos", ofertada no segundo semestre, que tem como objetivo discutir os fundamentos da ética, da moral e dos direitos humanos, bem como sua aplicação à segurança cibernética. A disciplina aborda temas como a privacidade, a liberdade de expressão, a não discriminação e a proteção dos dados pessoais.

Ao estudarem essa disciplina, os alunos da ACADI-TI têm a oportunidade de refletir sobre os conceitos de direitos humanos e sua importância na sociedade. Eles também aprendem sobre as implicações éticas da segurança cibernética e como os profissionais da área devem agir de forma responsável e ética.

Indiretamente, o tema de direitos humanos é abordado em outras disciplinas da matriz curricular, como:

- Introdução à segurança cibernética: a disciplina aborda os princípios básicos da segurança cibernética, incluindo a importância da proteção dos direitos humanos.
- Administração segura de sistemas Linux e Windows: as disciplinas abordam os conceitos de segurança de sistemas operacionais, incluindo a proteção dos dados pessoais e a privacidade dos usuários.
- Auditoria e avaliações de segurança: a disciplina aborda os processos de auditoria e avaliação de segurança, incluindo a verificação do cumprimento dos direitos humanos.
- Inteligência de ameaças cibernéticas: a disciplina aborda as técnicas de identificação e análise de ameaças cibernéticas, incluindo a identificação de ameaças que possam violar os direitos humanos.

Ao estudarem essas disciplinas, os alunos da ACADI-TI aprendem sobre as tecnologias e as ameaças cibernéticas, bem como sobre as medidas que podem ser tomadas para proteger os direitos humanos. Eles também desenvolvem as habilidades necessárias para identificar e avaliar as ameaças que podem violar os direitos humanos.

A abordagem do tema de direitos humanos na matriz curricular do curso de Defesa Cibernética da Faculdade ACADI-TI é um passo importante para garantir que os profissionais da área sejam capazes de proteger os direitos humanos na prática. Ao estudarem essa temática, os alunos da ACADI-TI desenvolvem um entendimento claro dos princípios e valores que devem orientar suas ações, bem como as habilidades necessárias para identificar e avaliar as ameaças que podem violar os direitos humanos.

2.5.8 Educação das relações étnico-raciais, africana e indígena

A inclusão da educação étnico-racial, com ênfase na história e cultura africana e indígena, é essencial na formação dos profissionais de segurança cibernética. Esta abordagem promove uma compreensão mais profunda e respeitosa acerca das diversidades culturais, contribuindo para o desenvolvimento de uma perspectiva mais inclusiva na sociedade. A importância dessa temática é reforçada pela Lei nº 10.639/2003, que modifica a Lei de Diretrizes e Bases da Educação Nacional (LDB), Lei nº 9.394/1996. Esta legislação torna obrigatória a inclusão de conteúdos relacionados à "História e Cultura Afro-Brasileira e Africana" nos currículos escolares. Tal inclusão é fundamental para que futuros profissionais

em todas as áreas, inclusive na segurança cibernética, estejam mais conscientes e preparados para atuar em uma sociedade diversificada e multicultural.

A abordagem da temática de Educação das relações étnico-raciais, africana e indígena na matriz curricular do curso de Defesa Cibernética, da Faculdade ACADI-TI, ocorre de forma direta e indireta.

Diretamente, o tema é abordado na disciplina "Educação para relações Étnico-Raciais e Sociodiversidade", que tem como objetivo discutir a história e a cultura dos povos indígenas e africanos no Brasil. A disciplina aborda temas como a escravidão, a resistência cultural e a luta por direitos.

Ao estudarem essa disciplina, os alunos da ACADI-TI têm a oportunidade de conhecer a história e a cultura dos povos indígenas e africanos, bem como as contribuições que eles deram para a formação da sociedade brasileira. Eles também desenvolvem uma compreensão crítica sobre o racismo e a discriminação.

Indiretamente, o tema de Educação das relações étnico-raciais, africana e indígena é abordado em outras disciplinas da matriz curricular, como:

- Introdução à segurança cibernética: a disciplina aborda os princípios básicos da segurança cibernética, incluindo a importância da inclusão e da diversidade.
- Administração segura de sistemas Linux e Windows: as disciplinas abordam os conceitos de segurança de sistemas operacionais, incluindo a proteção dos dados pessoais e a privacidade dos usuários.
- Inteligência de ameaças cibernéticas: a disciplina aborda as técnicas de identificação e análise de ameaças cibernéticas, incluindo a identificação de ameaças que possam ser motivadas por racismo ou discriminação.

Ao estudarem essas disciplinas, os alunos da ACADI-TI aprendem sobre as tecnologias e as ameaças cibernéticas, bem como sobre as medidas que podem ser tomadas para promover a inclusão e a diversidade. Eles também desenvolvem as habilidades necessárias para identificar e avaliar as ameaças que possam ser motivadas por racismo ou discriminação.

A abordagem da temática de Educação das relações étnico-raciais, africana e indígena na matriz curricular do curso de Defesa Cibernética da Faculdade Acadi-TI é importante para garantir que os profissionais da área sejam capazes de promover a inclusão e a diversidade na sociedade. Ao estudarem essa temática, os alunos da Acadi-TI desenvolvem uma compreensão

crítica sobre o racismo e a discriminação, bem como as habilidades necessárias para identificar e avaliar as ameaças que possam ser motivadas por esses fenômenos.

2.5.9 Diferenciação do curso dentro da área profissional.

No mercado de trabalho atual, cada vez mais competitivo, é fundamental que os profissionais se diferenciem para se destacarem. Isso é especialmente importante para profissionais de áreas emergentes, como a segurança cibernética.

A proposta do curso de Defesa Cibernética da Faculdade ACADI-TI se destaca da do mercado por oferecer uma formação abrangente e atualizada, que prepara os alunos para atuarem em diversas áreas da segurança cibernética.

A matriz curricular do curso inclui disciplinas obrigatórias que cobrem um amplo espectro de tópicos, desde os fundamentos da segurança da informação até técnicas avançadas de defesa cibernética e disciplinas optativa para que o aluno se aprofunde aquelas que ele tiver maior aptidão. Além disso, o curso oferece disciplinas específicas que prepara os alunos para atuarem em áreas emergentes da segurança cibernética, como segurança de aplicações móveis, IoT e infraestrutura crítica.

Essas diferenciações tornam o curso de Defesa Cibernética da ACADI-TI uma opção atraente para os alunos que buscam uma formação profissional que os prepare para atuarem nessa área promissora. Algumas das principais diferenciações do curso da ACADI-TI são:

- Educação para relações Étnico-Raciais e Sociodiversidade: esta disciplina é importante para preparar os alunos para atuarem em um mercado de trabalho cada vez mais diverso e inclusivo.
- Disciplinas que tratam da segurança Cibernética para aplicações móveis: essas disciplinas são importantes para preparar os alunos para atuarem na crescente área de segurança de aplicações móveis.
- Segurança Cibernética para IoT: essas disciplinas são importante para preparar os alunos para atuarem na crescente área de segurança da Internet das Coisas.
- Disciplinas que tratam da Segurança Cibernética para infraestrutura crítica: essas disciplinas são importantes para preparar os alunos para atuarem na área de segurança de infraestruturas críticas, como sistemas de energia, transporte e comunicação.

Essas disciplinas específicas oferecem aos alunos conhecimentos e habilidades que não são encontrados em outros cursos de Defesa Cibernética. Isso os torna mais competitivos no mercado de trabalho, pois lhes permite atender às necessidades específicas das empresas e organizações.

2.5.10 Incentivo ao contato com conhecimento recente e inovador.

O conhecimento recente e inovador ajudam os alunos a se preparar para o mercado de trabalho, que está cada vez mais exigente em relação às habilidades e conhecimentos dos profissionais de defesa cibernética. Além disso, o conhecimento recente e inovador ajudam os alunos a entender as últimas tendências e tecnologias em defesa cibernética, o que é essencial para que eles possam desenvolver soluções para proteger os sistemas e dados críticos.

Para incentivar o contato com conhecimento recente e inovador no curso de Tecnologia em Defesa Cibernética, a Faculdade ACADI-TI adota uma série de estratégias, como:

- Conteúdos curriculares atualizados: Os conteúdos curriculares do curso devem abordar as últimas tendências e tecnologias em defesa cibernética. Isso é feito por meio de parcerias com empresas e organizações do setor, participação de especialistas de renome, e pesquisa acadêmica.
- Atividades extracurriculares: As atividades extracurriculares são uma excelente forma de os alunos se manterem atualizados com as últimas tendências. O curso de Defesa Cibernética oferecerá palestras, workshops, e eventos culturais sobre temas relacionados à defesa cibernética.
- Incentivo à pesquisa: A pesquisa é uma forma importante de os alunos se envolverem com conhecimento recente e inovador. A Faculdade ACADI-TI oferecerá, dentro do seu programa de iniciação cientifica, bolsas de estudo, laboratórios de pesquisa, e eventos acadêmicos para incentivar a pesquisa entre alunos e professores.

A implementação dessas estratégias ajudara a garantir que os alunos do curso de Tecnologia em Defesa Cibernética tenham acesso ao conhecimento mais recente e inovador nessa área.

No caso da matriz curricular apresentada neste PPC, é possível identificar algumas oportunidades de contato com conhecimento recente e inovador. Exemplificando, as disciplinas de "Design Thinking e Inovação em Cibersegurança", "Inteligência Artificial Aplicada à

Segurança Cibernética", e "Fundamentos de Virtualização e Computação em Nuvem" abordam conceitos e tecnologias que são essenciais para a defesa cibernética moderna. Além disso, a disciplina "Digital Forense em Defesa Cibernética" oferece oportunidades para os alunos participarem de projetos de pesquisa sobre as últimas técnicas de auditoria e avaliação de segurança.

2.6 METODOLOGIA

Para o sucesso do curso, em fase de autoriza, e da Faculdade ACADI-TI em fase de credenciamento é fundamental que curso de Defesa Cibernética ofereça uma metodologia de ensino-aprendizagem inovadora, que seja capaz de atender às necessidades dos alunos e do mercado de trabalho. É nesta metodologia que está o secreto do curso.

A metodologia proposta para o curso de Defesa Cibernética da Faculdade ACADI-TI é baseada em quatro pilares:

I. **Aprendizagem prática**: O curso é prático, com atividades que permitam aos alunos aplicar os conhecimentos adquiridos nas aulas.
II. **Gamificação**: O uso de gamificação ajuda o aprendizado mais divertido e envolvente.
III. **Recursos de interação**: Os recursos de interação, como fóruns, chats e videoconferências, ajudará os alunos a se conectarem uns com os outros e com os professores.
IV. **Trabalho em equipe**: O trabalho em equipe ajudará os alunos a desenvolverem habilidades de colaboração e resolução de problemas.

Vamos com maior atenção apresentar esses pilares

- Aprendizagem prática

A aprendizagem prática é uma abordagem pedagógica que enfatiza a aplicação dos conhecimentos adquiridos em situações reais. Essa abordagem é importante para o curso de defesa cibernética, pois permite aos alunos desenvolverem as habilidades necessárias para lidar com problemas reais de segurança cibernética.

A aprendizagem prática se realizará por meio de atividades como:

- Exercícios: Exercícios que permitem aos alunos aplicar os conceitos aprendidos.

- Projetos: Projetos que permitem aos alunos aplicar os conhecimentos adquiridos em um contexto real.
- Jogos: Jogos que podem ajudar os alunos a aprender de forma divertida e envolvente.

Os jogos são uma forma de aprendizagem prática particularmente interessante para o curso de defesa cibernética, pois permitem aos alunos simular situações reais de ataques cibernéticos. Os jogos podem ser usados para ensinar conceitos, habilidades e estratégias de defesa cibernética.

- Gamificação

A gamificação é o uso de elementos de jogos em contextos não-jogos. Essa abordagem será usada para tornar o aprendizado mais divertido e envolvente.

A gamificação será feita de diversas maneiras, como:

- Atribuição de pontos: Os alunos recebem pontos por concluir atividades ou atingir metas.
- Níveis: Os alunos avançam de nível conforme completam atividades.
- Recompensas: Os alunos recebem recompensas, como badges ou avatares, por concluir atividades.

A gamificação é usada para motivar os alunos a aprender, aumentar a participação nas atividades e promover o senso de colaboração.

- Recursos de interação

Os recursos de interação são ferramentas que permitem aos alunos se conectarem uns com os outros e com os professores. Esses recursos são importantes para o curso de defesa cibernética, pois podem ajudar os alunos a compartilhar suas ideias e a aprender uns com os outros.

Os recursos de interação são usados para:

- Fóruns: Os alunos usam fóruns para discutir o conteúdo das aulas e compartilhar suas ideias.
- Chats: Os alunos usam chats para conversar com os professores e com os colegas de turma.
- Videoconferências: Os alunos usam videoconferências para assistir a palestras e participar de debates.

Os recursos de interação são usados para promover a colaboração entre os alunos, o desenvolvimento de habilidades de comunicação e a construção de uma comunidade de aprendizagem.

- Trabalho em equipe

O trabalho em equipe é uma habilidade importante para profissionais da área de tecnologia e tanto mais para os de segurança cibernética. Essa habilidade é desenvolvida por meio de atividades que incentivem os alunos a trabalharem juntos.

O trabalho em equipe será incentivado de diversas maneiras, como:

- Atribuição de projetos em grupo: Os alunos podem trabalhar em grupo para concluir projetos.
- Formação de grupos de estudo: Os alunos podem formar grupos de estudo para se ajudarem a aprender.
- Atividades de colaboração: As atividades de colaboração podem ser usadas para promover a interação entre os alunos.

O trabalho em equipe será usado para desenvolver habilidades de comunicação, colaboração, resolução de problemas e gestão de projetos.

A metodologia proposta para o curso de defesa cibernética da Faculdade ACADI-TI é inovadora, pois combina elementos de diferentes abordagens pedagógicas. Essa metodologia é voltada para alunos com pouca formação acadêmica e com lacunas de formação no ensino médio. Além disso, é envolvente e motivadora, para garantir que os alunos estejam engajados no curso e ao mesmo tempo aprendendo.

2.6.1 Atendimento ao desenvolvimento de conteúdos

A matriz curricular apresentada é composta por 2080 horas de carga horária, distribuídas em cinco semestres. Os conteúdos curriculares estão organizados em módulos, cada um com um tema específico. O atendimento ao desenvolvimento de conteúdos curriculares a partir desta matriz é realizado de acordo com a metodologia proposta neste PPC. Essa metodologia é baseada nos seguintes pilares. A seguir, vamos apresentada uma descrição de como cada pilar é aplicado no atendimento ao desenvolvimento de conteúdos curriculares:

Aprendizagem prática

A aprendizagem prática é aplicada por meio de atividades como:

- Exercícios: Exercícios que permitem aos alunos aplicar os conceitos aprendidos.
- Projetos: Projetos que permitem aos alunos aplicar os conhecimentos adquiridos em um contexto real.
- Jogos: Jogos que podem ajudar os alunos a aprender de forma divertida e envolvente.

Dando contexto prático, no módulo sobre segurança de redes, os alunos podem realizar um projeto prático em que eles teriam que proteger uma rede de computadores de ataques virtuais.

Gamificação

A gamificação é aplicada por meio de elementos de jogos, como:

- Atribuição de pontos: Os alunos podem receber pontos por concluir atividades ou atingir metas.
- Níveis: Os alunos podem avançar de nível conforme completam atividades.
- Recompensas: Os alunos podem receber recompensas, como badges ou avatares, por concluir atividades.

Exemplificando, no módulo sobre criptografia, os alunos podem jogar um jogo de tabuleiro em que eles teriam que decifrar mensagens criptografadas.

Recursos de interação

Os recursos de interação são usados para:

- Fóruns: Os alunos podem usar fóruns para discutir o conteúdo das aulas e compartilhar suas ideias.
- Chats: Os alunos podem usar chats para conversar com os professores e com os colegas de turma.
- Videoconferências: Os alunos podem usar videoconferências para assistir a palestras e participar de debates.

Na prática, no módulo sobre forense digital, os alunos podem participar de um fórum em que eles discutiriam um caso real de crime cibernético.

Trabalho em equipe

O trabalho em equipe é incentivado por meio de atividades como:

- Atribuição de projetos em grupo: Os alunos podem trabalhar em grupo para concluir projetos.

- Formação de grupos de estudo: Os alunos podem formar grupos de estudo para se ajudarem a aprender.
- Atividades de colaboração: As atividades de colaboração podem ser usadas para promover a interação entre os alunos.

Neste caso, no módulo sobre ética, os alunos podem trabalhar em grupo para desenvolver um código de ética para profissionais de defesa cibernética.

A aplicação da metodologia proposta garante que os alunos desenvolvam as habilidades e conhecimentos necessários para atuar na área de defesa cibernética. As atividades práticas permitem aos alunos aplicar os conhecimentos adquiridos em situações reais, a gamificação torna o aprendizado mais divertido e envolvente, os recursos de interação promovem a colaboração entre os alunos e o trabalho em equipe desenvolve habilidades essenciais para profissionais de defesa cibernética.

2.6.2 Estratégias de aprendizagem

A estratégia de aprendizagem é o plano que o professor usa para organizar o ensino e a aprendizagem. Ela deve ser baseada nos objetivos de aprendizagem, no conteúdo a ser ensinado e nas características dos alunos.

A estratégia de aprendizagem proposta para o curso de defesa cibernética da Faculdade ACADI-TI é baseada na metodologia que foi apresentada neste texto páginas atrás. Essa metodologia é baseada nos seguintes pilares, como estudamos:

- Aprendizagem prática: O curso é prático, com atividades que permitam aos alunos aplicar os conhecimentos adquiridos nas aulas.
- Gamificação: O uso de gamificação ajuda tornar o aprendizado mais divertido e envolvente.
- Recursos de interação: Os recursos de interação, como fóruns, chats e videoconferências, ajudam os alunos a se conectarem uns com os outros e com os professores.
- Trabalho em equipe: O trabalho em equipe ajuda os alunos a desenvolverem habilidades de colaboração e resolução de problemas.

A estratégia de aprendizagem é organizada em torno desses pilares, e as atividades e recursos são selecionados de acordo com cada pilar.

Para ilustra que o atende ao pilar da aprendizagem prática, o professor pode usar atividades como exercícios, projetos e jogos. Para atender ao pilar da gamificação, o professor pode usar elementos de jogos, como atribuição de pontos, níveis e recompensas. Para atender ao pilar dos recursos de interação, o professor pode usar fóruns, chats e videoconferências. Para atender ao pilar do trabalho em equipe, o professor pode atribuir projetos em grupo ou incentivar a formação de grupos de estudo.

A estratégia de aprendizagem é flexível e pode ser adaptada de acordo com as necessidades dos alunos e do curso. Como for o caso, se os alunos têm pouco conhecimento prévio sobre o assunto, o professor pode dedicar mais tempo às atividades práticas e à gamificação. Se os alunos são motivados por desafios, o professor pode usar projetos mais complexos e atividades de resolução de problemas.

A estratégia de aprendizagem proposta é eficaz para promover a aprendizagem dos alunos do curso de Defesa Cibernética. Ela permite que os alunos desenvolvam as habilidades e conhecimentos necessários para atuar na área, de forma divertida e envolvente.

Como ilustração, as atividades e recursos serão usados para atender aos pilares da estratégia de aprendizagem:

- Aprendizagem prática:
    - Exercícios: Os alunos podem realizar exercícios para aplicar os conceitos aprendidos.
    - Projetos: Os alunos podem trabalhar em projetos para aplicar os conhecimentos adquiridos em um contexto real.
    - Jogos: Os alunos podem jogar jogos para aprender de forma divertida e envolvente.

  Exercícios para aprender defesa cibernética
- Gamificação:
    - Atribuição de pontos: Os alunos podem receber pontos por concluir atividades ou atingir metas.
    - Níveis: Os alunos podem avançar de nível conforme completam atividades.
    - Recompensas: Os alunos podem receber recompensas, como badges ou avatares, por concluir atividades.
- Recursos de interação:

- Fóruns: Os alunos podem usar fóruns para discutir o conteúdo das aulas e compartilhar suas ideias.
- Chats: Os alunos podem usar chats para conversar com os professores e com os colegas de turma.
- Videoconferências: Os alunos podem usar videoconferências para assistir a palestras e participar de debates.

- Trabalho em equipe:
  - Atribuição de projetos em grupo: Os alunos podem trabalhar em grupo para concluir projetos.
  - Formação de grupos de estudo: Os alunos podem formar grupos de estudo para se ajudarem a aprender.
  - Atividades de colaboração: As atividades de colaboração podem ser usadas para promover a interação entre os alunos.

A metodologia prevê estratégias de aprendizagem que sejam adequadas ao perfil dos alunos e aos objetivos do curso acompanhamento das atividades

2.6.3 Acessibilidade metodológica da Metodologia

A acessibilidade metodológica é um princípio importante para o ensino-aprendizagem. Ela garante que todos os alunos, independentemente de suas habilidades ou necessidades, tenham acesso ao conhecimento e ao desenvolvimento de habilidades. Já tratamos noutros contextos páginas atrás abordagem específica da acessibilidade metodológica. A abordagem aqui não será diferente daquela que já falamos por duas ocasiões. Porém neste caso o recorte que queremos dar é como trabalharemos a acessibilidade no contexto da metodologia. Reforçamos que a metodologia adota pelo curso de Defesa Cibernética é baseada nos seguintes pilares:

- Aprendizagem prática: A aprendizagem prática permite aos alunos desenvolver habilidades e conhecimentos de forma concreta e aplicável ao mundo real. Isso é importante para alunos com diferentes habilidades, pois pode ser adaptado de acordo com as necessidades individuais.
- Gamificação: A gamificação pode tornar o aprendizado mais divertido e envolvente, o que pode motivar alunos com diferentes interesses e habilidades.

- Recursos de interação: Os recursos de interação permitem aos alunos se conectarem uns com os outros e com os professores, o que pode ajudar alunos com dificuldade de aprendizagem ou isolamento social.
- Trabalho em equipe: O trabalho em equipe pode ajudar alunos com diferentes habilidades a colaborar e aprender uns com os outros.

A metodologia proposta é flexível e pode ser adaptada de acordo com as necessidades dos alunos e do curso. Se um aluno, por exemplo, tem dificuldade de leitura, o professor pode fornecer materiais em áudio ou vídeo. Se um aluno tem dificuldade de comunicação, o professor pode usar recursos de tecnologia assistiva.

A acessibilidade metodológica é importante para garantir que todos os alunos tenham a oportunidade de aprender e se desenvolver. A metodologia proposta para o curso de defesa cibernética da Faculdade ACADI-TI é acessível metodologicamente e pode ajudar a garantir que todos os alunos tenham sucesso no curso.

Como ilustração de como a metodologia proposta pode ser adaptada para atender às necessidades de alunos com diferentes habilidades:

- Alunos com dificuldade de leitura: O professor pode fornecer materiais em áudio ou vídeo.
- Alunos com dificuldade de comunicação: O professor pode usar recursos de tecnologia assistiva, como um sintetizador de voz ou um intérprete de língua de sinais.
- Alunos com dificuldade de aprendizagem: O professor pode usar atividades de aprendizagem diferenciadas, como atividades de revisão ou atividades de reforço.
- Alunos com isolamento social: O professor pode incentivar a interação entre os alunos por meio de atividades de colaboração ou de discussão em grupo.

O professor deve trabalhar em conjunto com os alunos para identificar suas necessidades e adaptar a metodologia de acordo.

2.6.4 Práticas pedagógicas que integram teoria e prática

A integração da teoria e da prática é um princípio fundamental para o ensino-aprendizagem no curso de Defesa Cibernética da Faculdade ACADI-TI. Essa integração é essencial para que os alunos desenvolvam as habilidades e conhecimentos necessários para atuar na área, que é altamente dinâmica e complexa.

No curso de defesa cibernética da Faculdade ACADI-TI, diversas práticas pedagógicas são utilizadas para integrar teoria e prática. Alguns exemplos incluem:

- **Aprendizagem baseada em problemas**: Os alunos são apresentados a problemas reais do mundo da defesa cibernética e devem usar seus conhecimentos para resolvê-los. Por exemplo, os alunos podem ser desafiados a desenvolver um plano de resposta a incidentes de segurança cibernética ou a investigar um ataque cibernético.
- **Aprendizado por projetos**: Os alunos trabalham em projetos que lhes permitem aplicar seus conhecimentos em um contexto real. Por exemplo, os alunos podem ser divididos em equipes para desenvolver um sistema de segurança cibernética para uma empresa ou organização.
- **Aprendizado experimental**: Os alunos realizam experimentos para testar teorias e conceitos. Para ilustrar, os alunos realizar um experimento para testar a eficácia de um algoritmo de criptografia ou para avaliar a vulnerabilidade de um sistema de segurança cibernética.
- **Visitas a campo**: Os alunos visitam locais reais para aprender sobre conceitos e aplicações. Para citar um caso, os alunos podem visitar um centro de operações de segurança cibernética ou um laboratório de forense digital.

Benefícios da integração da teoria e da prática

A integração da teoria e da prática oferece diversos benefícios para os alunos do curso de defesa cibernética, incluindo:

- Melhor compreensão dos conceitos: Quando os alunos podem aplicar seus conhecimentos em um contexto real, eles têm uma melhor compreensão de como os conceitos funcionam.
- Desenvolvimento de habilidades: A prática permite aos alunos desenvolver habilidades concretas, como resolução de problemas, comunicação e colaboração.
- Maior motivação: Os alunos são mais motivados a aprender quando podem ver a relevância do que estão aprendendo.

Desafios da integração da teoria e da prática

A integração da teoria e da prática pode representar alguns desafios para os professores do curso de defesa cibernética, incluindo:

- Planificação: A planificação de atividades que integrem teoria e prática pode ser mais complexa.
- Recursos: Algumas atividades práticas podem exigir recursos que não estão disponíveis.
- Tempo: As atividades práticas podem levar mais tempo do que as atividades teóricas.

Apesar dos desafios, a integração da teoria e da prática é uma abordagem pedagógica eficaz que pode ajudar os alunos do curso de defesa cibernética a desenvolver habilidades e conhecimentos de forma significativa.

Em termos práticos, as atividades práticas no curso de defesa cibernética serão apresentados alguns exemplos de atividades práticas que podem ser utilizadas no curso de defesa cibernética da Faculdade ACADI-TI:

- Projeto: Desenvolvimento de um sistema de segurança cibernética para uma empresa ou organização. Os alunos seriam divididos em equipes para desenvolver um sistema de segurança cibernética que atenda às necessidades específicas de uma empresa ou organização. O projeto seria avaliado com base na sua eficácia, viabilidade e robustez.
- Aprendizagem baseada em problemas: Resposta a incidentes de segurança cibernética. Os alunos seriam apresentados a um problema real de resposta a incidentes de segurança cibernética e teriam que desenvolver um plano para resolvê-lo. O plano seria avaliado com base na sua eficácia e eficiência.
- Aprendizado experimental: Teste de algoritmos de criptografia. Os alunos realizariam experimentos para testar a eficácia de diferentes algoritmos de criptografia. Os resultados dos experimentos seriam analisados para determinar qual algoritmo é mais adequado para uma determinada aplicação.
- Visita a campo: Centro de operações de segurança cibernética. Os alunos visitariam um centro de operações de segurança cibernética para aprender sobre as operações e os desafios da segurança cibernética em tempo real.

Essas são apenas algumas das atividades práticas serão utilizadas no curso de defesa cibernética. A escolha das atividades será feita de acordo com os objetivos de aprendizagem do curso e as características dos alunos.

2.6.5 Caráter inovador da metodologia e uso de recursos diferenciadas.

O curso de defesa cibernética da Faculdade ACADI-TI adota uma metodologia de ensino inovadora, que integra teoria e prática. Essa integração é essencial para que os alunos desenvolvam as habilidades e conhecimentos necessários para atuar na área de tecnologia, que é altamente dinâmica e complexa.

No contexto do ensino online, a integração da teoria e da prática é ainda mais importante, pois os alunos precisam ter oportunidades de aplicar os conceitos aprendidos em um contexto real. Esses recursos permitem que a aprendizagem dos alunos seja sólida e ele se preparem para atuar na área de defesa cibernética e não apenas para uma prova. Além disso, esses recursos contribuem para a permanência dos alunos no curso, pois os ajudam a se sentirem motivados e envolvidos no processo de aprendizagem.

Recursos diferenciados

Além do carater inovador já mencionados neste texto sob o título METODOLOGIa, o curso de Defesa Cibernética da Faculdade ACADI-TI utiliza outros recursos diferenciados para promover a aprendizagem dos alunos. Esses recursos incluem:

- Gamificação: A gamificação é uma abordagem pedagógica que utiliza elementos de jogos para tornar o aprendizado mais divertido e envolvente. No curso de defesa cibernética, a gamificação é utilizada para incentivar os alunos a participarem de atividades práticas e a cumprirem metas de aprendizagem.
- Avaliação formativa: A avaliação formativa é uma avaliação contínua que ocorre ao longo do processo de aprendizagem. Ela fornece feedback aos alunos sobre seu progresso e ajuda os professores a identificar dificuldades de aprendizagem. No curso de defesa cibernética, a avaliação formativa é utilizada para promover a aprendizagem reflexiva e a autoavaliação dos alunos.
- Feedback personalizado: Os alunos recebem feedback personalizado dos professores sobre seu trabalho. Esse feedback é direcionado às necessidades individuais dos alunos e ajuda-os a melhorar seu desempenho.
- Suporte ao aluno: O curso oferece suporte ao aluno por meio de diversos canais, como e -mail, chat e fóruns. Esse suporte ajuda os alunos a resolver problemas, tirar dúvidas e obter orientação.

Esses recursos contribuem para a efetividade da metodologia de ensino proposta e ajudam os alunos a desenvolver as habilidades e conhecimentos necessários para atuar na área de defesa cibernética.

2.7 ESTÁGIO CURRICULAR SUPERVISIONADO

O curso de Defesa Cibernética da Faculdade ACADI-TI não prevê estágio curricular supervisionado, portanto esse indicador Não Se Aplica (NSA). No entanto, a instituição acredita na importância da prática desde o início da carreira profissional de seus alunos. Por isso, contará um departamento que fará convênio com empresas de São José dos Campos e Vale do Paraíba para que os alunos tenham acesso a estágios profissionais. Além da inserção no mercado de trabalho, essa será uma das formas de avaliar sua proposta curricular.

2.8 ATIVIDADES COMPLEMENTARES

As atividades complementares são uma exigência curricular presente em muitos cursos de graduação. Essas atividades consistem em uma carga horária extraclasse que o estudante deve cumprir ao longo do curso, a fim de complementar sua formação acadêmica. No entanto, no caso do curso de Defesa Cibernética da Faculdade ACADI-TI, não há a previsão de atividades complementares neste Projeto Pedagógico de Curso. Portanto esse indicador Não Se Aplica (NSA)

2.9 TRABALHO DE CONCLUSÃO DE CURSO (TCC)

O curso de Tecnologia em Defesa Cibernética é uma formação de nível superior que tem como objetivo proporcionar aos estudantes uma base sólida na sua formação em tecnologia, capacitando-os para atuar em diversas áreas de defesa cibernética. Entretanto, diferentemente de outros cursos de graduação, não há previsão na matriz curricular do trabalho de conclusão de curso (TCC) para este tecnólogo. Portanto esse indicador Não Se Aplica (NSA).

2.10 APOIO AO DISCENTE

A Faculdade ACADI-TI tem como premissa a adoção de políticas institucionais que promovam o apoio efetivo ao discente, garantindo condições adequadas para seu ingresso e permanência no ensino superior.

Desde o processo seletivo, a instituição adotará medidas para identificar e atender as demandas especiais dos candidatos, como no caso das Pessoas com Deficiência (PCDs). Dessa forma, são oferecidas formas de avaliação apropriadas para esses candidatos.

Ao ingressar no corpo discente da instituição, o aluno contará com uma série de ações que visam garantir sua permanência e sucesso acadêmico. Entre elas, destacam-se:

- Apoio financeiro: a Faculdade ACADI-TI oferecerá bolsas de estudo e financiamento estudantil para alunos de baixa renda.
- Apoio pedagógico: a instituição conta com uma equipe de professores qualificados e experientes, que estão disponíveis para auxiliar os alunos nos estudos.
- Apoio psicológico: a instituição oferecerá atendimento psicológico aos alunos que precisam de suporte emocional.
- Apoio extracurricular: a faculdade oferecerá atividades extracurriculares, como cursos, palestras e workshops, que contribuem para o desenvolvimento acadêmico e pessoal dos alunos.

No caso do curso de Defesa Cibernética, a Faculdade ACADI-TI oferecerá uma série de ações específicas para apoiar os alunos. Entre elas, destacam-se:

- Oferta de estágios profissional: a faculdade contará com uma rede de parceiros que oferecem estágios remunerados para os alunos do curso.
- Acompanhamento de carreira: a faculdade oferecerá orientação profissional aos alunos, para ajudá-los a desenvolver uma carreira de sucesso na área de tecnologia.
- Eventos e palestras: a faculdade realizará eventos e palestras com especialistas da área, para manter os alunos atualizados sobre as últimas tendências.

Essas ações são fundamentais para garantir que os alunos da Faculdade ACADI-TI tenham as melhores condições para ingressar e permanecer no ensino superior, e para se tornarem profissionais bem-sucedidos na área de Defesa Cibernética

2.10.1 Ações de acolhimento e permanência do estudante

O acolhimento do aluno se iniciará no primeiro dia de aula e seguirá durante os meses seguintes. Na primeira semana de aula, os alunos serão recepcionados pelo coordenador de curso e por representantes de alguns setores da instituição, que apresentarão os serviços que estão à disposição dos alunos e as principais informações institucionais. A primeira semana também será dedicada à integração entre os alunos calouros e veteranos. Considerando os números do Censo da Educação (2021), que nos demonstra a curva de evasão, de maneira geral, o primeiro semestre será acompanhado de maneira mais cuidadosa, para evitar processo de evasão e baixo aprendizado.

As ações de permanência, alinhadas às de acolhimento, vão no sentido de proporcionar o auxílio ao acadêmico. Com efeito, a Instituição se esmera em considerar os aspectos financeiros designados no sentido de promover o acesso e a permanência no ensino superior. Para isso, tem a intenção de participar de programas federais e estaduais de bolsas de estudos, iniciação científica e financiamentos (Prouni, UNIEDU, educa mais Brasil e FIES) e ainda manter o programa próprio de Bolsas Institucionais, e com convênio.

Preocupada com a integração dos alunos ao ensino superior e com sua permanência até a conclusão do curso, a Faculdade ACADI-TI desenvolveu o **Programa de Acolhimento e Permanência**, que está sob a supervisão da coordenação. O programa é essencial para garantir que os alunos tenham uma experiência positiva durante sua jornada acadêmica e consigam alcançar seus objetivos.

2.10.2 Acessibilidade metodológica e instrumental

A acessibilidade metodológica e instrumental será garantida aos alunos do curso de Defesa Cibernética, através de ações que ocorrem no âmbito institucional, norteadas pelo **Plano de Acessibilidade da instituição**.

A acessibilidade metodológica, qual diz resposto as metodologias e técnicas de aprendizagem, é priorizada da ACADI-TI por meio de adaptações curriculares de conteúdos programáticos. A Comunidade Acadêmica, em especial, os professores e tutores concebem o conhecimento, a avaliação e a inclusão educacional, promovendo processos de diversificação curricular, flexibilização do tempo e a utilização de recursos a fim de viabilizar a aprendizagem de estudantes com deficiência, sempre que se constata esta necessidade.

A acessibilidade instrumental se dá com o apoio de softwares (DOSVox, VLibras, Nvídea, Hand Talk, entre outros) que estão à disposição dos educandos nos equipamentos institucionais ou para serem instalados em dispositivos do educando a partir dos arquivos disponibilizados no site da instituição; e hardwares (teclado acessível, headset, entre outros) que estão à disposição dos educandos nos espaços da instituição (biblioteca e laboratório).

2.10.3 Monitoria para estudantes

A Faculdade ACADI-TI possui um **Programa Institucional de Monitoria Acadêmica**, que tem suas regras publicadas no Regulamento de monitoria.

O Programa Institucional de Monitoria Acadêmica Faculdade ACADI-TI tem como objetivo proporcionar ao aluno do curso de Defesa Cibernética a oportunidade de aprimorar seus conhecimentos em determinada disciplina, além de contribuir para a melhoria da qualidade do ensino. Por meio da monitoria, os alunos serão incentivados a participar de atividades de ensino, pesquisa e extensão, aprimorando sua formação acadêmica e profissional.

Processo seletivo:

A seleção dos monitores ocorrerá no início de cada semestre letivo. Serão avaliados critérios como desempenho acadêmico, habilidades e competências relacionadas à disciplina, além de disponibilidade de horários. O processo seletivo será conduzido por uma comissão formada pelo coordenador do curso, docentes da disciplina e representantes dos discentes.

Atividades da monitoria:

O aluno monitor será responsável por auxiliar o professor da disciplina em atividades como revisão de conteúdos, elaboração de exercícios e trabalhos, orientação de estudos dirigidos e realização de atividades práticas. O monitor deve estar disponível para atender os demais alunos, seja em horários previamente agendados ou em plantões de dúvidas.

Avaliação do desempenho:

Ao final de cada mês, o monitor apresentará um relatório de atividades desenvolvidas no período, incluindo o número de atendimentos realizados e a descrição das atividades desenvolvidas. Este relatório será avaliado pelo professor da disciplina e pelo coordenador do curso, que poderão sugerir ajustes ou melhorias no programa.

Benefícios aos monitores:

Os monitores selecionados receberão desconto na mensalidade do curso, de acordo com o número de horas dedicadas às atividades de monitoria. Além disso, a monitoria será uma atividade que pode ser incluída no currículo do aluno, enriquecendo sua formação acadêmica e profissional.

O Programa Institucional de Monitoria Acadêmica Faculdade ACADI-TI será uma iniciativa para aprimorar a formação dos alunos, incentivando a participação em atividades de ensino, pesquisa e extensão. Com a monitoria, os alunos têm a oportunidade de aprimorar seus conhecimentos em determinada disciplina, contribuindo para a melhoria da qualidade do ensino e para o sucesso acadêmico.

2.10.4 Programas de nivelamento

A Faculdade ACADI-TI, visando desenvolver as competências leitoras, de compreensão e interpretação de textos, bem como a habilidade de redigir de forma clara, coesa, coerente e objetiva, oferece os cursos de Português Instrumental destinados aos alunos dos cursos superiores da Instituição. Além do desenvolvimento das competências leitoras, a ACADI-TI oferece também curso de Matemática Básica, ensejando o aprimoramento do pensamento lógico, vital para as demais competências e habilidades. Há na IES um **Programa Institucional de Nivelamento.**

Por meio de ações que minimizem as lacunas de aprendizagem em relação aos conceitos básicos do programa de nivelamento tem como objetivo melhorar o desempenho e aproveitamento dos estudantes no transcorrer de sua formação acadêmica, de forma eficiente.

O programa será disponibilizado para os estudantes regularmente matriculados nos cursos de Graduação. O estudante deverá realizar a inscrição no programa, conforme calendário acadêmico e cronograma de oferta dos cursos no Ambiente Virtual de Aprendizagem – AVA.

Na fase de execução das ações de nivelamento, os estudantes deverão participar de um ou mais cursos de formação básica na modalidade a distância previamente planejada, conforme a área do curso de graduação indicado pela coordenação de curso:

- Curso de nivelamento em Informática;
- Curso de nivelamento em Matemática;
- Curso de nivelamento em português;

Os cursos possuem carga horária de 30 horas, são autoinstrucionais, possibilitando que o aluno tenha autonomia para gerenciar seus estudos e realizar diferentes trilhas de aprendizagem. Os cursos estão organizados por unidades de aprendizagem e possibilitam que o aluno tenha acesso a conteúdo atualizado, contextualizado e que respeite o seu ritmo e estilo de aprendizagem.

Na fase de avaliação diagnóstica, os estudantes serão acompanhados ao longo do curso de formação básica, por dois processos de avaliação diagnóstica:

- Avaliação inicial: antes de realizar as atividades do curso, o aluno realiza um teste com o objetivo de identificar o nível de conhecimento sobre as temáticas do curso.
- Avaliação final: ao final da realização das atividades do curso, o aluno realiza um teste com o objetivo de identificar os ganhos de conhecimento sobre as temáticas presentes no curso.

Os testes também permitem que o estudante autoanalise o seu conhecimento em determinadas temáticas do curso. O aluno que alcançar nota final 7,0 será considerado aprovado na disciplina de nivelamento.

Os dados comparativos entre a avaliação inicial e final darão subsídios para o estudante elaborar um plano de aprendizagem individual, visando à superação das dificuldades apresentadas.

Os dados gerais de desempenho dos alunos do curso darão subsídios para o planejamento de ações pedagógicas pela coordenação do curso, em conjunto com o Núcleo Docente Estruturante, para recuperar as defasagens apresentadas pelos alunos.

A avaliação do programa dar-se-á por meio de instrumentos que serão aplicados durante e após as atividades propostas no curso de nivelamento e possibilita um acompanhamento e monitoramento do desempenho dos alunos ao longo do curso de graduação:

- Acompanhamento do rendimento do estudante;
- Acompanhamento do rendimento da turma;
- Relatório de desempenho de cada estudante atendido;
- Acompanhamento do índice de evasão do curso;
- Instrumento de avaliação do programa respondido pelo estudante.

Para o acompanhamento e execução desse programa estão envolvidos a direção acadêmica, os Coordenadores dos Cursos e o Núcleo Docente Estruturante, e contará com o suporte técnico da Coordenação EaD.

2.10.5 Intermediação e acompanhamento de estágios não obrigatórios remunerados.

Os estágios não obrigatórios são intermediados e acompanhados pela coordenação do curso e pelo **Supervisor de Estágio**, sendo esta responsável pelo desenvolvimento de convênios com empresas de São José dos Campos e Vale do Paraíba para a oferta de oportunidades de estágio e emprego.

A divulgação das vagas de estágio e emprego para os estudantes da Faculdade ACADI-TI será realizada através do portal do aluno, na área de oportunidades.

Após o início das atividades de estágio, o **Serviço de Acompanhamento de Estágio** (SAE) fará o devido acompanhamento e controle dos termos de convênio, compromisso e plano de trabalho, para garantir que a Lei do Estágio seja cumprida em sua integralidade, resguardando os direitos do estagiário.

O estágio não curricular é opcional para o acadêmico e segue a Lei 11.788/08, para fins de formação prática nas áreas de atuação profissional.

2.10.6 Apoio psicopedagógico

A Faculdade ACADI-TI atende à legislação de proteção dos direitos da pessoa com transtorno do espectro autista, normatizado em Portaria. Há na instituição preocupação com os diferentes transtornos, para isso as ações decorrentes estão sob a responsabilidade do Núcleo de Apoio Psicopedagógico (NAP), os quais agem no sentido de promover, fortalecer e garantir a educação inclusiva, em seu sistema de ensino, propiciando o acesso à educação da pessoa portadora do transtorno de espectro autista, conforme previsto pela Lei n. 12.764/2012.

Em atendimento à Lei nº 12.764 de 27 de dezembro de 2012, Art. 3º, Inciso IV que prevê o acesso das Pessoas com Transtorno do Espectro Autista, à educação, a Faculdade ACADI-TI prevê em sua política de acessibilidade ações para o atendimento à pessoa com espectro autista, garantindo o ingresso e a sua permanência nos cursos de graduação. A Política de acessibilidade da instituição é coordenada pelo NAP em parceria com os demais setores da

instituição, integrando toda a comunidade acadêmica de forma a garantir o disposto no Art. 2º da referida lei, no que tange:

- Intersetorialidade: O atendimento à pessoa com espectro autista deve envolver diferentes setores da sociedade, como a educação, a saúde, a assistência social e a justiça.
- Participação da comunidade: As pessoas com espectro autista e suas famílias devem participar da formulação e implementação das políticas públicas voltadas para este público.
- Atenção integral às necessidades de saúde: As pessoas com espectro autista devem ter acesso a serviços de saúde de qualidade, que atendam às suas necessidades específicas.
- Atendimento educacional especializado: O atendimento educacional especializado é um serviço de educação especial que visa atender às necessidades específicas das pessoas com deficiência, transtornos globais do desenvolvimento e altas habilidades/superdotação.
- Inclusão: O atendimento educacional especializado deve ser realizado em ambiente inclusivo, ou seja, junto com os demais estudantes.

Sempre que constatada a necessidade de atendimento, a partir de solicitação do próprio educando, ou por indicação de outros membros do corpo social, são realizados atendimentos agendados com custeamento realizado pela instituição.

Essa prática possibilita a permanência de educandos, que sem este apoio não teriam condições de manter suas atividades escolares, visto que não é incomum em nosso país, que discentes abandonem seu curso superior por problemas de ordem pessoal, psicologicas ou profissional.

A partir dos atendimentos, é possível que o profissional identifique e contribua para a solução de dificuldades, que muitas vezes o educando tem condições de resolver sem apoio.

Algumas das ações específicas que a Faculdade ACADI-TI realiza para atender às necessidades dos estudantes com espectro autista incluem:

- Adaptações curriculares: A instituição oferece adaptações curriculares para os estudantes com espectro autista, de acordo com as suas necessidades específicas.

- Apoio psicopedagógico: A instituição oferece apoio psicopedagógico para os estudantes com espectro autista, com o objetivo de ajudá-los a desenvolver suas habilidades acadêmicas e sociais.
- Acompanhamento psicológico: A instituição oferece acompanhamento psicológico para os estudantes com espectro autista, com o objetivo de ajudá-los a lidar com as suas emoções e a desenvolver sua autonomia.
- Inclusão: A instituição promove a inclusão dos estudantes com espectro autista, garantindo que eles tenham acesso a todos os recursos e oportunidades oferecidas pela instituição.

A Faculdade ACADI-TI está comprometida em oferecer educação de qualidade para todos os estudantes, independentemente de suas necessidades especiais.

2.10.7 Centros acadêmicos e intercâmbios

A Faculdade ACADI-TI incentivará a participação dos alunos em centros acadêmicos e intercâmbios nacionais e internacionais. Acreditamos que essas experiências são essenciais para a formação completa dos profissionais de Defesa Cibernética.

Centros acadêmicos

Os centros acadêmicos serão organizações representativas dos alunos de um curso ou instituição de ensino. Eles desempenharão um importante papel na vida acadêmica, promovendo atividades extracurriculares, eventos e representando os interesses dos alunos junto à instituição e à sociedade.

A Faculdade ACADI-TI tem o projeto de constituir centros acadêmicos para os alunos do curso de Defesa Cibernética, e de outro curso que virem a serem constituídos com o credenciamento da Instituição. Esses centros serão responsáveis por organizar atividades extracurriculares, como palestras, workshops, competições e eventos culturais. Também representarão os interesses dos alunos junto à instituição e à sociedade. Há uma proposta de regulamento e estatuo que serão validados pelos alunos durante a constituição destas organizações.

Intercâmbios

Os intercâmbios são oportunidades de estudar ou trabalhar em outras regiões do Estado ou mesmo em outro país. Eles permitem aos alunos conhecer novas culturas, aprender novas línguas e expandir seus horizontes profissionais.

A Faculdade ACADI-TI tem o projeto, inclusive dotação orçamentária (cf PDI p. 167-172) de buscar intercâmbios com outras instituições de ensino e empresas de defesa cibernética nacionais e internacionais. Esses intercâmbios serão oferecidos aos alunos do curso com base em seu desempenho acadêmico e interesse na área.

Acreditamos que a participação em centros acadêmicos e intercâmbios seja uma oportunidade valiosa para os alunos do curso de Defesa Cibernética. Essas experiências contribuem para o desenvolvimento de habilidades e competências essenciais para o sucesso profissional na área de T.I, como:

- Capacidade de trabalhar em equipe
- Habilidade de liderança
- Comunicação interpessoal
- Adaptabilidade
- Resiliência

Os alunos que participam de centros acadêmicos ou intercâmbios também têm a oportunidade de construir uma rede de contatos profissionais, o que pode ser muito importante para o seu futuro.

2.10.8 Implementação de ações inovadoras no apoio ao estudante

A Cibersegurança ou Ciberdefesa é uma área de estudo relativamente nova e pouco explorada, muito embora extremamente estratégica nos países e organização. Ela exige um conhecimento profundo de tecnologias e técnicas de segurança cibernética. Como resultado, os estudantes de cursos de Defesa Cibernética enfrentam diversos desafios, como:

- Dificuldades de aprendizagem: o conteúdo dos cursos de defesa cibernética é complexo e desafiador, e pode ser difícil para os estudantes acompanharem o ritmo.
- Falta de experiência prática: a maioria dos cursos de defesa cibernética não oferece aos estudantes a oportunidade de aplicar os conhecimentos aprendidos em um ambiente real.

- Dificuldades de empregabilidade: o mercado de trabalho para profissionais de defesa cibernética é competitivo, e os estudantes precisam estar bem-preparados para se destacarem.

Em busca de superar esses desafios, a Faculdade ACADI-TI projeta em desenvolver diversas ações inovadoras de apoio ao aluno em cursos de Defesa Cibernética. Essas ações são importantes para garantir o sucesso acadêmico e profissional dos estudantes.

O apoio acadêmico é fundamental para ajudar os estudantes a desenvolverem as habilidades necessárias para a área de defesa cibernética. Essas habilidades incluem:

- Conhecimento técnico: os estudantes precisam ter um conhecimento profundo de tecnologias e técnicas de segurança cibernética.
- Habilidades analíticas: os estudantes precisam ser capazes de analisar dados e identificar ameaças cibernéticas.
- Habilidades de comunicação: os estudantes precisam ser capazes de comunicar suas ideias de forma clara e concisa.

As ações de apoio acadêmico incluem:

- Aulas invertidas: os conteúdos são disponibilizados antecipadamente, por meio de videoaulas, artigos, textos, etc., para que os alunos possam estudar no seu próprio ritmo. As aulas presenciais, então, são focadas na resolução de problemas, discussões, etc.
- Aprendizagem baseada em projetos: os alunos são convidados a desenvolver projetos reais, que tenham relevância para eles, para que possam aplicar os conhecimentos aprendidos.
- Aprendizagem por pares: os alunos são incentivados a interagir uns com os outros para que possam aprender uns com os outros.

O apoio pessoal também é importante para garantir o sucesso dos estudantes. Os desafios acadêmicos podem ser ainda mais difíceis de superar para estudantes que enfrentam questões pessoais, como dificuldades de aprendizagem, problemas de relacionamento, dificuldades financeiras, etc.

As ações de apoio pessoal incluem:

- Acompanhamento psicológico: os estudantes têm acesso a um serviço de acompanhamento psicológico, para que possam lidar com questões pessoais.

- Atendimento social: os estudantes têm acesso a um serviço de atendimento social, para que possam receber orientação sobre questões como moradia, alimentação, transporte, etc.

O apoio profissional é essencial para ajudar os estudantes a se preparar para o mercado de trabalho. O mercado de trabalho para profissionais de defesa cibernética é competitivo, e os estudantes precisam estar bem preparados para se destacarem.

As ações de apoio profissional incluem:

- Orientação profissional: os estudantes recebem orientação sobre como desenvolver suas habilidades profissionais e se preparar para o mercado de trabalho.
- Estágios: os estudantes são incentivados a realizar estágios em empresas ou organizações, para que possam adquirir experiência prática.

A Faculdade ACADI-TI, quando for credenciada e no curso de Defesa Cibernética for autorizado, oferecerá aos seus alunos diversas ações de apoio, com o objetivo de garantir o seu sucesso acadêmico e profissional. Essas ações incluem ações tradicionais, como aulas invertidas, aprendizagem baseada em projetos e orientação profissional, bem como ações inovadoras, como laboratórios de simulação cibernética, projetos de extensão em defesa cibernética e orientação profissional em defesa cibernética.

Acreditamos que essas ações de apoio contribuirão para o sucesso acadêmico e profissional dos alunos do curso de defesa cibernética da Faculdade ACADI-TI.

As ações de apoio ao aluno são essenciais para garantir o sucesso acadêmico e profissional dos estudantes de cursos de defesa cibernética. Essas ações devem ser abrangentes, abrangendo os aspectos acadêmico, pessoal e profissional.

2.11 GESTÃO DO CURSO E OS PROCESSOS DE AVALIAÇÃO INTERNA E EXTERNA

2.11.1 Utilização da autoavaliação institucional como base para o planejamento

A Faculdade ACADI-TI está comprometida com a qualidade da educação e entende que a avaliação é uma ferramenta essencial para o desenvolvimento e melhoria contínua dos seus cursos. Nesse contexto, a Comissão Própria de Avaliação (CPA) da faculdade realizará dentro

de seu Projeto de Avaliação Institucional avaliações internas dos cursos, com o objetivo de coletar informações sobre a percepção dos alunos, professores, egressos e demais stakeholders sobre o curso.

Os resultados dessas avaliações serão analisados pela CPA e apresentados à gestão do curso, que os utiliza como base para o planejamento de ações de melhoria. No caso do curso de Defesa Cibernética, os dados da avaliação da CPA serão utilizados para:

- Identificar as áreas de força e de melhoria do curso;
- Definir metas e objetivos para o desenvolvimento do curso;
- Desenvolver estratégias e ações para alcançar as metas e objetivos definidos;
- Avaliar o impacto das ações implementadas.

A análise dos dados da avaliação da CPA permitirá à gestão do curso de Defesa Cibernética tomar decisões mais informadas e eficazes para o desenvolvimento do curso. As ações de melhoria propostas serão baseadas nas necessidades reais dos alunos e do mercado de trabalho, garantindo que o curso ofereça uma formação de qualidade, alinhada às demandas da sociedade.

2.11.2 Resultados das avaliações externas

Além da avaliação da CPA, a gestão do curso de Defesa Cibernética da Faculdade ACADI-TI também utilizará as avaliações externas, como o Exame Nacional de Desempenho dos Estudantes (Enade), como insumos para o seu planejamento.

O Enade é um exame aplicado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) a todos os estudantes de graduação em um determinado período. O exame avalia o desempenho dos estudantes em relação aos conteúdos programáticos do curso e às competências e habilidades necessárias para o exercício da profissão.

Os resultados do Enade são utilizados para a avaliação dos cursos de graduação e das instituições de ensino superior. Também podem ser utilizados pelas instituições para o planejamento da gestão dos cursos.

No caso do curso de Defesa Cibernética da Faculdade ACADI-TI, os resultados do Enade serão utilizados para:

- Avaliar a qualidade da formação dos alunos do curso;
- Identificar áreas de melhoria do curso;

- Definir metas e objetivos para o desenvolvimento do curso;
- Desenvolver estratégias e ações para alcançar as metas e objetivos definidos;
- Avaliar o impacto das ações implementadas.

A análise dos resultados do Enade permitirá à gestão do curso de Defesa Cibernética tomar decisões mais informadas e eficazes para o desenvolvimento do curso. As ações de melhoria propostas serão baseadas nas necessidades reais dos alunos e do mercado de trabalho, garantindo que o curso ofereça uma formação de qualidade, alinhada às demandas da sociedade

2.11.3 Aprimoramento contínuo do planejamento do curso

A gestão do curso de Defesa Cibernética da Faculdade ACADI-TI é orientada por um **Plano de Gestão do curso**, que será construído coletivamente por professores e alunos, porém nesta primeira versão foi construído pelo NDE. O plano tem como objetivos estipular metas e objetivos a serem alcançados a curto, médio e longo prazo.

O Plano de Gestão do curso será reelaborado a partir da análise dos resultados das avaliações internas e externas, como a avaliação da CPA e o Enade. Também são consideradas as necessidades dos alunos, do mercado de trabalho e da sociedade.

O plano é dividido em três eixos principais:

- **Qualidade da formação**: Esse eixo busca garantir que o curso ofereça uma formação de qualidade, alinhada às demandas do mercado de trabalho e da sociedade.
- **Inserção no mercado de trabalho**: Esse eixo busca promover a inserção dos alunos no mercado de trabalho, por meio de atividades de formação prática, parcerias com empresas e organizações da área de cibersegurança, e divulgação da formação do curso.
- **Inovação e desenvolvimento**: Esse eixo busca promover a inovação e o desenvolvimento do curso, por meio da atualização do currículo, da oferta de atividades extracurriculares de formação prática, e da participação em projetos de pesquisa e extensão.

O plano será revisado anualmente, a fim de garantir que esteja alinhado às necessidades dos alunos, do mercado de trabalho e da sociedade.

As metas e objetivos são definidos no Plano de Gestão do curso de Defesa Cibernética:

- A curto prazo:

- Atualizar o currículo do curso para incluir novas tecnologias e tendências da área de cibersegurança;
- Oferecer atividades extracurriculares de formação prática, como workshops, palestras e hackathons;
- Fortalecer a relação entre o curso e o mercado de trabalho, por meio de parcerias com empresas e organizações da área de cibersegurança.

- A médio prazo:
  - Melhorar a qualidade do ensino, por meio de atividades de formação continuada para os professores;
  - Fortalecer a infraestrutura do curso, incluindo laboratórios de informática e equipamentos de última geração.
- A longo prazo:
  - Tornar o curso referência nacional na formação de profissionais de defesa cibernética;
  - Contribuir para o desenvolvimento da área de cibersegurança no Brasil.

O Plano de Gestão do curso é uma forma de garantir o desenvolvimento e a melhoria contínua do curso de Defesa Cibernética da Faculdade ACADI-TI. Com base no plano, a gestão do curso pode tomar decisões que garantam a qualidade da formação dos alunos e a sua inserção no mercado de trabalho.

2.11.4 Apropriação dos resultados pela comunidade acadêmica

A gestão do curso de Defesa Cibernética da Faculdade ACADI-TI entende que o compartilhamento dos resultados das avaliações com a comunidade acadêmica é essencial para garantir a apropriação dos resultados e o acompanhamento da implantação do Plano de Gestão do curso. Para isso, a gestão do curso planeja realizar as seguintes ações:

- Divulgação dos resultados das avaliações por meio de canais de comunicação oficiais da faculdade, como o site, o portal do aluno e as redes sociais.
- Realização de reuniões com professores, alunos e demais stakeholders para apresentar os resultados das avaliações e discutir as ações a serem implementadas.
- Inserção dos resultados das avaliações no Plano de Gestão do curso, de modo que todos os envolvidos estejam cientes das metas e objetivos a serem alcançados.

A coordenação do curso acredita que essas ações contribuirão para que a comunidade acadêmica se sinta parte do processo de avaliação e melhoria do curso. A escolha das estratégias de compartilhamento dos resultados das avaliações levará em consideração as características da comunidade acadêmica e os objetivos da gestão do curso.

2.11.5 Estabelecimento de um processo autoavaliativo periódico para o curso

Todos os membros d Faculdade ACADI-TI entendem que a avaliação é uma ferramenta essencial para o desenvolvimento e a melhoria contínua dos seus cursos. Nesse contexto, o curso de Defesa Cibernética estabelecerá um processo autoavaliativo periódico, que será realizado a cada dois anos. O processo autoavaliativo terá como objetivos:

- Identificar as áreas de força e de melhoria do curso;
- Definir metas e objetivos para o desenvolvimento do curso;
- Desenvolver estratégias e ações para alcançar as metas e objetivos definidos;
- Avaliar o impacto das ações implementadas.

O processo autoavaliativo será realizado por uma comissão composta por representantes da gestão do curso, professores, alunos e egressos. A comissão será responsável por elaborar um instrumento de avaliação, que será aplicado a todos os envolvidos no curso.

O instrumento de avaliação será composto por questões fechadas, abertas e semiabertas, que abordarão os seguintes aspectos:

- Currículo: adequação ao perfil do egresso, atualidade e relevância dos conteúdos programáticos;
- Metodologias de ensino: adequação às necessidades dos alunos, efetividade na aprendizagem;
- Infraestrutura: adequação às necessidades do curso, condições de trabalho e estudo;
- Relação com o mercado de trabalho: articulação com o mercado de trabalho, inserção dos alunos no mercado de trabalho;
- Satisfação dos alunos: percepção dos alunos sobre o curso, satisfação com a formação recebida.

Os resultados da autoavaliação serão analisados pela comissão e apresentados à gestão do curso. A gestão do curso será responsável por elaborar um plano de ação para atender às recomendações da autoavaliação.

A periodicidade da avaliação autoavaliativa do curso de Defesa Cibernética da Faculdade ACADI-TI será de dois anos. Essa periodicidade foi definida com base nos seguintes critérios:

- Necessidade de acompanhar as mudanças constantes da área de cibersegurança: a área de cibersegurança é uma área em constante evolução, com o surgimento de novas tecnologias e ameaças. Para garantir que o curso ofereça uma formação de qualidade, é importante que a avaliação seja realizada com periodicidade suficiente para identificar e atender às necessidades da área.
- Tempo necessário para implementar as ações de melhoria: a avaliação deve ser utilizada como uma ferramenta de melhoria contínua. Para que isso aconteça, é importante que haja tempo suficiente para implementar as ações de melhoria recomendadas pela avaliação.

A periodicidade de dois anos atende a esses critérios, uma vez que permite que a avaliação seja realizada com frequência suficiente para acompanhar as mudanças da área, mas também oferece tempo suficiente para implementar as ações de melhoria.

É importante ressaltar que a periodicidade da avaliação pode ser alterada, caso seja necessário. De forma ilustrativa, se a área de cibersegurança passar por mudanças significativas, a periodicidade da avaliação pode ser reduzida para garantir que o curso esteja sempre alinhado às necessidades da área.

O processo autoavaliativo periódico é uma ferramenta importante para o desenvolvimento e a melhoria contínua do curso de Defesa Cibernética. Com base nos resultados da autoavaliação, a gestão do curso poderá tomar decisões que garantam a qualidade da formação dos alunos e a sua inserção no mercado de trabalho.

2.12 ATIVIDADES DE TUTORIA

2.12.1 Atividades de tutoria na estrutura curricular.

As atividades de tutoria no curso de defesa cibernética da Faculdade ACADI-TI têm como objetivo apoiar o processo de aprendizagem dos alunos, tanto na dimensão teórica quanto prática. Os tutores são profissionais qualificados e experientes na área de Defesa Cibernética, e atuam como mentores dos alunos, guiando-os na trilha da aprendizagem.

As atividades de tutoria são desenvolvidas em diferentes formatos, incluindo:

- **Acompanhamento individual**: Os tutores estão disponíveis para atender os alunos individualmente, por meio de chats, e-mail ou videoconferências. O atendimento individual é uma ótima oportunidade para os alunos tirarem dúvidas, discutirem dificuldades e receberem feedback sobre o seu desempenho.
- **Atividades em grupo**: Os tutores também organizam atividades em grupo, como fóruns de discussão, oficinas e workshops. Essas atividades são uma oportunidade para os alunos interagirem uns com os outros e compartilharem conhecimentos.
- **Avaliação de atividades**: Os tutores também avaliam as atividades desenvolvidas pelos alunos, fornecendo feedback sobre o seu desempenho. A avaliação é uma importante ferramenta para o desenvolvimento da aprendizagem dos alunos.

As atividades de tutoria são uma parte essencial da estrutura curricular do curso de Defesa Cibernética. Elas contribuem para o sucesso dos alunos, pois os ajudam a:

- Compreender os conceitos e teorias abordados no curso
- Desenvolver as habilidades necessárias para a prática da defesa cibernética
- Aprimorar as suas competências de comunicação e colaboração

A Faculdade ACADI-TI acredita que o tutor é um profissional fundamental para o sucesso do ensino a distância. Por isso, os tutores do curso de Defesa Cibernética são selecionados com base em critérios rigorosos, que incluem:

- Formação acadêmica e experiência profissional na área de defesa cibernética
- Competências pedagógicas
- Capacidade de comunicação e colaboração

A Faculdade ACADI-TI investe na formação e capacitação contínua dos seus tutores. Isso garante que os alunos recebam o apoio de profissionais qualificados e atualizados.

Na modalidade a distância, o tutor assume um papel ainda mais importante do que na modalidade presencial. Ele é o responsável por acompanhar os alunos e garantir que eles estejam aprendendo de forma eficaz.

No curso de Defesa Cibernética, os tutores são responsáveis por:

- Acompanhar o desempenho dos alunos
- Tirar dúvidas dos alunos
- Orientar os alunos nas atividades práticas
- Fornecer feedback sobre o desempenho dos alunos

O tutor é um parceiro fundamental no processo de aprendizagem dos alunos na modalidade a distância. Ele é o responsável por garantir que os alunos tenham o apoio necessário para alcançar o sucesso.

2.12.2 Atendimento às demandas didático-pedagógicas

O tutor assemelha-se a um mentor da aprendizagem. Ele é um profissional qualificado e experiente na área de defesa cibernética, que atua como um guia para os alunos no processo de aprendizagem. Ele é responsável por apoiar os alunos em todas as dimensões da sua formação, tanto na dimensão teórica quanto prática. Para atender às demandas didático-pedagógicas do curso de Defesa Cibernética, o tutor-mentor deverá:

- Ter um conhecimento profundo da área de defesa cibernética: Isso é essencial para que o tutor-mentor possa responder às dúvidas dos alunos e orientá-los de forma eficaz.
- Ser um bom comunicador: O tutor-mentor deve ser capaz de se comunicar de forma clara e concisa, tanto por escrito quanto oralmente.
- Ser um bom mentor: O tutor-mentor deve ser capaz de motivar os alunos e ajudá-los a desenvolver as suas habilidades e competências.

Atendimento individual

O atendimento individual é uma das principais formas de o tutor-mentor atender às demandas didático-pedagógicas dos alunos. Nesse tipo de atendimento, o tutor-mentor está disponível para atender os alunos individualmente, por meio de chats, e-mail ou videoconferências. O atendimento individual é uma ótima oportunidade para os alunos tirarem dúvidas, discutirem dificuldades e receberem feedback sobre o seu desempenho. O tutor-mentor pode usar esse tipo de atendimento para:

- Responder a dúvidas específicas dos alunos
- Acompanhar o progresso dos alunos
- Oferecer feedback sobre o desempenho dos alunos

Além do atendimento individual, o tutor-mentor também organizará atividades em grupo, como fóruns de discussão, oficinas e workshops. Essas atividades serão uma oportunidade para os alunos interagirem uns com os outros e compartilharem conhecimentos.

As atividades em grupo podem ser usadas para:

- Promover a colaboração entre os alunos

- Aprofundar os conhecimentos dos alunos
- Desenvolver as competências de comunicação e colaboração dos alunos

Avaliação de atividades

O tutor-mentor também será responsável por avaliar as atividades desenvolvidas pelos alunos. A avaliação é uma importante ferramenta para o desenvolvimento da aprendizagem dos alunos. O tutor-mentor usará a avaliação para:

- Identificar as áreas de dificuldade dos alunos
- Fornecer feedback sobre o desempenho dos alunos
- Motivar os alunos a continuar aprendendo

2.12.3 Mediação pedagógica com os discentes incluindo momentos presenciais

As atividades presenciais no curso de defesa cibernética da Faculdade ACADI-TI serão concentradas em três momentos principais:

- **Projetos Multidisciplinares extensionistas**: Os projetos interdisciplinares são atividades práticas que envolvem alunos de diferentes disciplinas. Eles são uma oportunidade para os alunos aplicarem os conhecimentos adquiridos das disciplinas no semestre e desenvolverem habilidades colaborativas.
- **Avaliações das Disciplinas Curriculares**: Como definido no Projeto Pedagógico Institucional (PPI), as avaliações presenciais são realizadas em todos os cursos da Faculdade ACADI-TI, incluindo o curso de Defesa Cibernética. Elas são uma forma de garantir que os alunos tenham adquirido os conhecimentos e habilidades necessários para o curso.
- **Apresentações e orientações de trabalhos**: As apresentações e orientações de trabalhos são atividades que acontecerão durante o curso e que ajudarão os alunos a desenvolverem as suas habilidades de comunicação e apresentação.

Durante os projetos multidisciplinares, os tutores-mentores atuarão como orientadores dos alunos. Eles estarão disponíveis para ajudar os alunos a desenvolverem os seus projetos e a enfrentarem quaisquer desafios que possam surgir.

Durante as avaliações presenciais, os tutores-mentores estarão presentes para auxiliar os alunos e responder às suas dúvidas. Eles também estarão disponíveis para fornecer feedback aos alunos sobre o seu desempenho.

Durante as apresentações e orientações de trabalhos, os tutores-mentores atuarão como avaliadores dos trabalhos dos alunos. Eles fornecerão feedback aos alunos sobre o seu trabalho e ajudarão a melhorar a sua qualidade.

As atividades presenciais são importantes para o processo de aprendizagem dos alunos, pois permitem que eles interajam uns com os outros e com os tutores-mentores de forma mais direta. Isso ajuda a promover a colaboração, a aprendizagem colaborativa e o desenvolvimento de habilidades socioemocionais.

A Faculdade ACADI-TI tem o compromisso com a Sociedade e com o Ministério da Educação em oferecer um processo de aprendizagem completo para os seus alunos. As atividades presenciais são uma parte importante desse processo, pois permitem que os alunos interajam uns com os outros e com os tutores-mentores de forma mais direta.

2.12.4 Domínio do conteúdo, de recursos e dos materiais didáticos

O domínio do conteúdo, de recursos e dos materiais didáticos é uma competência essencial para os tutores na Faculdade ACADI-TI e, naturalmente àqueles que atuarão no curso de Defesa Cibernética. Isso porque, para que as atividades de tutoria sejam eficazes, os tutores devem ser capazes de:

- Entender os conceitos e teorias abordados no curso
- Conhecer os recursos e materiais didáticos disponíveis
- Saber como utilizar esses recursos e materiais de forma eficaz

O domínio do conteúdo é fundamental para que os tutores possam responder às dúvidas dos alunos de forma precisa e abrangente. Para a contratação, os tutores deverão ter um conhecimento profundo da área de Defesa Cibernética, incluindo os conceitos, teorias e práticas mais recentes, e é desejável também formação pedagógica.

O domínio dos recursos e materiais didáticos é importante para que os tutores possam orientar os alunos de forma correta. Os tutores deverão estar familiarizados com os recursos e materiais disponíveis, como livros, artigos, vídeos e softwares. Eles saberão como utilizar esses recursos e materiais para ajudar os alunos a aprender.

O domínio dos recursos e materiais didáticos também é importante para que os tutores possam desenvolver atividades de tutoria criativas e inovadoras. Os tutores deverão estar

abertos a experimentar novos recursos e materiais, de modo a atender às necessidades dos alunos.

A Faculdade ACADI-TI investirá na formação e capacitação contínua dos seus tutores. Há o **Plano de Capacitação do Corpo doente tutorial** que prevê formação deste perfil de tutores. Isso garante que os tutores tenham o conhecimento e as habilidades necessárias para realizar as suas atividades de forma pedagógica, com vistas a aprendizagem do aluno.

2.12.5 Acompanhamento dos discentes no processo formativo

As atividades de tutoria no curso de defesa cibernética da Faculdade ACADI-TI têm como objetivo apoiar o processo de aprendizagem dos alunos, tanto na dimensão teórica quanto prática. Os tutores são profissionais qualificados e experientes na área de defesa cibernética, e atuam como mentores dos alunos, guiando-os na trilha da aprendizagem. As atividades de tutoria são desenvolvidas em diferentes formatos, incluindo:

- Acompanhamento individual: Os tutores estão disponíveis para atender os alunos individualmente, por meio de chats, e-mail ou videoconferências. O atendimento individual é uma ótima oportunidade para os alunos tirarem dúvidas, discutirem dificuldades e receberem feedback sobre o seu desempenho.
- Atividades em grupo: Os tutores também organizam atividades em grupo, como fóruns de discussão, oficinas e workshops. Essas atividades são uma oportunidade para os alunos interagirem uns com os outros e compartilharem conhecimentos.
- Avaliação de atividades: Os tutores também avaliam as atividades desenvolvidas pelos alunos, fornecendo feedback sobre o seu desempenho. A avaliação é uma importante ferramenta para o desenvolvimento da aprendizagem dos alunos.

As atividades de tutoria são uma parte essencial da estrutura curricular do curso de defesa cibernética da Faculdade ACADI-TI. Elas contribuem para o sucesso dos alunos, pois os ajudam a:

- Compreender os conceitos e teorias abordados no curso
- Desenvolver as habilidades necessárias para a prática da defesa cibernética
- Aprimorar as suas competências de comunicação e colaboração

A Faculdade ACADI-TI acredita que o professor-tutor é um profissional fundamental para o sucesso do ensino a distância. Por isso, os tutores do curso de defesa cibernética são selecionados com base em critérios rigorosos, que incluem:

- Formação acadêmica e experiência profissional na área de defesa cibernética
- Competências pedagógicas
- Capacidade de comunicação e colaboração

A Faculdade ACADI-TI investe na formação e capacitação contínua dos seus tutores. Isso garante que os alunos recebam o apoio de profissionais qualificados e atualizados. O acompanhamento dos discentes no processo formativo é uma das principais funções dos tutores. Essa função é essencial para garantir que os alunos estejam aprendendo de forma eficaz e que estejam desenvolvendo as suas habilidades e competências. O acompanhamento dos discentes será realizado de diversas formas, incluindo:

- Avaliação do desempenho dos alunos: Os tutores avaliam o desempenho dos alunos por meio de atividades, avaliações e outras formas de verificação.
- Feedback aos alunos: Os tutores fornecem feedback aos alunos sobre o seu desempenho, de forma a ajudá-los a melhorar.
- Orientação aos alunos: Os tutores orientam os alunos sobre o curso, as atividades e as avaliações.
- Acompanhamento do progresso dos alunos: Os tutores acompanham o progresso dos alunos, de forma a identificar áreas de dificuldade ou de potencial.

O acompanhamento dos discentes deve ser realizado de forma contínua e personalizada. Os tutores estarão atentos às necessidades individuais de cada aluno, de modo a oferecer o apoio necessário para o seu desenvolvimento integral.

Neste sentido, para realizar o acompanhamento dos discentes de forma plena, os tutores serão orientado a:

- Estabelecer um relacionamento de confiança com os alunos: Os tutores devem criar um ambiente de confiança e respeito, de modo que os alunos se sintam à vontade para compartilhar as suas dificuldades e dúvidas.
- Serem proativos: Os tutores devem tomar a iniciativa de acompanhar os alunos, de forma a identificar áreas de necessidade.

- Serem flexíveis: Os tutores devem ser flexíveis e adaptar as suas atividades às necessidades dos alunos.

2.12.6 Planejamento de avaliação periódica por estudantes e equipe pedagógica

As atividades de tutoria serão avaliadas periodicamente, por estudantes e equipe pedagógica do curso, de modo a identificar pontos fortes e fracos e promover melhorias. A avaliação periódica das atividades de tutoria é será importante para garantir que elas estejam atendendo às necessidades dos alunos. A avaliação será realizada por estudantes e equipe pedagógica, de modo a obter uma visão holística do processo de tutoria. Há um documento detalhado desta avaliação chamado: **Processo de avaliação da tutoria**

A avaliação por estudantes é uma importante fonte de feedback para os tutores e para a equipe pedagógica. Os estudantes podem fornecer informações sobre a qualidade das atividades de tutoria, como:

- A relevância das atividades para o aprendizado
- A clareza e a organização das atividades
- A disponibilidade e a atenção dos tutores
- A qualidade do feedback fornecido pelos tutores

A avaliação por estudantes será realizada por meio de questionários.

A equipe pedagógica também deverá avaliar as atividades de tutoria, de modo a identificar pontos que podem ser melhorados. A equipe pedagógica avaliará as atividades de tutoria com base nos seguintes critérios:

- Conformidade com os objetivos do curso
- Abrangência dos conteúdos abordados
- Metodologias utilizadas
- Resultados obtidos

A avaliação por equipe pedagógica realizará por meio de análise de documentos, observações das atividades de tutoria e questionário.

Os resultados da avaliação das atividades de tutoria devem ser analisados e discutidos pelos tutores e equipe pedagógica. A partir da análise dos resultados, serão definidas ações para melhorar as atividades de tutoria, que poderá incluir, mas não se limitar a:

- Atualização dos conteúdos abordados

- Adaptação das metodologias utilizadas
- Fortalecimento das competências dos tutores

A avaliação periódica das atividades de tutoria é uma ferramenta importante para garantir a qualidade do processo de aprendizagem.

2.13 CONHECIMENTO, HABILIDADES E ATITUDES NECESSÁRIAS ÀS ATIVIDADES DE TUTORIA

2.13.1 Conhecimentos, habilidades e atitudes

O curso de Defesa Cibernética é um curso de graduação na modalidade a distância, que tem como objetivo formar profissionais capazes de atuar na defesa cibernética de organizações públicas e privadas. As atividades de tutoria, pelo contexto como o curso é oferecido, são essenciais para o sucesso do projeto, pois são responsáveis por apoiar os estudantes no processo de aprendizagem e garantir que eles alcancem os objetivos do curso.

Os conhecimentos, habilidades e atitudes da equipe de tutoria serão adequados para que as atividades e ações estejam alinhadas deste PPC com as às demandas comunicacionais e às tecnologias previstas para o curso.

Conhecimentos

Os tutores deverão conhecimentos sólidos sobre os conteúdos abordados no curso, incluindo:

- Fundamentos de cibernética
- Segurança da informação
- Leis e regulamentos de cibersegurança
- Ética e compliance
- Gestão de riscos cibernéticos
- Investigações de incidentes cibernéticos

Além disso, os tutores deverão ter conhecimentos sobre as seguintes áreas:

- Metodologias de ensino a distância
- Tecnologias da informação e comunicação
- Educação a distância

- Tutoria

Habilidades

Os tutores deverão ter as seguintes habilidades para desempenhar suas atividades de forma plena:

- Habilidades de comunicação: os tutores devem ser capazes de se comunicar de forma clara e eficaz com os estudantes, por meio de diferentes canais de comunicação.
- Habilidades de interação: os tutores devem ser capazes de interagir de forma positiva e construtiva com os estudantes, promovendo a aprendizagem colaborativa.
- Habilidades de resolução de problemas: os tutores devem ser capazes de resolver problemas técnicos e acadêmicos que possam surgir durante o processo de aprendizagem.
- Habilidades de gestão: os tutores devem ser capazes de gerenciar suas atividades de forma eficiente, garantindo que elas estejam alinhadas aos objetivos do curso.

Atitudes

Para o sucesso do curso, na contratação dos professores tutores, serão consideradas com preponderante as seguintes atitudes para desempenhar suas atividades de forma ética e profissional:

- Disponibilidade: os tutores devem estar disponíveis para atender aos estudantes, dentro do horário de atendimento estabelecido.
- Empatia: os tutores devem ser capazes de se colocar no lugar dos estudantes, compreendendo suas dificuldades e necessidades.
- Proatividade: os tutores devem ser proativos, buscando identificar e resolver problemas antes que eles se agravem.
- Resiliência: os tutores devem ser capazes de lidar com situações adversas, sem perder a motivação e o foco.

A Faculdade ACADI-TI realizará um processo de seleção rigoroso para a contratação de tutores, a fim de garantir que os profissionais selecionados tenham os conhecimentos, habilidades e atitudes necessários para desempenhar suas atividades de forma eficaz.

2.13.2 Alinhamento das atividades e ações dos tutores ao PPC

A gestão do curso manterá plena atenção a este quesito, pois as atividades e ações dos tutores deverão estar alinhadas a este PPC, de modo a garantir que elas estejam de acordo com os objetivos do curso. Para isso, é importante que os tutores tenham um conhecimento profundo deste PPC, incluindo os seguintes aspectos:

- Objetivos gerais e específicos do curso: os tutores devem compreender os objetivos gerais e específicos do curso, a fim de orientar suas atividades de forma a contribuir para o alcance desses objetivos.
- Conteúdos programáticos: os tutores devem ter conhecimento dos conteúdos programáticos do curso, a fim de orientar os estudantes na aprendizagem dos conteúdos.
- Metodologias de ensino e aprendizagem: os tutores devem conhecer as metodologias de ensino e aprendizagem utilizadas no curso, a fim de aplicar essas metodologias de forma eficaz.
- Critérios de avaliação: os tutores devem conhecer os critérios de avaliação do curso, a fim de orientar os estudantes na realização das atividades e avaliações.

Além do conhecimento deste PPC, que será promovido no curso de formação, os tutores também deverão as seguintes habilidades e atitudes:

- Habilidades de comunicação: os tutores devem ser capazes de se comunicar de forma clara e eficaz com os estudantes, por meio de diferentes canais de comunicação.
- Habilidades de interação: os tutores devem ser capazes de interagir de forma positiva e construtiva com os estudantes, promovendo a aprendizagem colaborativa.
- Habilidades de resolução de problemas: os tutores devem ser capazes de resolver problemas técnicos e acadêmicos que possam surgir durante o processo de aprendizagem.
- Habilidades de gestão: os tutores devem ser capazes de gerenciar suas atividades de forma eficiente, garantindo que elas estejam alinhadas aos objetivos do curso.

2.13.3 Atendimento às demandas comunicacionais do curso

As demandas comunicacionais do curso são as necessidades de comunicação que os estudantes têm durante o processo de aprendizagem. Essas demandas podem ser de natureza

acadêmica, técnica ou social. A equipe de tutores da Faculdade ACADI-TI realizará o atendimento às demandas comunicacionais do curso por meio de uma variedade de canais de comunicação, incluindo:

- Ambiente virtual de aprendizagem (AVA): o AVA é o principal canal de comunicação entre os tutores e os estudantes. No AVA, os tutores podem disponibilizar materiais de estudo, responder a dúvidas, e promover atividades de interação e colaboração.
- Fóruns de discussão: os fóruns de discussão são um canal de comunicação eficaz para que os estudantes possam tirar dúvidas e compartilhar ideias.
- Protocolo no sistema acadêmico: o sistema acadêmico é um canal de comunicação privado que pode ser utilizado pelos estudantes para enviar dúvidas ou solicitar apoio aos tutores.
- Chat: o chat é um canal de comunicação instantâneo que pode ser utilizado pelos estudantes para tirar dúvidas ou solicitar apoio aos tutores em tempo real.

A equipe de tutores também realizará atividades de orientação sobre as ferramentas de comunicação disponíveis no AVA, a fim de ajudar os estudantes a aproveitarem ao máximo esses recursos.

2.13.4 Uso de tecnologias previstas para o curso na tutoria

As tecnologias previstas para o curso são as ferramentas e recursos tecnológicos que serão utilizados no processo de ensino e aprendizagem. Essas tecnologias serão utilizadas pelos tutores para realizar uma variedade de atividades, incluindo:

- **Orientação acadêmica**: os tutores disponibilizarão materiais de estudo em formato digital, responderão a dúvidas por meio de ferramentas de comunicação online, e promoverão atividades de aprendizagem colaborativa por meio de plataformas de colaboração.
- **Apoio técnico**: os tutores oferecerão suporte técnico aos estudantes por meio de ferramentas de atendimento online, e solucionarão problemas relacionados ao uso de tecnologias educacionais.
- **Interação e colaboração**: os tutores promoverão a interação e colaboração entre os estudantes por meio de fóruns de discussão, chats, videoconferências, e outras ferramentas de comunicação online.

- **Acompanhamento e avaliação**: os tutores acompanharão o desempenho dos estudantes por meio de ferramentas de avaliação online, e fornecer feedback aos estudantes de forma individualizada.

Tecnologias previstas para o curso que serão utilizadas na tutoria:

- Ambiente virtual de aprendizagem (AVA): o AVA é uma ferramenta fundamental para a tutoria, pois permite que os tutores se comuniquem com os estudantes, disponibilizem materiais de estudo, e promovam atividades de aprendizagem colaborativa.
- Ferramentas de comunicação online (chat do moodle): as ferramentas de comunicação online serão utilizadas pelos tutores para responder a dúvidas, promover interações entre os estudantes, e realizar atendimentos individualizados.
- Plataformas de colaboração (Teams): as plataformas de colaboração será o Microsoft Teams, o qual será utilizado pelos tutores para promover atividades de aprendizagem colaborativa, como projetos, pesquisas, e trabalhos em grupo.

Para que o uso de tecnologias previstas (moodle e teams) para o curso na tutoria seja eficiente, é importante que a equipe de tutores esteja alinhada às seguintes questões:

- Conhecimento das tecnologias: os tutores deverão ter conhecimento das tecnologias previstas para o curso, a fim de utilizá-las de forma eficaz.
- Competências tecnológicas: os tutores deverão ter as competências necessárias para utilizar as tecnologias previstas para o curso, incluindo habilidades de navegação, utilização de ferramentas, e resolução de problemas técnicos.
- Atitude positiva em relação às tecnologias: os tutores deverão uma atitude positiva em relação às tecnologias, a fim de utilizá-las de forma criativa e inovadora.

A Faculdade ACADI-TI oferece treinamento aos tutores sobre as tecnologias previstas para o curso, a fim de garantir que eles tenham as competências necessárias para utilizá-las de forma eficaz

2.13.5 Planejamento de avaliações periódicas da equipe de tutoria

As atividades de avaliação de tutoria serão avaliadas periodicamente, para identificar necessidade de capacitação dos tutores. A avaliação permite que ACADI-TI identifique os

pontos fortes e fracos das atividades de tutoria, a fim de promover melhorias. O planejamento de avaliações periódicas da equipe de tutoria incluirão os seguintes aspectos:

- Frequência: a frequência das avaliações será definida de acordo com as necessidades da ACADI-TI e do curso de Defesa Cibernética. Avaliações serão semestrais.
- Instrumentos: os instrumentos de avaliação serão escolhidos de acordo com os objetivos da avaliação. Os instrumentos serão qualitativos e quantitativos.
- Participantes: os participantes da avaliação serão definidos de acordo com os objetivos da avaliação. Os participantes serão estudantes, tutores, coordenadores de curso, e outros.

O planejamento de avaliações periódicas da equipe de tutoria é uma ferramenta importante para garantir a qualidade das atividades de tutoria e a formação de profissionais qualificados.

2.13.6 Apoio institucional para adoção de práticas criativas e inovadoras

A ACADI-TI oferece aos tutores do curso de Defesa Cibernética um plano de formação continuada que aborda temas como metodologias de ensino inovadoras, tecnologias educacionais, design thinking, gamificação e aprendizagem baseada em problemas. Essas atividades são ministradas por profissionais experientes e qualificados, e visam a proporcionar aos tutores os conhecimentos e habilidades necessários para desenvolver práticas criativas e inovadoras.

A ACADI-TI também apoiará o desenvolvimento de habilidades dos tutores que são essenciais para a criatividade e a inovação. Essas habilidades incluem curiosidade, abertura para o novo, capacidade de pensar fora da caixa, resiliência e colaboração. A instituição oferece aos tutores oportunidades de participar de atividades que contribuem para o desenvolvimento dessas habilidades, como workshops, palestras e projetos de pesquisa.

A ACADI-TI promoverá ações que incentivam os tutores a experimentarem novas ideias e a compartilharem suas experiências. A instituição organizará eventos de inovação, programas de reconhecimento e espaços de colaboração que possibilitam aos tutores trocar ideias e experiências com colegas e profissionais da área. Alguns exemplos de apoios específicos que a ACADI-TI oferecerá aos tutores do curso de Defesa Cibernética incluem:

- Acesso a recursos de aprendizagem, como livros, artigos, vídeos e cursos online.
- Oportunidades de participar de redes de profissionais da educação.
- Recursos financeiros para o desenvolvimento de projetos inovadores propostos pelos tutores.

A adoção dessas ações contribuirá para o desenvolvimento de práticas criativas e inovadoras que promovem a aprendizagem dos estudantes do curso de Defesa Cibernética. Alguns exemplos de práticas criativas e inovadoras desenvolvidas por tutores do curso de Defesa Cibernética incluem:

- Uso de gamificação para ensinar conceitos de segurança cibernética.
- Desenvolvimento de projetos de pesquisa sobre segurança cibernética.
- Organização de eventos e workshops sobre segurança cibernética.

Essas práticas contribuem para a formação de profissionais mais qualificados e preparados para enfrentar os desafios da segurança cibernética

2.14 TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO (TIC) NO PROCESSO DE ENSINO-APRENDIZAGEM

2.14.1 Execução do projeto pedagógico

As Tecnologias de Informação e Comunicação (TIC) têm sido cada vez mais utilizadas no processo de ensino-aprendizagem, em todos os níveis de ensino, inclusive no Ensino Superior. No curso de Defesa Cibernética, as TICs têm um papel fundamental, pois permitem que os alunos desenvolvam as competências necessárias para atuar nessa área emergente.

As TICs contribuirão para execução deste Projeto Pedagógico sendo utilizadas no curso de Defesa Cibernética para atender a diversos objetivos, como:

- Apresentação de conteúdos: as TICs serão utilizadas para apresentar conteúdos de forma mais dinâmica e interativa, por meio de videoaulas, apresentação em slides e podcasts. Isso permite que os alunos aprendam de forma mais significativa e retenham melhor o conteúdo.
- Realização de atividades práticas: as TICs serão utilizadas para realizar atividades práticas, como simulações, experimentos e jogos. Isso permite que os alunos desenvolvam habilidades práticas e apliquem os conhecimentos adquiridos na teoria.

- Avaliação da aprendizagem: as TICs serão utilizadas para avaliar a aprendizagem dos alunos de forma mais diversificada e inclusiva. Isso permite que os alunos sejam avaliados de acordo com suas necessidades e habilidades.

As TICs podem contribuir para a execução do Projeto Pedagógico do Curso de Defesa Cibernética, de modo a garantir que os objetivos do curso sejam alcançados. Isso ocorre porque as TICs permitem que os alunos:

- Desenvolvam as competências necessárias para atuar na área de Defesa Cibernética: as TICs permitem que os alunos aprendam sobre conceitos teóricos e práticos da Defesa Cibernética, além de desenvolver habilidades para identificar e responder a ataques cibernéticos.
- Se mantenham atualizados com as últimas tendências da área: as TICs permitem que os alunos tenham acesso a informações atualizadas sobre a Defesa Cibernética, por meio de sites, blogs, e-books e outros recursos digitais.
- Participem de atividades colaborativas: as TICs permitem que os alunos colaborem com outros alunos e profissionais da área de Defesa Cibernética, por meio de plataformas de aprendizagem online, redes sociais e outros recursos digitais.

2.14.2 Facilitação da acessibilidade digital e comunicacional

As Tecnologias de Informação e Comunicação (TICs) têm o potencial de promover a acessibilidade digital e comunicacional, de modo a garantir que todos os alunos tenham acesso ao processo de ensino-aprendizagem. Acessibilidade digital refere-se à possibilidade de pessoas com deficiência ou mobilidade reduzida utilizarem recursos tecnológicos de forma independente e eficaz. Já acessibilidade comunicacional refere-se à possibilidade de pessoas com deficiência auditiva ou visual compreenderem e produzirem mensagens.

As TICs podem contribuir para a acessibilidade digital e comunicacional de diversas formas. Elas promoverão a criação de conteúdo acessível, ou seja, que possa ser compreendido e utilizado por pessoas com deficiência. Em termos práticos, promoverão a criação de legendas e transcrições de vídeos, áudios e textos; promoverão a criação de versões em braile de materiais impressos; e promoverão a utilização de recursos de acessibilidade, como leitores de tela e ampliadores de tela. ACADI-TI, as TICs promoverão a criação de conteúdo acessível de

forma ainda mais eficaz. Para exemplificar, promoverão a criação de conteúdo acessível de forma automática, por meio de inteligência artificial. Além disso, promoverão a utilização de recursos de acessibilidade de forma mais integrada, de modo que os alunos possam acessar o conteúdo e interagir com os recursos de forma natural.

Em relação a acessibilidade de ferramentas, as TICs promoverão a criação de ferramentas acessíveis, ou seja, que possam ser utilizadas por pessoas com deficiência. Por exemplo, promoverão a criação de teclados virtuais, mouses adaptados e softwares de apoio à aprendizagem. Na ACADI-TI, as TICs promoverão a criação de ferramentas acessíveis que sejam ainda mais intuitivas e fáceis de usar. Além disso, promoverão a compatibilidade das ferramentas acessíveis com diferentes tipos de deficiência.

Quanto a acessibilidade de ambientes, as TICs promoverão a criação de ambientes acessíveis, ou seja, que possam ser utilizados por pessoas com deficiência. Por exemplo, promoverão a utilização de recursos de acessibilidade, como plataformas elevatórias, sinalética em braile e recursos de tradução de língua de sinais. ACADI-TI, as TICs promoverão a criação de ambientes acessíveis que sejam ainda mais inclusivos. Por exemplo, promoverão a utilização de recursos de acessibilidade para facilitar a interação entre alunos com deficiência e alunos sem deficiência.

A ACADI-TI tem um olhar especial à adoção de medidas para promover a acessibilidade digital e comunicacional no processo de ensino-aprendizagem de nossos futuros alunos, pois elas serão fundamentais para garantir que todos os alunos tenham acesso ao conhecimento e possam desenvolver seu potencial.

Para que as TICs sejam utilizadas de forma eficaz para promover a acessibilidade digital e comunicacional, a ACADI-TI:

- Investirá em infraestrutura: a IES investirá cada vez mais em recursos tecnológicos acessíveis, como computadores com leitores de tela, ampliadores de tela e softwares de apoio à aprendizagem.
- Ofereceremos formação: a ACADI-TI oferecerá formação para professores e funcionários sobre acessibilidade digital e comunicacional.
- Promoveremos ações de sensibilização: a ACADI-TI promoverá ações de sensibilização para conscientizar os alunos e a comunidade escolar sobre a importância da acessibilidade.

Com os investimentos necessários em infraestrutura, formação e sensibilização a ACADI-TI poderá garantir que as TICs sejam utilizadas de forma eficaz para promover a acessibilidade digital e comunicacional, contribuindo para a inclusão de todos os alunos no processo de ensino-aprendizagem.

Na ACADI-TI, por nosso NDA na área de Tecnologia, acreditamos que as TICs têm o potencial de revolucionar a educação, tornando-a mais acessível e inclusiva. Para que esse potencial seja plenamente realizado, a ACADI investirá em infraestrutura, formação e ações de sensibilização sobre acessibilidade digital e comunicacional.

2.14.3 Promoção da interatividade entre docentes, discentes e tutores

Na Faculdade ACADI-TI, a interatividade entre docentes, discentes e tutores é uma prioridade, implementada de forma inovadora através das TICs. A instituição adota ferramentas de comunicação síncrona e assíncrona, como plataformas de ensino a distância e redes sociais, para facilitar a troca de informações e o debate acadêmico fora das salas de aula tradicionais. Isso permite que a aprendizagem ocorra de forma contínua, com a participação ativa dos alunos em fóruns de discussão e videoconferências, onde podem interagir diretamente com professores e colegas.

Além disso, a ACADI-TI incentiva o uso de recursos colaborativos, como wikis e ferramentas de compartilhamento de arquivos, permitindo que os estudantes trabalhem juntos em projetos e pesquisas, fomentando o desenvolvimento de habilidades de trabalho em equipe e pensamento crítico. Softwares de brainstorming online são também utilizados para estimular a criatividade e a inovação, possibilitando que discentes e docentes construam conhecimento de forma coletiva.

A instituição não se limita apenas à interação e colaboração; ela também emprega métodos de gamificação e conteúdos interativos, transformando o processo de aprendizado em uma experiência mais envolvente e eficaz. Através de simulações, jogos educativos e plataformas de gamificação, os alunos são motivados a participar ativamente de seu processo de aprendizagem, o que contribui para um entendimento mais profundo dos conteúdos. Essa abordagem moderna e integrada prepara os estudantes para os desafios do século XXI, destacando a Faculdade ACADI-TI como um modelo de inovação educacional

2.14.4 Disponibilidade de materiais ou recursos didáticos a qualquer hora e lugar

O material didático e as ferramentas de aprendizagem estão acessíveis para os alunos e tutores 24 horas por dia, 7 dias por semana, via plataformas digitais. Isso proporciona flexibilidade incomparável, permitindo que os estudantes organizem seus estudos de acordo com seus próprios horários e compromissos. A disponibilidade constante dos recursos educacionais assegura que todos possam acessar o conteúdo e suporte necessários a qualquer momento, facilitando a aprendizagem autônoma e contínua, essencial para o sucesso acadêmico no ambiente de ensino moderno.

2.14.5 Criação de experiências diferenciadas de aprendizagem através do uso de tecnologias.

Com sua proposta de um ensino significativo, a Faculdade ACADI-TI certamente se destacará no cenário educacional de São José dos Campos por sua vanguarda na aplicação de tecnologias inovadoras que transformam a experiência de aprendizagem. A instituição reconhece que as Tecnologias da Informação e Comunicação (TICs) transcendem o mero suporte didático, assumindo um papel central na construção de um ensino-aprendizagem mais significativo, envolvente e personalizado.

A plataforma virtual Moodle da ACADI-TI vai além da mera disponibilização de conteúdos. Através de fóruns, quizzes, portfólios e ferramentas de videoconferência, alunos e professores interagem em um ambiente dinâmico e personalizado, construindo conhecimento de forma conjunta e ativa. Ambientes Virtuais de Aprendizagem (AVAs) como o Second Life simulam cenários reais, permitindo aos alunos praticar suas habilidades em um ambiente seguro e controlado. Na área de Administração, por exemplo, simulações de negócios permitem a experimentação de estratégias em um contexto virtual realista, aproximando os alunos da realidade profissional que os espera.

Simulações e jogos educativos facilitam o aprendizado de conceitos complexos de forma interativa e imersiva. Na área de Engenharia, simulações de softwares permitem que os alunos projetem e testem estruturas antes de construí-las na vida real, tornando o processo de aprendizagem mais intuitivo e eficaz. Em Ciberdefesa fazemos simulações de ataca a sistema com alto grau de realismos.

A ACADI-TI também explorará o potencial da Realidade Aumentada e Virtual para permitir que os alunos explorem conteúdos em 3D e interajam com objetos virtuais em tempo real.

Ferramentas de Colaboração Online como Google Docs, Microsoft Teams e Zoom promoverão o trabalho colaborativo em projetos multidisciplinares e tarefas, mesmo à distância. Essa prática desenvolve habilidades de comunicação, trabalho em equipe e resolução de problemas, preparando os alunos para o mercado de trabalho cada vez mais conectado e globalizado.

A ACADI-TI incentivará, como está em sua matriz curricular, a aprendizagem baseada em projetos, onde os alunos trabalham em equipe para resolver problemas reais, utilizando seus conhecimentos e habilidades de forma prática e colaborativa. Essa metodologia estimula a autonomia, a criatividade e o senso crítico, formando cidadãos mais engajados e proativos.

A ACADI-TI utilizará Sistemas de Tutoria Inteligente (como o Speaker Coach, da Microsolt) fornecem feedback individualizado aos alunos sobre seu desempenho, ajudando-os a identificar seus pontos fortes e fracos e a melhorar seu aprendizado de forma personalizada. Essa ferramenta garante que cada aluno receba o suporte necessário para alcançar seu potencial máximo.

Ao investir em tecnologias inovadoras e metodologias ativas, a ACADI-TI se consolidará como referência em educação de qualidade, proporcionando aos seus alunos uma jornada de aprendizado única e transformadora. A instituição reconhece que o futuro da educação está na personalização, na imersão e na interatividade, e se coloca na vanguarda dessa transformação, preparando seus alunos para os desafios e oportunidades do mundo em constante mudança.

2.15 AMBIENTA VIRTUAL DE APRENDIZAGEM – AVA

2.15.1 Materiais, recursos e tecnologias apropriadas

A Faculdade ACADI-TI reconhece o papel fundamental da tecnologia na educação moderna e, para o curso de Defesa Cibernética, investe em um Ambiente Virtual de Aprendizagem (AVA) robusto e personalizado, com base na plataforma Moodle. Como já dissemos acima, o AVA da ACADI-TI vai além da mera disponibilização de conteúdos,

configurando-se como um verdadeiro espaço de interação, colaboração e desenvolvimento de habilidades essenciais para o profissional de Defesa Cibernética.

O AVA oferece materiais didáticos discutido pelo NDE do curso e cuidadosamente selecionados e organizados pela Equipe Multidisciplinar forma didática e sequencial, facilitando o aprendizado. Simulações, jogos educativos e laboratórios virtuais permitem que os alunos coloquem em prática seus conhecimentos, vivenciando situações reais do mundo da Defesa Cibernética. Fóruns de discussão, chats e videoconferências promovem a interação entre alunos e professores, estimulando o debate, a troca de ideias e a construção conjunta do conhecimento.

A ACADI-TI acredita que cada aluno tem seu ritmo de aprendizado. Por isso, o AVA oferece tutoria personalizada e feedback contínuo, por meio de ferramentas de comunicação e acompanhamento individual. Essa atenção individualizada garante que todos os alunos tenham o suporte necessário para alcançar seus objetivos.

O AVA da ACADI-TI é acessível 24 horas por dia, 7 dias por semana, de qualquer lugar do mundo. Essa flexibilidade permite que os alunos aprendam em seu próprio ritmo e de acordo com sua disponibilidade, conciliando os estudos com outras atividades pessoais e profissionais. A ACADI-TI investe constantemente na atualização de sua plataforma AVA, incorporando as tecnologias mais recentes de ensino online. Essa busca incessante pela inovação garante aos alunos uma experiência de aprendizado de vanguarda, com recursos que facilitam e otimizam o processo de ensino-aprendizagem.

2.15.2 Cooperação entre tutores, discentes e docentes

Fóruns, grupos de estudo e chats no AVA da ACADI-TI promovem a troca de experiências entre alunos, tutores e professores. Essa interação permite a construção de um ambiente de aprendizado colaborativo e enriquecedor, onde todos podem contribuir e aprender com os demais.

A ACADI-TI reconhece que cada aluno tem seu ritmo e necessidades específicas. O AVA oferece tutoria personalizada e acompanhamento individual por tutores experientes, que orientam os alunos em suas dúvidas e auxiliam na superação de desafios. Essa atenção individualizada garante que todos os alunos tenham o suporte necessário para alcançar seus objetivos.

A matriz o curso está construída de maneira a aprendizagem baseada em projetos e o a AVA é uma ferramenta para cumprir os objetivos no curso, vez que o é onde os alunos trabalham em equipe para resolver problemas reais da área de Defesa Cibernética. Essa metodologia estimula o desenvolvimento de habilidades como trabalho em equipe, comunicação, resolução de problemas e pensamento crítico, essenciais para o futuro profissional dos alunos.

O AVA da ACADI-TI oferece ferramentas para que tutores e professores forneçam feedback contínuo e construtivo aos alunos sobre seu desempenho. Essa avaliação constante permite que os alunos identifiquem seus pontos fortes e fracos, ajustando suas estratégias de estudo e buscando o aprimoramento contínuo. A Instituição incentiva o compartilhamento de melhores práticas entre os membros da comunidade acadêmica. Através de fóruns, blogs e outras ferramentas, alunos, tutores e professores podem compartilhar suas experiências, ideias e soluções inovadoras, promovendo o aprendizado mútuo e a constante evolução do processo educacional.

A coordenação do curso de Defesa Cibernética acredita que a cooperação entre tutores, discentes e docentes do curso é fundamental para a construção de um ambiente de aprendizado dinâmico, engajador e eficaz. O AVA da instituição oferece ferramentas e recursos que facilitam a comunicação, a colaboração e o compartilhamento de conhecimentos, promovendo uma experiência educacional completa e transformadora para toda a comunidade acadêmica. Através da cooperação, o AVA se torna um espaço onde o conhecimento é construído de forma conjunta, preparando os alunos para os desafios do futuro com as ferramentas e habilidades necessárias para o sucesso.

2.15.3 Reflexão sobre o conteúdo das disciplinas

O Ambiente Virtual de Aprendizagem (AVA) é um espaço propício para a reflexão crítica e a aprendizagem significativa. Através de recursos cuidadosamente selecionados e atividades especialmente desenhadas, o AVA incentiva os alunos a se engajarem ativamente no processo de aprendizagem, construindo seu próprio conhecimento de forma autônoma e crítica.

O AVA oferece diversas ferramentas que estimulam a reflexão crítica dos alunos sobre o conteúdo das disciplinas. Fóruns de discussão, atividades de debate e questionamentos

cuidadosamente elaborados desafiam os alunos a analisar diferentes perspectivas, formular argumentos consistentes e defender suas ideias com base em fatos e conhecimentos adquiridos.

O Ambiente utiliza uma abordagem interativa e diversificada para promover a aprendizagem significativa. Videoaulas, simulações, jogos educativos e estudos de caso permitem que os alunos explorem os conteúdos de forma dinâmica e engajadora, conectando a teoria à prática e construindo uma compreensão mais profunda dos conceitos abordados.

Além disso, o AVA incentiva a aprendizagem ativa e colaborativa através de atividades em grupo, projetos multidisciplinares e fóruns de discussão. Pela própria natureza da área de T.I e no curso de Defesa Cibernética, os alunos são desafiados a trabalhar em conjunto, compartilhar conhecimentos, ideias e diferentes perspectivas, desenvolvendo habilidades essenciais para o mercado de trabalho, como comunicação, trabalho em equipe e resolução de problemas.

Certamente, o AVA que é usado pelo curos de Defesa Cibernética se destaca como um espaço inovador que promove a reflexão crítica, a aprendizagem significativa e a construção autônoma do conhecimento. O uso de recursos interativos, atividades diversificadas e acompanhamento individualizado prepara os alunos de Defesa Cibernética para serem protagonistas de sua própria aprendizagem e para atuarem de forma crítica e autônoma na sociedade.

2.15.4 Acessibilidade metodológica, instrumental e comunicacional

O Moodle se destaca como plataforma de ensino a distância por sua robustez e flexibilidade. Mas, além disso, o Moodle se preocupa com a inclusão, oferecendo recursos para garantir a acessibilidade metodológica, instrumental e comunicacional a todos os alunos, independentemente de suas necessidades. Por isso, a ACADI-TI o escolheu, e não outras plataformas como o CANVA ou o Blackboar.

Acessibilidade Metodológica

- Flexibilidade de Criação de Cursos: O Moodle permite que os professores utilizem diversos formatos de conteúdo, como textos, vídeos, imagens e podcasts, atendendo a diferentes estilos de aprendizado.

- Atividades Diversificadas: A plataforma oferece uma gama de atividades, desde quizzes e questionários até fóruns de discussão e trabalhos em grupo, promovendo a participação e o engajamento de todos os alunos.
- Avaliação Personalizada: O Moodle permite que os professores utilizem diferentes métodos de avaliação, como testes, trabalhos e portfólios, adaptando-se às necessidades de cada aluno.

Acessibilidade Instrumental

- Recursos de Acessibilidade Integrados: O Moodle possui ferramentas como legendas para vídeos, transcripts de áudio e navegação por teclado, facilitando o acesso para alunos com deficiência visual ou auditiva.
- Compatibilidade com Tecnologias Assistivas: A plataforma é compatível com a maioria das tecnologias assistivas, como leitores de tela e softwares de ampliação de tela.
- Temas Acessíveis: Diversos temas visuais com alto contraste e legibilidade estão disponíveis, proporcionando uma experiência de navegação mais confortável para todos os usuários.

Acessibilidade Comunicacional

- Linguagem Clara e Objetiva: O Moodle utiliza linguagem simples e direta em sua interface e materiais de ajuda, facilitando a compreensão para todos os alunos.
- Recursos de Tradução: A plataforma oferece suporte a diversos idiomas, permitindo que os alunos utilizem a interface em sua língua materna.
- Comunicação Inclusiva: O Moodle incentiva a comunicação respeitosa e inclusiva entre professores e alunos, promovendo um ambiente de aprendizado acolhedor para todos.

O Moodle se destaca como uma plataforma de ensino a distância comprometida com a inclusão. Através de recursos abrangentes de acessibilidade metodológica, instrumental e comunicacional, o Moodle garante que todos os alunos tenham acesso a um ensino de qualidade, independentemente de suas necessidades.

2.15.5 Realização de avaliações periódicas no AVA

A Faculdade ACADI-TI, comprometida com a excelência no ensino e aprendizagem, temum o **Plano Detalhado de Avaliação do Ambiente Virtual de Aprendizagem (AVA)**. A iniciativa visa garantir que o AVA atenda às necessidades e expectativas de toda a comunidade acadêmica, composta por alunos, professores e tutores. Através de um processo abrangente e periódico, a ACADI-TI busca identificar pontos fortes e fracos da plataforma, implementar melhorias contínuas e proporcionar uma experiência de ensino e aprendizagem cada vez mais rica e eficaz.

A avaliação do AVA será realizada em três etapas distintas, cada uma com seus objetivos específicos e metodologias de coleta de dados:

Etapa 1: Questionário:

- **Público-alvo:** Alunos, professores e tutores.
- **Objetivo:** Avaliar a usabilidade, navegabilidade, satisfação e percepção dos usuários sobre o AVA.
- **Período:** semestral.
- **Metodologia:** Questionário online anônimo, com perguntas de múltipla escolha, escala Likert e questões abertas para comentários e sugestões.

Etapa 2: Análise de Logs:

- **Objetivo:** Avaliar a frequência de uso, os recursos mais utilizados, os padrões de acesso e as dificuldades dos usuários.
- **Período:** semestral.
- **Metodologia:** Análise quantitativa dos logs do AVA, utilizando ferramentas de análise de dados e relatórios customizados.

Etapa 3: Grupos Focais:

- **Público-alvo:** Alunos e professores.
- **Objetivo:** Avaliar a percepção dos usuários sobre o AVA, suas dificuldades e sugestões de melhorias.
- **Data e Local:** A definir, com base na disponibilidade dos participantes.

- **Metodologia:** Discussões em grupo moderadas por um facilitador, com foco em temas específicos relacionados ao AVA.

Critérios de Avaliação:

A avaliação do AVA será realizada com base em cinco critérios principais:

- **Usabilidade:** Facilidade de uso e navegação na plataforma, incluindo layout, organização e intuitividade.
- **Funcionalidades:** Recursos disponíveis no AVA e sua utilidade para o ensino e aprendizagem, como ferramentas de comunicação, atividades interativas, materiais didáticos e recursos de acessibilidade.
- **Atividades:** Qualidade e variedade das atividades propostas no AVA, considerando sua relevância para os objetivos de aprendizagem, nível de engajamento dos alunos e potencial para o desenvolvimento de habilidades e competências.
- **Suporte técnico:** Eficiência e qualidade do suporte técnico oferecido aos usuários, incluindo tempo de resposta, resolução de problemas e canais de comunicação disponíveis.
- **Satisfação dos usuários:** Nível de satisfação dos alunos, professores e tutores com o AVA, avaliando aspectos como utilidade da plataforma, facilidade de uso, qualidade dos materiais e suporte técnico.

Projeto de Avaliação Periódica:

A avaliação do AVA da ACADI-TI não se limita a um evento único, mas sim se configura como um **Projeto de Avaliação Periódica**. Através da coleta e análise contínua de dados, a instituição busca identificar necessidades e expectativas em constante mudança, garantindo que o AVA esteja sempre atualizado e adaptado às demandas da comunidade acadêmica.

Os resultados da avaliação serão publicados no site da Faculdade ACADI-TI e utilizados para:

- Identificar pontos fortes e fracos do AVA, com foco em áreas que necessitem de aprimoramento.

- Implementar melhorias contínuas na plataforma, com base nas sugestões e feedbacks coletados dos diferentes públicos envolvidos.
- Atender às necessidades e expectativas de alunos, professores e tutores, proporcionando uma experiência de ensino e aprendizagem cada vez mais rica, eficaz e personalizada.

A ACADI-TI acredita que a avaliação periódica do AVA, e da IES como um todo, é fundamental para garantir a qualidade da educação online oferecida. Através de um processo transparente e participativo, a instituição se compromete a aprimorar continuamente sua plataforma virtual, proporcionando um ambiente de aprendizagem inovador, interativo e acessível a todos.

2.16 MATERIAL DIDÁTICO

2.16.1 A equipe multidisciplinar e o material didático

Na era da informação, onde o conhecimento se expande exponencialmente e a demanda por profissionais qualificados se intensifica, a educação se torna cada vez mais crucial para o desenvolvimento individual e coletivo. Nesse contexto, o material didático assume um papel fundamental como ferramenta de ensino e aprendizagem, especialmente da área de Tecnologia, e mais particularmente na Cyber Defesa.

A Faculdade ACADI-TI reconhece a importância de um material didático de excelência e, por isso, investe na criação de conteúdos de alta qualidade por uma equipe multidisciplinar de profissionais experientes. A Equipe Multidisciplinar garante que o material atende às necessidades de todos os alunos, independentemente de sua área de formação ou de suas habilidades específicas.

A equipe multidisciplinar da ACADI-TI é composta por professores renomados, pedagogos, especialistas em educação, design instrucional, tecnologia educacional, avaliação e acessibilidade. Essa diversidade de expertise permite a criação e validação de um material didático abrangente, completo e que promove o engajamento e a participação ativa dos alunos.

Através da colaboração entre diferentes áreas, a ACADI-TI garante que seu material didático seja:

- Abrangente e completo: abrangendo diferentes perspectivas e necessidades dos alunos.

- Engajador e participativo: com conteúdos relevantes e contextualizados, utilizando diferentes recursos didáticos.
- Acessível e inclusivo: adaptado para atender às necessidades de todos os alunos, independentemente de suas habilidades ou estilos de aprendizagem.
- Atualizado e relevante: com conteúdos atualizados e relevantes para a área de atuação do curso.

O processo de criação e validação do material didático da ACADI-TI é rigoroso e inclui:

- Planejamento e definição dos objetivos de aprendizagem: com base nas diretrizes curriculares e nas necessidades dos alunos.
- Desenvolvimento do material didático: por especialistas em cada área, com revisão e validação pela equipe multidisciplinar.
- Validação com alunos: por meio de testes e coleta de feedback, para garantir a qualidade e a efetividade do material.

A ACADI-TI está comprometida em oferecer aos seus alunos o melhor material didático possível, para que eles possam ter uma experiência de aprendizado rica e significativa. Os diferenciais do material didático da ACADI-TI incluem:

- Conteúdo atualizado e relevante: com base nas últimas pesquisas e tendências do mercado.
- Abordagem interdisciplinar: conectando diferentes áreas do conhecimento para uma visão holística.
- Metodologias ativas de aprendizagem: que promovem o protagonismo do aluno e o desenvolvimento de habilidades essenciais.
- Acessibilidade e inclusão: com recursos para atender às necessidades de todos os alunos.

Ao investir em um material didático de qualidade e elaborado por uma equipe multidisciplinar, a ACADI-TI demonstra seu compromisso com a formação de profissionais completos, preparados para os desafios do mercado de trabalho e para contribuir para o desenvolvimento da sociedade.

2.16.2 Contribuição do material didático ao desenvolvimento do perfil do egresso

O material didático assume um papel crucial na formação do profissional em Defesa Cibernética. Elaborado com base no Projeto Pedagógico do Curso, ele contribui para o desenvolvimento das competências e habilidades essenciais para que o egresso atue de forma eficaz na proteção de sistemas e dados contra ataques cibernéticos. O material didático da ACADI-TI é cuidadosamente elaborado para garantir:

- **Abrangência:** cobertura de todos os tópicos relevantes da área de Defesa Cibernética, desde os conceitos básicos até as técnicas mais avançadas de proteção contra ataques cibernéticos.
- **Aprofundamento:** estudo detalhado dos principais temas da área, com foco na aplicação prática dos conhecimentos adquiridos.
- **Coerência Teórica:** organização dos conteúdos de forma lógica e sequencial, com base nas mais recentes pesquisas e tendências da área.

O material didático da ACADI-TI está diretamente relacionado ao perfil do egresso em Defesa Cibernética, definido neste Projeto Pedagógico do Curso. O conteúdo é estruturado para que o aluno desenvolva as seguintes competências e habilidades:

- **Conhecimento técnico aprofundado:** domínio dos conceitos e técnicas de Defesa Cibernética, incluindo criptografia, segurança de redes, análise de malwares e investigação de incidentes.
- **Capacidade de análise e resolução de problemas:** habilidade para identificar, analisar e solucionar problemas de segurança cibernética de forma eficaz.
- **Pensamento crítico e reflexivo:** capacidade de avaliar criticamente as informações e tomar decisões estratégicas em situações complexas.
- **Comunicação eficaz:** habilidade para se comunicar de forma clara e concisa, tanto em linguagem técnica quanto em linguagem não técnica.
- **Atuação ética e profissional:** compromisso com os princípios éticos e legais da profissão, incluindo a responsabilidade social e a confidencialidade das informações.

O material didático da ACADI-TI incorpora diversas metodologias ativas de aprendizagem, como estudos de caso, simulações, projetos práticos e debates em grupo. Essas metodologias promovem:

- **Engajamento e participação ativa dos alunos:** o aprendizado se torna mais dinâmico e interessante, estimulando a autonomia e a criticidade dos alunos.
- **Desenvolvimento de habilidades essenciais:** os alunos colocam em prática os conhecimentos adquiridos, desenvolvendo habilidades como trabalho em equipe, comunicação, resolução de problemas e pensamento crítico.

- **Preparo para o mercado de trabalho:** os alunos se familiarizam com as ferramentas e técnicas utilizadas pelos profissionais de Defesa Cibernética, aumentando suas chances de sucesso na carreira.

O material didático do curso é um instrumento fundamental para a formação de profissionais em Defesa Cibernética completos e preparados para os desafios do mercado de trabalho. Através de sua abrangência, aprofundamento, coerência teórica e utilização de metodologias ativas de aprendizagem, o material didático contribui para o desenvolvimento do perfil do egresso definido no Projeto Pedagógico do Curso, formando profissionais éticos, competentes e capazes de atuar com excelência na proteção de sistemas e dados contra-ataques cibernéticos.

2.16.3 Acessibilidade metodológica e instrumental do material didático

A acessibilidade metodológica e instrumental do material didático é um pilar fundamental para a construção de um ambiente de aprendizagem inclusivo e equitativo e ele é uma preocupação fundamental da Equipe Multidisciplinar. Ela garante que todos os alunos, independentemente de suas características individuais ou necessidades específicas, tenham acesso ao conhecimento e participem ativamente do processo educativo.

Do ponto de vista metodológico, a acessibilidade se traduz na utilização de estratégias de ensino flexíveis e adaptáveis às diferentes formas de aprender. Isso significa diversificar os recursos didáticos, oferecer diferentes opções de atividades e avaliações, e adaptar o ritmo das aulas às necessidades individuais dos alunos.

No âmbito instrumental, a acessibilidade se refere à disponibilidade de ferramentas e recursos que possibilitem o acesso ao conteúdo e a participação nas atividades por todos os alunos. Isso inclui materiais didáticos em formatos acessíveis, tecnologias assistivas e adaptação do ambiente de aprendizagem.

A implementação da acessibilidade no material didático traz diversos benefícios para todos os alunos, como:

- Maior inclusão e equidade: Todos se sentem acolhidos e valorizados, independentemente de suas características individuais.
- Melhor desempenho acadêmico: A motivação e o engajamento aumentam, o que contribui para a melhoria do desempenho.

- Desenvolvimento de habilidades socioemocionais: O respeito às diferenças e a colaboração entre os alunos são incentivados, promovendo uma sociedade mais justa e inclusiva.

A Faculdade ACADI-TI, por meio de sua Equipe Multidisciplinar, está comprometida com a construção de um ambiente de aprendizagem acessível e acolhedor. O material didático da instituição é elaborado com base nos princípios do Universal Design for Learning (UDL), priorizando a flexibilidade, a adaptabilidade e a utilização de recursos multimídia e tecnologias assistivas.

Ao investir na acessibilidade metodológica e instrumental, a ACADI-TI demonstra seu compromisso com a formação de cidadãos críticos, autônomos e preparados para os desafios do mundo contemporâneo, em um ambiente que valoriza a diversidade e promove a inclusão de todos.

2.16.4 Adequação da bibliografia do material didático às exigências da formação.

A escolha da bibliografia feita pelo NDE foi essencial para a formação profissional do aluno do curso de Defesa Cibernética, uma vez que ela assegura que os estudantes adquiram conhecimento contemporâneo e aplicável, crucial para navegar os desafios na área da tecnologia. Por meio da consulta a obras recentes e de credibilidade, os alunos permanecem alinhados às inovações e metodologias mais atuais em suas respectivas áreas de estudo.

No curso de Defesa Cibernética se priorizou a seleção bibliográfica que obedece a critérios estritos, enfocando a relevância das obras para alcançar o perfil do egresso desenhado neste PPC e para entregar ao mercado de trabalho profissional que preparados para os desafios. Esse posicionamento garantiu a inclusão de trabalhos de autores renomados e especialistas, proporcionando uma base de conhecimento sólida e confiável.

A adoção de uma bibliografia pertinente traz múltiplos benefícios aos alunos de Defesa Cibernética, desde o acesso a informações atuais e verificadas até o estímulo ao pensamento crítico, encorajando a análise de diversas perspectivas e a formação de juízos próprios sobre os temas estudados. Além disso, a leitura de obras significativas permite um entendimento mais aprofundado do campo de estudo, capacitando os estudantes para enfrentar desafios complexos no ambiente profissional e a se familiarizarem com as ferramentas e técnicas usadas por profissionais da área.

A ACADI-TI emprega um processo de seleção rigoroso para suas fontes bibliográficas, incluindo livros, artigos científicos de periódicos de prestígio, e recursos online de instituições de pesquisa reconhecidas e órgãos governamentais, garantindo uma variedade de materiais ricos e informativos que enriquecem a jornada educacional dos estudantes. Há, portanto, uma preocupação com a bibliografia do material didático, e modo que esteja alinhado aos objetivos do curso.

Assim, ao priorizar uma bibliografia de alta qualidade, o curso de Defesa Cibernética reafirma seu comprometimento com uma formação abrangente e atual, incentivando os estudantes de Tecnologia a desenvolver habilidades críticas, expandir seus horizontes de conhecimento e preparar-se eficientemente para uma trajetória profissional bem-sucedida.

2.16.5 Uso de linguagem inclusiva e acessível no material didático.

Gerenciada pela Equipe Multidisciplinar, a adoção de uma linguagem inclusiva e acessível nos materiais didáticos emerge como um pilar fundamental para assegurar a inclusão e participação de todos os estudantes no processo educativo. Essa prática reconhece e respeita as diversas origens, características e necessidades dos alunos, possibilitando um acesso equânime ao conhecimento. Ao adotar uma abordagem que valoriza a diversidade, a Faculdade ACADI-TI contribui para a formação de uma comunidade acadêmica mais inclusiva e coesa.

Em seu compromisso com a excelência educacional, o material didático do curso de Defesa Cibernética emprega uma linguagem que é ao mesmo tempo clara e concisa. Este método prioriza frases curtas e um vocabulário de fácil compreensão, minimizando o uso de jargões técnicos desnecessários. Ao evitar gírias e expressões coloquiais, o material didático assegura o emprego de uma linguagem formal e neutra, que não somente facilita a compreensão do conteúdo mas também promove um ambiente de respeito mútuo.

A neutralidade de gênero na comunicação é outra característica essencial da linguagem inclusiva adotada pelo material didático, manifestada pelo uso de termos genéricos como "pessoas", "alunos", e "profissionais". Esta abordagem evita a marcação de gênero binária, refletindo o reconhecimento e a valorização da diversidade de gênero. Adicionalmente, a instituição abraça as múltiplas formas de leitura e aprendizagem, incorporando recursos visuais, auditivos e interativos para enriquecer a experiência educacional de todos os alunos.

Os benefícios de uma linguagem inclusiva e acessível são vastos e variados. Ela promove uma maior inclusão e equidade, fazendo com que todos os estudantes se sintam acolhidos e respeitados, independentemente de suas individualidades. Essa abordagem contribui para a melhoria do desempenho acadêmico, pois facilita a compreensão dos conteúdos. Além disso, estimula o desenvolvimento de habilidades socioemocionais importantes, como o respeito às diferenças e a valorização da diversidade, preparando os alunos para um mercado de trabalho que cada vez mais valoriza a comunicação inclusiva.

Entre as práticas específicas de linguagem inclusiva e acessível implementadas pelo material didático do curso de Defesa Cibernética destacam-se o uso de termos genéricos e não binários para evitar a discriminação, a eliminação de expressões que possam ser consideradas preconceituosas e a utilização de recursos multimídia, como imagens, gráficos, vídeos e podcasts. A instituição também se empenha em disponibilizar materiais em formatos variados, atendendo às necessidades de alunos com deficiências visuais ou auditivas, por exemplo, através de textos audiolivros e legendas.

2.16.6 Inclusão de recursos inovadores no material didático

No curso de Defesa Cibernética, os recursos didáticos inovadores assumem um papel fundamental, trazendo uma série de metodologias e tecnologias avançadas para enriquecer a experiência de aprendizagem dos alunos. A incorporação de Realidade Aumentada (RA) e Realidade Virtual (RV) destaca-se como uma dessas inovações, oferecendo simulações imersivas e objetos 3D interativos que permitem aos estudantes explorar conceitos complexos e cenários reais de maneira segura e controlada. Tais tecnologias transformam o ensino de temas avançados em Defesa Cibernética, facilitando a compreensão de ataques virtuais, sistemas de segurança e protocolos de defesa através de ambientes virtuais que simulam o mundo real.

Além disso, a gamificação vem se estabelecendo como uma estratégia pedagógica poderosa, envolvendo jogos educativos, dinâmicas de pontuação e recompensas, além de avatares e personalização. Esses elementos tornam o aprendizado mais atraente e motivador, estimulando habilidades vitais na área de Defesa Cibernética, como resolução de problemas, trabalho em equipe e pensamento estratégico. Ao transformar o estudo em uma experiência lúdica, a gamificação incentiva a persistência e o engajamento dos alunos nas atividades propostas.

A Inteligência Artificial (IA) é outra tecnologia revolucionária no material didático, com a implementação de chatbots e tutores virtuais para suporte individualizado, sistemas de adaptação curricular e feedback automático personalizado. Essas ferramentas proporcionam uma experiência de aprendizado mais adaptada e responsiva, ajustando-se ao ritmo e às necessidades específicas de cada aluno, um diferencial importante na formação em Defesa Cibernética, onde os conteúdos podem variar amplamente em complexidade e aplicabilidade.

Recursos audiovisuais interativos, como videoaulas com animações e gráficos, podcasts e audiobooks, e webinars e videoconferências, são fundamentais para transmitir conteúdos complexos de maneira clara e dinâmica. Esses formatos complementam os métodos tradicionais de ensino, oferecendo alternativas acessíveis e flexíveis que se adaptam às diversas preferências de aprendizado dos alunos, facilitando a absorção de conhecimento em tópicos como criptografia, análise de vulnerabilidades e estratégias de proteção cibernética.

A Aprendizagem Baseada em Projetos (ABP) integra os recursos inovadores ao material didático, promovendo o desenvolvimento de projetos práticos que refletem desafios reais do mercado de trabalho. Essa abordagem permite que os alunos apliquem teorias em contextos práticos, estimulando a colaboração, a resolução de problemas e o pensamento crítico, habilidades indispensáveis na área de Defesa Cibernética.

Recursos de acessibilidade, como legendas para videoaulas e podcasts, transcrição de textos para audiolivros, e ferramentas de leitura assistiva, garantem que o curso de Defesa Cibernética seja inclusivo e acessível a todos os alunos, independentemente de suas limitações ou necessidades especiais. Essa inclusão é essencial para promover a equidade na educação e assegurar que todos tenham as mesmas oportunidades de aprendizado e desenvolvimento profissional.

2.17 PROCEDIMENTOS DE ACOMPANHAMENTO E DE AVALIAÇÃO DOS PROCESSOS DE ENSINO-APRENDIZAGEM

2.17.1 Facilitação do desenvolvimento e autonomia do discente de forma contínua e efetiva

Na Faculdade ACADI-TI enfatizamos a importância de facilitar o desenvolvimento e a autonomia do discente de forma contínua e efetiva. Compreendemos que os procedimentos de acompanhamento e de avaliação são cruciais para garantir que os alunos não apenas aprendam, mas também evoluam ao longo de sua jornada educacional. Por isso, a avaliação formativa se destaca como uma abordagem central em nossa metodologia de ensino.

Essa abordagem de avaliação proporciona feedback imediato e orientações específicas, permitindo que os estudantes corrijam erros e aprimorem suas competências, além de projetada para respeitar as diferenças individuais. Reconhecendo que cada estudante possui um conjunto único de habilidades, necessidades e estágios de desenvolvimento, ajustamos nossos métodos de ensino e avaliação para atender de forma personalizada, promovendo assim uma aprendizagem significativa e o desenvolvimento da autonomia do estudante.

A implementação da avaliação formativa na Faculdade ACADI-TI visa criar um ambiente de aprendizado que não apenas educa, mas também empodera os estudantes, incentivando-os a se tornarem aprendizes autônomos e proativos. Ao promover a autoavaliação, a colaboração entre pares e a reflexão crítica, estimulamos nossos alunos a assumirem responsabilidade por seu próprio aprendizado, equipando-os com as ferramentas necessárias para se adaptarem e prosperarem em um mundo em constante mudança.

Através de um processo de acompanhamento contínuo, proporcionado por feedback constante dos professores e atividades colaborativas, os estudantes da ACADI-TI são encorajados a desenvolver um entendimento mais profundo de seus pontos fortes e áreas a melhorar. Este processo não apenas os ajuda a avançar academicamente, mas também a desenvolver habilidades importantes para sua futura carreira profissional, como pensamento crítico, solução de problemas e adaptabilidade.

Adotamos essa abordagem conscientes de que o processo avaliativo é dinâmico e requer revisões constantes para permanecer eficaz. Estamos comprometidos com o aprimoramento contínuo de nossos métodos de avaliação e acompanhamento, garantindo que sejam sempre realizados com a supervisão da coordenação do curso, o suporte da direção e a máxima transparência para com nossos alunos. Nosso objetivo é assegurar que a Faculdade ACADI-TI

não só eduque, mas também prepare os estudantes para serem profissionais autônomos, resilientes e adaptáveis, prontos para enfrentar os desafios do mundo moderno

2.17.2 Sistematização e disponibilização de informações das avaliações aos estudantes.

No curso de Defesa Cibernética a importância de uma comunicação transparente e eficaz entre docentes e discentes é reforçada, especialmente no que tange à sistematização e disponibilização de informações oriundas das avaliações. Compreendemos que para promover o desenvolvimento contínuo e a autonomia dos estudantes, é necessário não apenas avaliar, mas também garantir que eles compreendam profundamente seu desempenho e como podem aprimorá-lo.

Para atingir esse objetivo, estabelecemos procedimentos de acompanhamento e avaliação dos processos de ensino-aprendizagem, que são fundamentais para uma pedagogia orientada para o futuro. Esses procedimentos identificam áreas de excelência e de necessidade de melhoria, e fornecem um roteiro claro para o desenvolvimento pessoal e acadêmico do estudante.

Uma das estratégias chave é a utilização dos recursos nativos do próprio moodle, os quais estão acessíveis tanto por professores quanto por alunos. O Moodle é projetado para registrar e apresentar os resultados das avaliações de maneira organizada, permitindo que os estudantes acessem facilmente informações detalhadas sobre seu desempenho acadêmico. Através destes sistemas, os alunos podem revisar suas notas, feedbacks dos professores, e análises comparativas de seu progresso ao longo do tempo.

Além da disponibilização digital, promoveremos sessões regulares de feedback individual. Nestas sessões, os professores discutirão as avaliações de maneira mais detalhada, esclarecendo dúvidas e oferecendo orientações específicas para cada estudante. Isso permite uma interação rica e personalizada, na qual o aluno pode explorar profundamente os aspectos de seu desempenho que requerem atenção.

Para garantir uma análise completa, os procedimentos de avaliação são projetados para serem holísticos, abrangendo não apenas o desempenho acadêmico, mas também o desenvolvimento de competências e habilidades essenciais. Assim, os estudantes são

encorajados a refletir sobre o conhecimento técnico, e sobre habilidades interpessoais, trabalho em equipe e capacidade de solucionar problemas.

A sistematização dessas informações não serve apenas para informar o estudante sobre onde ele precisa melhorar, mas também celebra seus sucessos. Reconhecendo conquistas e progressos, incentivamos a motivação intrínseca e a resiliência, componentes vitais para a aprendizagem autodirigida e contínua.

Além disso, encorajamos os alunos a participarem ativamente do processo de avaliação, através da autoavaliação e da avaliação por pares. Essas práticas promovem a conscientização crítica sobre o próprio aprendizado e fomentam um ambiente educacional colaborativo, onde os estudantes aprendem uns com os outros, compartilhando insights e estratégias de estudo.

Por fim, estamos comprometidos em revisar e aprimorar continuamente nossos métodos de acompanhamento e avaliação, assegurando que eles permaneçam alinhados com as melhores práticas pedagógicas e com as necessidades em evolução de nossos estudantes. Através deste processo dinâmico e interativo, a Faculdade ACADI-TI assegura a excelência acadêmica, ao mesmo tempo em que prepara seus estudantes para serem profissionais competentes, autônomos e adaptáveis, prontos para enfrentar os desafios do futuro.

Para ser aprovado na disciplina, é necessário obter uma nota mínima de 7,0. A nota final é calculada com base em dois tipos de avaliações, cada uma representando 50% da nota total:

1. **Avaliações Formativas (50% do total)**: Estas avaliações são focadas no processo de aprendizagem e incluem:
    - Participação em fóruns e debates online, que contribui com 10% da nota final.
    - Realização de atividades, tanto individuais quanto em grupo, que representam 20% da nota.
    - Desenvolvimento de um portfólio digital, também valendo 20%.
2. **Avaliações Somativas (50% do total)**: Estas avaliações têm o objetivo de medir o conhecimento acumulado e incluem:
    - Projetos práticos e desafios, que correspondem a 30% da nota final.
    - Um exame prático, contribuindo com 20% da nota.

Para alunos com nota entre 3,0 e 6,9, serão oferecidas oportunidades de recuperação:

- **Exame de Recuperação**: Uma prova escrita sobre o conteúdo da disciplina. A data será definida pelo professor, e a nota mínima para aprovação é 7,0.
- **Exame Final**: Uma avaliação que pode ser escrita e/ou prática, abrangendo todo o conteúdo da disciplina. A data será definida pelo professor, e a nota mínima para ser aprovado é 7,0.

  Situações de Reprovação incluem:

  - Obter uma nota final inferior a 3,0.
  - Faltar em mais de 25% das atividades presenciais ou síncronas planejadas.
  - Não entregar mais de 25% das atividades avaliativas.

2.17.3 Garantia da natureza formativa dos mecanismos de avaliação.

A garantia da natureza formativa dos mecanismos de avaliação constitui um pilar essencial no processo de ensino-aprendizagem no curso de Defesa Cibernética. Esse enfoque amplia a compreensão sobre o papel das avaliações, e enfatiza sua importância como ferramentas de desenvolvimento contínuo. Ao assegurar que os procedimentos de acompanhamento e de avaliação mantenham sua essência formativa, cria-se um ambiente educacional onde o feedback e a orientação atuam diretamente no aprimoramento das competências dos alunos.

Para que os mecanismos de avaliação cumpram com seu propósito formativo eles são incorporados aos procedimentos que permitam a coleta, análise e utilização das informações de maneira estratégica. Isso envolve a implementação de um sistema de feedback contínuo, onde os alunos recebam retornos construtivos sobre seu desempenho de forma regular. Este processo não se limita a identificar as áreas que necessitam de melhoria, mas a reconhecer os pontos de excelência, incentivando o estudante a construir sobre suas forças.

Além disso, a natureza formativa da avaliação pressupõe uma abordagem personalizada, reconhecendo as necessidades individuais de aprendizagem de cada aluno. Isso significa adaptar os métodos de ensino e as estratégias de avaliação para melhor atender às diferentes formas de aprender, garantindo que todos tenham a oportunidade de se desenvolver plenamente. Para tal, é importante que os professores estejam equipados com as habilidades e ferramentas necessárias para interpretar os dados da avaliação e aplicá-los eficazmente na orientação dos estudantes.

Outro aspecto crucial é a promoção da autoavaliação e da reflexão entre os alunos, incentivando-os a tomar um papel ativo em seu processo de aprendizagem. Ao compreenderem melhor seus próprios progressos e dificuldades, os estudantes são capazes de estabelecer metas de aprendizagem mais realistas e estratégias de estudo mais eficazes, fomentando sua autonomia e responsabilidade.

A transparência também desempenha um papel importante na garantia da natureza formativa da avaliação. Isso envolve manter os alunos informados sobre os critérios de avaliação, os objetivos de aprendizagem e como seus trabalhos serão avaliados. Compreender claramente o que é esperado e como alcançar essas expectativas pode ajudar os alunos a direcionar seus esforços de maneira mais eficiente, resultando em uma experiência de aprendizado mais eficaz e gratificante.

Implementar mecanismos que assegurem a natureza formativa dos processos de avaliação requer um compromisso contínuo com a inovação e a melhoria da prática pedagógica. Isso pode incluir a revisão periódica dos métodos de avaliação, a capacitação docente e o desenvolvimento de recursos que suportem uma avaliação mais eficaz e orientada para o crescimento. Ao priorizar a avaliação como um instrumento de aprendizagem, as instituições de ensino podem cultivar um ambiente que não apenas mede, mas também melhora a aprendizagem dos alunos de maneira significativa e sustentável.

2.17.4 Planejamento de ações para melhorar a aprendizagem com base nas avaliações

O planejamento de ações concretas para aprimorar a aprendizagem dos alunos, com base nos resultados das avaliações, está a cargo do NDE, o qual valoriza os dados coletados durante os procedimentos de acompanhamento e de avaliação, e os emprega em informações estrategicamente, com o objetivo de promover um ambiente de aprendizado mais efetivo e inclusivo. O sucesso deste processo depende do compromisso com a análise detalhada dos resultados e a implementação de iniciativas que atendam às necessidades identificadas.

Inicialmente, a análise dos resultados das avaliações será realizado com o intuito de identificar tanto as áreas de destaque quanto aquelas que necessitam de aprimoramento. Este diagnóstico permitirá aos educadores compreender as lacunas de conhecimento, as dificuldades de aprendizado e os padrões de desempenho dos alunos. Com essas informações em mãos, será

possível desenvolver um plano de ação que aborde de forma específica e direcionada as necessidades de aprendizagem identificadas.

Uma das ações concretas será a revisão e adaptação do currículo ou dos métodos de ensino para torná-los mais alinhados com as necessidades dos alunos. Isso envolve a introdução de novos materiais didáticos, técnicas de ensino diferenciadas, e até mesmo o uso de tecnologias educacionais que possam facilitar o processo de aprendizagem e torná-lo mais interativo e engajador.

Outra ação importante será o fortalecimento do suporte individualizado aos estudantes, especialmente àqueles que apresentam maior dificuldade. Isso será realizado por meio de tutorias, sessões de reforço, grupos de estudo ou aconselhamento acadêmico, proporcionando um acompanhamento mais personalizado e focado na superação dos obstáculos de aprendizagem.

Além disso, o incentivo à autoavaliação e ao estabelecimento de metas de aprendizagem personalizadas serão práticas valiosas que motivarão os alunos a refletirem sobre seu próprio processo de aprendizado e a assumirem um papel ativo em seu desenvolvimento acadêmico. Essas estratégias fomentam a autonomia do estudante e o encorajam a buscar constantemente a melhoria e o aprofundamento de seus conhecimentos.

Promover a colaboração entre os alunos também será mais uma ação concreta derivada da análise dos resultados das avaliações. A criação de projetos colaborativos ou de grupos de estudo pode facilitar a troca de conhecimentos e experiências, enriquecendo o processo de aprendizagem e incentivando a construção coletiva do conhecimento.

A comunicação eficaz dos resultados das avaliações e das ações planejadas será fundamental para o sucesso dessas iniciativas. Os alunos estarão cientes de como seu desempenho influencia o planejamento pedagógico e como as ações implementadas visam apoiar seu desenvolvimento acadêmico. Essa transparência contribui para a criação de um ambiente de confiança e colaboração entre alunos e educadores.

Por fim, será estabelecido um ciclo contínuo de avaliação e revisão das ações implementadas, garantindo que elas sejam eficazes na melhoria da aprendizagem. Este processo iterativo permite ajustes e refinamentos constantes das estratégias pedagógicas, assegurando que a educação oferecida seja sempre relevante, desafiadora e adaptada às necessidades dos alunos.

2.18 NÚMERO DE VAGAS

No contexto da formação em Defesa Cibernética, a definição do número de vagas oferecidas busca alinhar as oportunidades educacionais com as demandas e capacidades institucionais. Na introdução neste PPC apresentamos um longo estudo do potencial em termos quantitativo e qualitativo, da instalação da Faculdade ACADI-TI em São José dos Campos e Vale do Paraíba. A Luz dos números fica evidente a adequação da demanda da região com as vagas solicitadas. Porém, importante ressaltar que há um estudo a parte sobre a determinação da quantidade destas vagas, chamado: **Estudo de vagas.**

2.18.1 Estudos periódicos

A determinação das 800 vagas para o curso de Defesa Cibernética não é estática; ela é embasada em estudos periódicos. Isso assegura que o número de vagas permaneça relevante e alinhado às necessidades emergentes do campo. Os estudos periódicos permitem ajustes proativos, garantindo que o curso continue a ser uma via robusta e atualizada de ingresso na área de Defesa Cibernética, refletindo as tendências do mercado e as inovações tecnológicas.

2.18.2 Estudos quantitativos e qualitativos

A análise para chegar às 800 vagas é tanto quantitativa quanto qualitativa, englobando uma gama de fatores que vão além dos números puros. Isso envolve considerar a qualidade do ensino, as expectativas dos estudantes, e as perspectivas de carreira no campo da Defesa Cibernética. A abordagem quantitativa assegura que o volume de vagas esteja em consonância com as demandas do mercado, enquanto a perspectiva qualitativa garante que o curso mantenha sua relevância e qualidade, proporcionando uma formação que atenda às exigências contemporâneas da área

2.18.3 Pesquisas com a comunidade acadêmica

A voz da comunidade acadêmica, incluindo alunos e docentes, é crucial no processo de determinação do número de vagas. Realizar pesquisas com essa comunidade permite identificar as necessidades, expectativas e possíveis lacunas no currículo. Essa interação direta assegura que o número de vagas para o curso de Defesa Cibernética seja um reflexo fiel das necessidades

educacionais e profissionais de alunos e professores, promovendo um ambiente de aprendizado dinâmico e engajado.

2.18.4 Adequação à dimensão do corpo docente

A decisão de ofertar 800 vagas leva em consideração também a capacidade e dimensão do corpo docente. É imperativo que haja professores suficientes para manter uma relação aluno-professor que favoreça um ensino de alta qualidade. A qualidade da educação depende diretamente da disponibilidade dos docentes para orientar, ensinar e apoiar os alunos, garantindo assim um aprendizado eficaz e aprofundado.

2.18.5 Adequação às condições de infraestrutura física e tecnológica

Por fim, a infraestrutura física e tecnológica é um pilar fundamental na definição do número de vagas. Para suportar as 800 vagas, é necessário que as instalações e os recursos tecnológicos sejam suficientes e estejam à altura dos desafios e necessidades específicas do curso de Defesa Cibernética. Isso inclui laboratórios bem equipados, acesso a softwares de última geração e uma rede que suporte o intenso tráfego de dados, essenciais para a prática e pesquisa na área.

A definição de 800 vagas para o curso de Defesa Cibernética reflete, portanto, um equilíbrio cuidadosamente calculado entre as necessidades de formação na área, a capacidade institucional e a demanda do mercado, assegurando que o curso permaneça relevante, acessível e de alta qualidade.

3. CORPO DOCENTE E TUTORIAL

3.1 NÚCLEO DOCENTE ESTRUTURANTE – NDE

A Sob a coordenação do Professor Fábio Sena da Luz, que atua como presidente do Núcleo Docente Estruturante (NDE) do curso de Defesa Cibernética, o NDE tem um papel crucial no desenvolvimento e na atualização deste Projeto Pedagógico do Curso, garantindo seu alinhamento com as necessidades operacionais, sociais e complementares da graduação. Essa liderança é essencial para dirigir as discussões, organizar as reuniões e definir as diretrizes que orientam as atividades do núcleo, assegurando uma abordagem coesa e integrada à evolução do curso. A estrutura de suporte para o NDE inclui a alocação dedicada de carga horária para as atividades do núcleo, além do apoio por meio de recursos técnicos, tecnológicos e financeiros, facilitando o cumprimento de suas responsabilidades.

O NDE atua como um órgão consultivo vital, empenhado em acompanhar e aprimorar continuamente o PPC através de estudos e atualizações periódicas. Essas atividades incluem a avaliação do sistema de avaliação de aprendizagem e a análise da congruência entre o perfil do egresso e as Diretrizes Curriculares Nacionais (DCN), além das novas exigências do mercado de trabalho. Este processo contínuo de revisão e atualização assegura que o curso de Defesa Cibernética se mantenha relevante e eficaz na preparação dos estudantes para os desafios profissionais que encontrarão.

Além disso, o NDE se beneficia das orientações da Comissão Própria de Avaliação (CPA) e da colaboração de membros convidados e professores do Colegiado do curso, enriquecendo o desenvolvimento técnico, metodológico e operacional do curso. Essa interação multidisciplinar fortalece o projeto pedagógico, garantindo que este reflita uma visão holística e integrada da formação oferecida, alinhada com os critérios de avaliação e as expectativas educacionais e profissionais, proporcionando uma base sólida para o sucesso contínuo e a evolução do curso de Defesa Cibernética na ACADI-TI.

3.1.1 Composição do NDE do curso

DOCENTES DO NÚCLEO DOCENTE ESTRUTURANTE - NDE		
Nome	**Titulação**	**R.T**
Fábio Sena da Luz	Especialista	Integral
Bruno Botelho	Especialista	Integral
Eduardo dos Santos Pereira	Doutorado	Parcial
Egberto Gomes Franco	Doutorado	Parcial
Josemar Monteiro Silva	Doutorado	Parcial

3.1.2 Regime de trabalho dos membros do NDE

O curso de Defesa Cibernética destaca-se por sua aderência estrita às diretrizes estabelecidas pela Resolução Nº 01, de 17 de junho de 2010, especialmente no que tange ao Inciso III do artigo 3º. Esta resolução estipula critérios rigorosos para a composição do corpo docente em instituições de ensino, assegurando uma alta qualidade acadêmica e profissional. Em conformidade com estas diretrizes, o curso manter um percentual de 40% de seus professores em regime de tempo integral (prof. Fábio Luz e Prof. Bruno Botelho), valor este superior ao mínimo de 20% exigido pela legislação.

3.1.3 Qualificação dos membros do NDE

O curso de Defesa Cibernética destaca-se também pelo cumprimento rigoroso do Inciso II da Resolução Nº 01, de 17 de junho de 2010, mantendo o percentual de 60% de mestres e doutores no Núcleo Docente Estruturante (NDE) do curso (prof. Egberto, Prof Josemar e Prof. Eduardo). Esta política vai além das expectativas mínimas estabelecidas pela legislação, refletindo o compromisso da instituição em oferecer um ensino de vanguarda, pautado pela excelência acadêmica e pela profundidade científica. A presença de um corpo docente qualificado, com vasta experiência em pesquisa e prática na área de Tecnologia, assegura um currículo atualizado e alinhado às necessidades do mercado, além de promover um ambiente de ensino rico em conhecimento avançado e inovação tecnológica. Este aspecto é fundamental para a formação de profissionais capacitados a desenvolver soluções inovadoras frente aos complexos desafios da segurança cibernética contemporânea.

3.1.4 Inclusão do coordenador de curso como integrante do NDE.

Conforme portaria emitida pelo Diretor Geral da Faculdade ACADI-TI, o Professor Fábio Sena da Luz, coordenador do curso de Defesa Cibernética, é nomeado como membro presidente do Núcleo Docente Estruturante (NDE) do curso de Defesa Cibernética.

3.1.5 Funções do NDE

O Núcleo Docente Estruturante (NDE) desempenha um papel fundamental na garantia da qualidade e relevância do ensino superior, sendo responsável pelo acompanhamento, consolidação e atualização contínua do Projeto Pedagógico do Curso (PPC). Esta função vital assegura que o currículo permaneça alinhado tanto às necessidades dos estudantes quanto às exigências do mercado de trabalho, incorporando avanços tecnológicos, mudanças na legislação educacional e novas práticas pedagógicas. O NDE, ao focar na evolução do PPC, contribui para que o curso ofereça uma formação sólida, abrangente e atualizada, preparando os estudantes não apenas para enfrentar os desafios atuais de sua área de atuação, mas também para antecipar tendências futuras.

Outra função crítica do NDE é a avaliação do impacto do sistema de avaliação de aprendizagem na formação dos estudantes. Esta análise envolve verificar se os métodos de avaliação adotados pelo curso estão efetivamente contribuindo para o desenvolvimento das competências esperadas nos formandos. O objetivo é garantir que a avaliação seja um processo contínuo de aprendizado, capaz de refletir o progresso dos estudantes de maneira justa e precisa, além de identificar áreas que necessitam de melhorias. Por meio dessa avaliação, o NDE busca assegurar que o sistema de avaliação promova uma educação de qualidade, estimulando o estudante a desenvolver não só conhecimentos específicos da área, mas também habilidades críticas, criativas e de resolução de problemas.

Por fim, o NDE ocupa-se da análise da adequação do perfil do egresso em relação às Diretrizes Curriculares Nacionais (DCN) e às novas demandas do mercado de trabalho. Este ponto é crucial para manter a relevância e a eficácia do curso, assegurando que os formandos possuam as competências, habilidades e conhecimentos demandados pelos empregadores e pela sociedade como um todo. Através de um diálogo constante com o mercado de trabalho e com base nas DCN, o NDE avalia e reajusta o perfil desejado dos egressos, garantindo que o curso mantenha seu alinhamento com as expectativas profissionais e sociais. Assim, o NDE contribui

significativamente para a formação de profissionais qualificados, aptos a contribuir positivamente em seus campos de atuação e na sociedade.

3.1.6 Planejamento para permanência de parte dos membros do NDE.

A garantia de permanência dos membros do Núcleo Docente Estruturante (NDE) até o reconhecimento do curso de Defesa Cibernética é uma estratégia essencial para assegurar a continuidade e a qualidade do projeto pedagógico. Nesse contexto, a decisão de estender a portaria de nomeação dos membros do NDE por um período de 4 anos, alinhado ao prazo para o reconhecimento do curso, revela-se uma medida prudente e estratégica. Esse planejamento antecipado permite uma gestão curricular coesa e uma implementação eficaz das políticas educacionais, mantendo a estabilidade do corpo docente e a continuidade pedagógica que são cruciais para o sucesso e a integridade do curso durante este período formativo e crítico.

Além de assegurar a continuidade pedagógica, a extensão da nomeação dos membros do NDE fortalece o processo de autoavaliação e o aprimoramento contínuo do curso. Com a permanência garantida até o reconhecimento, o NDE tem a oportunidade de implementar, monitorar e ajustar o projeto pedagógico com base em uma visão de longo prazo, antecipando desafios e respondendo às mudanças no ambiente educacional e tecnológico. Esse acompanhamento continuado promove a aderência às Diretrizes Curriculares Nacionais e às expectativas do mercado, além a incorporação de inovações pedagógicas e tecnológicas que enriquecem o currículo e a experiência de aprendizagem dos estudantes.

A estabilidade do NDE contribui igualmente para o fortalecimento das relações com a comunidade acadêmica e o setor de Defesa Cibernética. Manter parte do NDE até o reconhecimento do curso facilita o desenvolvimento de parcerias estratégicas com outras instituições, empresas e órgãos governamentais, abrindo portas para oportunidades de pesquisa, estágios e projetos conjuntos que enriquecem o curso e proporcionam experiências valiosas aos estudantes. Essas relações fortalecidas ajudam a garantir que o curso permaneça alinhado às necessidades atuais e futuras do campo de Defesa Cibernética, preparando os estudantes não apenas para ingressar no mercado de trabalho, mas para liderá-lo com competência e visão inovadora.

3.2 EQUIPE MULTIDISCIPLINAR

A Faculdade ACADI-TI, comprometida com a excelência na oferta de cursos de Educação a Distância (EAD) no ensino superior, cumpri as diretrizes e legislações vigentes, assegurando uma educação de qualidade e acessível a um espectro diversificado de alunos. A instituição, ao integrar uma Equipe Multidisciplinar qualificada em sua estrutura, não apenas cumpre com a regulamentação exigida pelo Ministério da Educação (MEC) – conforme estabelecido pela Lei 9.394 e pelo Decreto 9.057 –, mas também promove um ambiente de aprendizado enriquecedor e adaptado às necessidades contemporâneas dos estudantes.

A Equipe Multidisciplinar da Faculdade ACADI-TI é composta por profissionais altamente qualificados em áreas diversas, incluindo pedagogos, tecnólogos educacionais, tutores, especialistas em conteúdo, designers instrucionais. Esta equipe colabora estreitamente para desenvolver e implementar cursos que alcançam e superam os padrões de qualidade no ensino a distância. Suas funções abrangem o planejamento cuidadoso do curso, a produção de materiais didáticos inovadores, o acompanhamento personalizado dos alunos e a avaliação contínua do curso para garantir a constante evolução e aprimoramento.

3.2.1 Constituição de uma equipe multidisciplinar em acordo com o PPC

A Equipe Multidisciplinar na Faculdade ACADI-TI, seguindo as diretrizes estabelecidas pela legislação educacional para cursos de Educação a Distância (EaD) no ensino superior, é formada por um conjunto de profissionais de diferentes áreas de conhecimento e expertise, trabalhando em conjunto para oferecer uma educação de qualidade, rica e diversificada. Esta equipe é composta por pedagogos, responsáveis pelo desenvolvimento do projeto pedagógico do curso, pela definição das metodologias de ensino e pela avaliação da aprendizagem; tecnólogos educacionais, que criam e gerenciam ambientes virtuais de aprendizagem, produzem materiais didáticos multimídia e oferecem suporte técnico; tutores, que orientam e acompanham os alunos durante o curso, auxiliando-os nas dúvidas e dificuldades; especialistas em conteúdo, que garantem a qualidade e a atualidade dos conteúdos programáticos; designers instrucionais, responsáveis pela criação de materiais didáticos que promovem uma aprendizagem interativa e acessível; e administradores, que gerenciam os recursos humanos, financeiros e materiais necessários para a execução do curso.

Cada membro da equipe multidisciplinar desempenha funções específicas que são cruciais para o desenvolvimento, implementação e aprimoramento do curso, garantindo não apenas o cumprimento da legislação vigente, mas também a qualidade do ensino, a excelência do curso e a satisfação dos alunos. A colaboração e integração entre esses profissionais facilitam a produção de conteúdos de alta qualidade, a oferta de tutoria individualizada, a realização de avaliações efetivas do processo de aprendizagem e a promoção de melhorias contínuas no curso, destacando a importância fundamental da equipe multidisciplinar no sucesso dos cursos de EaD no ensino superior.

3.2.2 Responsabilidades da equipe multidisciplinar

A equipe multidisciplinar desempenha um papel crucial na elaboração, desenvolvimento e distribuição de tecnologias, metodologias e recursos educacionais empregados nos cursos oferecidos na modalidade de educação a distância. Essencialmente, esta equipe é incumbida de realizar avaliações periódicas do material didático, assegurando que este atenda aos objetivos de formação dos estudantes em termos de escopo, profundidade e consistência teórica. Além disso, a equipe garante a acessibilidade e a pertinência metodológica e instrumental dos materiais, bem como a relevância das bibliografias com relação às necessidades formativas.

As iniciativas conduzidas pela equipe multidisciplinar são detalhadas em um plano de ação estruturado, cujo propósito é "Administrar as tecnologias e conteúdos envolvidos nos sistemas educativos virtuais, promovendo um aprimoramento da qualidade do processo de ensino e aprendizagem". Este plano é acompanhado de documentação rigorosa, incluindo o registro de discussões e decisões tomadas, para formalizar os procedimentos adotados e assegurar a transparência e eficácia dos processos educacionais.

3.2.3 Previsão de um plano de ação documentado e implementado pela equipe.

A Equipe Multidisciplinar possui um plano de ação estrategicamente documentado e devidamente implementado, o qual é essencial para assegurar a organização e a eficácia das suas atividades. Este plano serve como um roteiro detalhado, delineando as etapas, os objetivos e as metodologias a serem seguidas pela equipe, garantindo assim que todos os esforços estejam alinhados com os propósitos educacionais estabelecidos. A documentação e implementação

desse plano permitem uma gestão eficiente dos processos educacionais, assegurando a qualidade e a coerência das iniciativas de ensino e aprendizagem na modalidade a distância.

3.2.4 Formalização dos processos de trabalho da equipe multidisciplinar.

A formalização do trabalho da Equipe Multidisciplinar está consolidada por meio de atas detalhadas, que registram as discussões, decisões e diretrizes estabelecidas em cada reunião. Este método de documentação assegura transparência, responsabilidade e facilita o acompanhamento de progresso das atividades planejadas. As atas funcionam como um histórico oficial do planejamento e execução das ações, reforçando a organização e a continuidade dos projetos em andamento, além de servirem como referência para futuras iniciativas.

3.3 Regime de Trabalho do Coordenador de Curso

3.3.1 Regime de trabalho do coordenador do curso: tempo integral.

O regime de trabalho do coordenador do curso de Defesa Cibernética, estabelecido como tempo integral, é fundamental para assegurar o desempenho eficaz e eficiente de suas múltiplas responsabilidades. Operando em uma jornada de 40 horas semanais, este regime permite que o coordenador se dedique plenamente às exigências complexas e variadas do cargo, desde a gestão administrativa e pedagógica até o desenvolvimento e implementação de estratégias inovadoras de ensino. Esse compromisso de tempo integral é crucial para facilitar a comunicação contínua com professores, estudantes e outros membros da comunidade acadêmica, bem como para participar ativamente em colegiados superiores, garantindo que o curso esteja alinhado com os objetivos institucionais e as necessidades dos alunos. Além disso, permite ao coordenador liderar pelo exemplo, promovendo uma cultura de excelência, inovação e inclusão que é vital para o sucesso e a relevância contínua do curso no cenário educacional competitivo de hoje.

3.3.2 Capacidade do regime de trabalho integral para atender a demanda do curso.

O regime de trabalho integral do coordenador do curso permite ele atender à demanda do curso Defesa Cibernética. Através de um compromisso de 40 horas semanais, este regime assegura que o coordenador possa adequadamente planejar, executar e monitorar todas as

atividades necessárias para manter a qualidade e relevância do curso. Esse tempo dedicado permite uma gestão abrangente que aborda não apenas a administração cotidiana e a solução de problemas emergentes, mas também o desenvolvimento de estratégias de longo prazo para a evolução do curso.

Ao ter a capacidade de imergir completamente nas necessidades do curso de Defesa Cibernética, o coordenador está em posição de promover a integração entre docentes e discentes, estimular a inovação pedagógica, e garantir a conformidade com padrões acadêmicos e regulamentações educacionais. Essencialmente, o regime de trabalho integral viabiliza uma resposta ágil e eficaz às demandas dinâmicas do ambiente acadêmico, fortalecendo o curso em sua missão de fornecer uma educação de qualidade e formar profissionais competentes

3.3.3 Responsabilidades do coordenador

As responsabilidades do coordenador do curso são multifacetadas e abrangentes, refletindo a complexidade e a importância de sua função dentro da instituição de ensino. Elas se estendem desde a liderança acadêmica e administrativa até a promoção de um ambiente educacional que seja inovador, inclusivo e propício ao desenvolvimento profissional e pessoal dos estudantes. O coordenador é encarregado de representar o curso perante os órgãos superiores da instituição, assegurando que as necessidades e os objetivos do curso sejam adequadamente comunicados e considerados nas decisões institucionais. Este papel também envolve a convocação e presidência de reuniões do Colegiado e do Núcleo Docente Estruturante (NDE), o que é fundamental para a gestão curricular e a qualidade do ensino.

Adicionalmente, o coordenador supervisiona a execução das atividades programáticas, fiscalizando a assiduidade e o desempenho de professores, tutores e alunos, além de apresentar relatórios anuais de atividades, sugerir a contratação ou dispensa de pessoal e exercer outras atribuições ligadas aos processos de ensino-aprendizagem. A manutenção e atualização do Projeto Pedagógico do Curso (PPC) e de indicadores de qualidade também estão sob sua responsabilidade, requerendo um esforço contínuo para atender e superar os padrões acadêmicos.

Outras responsabilidades cruciais incluem a promoção de ações que visem o atingimento dos objetivos da Faculdade ACADI.TI, descritos no regimento e no Plano de Desenvolvimento Institucional (PDI), e a aprovação de planos de ensino. O coordenador ainda

desempenha um papel vital na análise e deferimento de aproveitamento de estudos, na distribuição das atividades de ensino e iniciação científica entre os professores e na coordenação de suas atividades. Ademais, é esperado que ele promova a educação em direitos humanos, relações étnico-raciais, educação ambiental, e a proteção dos direitos de pessoas com transtorno do espectro autista (TEA), além de administrar as potencialidades do corpo docente para favorecer a integração e a melhoria contínua do ensino.

Essencialmente, o coordenador atua como um elo vital entre os estudantes, o corpo docente, a administração da instituição e a comunidade mais ampla, trabalhando incansavelmente para garantir que o curso não apenas atenda, mas exceda as expectativas de todas as partes interessadas, contribuindo significativamente para a reputação e o sucesso da instituição.

3.3.4 Representatividade nos colegiados superiores

A representatividade nos colegiados superiores, como o Conselho de Ensino, Pesquisa e Extensão (CONSEPE) e na Congregação desempenha um papel crucial na integração do curso de Defesa Cibernética às estratégias e políticas gerais na Faculdade ACADI-TI. Ao representar o curso nesses espaços decisórios, o coordenador assegura que os interesses, as necessidades e as particularidades do curso sejam considerados nas deliberações que afetam o corpo discente, o corpo docente e o currículo. Essa presença ativa nos colegiados superiores é essencial para garantir que o curso de Defesa Cibernética tenha voz ativa nas decisões que impactam diretamente sua estrutura, seus objetivos educacionais e suas metas de pesquisa e extensão.

A representatividade efetiva nesses fóruns permite ao coordenador defender a alocação adequada de recursos e o apoio institucional necessário para a excelência acadêmica, além de influenciar a criação e a reformulação de políticas que promovam a inovação, a segurança cibernética e a interdisciplinaridade. Além disso, contribui para a visibilidade e o reconhecimento do curso dentro e fora da instituição, facilitando parcerias estratégicas, intercâmbios acadêmicos e oportunidades de financiamento para projetos de pesquisa.

Por meio da representação eficaz no CONSEPE e em outros colegiados superiores, o coordenador tem a oportunidade de participar ativamente na formulação de estratégias que alinhem o curso de Defesa Cibernética às tendências globais e demandas do mercado de trabalho, garantindo assim a atualidade e a relevância do currículo. Essa participação estratégica

é vital para a sustentabilidade e o crescimento do curso, assegurando que ele continue a atrair estudantes de alto calibre e a formar profissionais qualificados, capazes de enfrentar os desafios complexos da cibersegurança no cenário digital contemporâneo.

3.3.5 Plano de ação para gestão e da administração do corpo docente:

A gestão eficaz e a administração do corpo docente são elementos fundamentais para o sucesso e a excelência de qualquer curso. Reconhecendo essa importância, existe um plano de ação meticulosamente elaborado para a gestão e administração do corpo docente, que é desenvolvido sob a liderança do coordenador. Este plano de ação não só articula estratégias e objetivos claros para a gestão do corpo docente, mas também estabelece mecanismos de avaliação e acompanhamento por meio de indicadores de desempenho específicos.

O coordenador assume a responsabilidade de elaborar esse plano de ação de forma documentada e compartilhada, garantindo transparência e facilitando a comunicação entre todos os envolvidos no processo educativo. A documentação e compartilhamento do plano permitem que professores, estudantes, e outros membros da comunidade acadêmica tenham acesso às diretrizes, objetivos e métricas que guiam a administração docente. Isso promove um ambiente de colaboração e responsabilidade coletiva, onde todos estão cientes das expectativas e contribuem ativamente para o alcance dos objetivos estabelecidos.

Os indicadores de desempenho da coordenação, previstos no plano de ação, são disponibilizados publicamente, reforçando o compromisso com a transparência e a prestação de contas. Esses indicadores são essenciais para monitorar a eficácia das estratégias implementadas, avaliar o desempenho do corpo docente, e identificar áreas para melhorias contínuas. Ao tornar essas métricas acessíveis, o coordenador fomenta um ciclo de feedback positivo que permite ajustes e refinamentos proativos nas práticas de gestão, visando sempre a melhoria da qualidade do ensino e a satisfação dos estudantes.

Essa abordagem estratégica para a gestão do corpo docente, fundamentada em um plano de ação claro e na avaliação contínua por meio de indicadores de desempenho, demonstra o comprometimento do coordenador com a excelência acadêmica e a inovação pedagógica. Ela é crucial para assegurar que o corpo docente seja não apenas altamente qualificado, mas também motivado e alinhado com os valores e objetivos institucionais, contribuindo assim para a formação de profissionais competentes e preparados para os desafios do futuro.

3.4 CORPO DOCENTE: TITULAÇÃO

3.4.1 Plano Individual de Atividade - PIT

O curso de Defesa Cibernética da Faculdade ACADI-TI, atualmente em processo de autorização junto ao credenciamento institucional, é sustentado por um corpo docente de notável expertise e qualificação acadêmica. Este grupo é composto por nove professores altamente capacitados, dentre os quais cinco possuem titulação de mestrado e doutorado, enquanto os quatro restantes são especialistas em suas respectivas áreas de conhecimento. Essa diversidade de formações acadêmicas garante uma abordagem rica e multidisciplinar aos conteúdos do curso, essencial para a formação de profissionais competentes e adaptáveis às dinâmicas exigências do campo da Defesa Cibernética.

A Faculdade ACADI-TI adota o **Plano Individual de Trabalho** (PIT) para cada um de seus docentes, um documento que reflete o compromisso da instituição com a excelência educacional. O PIT não é um requisito burocrático, mas uma ferramenta estratégica de planejamento e avaliação do desempenho docente. Por meio dele, é possível identificar, desenvolver e potencializar as habilidades individuais de cada professor, alinhando-as com as necessidades e objetivos específicos do curso de Defesa Cibernética.

Importante destacar, o PIT funciona como um relatório de estudo detalhado que, levando em consideração o perfil do egresso delineado neste Projeto Pedagógico do Curso (PPC), demonstra e justifica a relação direta entre a titulação do corpo docente e sua eficácia em sala de aula. Esse processo de análise e justificação é fundamental para assegurar que a formação oferecida esteja em perfeita consonância com as expectativas de desempenho e competência dos futuros profissionais da área.

A estratégia educacional embasada no PIT e na qualificação do corpo docente visa, portanto, criar um ambiente de aprendizado dinâmico, inovador e profundamente alinhado com as tendências e necessidades do setor de Defesa Cibernética. A interação entre professores altamente qualificados e metodologias de ensino avançadas possibilita o desenvolvimento de habilidades técnicas, críticas e analíticas essenciais para a atuação eficaz e responsável dos futuros especialistas em segurança cibernética.

3.4.2 Relacionando da qualificação docente com o desenvolvimento acadêmico

No curso de Defesa Cibernética, a qualificação dos professores é a chave para o desenvolvimento do pensamento crítico nos alunos, além da compreensão aprofundada dos conteúdos tradicionais. A formação acadêmica e a experiência profissional do corpo docente criam um alicerce robusto que facilita o acesso a pesquisas avançadas e tendências emergentes no setor, além de incentivar a exploração criativa e inovadora de novas ideias. Projetos multidisciplinares, integrados ao currículo, exemplificam essa abordagem ao promover uma combinação de habilidades práticas e teóricas, estimulando assim a inovação e a criatividade nos alunos. Estas iniciativas destacam como a expertise dos professores ultrapassa a transmissão de conhecimento, fomentando uma experiência educacional rica que valoriza tanto a pesquisa aplicada quanto a teoria.

A escolha criteriosa dos membros do corpo docente reflete um equilíbrio perfeito entre a excelência acadêmica e a relevância prática. Professores que são reconhecidos tanto por suas contribuições acadêmicas quanto por suas experiências no mercado de trabalho trazem perspectivas únicas para a sala de aula, combinando estudos de caso reais, inovações tecnológicas e um profundo entendimento das dinâmicas atuais da cibersegurança. Esta fusão entre a teoria e a prática enriquece o aprendizado, permitindo que os alunos não só adquiram conhecimentos fundamentais, mas também desenvolvam uma habilidade crítica para aplicar esses conceitos de forma inovadora e eficaz em contextos reais.

Através da integração de conceitos avançados e tecnologias de ponta no ensino, o curso se posiciona na vanguarda da formação em Defesa Cibernética. As aulas dinâmicas, os projetos de pesquisa e a orientação personalizada proporcionam aos alunos uma exposição direta às últimas inovações do setor, equipando-os com as ferramentas necessárias para se destacarem como líderes inovadores. Este enfoque na aplicabilidade direta do conhecimento e na exploração de fronteiras tecnológicas prepara os alunos para contribuir com o avanço da segurança digital, enquanto enfatiza a importância da capacidade de pensar criticamente, desafiando-os a ir além da bibliografia proposta e a engajar-se ativamente com as questões mais prementes da área.

A base sólida proporcionada pela titulação e pela experiência dos professores do curso de Defesa Cibernética fundamenta uma abordagem educacional que prioriza o desenvolvimento do raciocínio crítico e a capacidade de inovação entre os alunos. Essa estratégia não só prepara

os discentes para enfrentar e antecipar os desafios futuros da cibersegurança, mas também os habilita a contribuir de maneira significativa tanto no âmbito profissional quanto acadêmico, fortalecendo o perfil do egresso como um profissional completo e adaptável às demandas de um campo em constante transformação.

3.4.3 Relacionar os conteúdos de pesquisa aos objetivos das disciplinas e ao perfil do egresso

A titulação do corpo docente do curso de Defesa Cibernética, composto por cinco professores com formação stricto sensu (mestrado e doutorado) e quatro com formação lato sensu (especialização), constitui a base sólida para estabelecer a conexão essencial entre a pesquisa, os objetivos de conhecimento e o perfil desejado do egresso. Esta diversificação nas qualificações acadêmicas dos professores não apenas enriquece o conteúdo programático, mas também garante que os métodos de ensino estejam alinhados às necessidades práticas e teóricas do campo de Defesa Cibernética. O alto nível de formação dos professores stricto sensu facilita a integração de pesquisas avançadas e conhecimentos de ponta nas disciplinas, promovendo uma educação que é ao mesmo tempo profundamente teórica e imediatamente aplicável aos desafios reais da área.

A experiência acadêmica e profissional desse corpo docente altamente qualificado possibilita uma abordagem pedagógica que transita com fluidez entre teoria e prática. Professores com doutorado e mestrado trazem para o ambiente de aprendizado uma perspectiva de pesquisa avançada, fundamentada na investigação científica, o que permite aos alunos acessar e contribuir para o corpo de conhecimento em Defesa Cibernética. Essa profundidade teórica, combinada com a aplicabilidade prática trazida pelos especialistas com formação lato sensu, que frequentemente possuem experiência direta nos mais diversos cenários da indústria de tecnologia, cria um cenário educacional onde os alunos podem vivenciar a aplicação real dos conceitos aprendidos, alinhando-se assim ao perfil desejado do egresso.

Ademais, a composição do corpo docente reflete uma estratégia deliberada para cobrir todos os aspectos necessários para uma formação abrangente em Defesa Cibernética. Os professores *stricto sensu*, com suas habilidades de pesquisa e análise, estão equipados para liderar os alunos na exploração de novas áreas do conhecimento, encorajando a inovação e a busca por soluções inéditas. Já os professores *lato sensu*, com sua vasta experiência prática, são

fundamentais para transmitir conhecimentos aplicados, garantindo que os alunos estejam preparados para os desafios práticos da profissão. Essa combinação assegura que o curso atenda aos seus objetivos pedagógicos, formando profissionais qualificados, criativos e prontos para contribuir efetivamente no campo da cibersegurança.

A titulação do corpo docente é, portanto, mais do que uma simples formalidade acadêmica; ela é a pedra angular do processo de ensino-aprendizagem no curso de Defesa Cibernética. Garante que o curso mantenha um padrão de excelência e atualidade, fundamentais para preparar os alunos para um mercado de trabalho competitivo e em constante evolução. Ao promover uma integração efetiva entre pesquisa, prática e os objetivos de aprendizagem, a Faculdade ACADI-TI assegura que seus egressos sejam não apenas especialistas em suas áreas, mas também inovadores capazes de liderar o avanço tecnológico e de enfrentar os desafios emergentes no mundo da cibersegurança.

3.4.4 Incentivar a produção de conhecimento

A excelência acadêmica e a inovação no campo da pesquisa são pilares fundamentais, impulsionados por um corpo docente altamente qualificado. Os professores, especialmente aqueles com formação stricto sensu, desempenham um papel crucial no incentivo à produção do conhecimento, promovendo ativamente a criação de grupos de estudo e pesquisa, bem como a publicação acadêmica. Este compromisso com a pesquisa avançada é uma característica distintiva do curso, refletindo o objetivo de não transmitir conhecimento, mas de gerar novas ideias e soluções inovadoras no campo da cibersegurança.

Adotando metodologias ativas de ensino e uma abordagem baseada em projetos, como foi trabalhado página atrás na matriz curricular e na seção de metodologia, o curso está desenhado para colocar os alunos em um processo contínuo de pesquisa e descoberta. Essa estratégia pedagógica fomenta uma aprendizagem engajada, onde os estudantes são protagonistas do seu processo educacional, encorajados a explorar problemas reais e desenvolver soluções criativas. Tal abordagem facilita a aquisição de conhecimento prático e teórico, e estimula o pensamento crítico e a capacidade de inovação entre os alunos.

Reconhecendo a importância da pesquisa para o desenvolvimento acadêmico e profissional dos estudantes, a Faculdade ACADI-TI alocou uma dotação orçamentária significativa para investimentos nessa área. Este comprometimento financeiro demonstra o

suporte institucional para a pesquisa e a inovação, assegurando que os recursos necessários estejam disponíveis para que alunos e professores possam conduzir seus estudos e projetos com eficácia.

Além disso, o curso de Defesa Cibernética introduzirá um programa de Iniciação Científica, liderado por professores com formação stricto sensu, denominado "**CiberInova**". Este programa visa aprimorar as habilidades de pesquisa dos alunos desde o início de sua jornada acadêmica, promovendo a participação em projetos de pesquisa, desenvolvimento de publicações científicas e contribuindo significativamente para o avanço do conhecimento na área de cibersegurança. O **"CiberInova**" reforça o compromisso do curso com a excelência acadêmica, e prepara os estudantes para se tornarem futuros líderes e inovadores no campo da Defesa Cibernética, equipados com uma sólida base de conhecimento teórico e experiência prática em pesquisa.

Em alinhamento com o compromisso da Faculdade ACADI-TI em promover a produção e disseminação do conhecimento, será inaugurada a "**CyberInova Journal**", uma Revista Acadêmica focada na publicação de projetos multidisciplinares e artigos derivados das pesquisas realizadas no curso de Defesa Cibernética. Esta plataforma ampliará a visibilidade dos trabalhos acadêmicos e científicos desenvolvidos, ao mesmo tempo que motivará os estudantes e docentes a se envolverem ainda mais com investigações aplicadas e teóricas. A "**CyberInova Journal**" visa estabelecer um elo contínuo entre a academia e os desafios práticos do campo de cibersegurança, consolidando a posição da Faculdade ACADI-TI como uma referência em inovação, pesquisa e excelência educacional na área.

Docente tutor	Titulação
Paulo Salvador Ribeiro Perrotti	Especialista
Bruno Botelho	Especialista
Fábio Sena da Luz	Especialista
Marlon Luís Petry	Especialista
Thiago Muniz	Especialista
Leonardo de la Rosa	Especialista
Josemar Monteiro Silva	Doutor
Egberto Gomes Franco	Doutor
Fábio Cristiano de Moraes	Doutor
Eduardo dos Santos Pereira	Doutor
Victor de Andrade Machado	Mestre

3.5 REGIME DE TRABALHO DO CORPO DOCENTE DO CURSO

3.5.1 Regime de trabalho do corpo docente para atender a demanda do curso

O regime de trabalho do corpo docente do curso de Defesa Cibernética está cuidadosamente planejado para atender às necessidades específicas do curso e garantir uma oferta educacional de qualidade. Dentre os nove professores que compõem a equipe, quatro serão contratados em regime de Tempo Integral, enquanto os outros cinco atuarão em Tempo Parcial. Essa estrutura é desenhada para oferecer flexibilidade e, ao mesmo tempo, assegurar a disponibilidade de professores altamente qualificados para cobrir todas as áreas de conhecimento necessárias, promovendo um ambiente de aprendizado rico e diversificado.

Os professores em regime de tempo integral terão um papel crucial no desenvolvimento e na implementação do currículo, além de liderar projetos de pesquisa e extensão. Sua presença constante na instituição facilita uma interação mais profunda e contínua com os alunos, proporcionando um suporte acadêmico robusto e acessível. Por outro lado, os docentes em tempo parcial trazem para o curso uma perspectiva valiosa do mercado de trabalho atual e das tendências emergentes no campo da cibersegurança, enriquecendo o currículo com suas experiências práticas e conhecimento especializado.

A distribuição entre regimes de trabalho integral e parcial foi pensada para assegurar que o curso de Defesa Cibernética inicie suas operações com uma base sólida e apta a atender plenamente às demandas dos alunos. Essa configuração permite a implementação de uma pedagogia dinâmica e interativa, caracterizada pela presença de docentes dedicados tanto à teoria quanto à prática, garantindo assim uma formação acadêmica equilibrada e alinhada às exigências do mercado de trabalho.

Além disso, a gestão do curso, juntamente com a Comissão Própria de Avaliação (CPA) da Faculdade ACADI-TI, compromete-se a avaliar semestralmente o regime de trabalho do corpo docente. Esse processo de avaliação contínua tem como objetivo garantir que a estrutura docente permaneça alinhada às necessidades evolutivas do curso e aos interesses dos alunos. Essa abordagem adaptativa e reflexiva assegura a manutenção de altos padrões de qualidade educacional e a capacidade do curso de Defesa Cibernética em formar profissionais competentes e preparados para enfrentar os desafios do futuro.

3.5.2 Aspectos considerados no regime de trabalho dos docentes

O regime de trabalho dos professores do curso de Defesa Cibernética é pensando para abranger uma série de responsabilidades essenciais, garantindo uma educação de alta qualidade e um acompanhamento próximo do desenvolvimento dos alunos. Uma parcela significativa desse regime é destinada à dedicação à docência, elemento central no processo aprendizagem e desenvolvimento. Os professores são incentivados a desenvolver e aplicar metodologias de ensino inovadoras como já descrito em diversas momento neste PPC, que estimulem o engajamento e o aprendizado dos estudantes, criando um ambiente acadêmico rico e propício ao desenvolvimento intelectual e profissional dos discentes.

Além da docência, o regime de trabalho dos docentes inclui o atendimento aos discentes, permitindo um espaço para orientação acadêmica, esclarecimento de dúvidas e reforço dos conteúdos estudados. Esse atendimento personalizado promove o sucesso acadêmico dos alunos e para fortalecer a relação professor-aluno, criando um ambiente de apoio e confiança mútua. A participação dos professores em colegiados (NDE, CONCUR, CONSEP, Congregação) e comissões (CPA) também é um aspecto crucial, pois permite que contribuam ativamente para o desenvolvimento curricular, políticas educacionais e tomada de decisões, assegurando que o curso permaneça alinhado às necessidades dos alunos e às exigências do mercado.

O planejamento didático e a preparação e correção de avaliações de aprendizagem também ocupam uma parte importante do regime de trabalho dos professores. Essas atividades garantem que o processo educativo seja cuidadosamente planejado e alinhado com os objetivos do curso, promovendo uma avaliação o mais justa possível do desempenho dos alunos. Esse planejamento detalhado e a atenção dedicada à avaliação reforçam a qualidade do ensino, e fornecem feedback valioso para os estudantes, contribuindo para seu crescimento acadêmico e profissional. Ao abraçar essas responsabilidades, o corpo docente da Faculdade ACADI-TI assegura um compromisso com a excelência educacional e com o sucesso dos seus discentes no campo da Defesa Cibernética

3.5.3 Plano Individual de Trabalho (PIT)

A distribuição das cargas horárias e das atividades dos professores do curso de Defesa Cibernética na Faculdade ACADI-TI é estabelecida através do **Plano de Trabalho Individual**

(PIT). Este documento é essencial para organizar e planejar as responsabilidades dos docentes, cobrindo a dedicação à docência, o atendimento aos discentes, a participação em colegiados, o planejamento didático e a preparação e correção de avaliações de aprendizagem. O PIT define as expectativas e compromissos de cada professor com o curso e seus alunos, servindo como um guia para uma gestão eficiente do tempo e dos recursos, garantindo que todas as atividades sejam executadas com eficácia.

Elaborado em colaboração entre a coordenação do curso e os professores, o PIT é uma ferramenta adaptável, preparada para ajustar-se às mudanças nas demandas do curso e dos alunos. Isso possibilita uma adaptação ágil a novos desafios e oportunidades, mantendo o curso atualizado com práticas pedagógicas avançadas e as últimas tendências no campo da cibersegurança. A documentação clara das cargas horárias e responsabilidades promove a transparência e facilita a comunicação entre docentes, discentes e administração, contribuindo para um ambiente acadêmico coeso e eficiente.

O PIT também reflete o empenho da Faculdade ACADI-TI em manter a excelência do ensino e fomentar o desenvolvimento profissional dos docentes. Com um planejamento detalhado das atividades docentes, a instituição garante o alcance dos objetivos educacionais do curso de Defesa Cibernética e apoia o desenvolvimento e a satisfação dos professores em seu papel educacional. Este planejamento evidencia a valorização da faculdade pelo trabalho docente e seu impacto significativo na trajetória acadêmica e profissional dos alunos, destacando o compromisso dos professores na missão educacional da Faculdade ACADI-TI.

3.5.4 Planejamento e gestão

O Plano de Trabalho Individual (PIT) implementado no curso de Defesa Cibernética da Faculdade ACADI-TI serve como uma ferramenta fundamental de gestão e melhoria contínua. Essencial para a organização e o planejamento das atividades docentes, o PIT permite um alinhamento preciso entre as expectativas da instituição e a atuação dos professores, garantindo uma execução eficaz das tarefas acadêmicas. Este documento detalha as responsabilidades de cada docente, incluindo aulas, pesquisa, atendimento aos alunos e participação em comissões, proporcionando uma visão clara das contribuições individuais para os objetivos educacionais do curso.

Além de servir como uma diretriz para as atividades diárias dos professores, o PIT é uma peça-chave no processo de avaliação e desenvolvimento profissional. Por meio de revisões periódicas, a Faculdade ACADI-TI utiliza o PIT para identificar oportunidades de aprimoramento, tanto no nível individual quanto no coletivo, estimulando a adoção de práticas pedagógicas inovadoras e o envolvimento dos docentes em projetos de pesquisa e extensão. Este ciclo de feedback contínuo promove a excelência acadêmica e permite que a faculdade responda de maneira ágil às mudanças nas demandas do mercado e às necessidades dos estudantes.

Assim, o PIT transcende a função básica de documentação das cargas horárias, transformando-se em um instrumento estratégico de gestão. Ele é essencial para fomentar uma cultura de melhoria contínua, onde a autoavaliação e o desenvolvimento profissional dos professores são incentivados. A implementação do PIT demonstra o compromisso da Faculdade ACADI-TI com a qualidade do ensino e com a satisfação dos alunos, reforçando sua missão de formar profissionais altamente qualificados e prontos para enfrentar os desafios do campo da Defesa Cibernética.

Docente tutor	Regime de trabalho
Paulo Salvador Ribeiro Perrotti	Tempo Parcial
Bruno Botelho	Tempo Integral
Fábio Sena da Luz	Tempo Integral
Marlon Luís Petry	Tempo Parcial
Thiago Muniz	Tempo Parcial
Leonardo de la Rosa	Tempo Parcial
Josemar Monteiro Silva	Tempo Parcial
Egberto Gomes Franco	Tempo Parcial
Fábio Cristiano de Moraes	Tempo Integral
Eduardo dos Santos Pereira	Tempo Parcial
Victor de Andrade Machado	Tempo Parcial

3.6 EXPERIÊNCIA PROFISSIONAL DO DOCENTE

3.6.1 Relatório de estudo

No curso de Defesa Cibernética a importância da experiência profissional dos professores é fundamentada e detalhada em um documento específico, intitulado "**Perfil do Corpo Docente**". Este relatório complementar ao Projeto Pedagógico do Curso (PPC) realiza uma análise aprofundada, considerando o perfil do egresso deste curso e que já foi tratado neste

PPC em sua seção própria. O estudo destaca a qualificação acadêmica dos docentes, e enfatiza suas trajetórias profissionais no campo da cibersegurança ou área corretada que são uteis ao egresso, demonstrando como essa experiência é essencial para alcançar os objetivos educacionais e profissionais do curso.

A experiência prática que os professores trazem para a sala de aula enriquece significativamente o processo de aprendizagem. Por meio de exemplos contextualizados e estudos de caso reais, eles são capazes de ilustrar a aplicação direta dos conceitos teóricos em situações práticas enfrentadas por profissionais da área. Isso facilita a compreensão e a retenção do conhecimento por parte dos alunos e os prepara de maneira mais efetiva para os desafios do mercado de trabalho. O "Perfil do Corpo Docente" sublinha a importância dessa integração entre teoria e prática, assegurando que o curso permaneça atualizado e alinhado com as tendências e necessidades contemporâneas do setor de cibersegurança.

Além disso, o relatório evidencia o compromisso da faculdade em promover a interdisciplinaridade e em desenvolver as competências previstas no PPC, conectando-as com a experiência profissional dos docentes. Ao analisar as competências em relação ao conteúdo programático e às exigências da profissão, o documento "Perfil do Corpo Docente" serve como um testemunho do alinhamento entre os objetivos do curso e a prática pedagógica. Isso reforça o papel vital da experiência dos professores na preparação dos alunos para se tornarem profissionais qualificados, capazes de contribuir significativamente para o avanço da cibersegurança.

3.6.2 Relação entre experiência profissional e desempenho em sala de aula

Professores que acumularam uma vasta experiência no setor da cibersegurança enriquecem as aulas com conhecimento técnico avançado e uma visão clara dos desafios da indústria. Eles transformam o ambiente de aprendizado ao conectar diretamente teorias com práticas do mundo real, oferecendo aos alunos exemplos concretos e relevantes que ilustram a aplicação dos conceitos estudados.

Esses professores aplicam métodos de ensino dinâmicos, como estudos de caso, simulações e projetos práticos, que engajam os alunos e desenvolvem habilidades críticas necessárias no mercado de trabalho. Eles enfatizam a importância de habilidades técnicas e competências transversais, como liderança e comunicação eficaz, compartilhando experiências

do ambiente profissional que preparam os alunos para além dos aspectos técnicos da carreira de cibersegurança.

A experiência dos docentes contribui para o desenvolvimento de uma educação que abrange conhecimentos técnicos e habilidades interpessoais. Isso prepara os alunos para enfrentar os desafios profissionais com uma perspectiva abrangente, necessária para o sucesso na área de cibersegurança. A abordagem educacional do curso, enraizada na prática profissional dos professores, destaca-se como um diferencial significativo, promovendo um ambiente de aprendizado rico e aplicável.

Este impacto se estende à motivação e ao engajamento dos alunos, que percebem a relevância e a aplicabilidade do seu aprendizado no contexto profissional. Tal percepção inspira os estudantes a dedicarem-se mais profundamente ao seu desenvolvimento acadêmico e profissional. A influência positiva da experiência profissional dos professores fomenta uma cultura de excelência e inovação entre os alunos, preparando-os para serem não só competentes, mas também inovadores na área de cibersegurança.

3.6.3 Capacidade de apresentar exemplos contextualizados

A habilidade dos professores do curso de Defesa Cibernética em apresentar exemplos contextualizados constitui uma ferramenta pedagógica valiosa que enriquece o processo de ensino-aprendizagem. Utilizando sua vasta experiência profissional, eles são capazes de desdobrar teorias complexas em situações práticas, tornando o conteúdo mais acessível e compreensível para os alunos. Esta abordagem facilita a compreensão dos conceitos, enquanto demonstra a relevância direta do currículo para os desafios que os estudantes enfrentarão em suas carreiras profissionais. Os exemplos práticos servem como pontes entre o conhecimento teórico e sua aplicação no mundo real, permitindo aos alunos visualizar como as soluções podem ser implementadas efetivamente no campo da cibersegurança.

Além disso, a apresentação de casos reais e exemplos contextualizados estimula o pensamento crítico e a análise, incentivando os alunos a pensar além das soluções convencionais. Esse método de ensino promove uma aprendizagem ativa, onde os estudantes são encorajados a questionar, explorar e propor novas soluções para problemas reais. Através dessas discussões e atividades práticas, os alunos desenvolvem uma compreensão mais profunda dos tópicos abordados e adquirem a capacidade de aplicar teorias em contextos

variados. Isso prepara os futuros profissionais de cibersegurança para serem adaptáveis e inovadores, qualidades essenciais em um campo que evolui rapidamente.

O uso de exemplos contextualizados pelos professores reflete uma abordagem educacional que valoriza a aplicabilidade do conhecimento. Preparando os alunos com uma base teórica sólida, e com uma compreensão prática de como essa teoria se aplica em situações do dia a dia na profissão de cibersegurança. Essa metodologia de ensino reforça a conexão entre a sala de aula e o ambiente de trabalho, equipando os alunos com as ferramentas e o pensamento crítico necessários para enfrentar os desafios futuros na área de cibersegurança, tornando-os profissionais mais competentes e prontos para contribuir significativamente para o setor.

3.6.4 Atualização de conteúdo e prática

No dinâmico campo da Defesa Cibernética, a atualização constante do conteúdo teórico e prático é essencial para manter o currículo alinhado com as inovações tecnológicas e as emergentes ameaças cibernéticas. Nesse contexto, os professores do curso de Defesa Cibernética desempenham um papel crucial, sublinhando a importância da integração entre a teoria ensinada e a prática profissional. Eles dedicam-se a uma contínua atualização profissional, garantindo que o conhecimento transmitido aos alunos seja atual, e aplicável aos desafios reais da área. Deste modo, asseguramos que o ensino oferecido esteja sempre na vanguarda da tecnologia e das práticas de segurança cibernética, preparando os alunos para se adaptarem e prosperarem em um ambiente profissional em constante mudança.

A integração entre conteúdo teórico e prática profissional demanda que os docentes estejam engajados com as últimas pesquisas, tendências, ferramentas e metodologias do campo. Isso envolve a participação em conferências, workshops e seminários, e o envolvimento direto em projetos de pesquisa e colaborações com a indústria. Tal compromisso com a atualização contínua enriquece o currículo e proporciona aos alunos insights valiosos sobre como aplicar o conhecimento teórico em contextos práticos. Além disso, prepara os estudantes para serem pensadores críticos e solucionadores de problemas, capazes de desenvolver novas estratégias de defesa contra ameaças cibernéticas cada vez mais sofisticadas. No âmbito do curso, tanto o grupo de pesquisa **CyberInova,** quanto a revista **CyberInova Journal** são aliados a prática docente de atualização dos conteúdos.

A prática de manter o conteúdo do curso atualizado reflete um compromisso com a excelência educacional e com a preparação dos alunos para as demandas do futuro. Ao priorizar a atualização constante, os professores da Faculdade ACADI-TI garantem que os graduandos do curso de Defesa Cibernética adquiram conhecimento teórico robusto, e desenvolvam habilidades práticas relevantes. Isso por um lado aumenta a empregabilidade dos alunos ao se formarem, e por outro os capacita a contribuir para a segurança cibernética em um espectro global, enfrentando com confiança e competência os desafios que surgirem em suas carreiras profissionais.

3.6.5 Promoção da compreensão da interdisciplinaridade

No curso de Defesa a promoção da compreensão da interdisciplinaridade por parte dos professores reflete um aspecto crucial da formação dos alunos. Ao destacar como diversas disciplinas se entrelaçam para resolver complexos desafios da cibersegurança, os docentes ilustram a importância de uma abordagem holística no contexto profissional. Essa ênfase na interdisciplinaridade é evidenciada através dos **projetos multidisciplinares** integrados ao currículo, os quais são projetados para que os estudantes apliquem conhecimentos teóricos de campos variados, como tecnologia da informação, leis de proteção de dados, ética digital e gestão de riscos, em situações práticas.

Os projetos multidisciplinares previstos no curso servem como exemplos concretos da aplicação da interdisciplinaridade. Eles incentivam os alunos a colaborar com colegas de diferentes especializações, promovendo um ambiente de aprendizado colaborativo onde a troca de conhecimentos e perspectivas diversas enriquece a solução de problemas. Essa estratégia pedagógica reforça o entendimento dos alunos sobre como as diversas áreas de conhecimento se complementam na prática profissional, e prepara-os para a realidade do mercado de trabalho, onde a capacidade de integrar conhecimentos e trabalhar em equipes multidisciplinares é altamente valorizada.

Além disso, ao participarem desses projetos, os estudantes desenvolvem uma compreensão mais profunda das nuances da cibersegurança, reconhecendo que soluções eficazes exigem uma visão abrangente que transcenda as fronteiras tradicionais do conhecimento. Essa exposição prática prepara os futuros profissionais de cibersegurança para enfrentarem os desafios emergentes do setor com um arsenal de soluções criativas e efetivas.

Os professores da Faculdade ACADI-TI, por meio de sua ênfase na interdisciplinaridade e na implementação de projetos multidisciplinares, asseguram que os alunos não apenas adquiram conhecimento técnico, mas também desenvolvam habilidades essenciais para uma carreira de sucesso e inovadora no campo da cibersegurança.

3.6.6 Análise de competências em relação ao conteúdo e profissão

A análise das competências em relação ao conteúdo abordado em sala de aula e as exigências da profissão são dimensões indissociáveis na estrutura do curso de Defesa Cibernética. Essa avaliação, alinhada ao Projeto Pedagógico do Curso (PPC), garante que o ensino esteja em perfeita sintonia com as habilidades e conhecimentos necessários para uma atuação profissional eficaz no campo da cibersegurança. Os professores, por meio de sua participação ativa no Núcleo Docente Estruturante (NDE), desempenham um papel vital nesta análise, assegurando que o currículo atenda às expectativas acadêmicas, e às demandas dinâmicas e em constante evolução do mercado de trabalho.

O envolvimento do corpo docente na revisão semestral das competências previstas no PPC através do NDE permite uma reflexão contínua sobre a relevância do conteúdo ensinado. Essa prática regular de revisão e atualização pedagógica possibilita a incorporação de novas tecnologias, metodologias e desafios emergentes do setor na estrutura curricular. Ao sugerir evoluções e melhorias no PPC, os professores garantem que os alunos se formem com uma base de conhecimento e habilidades que reflete as últimas tendências e necessidades da área de cibersegurança. Esse processo assegura a formação de profissionais capazes de se adaptar, inovar e liderar em um ambiente profissional que está sempre à frente de novos desafios.

Além disso, essa abordagem colaborativa para o desenvolvimento curricular enfatiza a importância da educação contínua e do aprendizado ao longo da vida como componentes essenciais para o sucesso na área de cibersegurança. Ao ajustar o PPC para refletir as mudanças no campo profissional, a Faculdade ACADI-TI prepara os alunos para os desafios atuais, e os equipa com a capacidade de continuar aprendendo e se desenvolvendo em suas carreiras. Esse comprometimento com a atualização constante e a melhoria do currículo demonstra a dedicação da instituição e de seus professores em fornecer uma educação que não apenas atenda, mas exceda as expectativas do mercado, preparando os alunos para serem líderes inovadores no campo da Defesa Cibernética.

3.7 Experiência no Exercício da Docência Superior

3.7.1 Relatório de adequação da experiência docente com o perfil do egresso

Complementar ao PPC, existe um estudo detalhado sobre a adequação da experiência docente ao perfil do egresso desejado pelo curso, intitulado "**Perfil do Corpo Docente",** como já mencionamos páginas atrás. Este relatório complementar foca em assegurar que a expertise e o conhecimento prático dos professores estejam em perfeita sintonia com as competências e habilidades que os alunos devem adquirir durante sua jornada educativa.

Considerando o perfil do egresso, que inclui competências técnicas profundas em áreas como segurança da informação, análise de vulnerabilidades, forense digital, e habilidades gerais como liderança, capacidade analítica e ética profissional, este documento complementar destaca a importância de um corpo docente altamente qualificado e experiente. Por exemplo, a disciplina "Avaliação de Ameaças de Invasão", crucial para formar profissionais capazes de identificar e avaliar vulnerabilidades, exige professores com experiência real em segurança cibernética e uma compreensão prática sobre as ameaças mais recentes e as tecnologias de defesa.

Para ministrar tal disciplina, o perfil do professor ideal inclui a sólida formação acadêmica, e uma vasta experiência profissional na área de cibersegurança, com conhecimentos específicos em ferramentas de avaliação de segurança e técnicas de invasão e defesa. Além disso, espera-se que este professor tenha habilidades comprovadas em didática e metodologias de ensino que facilitem a aplicação prática dos conceitos teóricos, promovendo um ambiente de aprendizado dinâmico e interativo. Por isso, neste caso exemplar, foi alocado a essa disciplina o prof. Leonardo de la Rosa.

O documento complementar ao PPC evidencia a metodologia de seleção e avaliação do corpo docente, assegurando que cada professor contribua significativamente para o desenvolvimento das competências e habilidades previstas no perfil do egresso. Além disso, ressalta a importância da interdisciplinaridade e da aplicação prática dos conhecimentos, características essenciais para preparar os alunos para os desafios complexos e multifacetados da defesa cibernética.

O estudo de adequação da experiência docente ao perfil do egresso é um componente essencial para garantir a qualidade e a relevância do ensino oferecido no curso de Defesa

Cibernética da Faculdade ACADI-TI. Ele reforça o compromisso da instituição em formar profissionais altamente qualificados, preparados para enfrentar as ameaças cibernéticas contemporâneas e contribuir para a segurança da informação no âmbito global.

3.7.2 Avaliação da capacidade dos docentes

No âmbito do Projeto Pedagógico do Curso (PPC) de Defesa Cibernética da Faculdade ACADI-TI, destaca-se uma iniciativa inovadora de colaboração com a Comissão Própria de Avaliação (CPA) visando aprimorar a qualidade e a eficácia do corpo docente em relação às expectativas e necessidades do curso. Esse projeto conjunto foca na avaliação da capacidade docente, um processo crucial para assegurar que a formação oferecida esteja em harmonia com o perfil do egresso, as demandas do mercado e as diretrizes curriculares estabelecidas.

O perfil do egresso do curso de Defesa Cibernética, meticulosamente delineado neste PPC, enfatiza a aquisição de conhecimentos técnicos avançados em áreas como análise de vulnerabilidades, criptografia e gestão de riscos, e o desenvolvimento de competências interpessoais, como trabalho em equipe, pensamento crítico e ética profissional. Este perfil exige, portanto, um corpo docente que domine profundamente os conteúdos teóricos e práticos, e possua habilidades pedagógicas para inspirar e engajar os alunos em seu processo de aprendizagem e desenvolvimento profissional.

A avaliação da capacidade docente, portanto, engloba uma série de critérios, como a experiência prática dos professores no campo da cibersegurança, sua contribuição para a produção científica e técnica na área, e sua habilidade em aplicar metodologias de ensino que estimulem o pensamento crítico e a resolução de problemas. Um exemplo claro dessa intersecção entre o perfil do egresso e a capacidade docente é observado na disciplina "Gestão de Riscos em Segurança da Informação", que requer um professor com sólida experiência em análise e mitigação de riscos, bem como competências para transmitir esses conhecimentos de forma aplicada, incentivando os alunos a desenvolverem suas próprias estratégias de gestão de riscos. E para esse caso exemplar é alocado o coordenador do curso, prof Fábio Sena da Luz.

Este projeto conjunto entre a CPA e o curso de Defesa Cibernética estabelece um mecanismo dinâmico de feedback e aprimoramento contínuo, onde os resultados das avaliações docentes são utilizados para identificar oportunidades de desenvolvimento profissional dos professores e ajustes no currículo, garantindo assim a alinhamento constante com os objetivos

educacionais do curso e as necessidades do mercado. Através desta abordagem colaborativa e reflexiva, a Faculdade ACADI-TI reafirma seu compromisso com a excelência acadêmica e a formação de profissionais altamente qualificados e adaptáveis às demandas crescentes e evolutivas do campo da cibersegurança.

3.7.3 Uso dos resultados das avaliações para aprimoramento da prática docente

No contexto do Curso Superior de Tecnologia em Defesa Cibernética a gestão do curso enfatiza a importância de utilizar os resultados das avaliações para o aprimoramento contínuo da prática docente. Através de um processo sistemático e semestral de avaliação, realizado pela Comissão Própria de Avaliação (CPA), os professores recebem feedback direto sobre suas disciplinas. Este processo não apenas realça áreas de sucesso, mas também identifica oportunidades de melhoria, orientando os esforços de desenvolvimento profissional e pedagógico dos docentes.

Essa estratégia de avaliação e feedback é vital para garantir a alinhamento das práticas de ensino com o perfil do egresso desejado, que inclui não apenas competências técnicas específicas na área de defesa cibernética, mas também habilidades transversais como pensamento crítico, capacidade de trabalhar em equipe e ética profissional. Ao contextualizar o feedback dentro das necessidades específicas de disciplinas, como por exemplo, “Gestão de Segurança da Informação”, é possível orientar o desenvolvimento docente de maneira mais focada, assegurando que os professores estejam equipados tanto com o conhecimento teórico quanto com as competências didáticas necessárias para instruir eficazmente os estudantes.

Para garantir a eficácia deste processo, o perfil do docente para ministrar cada disciplina é cuidadosamente considerado. Professores com experiência prática relevante e uma sólida base acadêmica na área de defesa cibernética são selecionados, assegurando que possuam não apenas o conhecimento técnico necessário, mas também habilidades pedagógicas para promover um ambiente de aprendizado envolvente e eficaz. Além disso, espera-se que estes professores demonstrem capacidade de liderança e contribuição para o campo, seja através de pesquisa aplicada, publicações ou prática profissional, reforçando a ponte entre teoria e prática.

Este enfoque na avaliação da CPA e no feedback semestral como ferramentas para o aprimoramento da prática docente evidencia o compromisso do curso com a qualidade do ensino e com a formação de profissionais altamente qualificados em defesa cibernética. Por

meio da reflexão contínua e do desenvolvimento profissional orientado, a Faculdade ACADI-TI assegura que seus professores estejam sempre alinhados com as últimas tendências e demandas do campo, contribuindo significativamente para a preparação dos alunos para os desafios do mercado de trabalho na área de cibersegurança.

3.7.4 Liderança dos docentes a frente das pesquisas

O curso de Defesa Cibernética destaca a importância crucial dos projetos de pesquisa (CyberInova), da revista acadêmica e dos projetos de extensão como pilares para a formação integral dos alunos e para o desenvolvimento de um corpo docente altamente qualificado e engajado na vanguarda da cibersegurança. Este compromisso é refletido na meticulosa seleção de professores, os quais são escolhidos não apenas por suas credenciais acadêmicas, mas também por suas contribuições significativas à pesquisa e prática profissional na área de cibersegurança.

A implementação de projetos de pesquisa permite que os estudantes mergulhem em investigações relevantes, trabalhando lado a lado com professores que lideram essas iniciativas. Essa colaboração não apenas enriquece a experiência de aprendizado, fornecendo um contexto prático para os conceitos teóricos, mas também posiciona a Faculdade ACADI-TI como um centro de inovação e descoberta na área de defesa cibernética. A revista acadêmica "CyberInova Journal", por exemplo, é uma iniciativa que ilustra o compromisso da instituição com a disseminação do conhecimento. Através dela, projetos de pesquisa e artigos de alta qualidade são publicados, ampliando a visibilidade dos trabalhos desenvolvidos e estimulando a participação ativa de professores e alunos no debate acadêmico global.

Adicionalmente, os projetos de extensão desempenham um papel vital na aplicação do conhecimento acadêmico em contextos reais, fortalecendo o vínculo entre a universidade e a comunidade. Sob a orientação de docentes com vasta experiência em suas áreas, esses projetos promovem a integração de soluções tecnológicas inovadoras em diversos setores da sociedade, contribuindo assim para o desenvolvimento social e a solução de problemas concretos.

A Faculdade ACADI-TI estabelece que apenas docentes com comprovada pesquisa e trabalho relevante são escolhidos para liderar essas importantes iniciativas. Isso garante que o corpo docente não apenas transmita conhecimento, mas também inspire, através de sua própria

experiência e realizações, a próxima geração de profissionais em defesa cibernética a buscar a excelência, a inovação e o impacto positivo na sociedade.

3.8 Experiência no Exercício da Docência na Educação a Distância

3.8.1 Relatório de adequação da experiência em Educação a Distância ao perfil do egresso

No âmbito do Curso Superior de Tecnologia em Defesa Cibernética, uma ênfase particular é dada à experiência dos professores no exercício da docência na educação a distância, conforme detalhado no segmento "Perfil do Corpo Docente". Este enfoque sublinha a importância de adaptar-se às modalidades educacionais contemporâneas, e destaca o compromisso da instituição em alinhar essa experiência com o perfil desejado do egresso.

O relatório de estudo de adequação da experiência na Educação a Distância com o perfil do egresso, no Documento Perfil do Corpo Docente, realiza uma análise da capacidade docente nesse contexto específico. Este relatório evidencia um processo de seleção criterioso, assegurando que todos os professores possuam a qualificação acadêmica necessária, e ao mesmo tempo, uma comprovada experiência em educar através de plataformas digitais. Tal experiência é fundamental para enfrentar os desafios inerentes ao ensino online, como manter o engajamento dos alunos, aplicar metodologias pedagógicas adaptativas e utilizar eficazmente as tecnologias educacionais.

A experiência prévia dos docentes em ambientes virtuais de aprendizagem (AVAs) e o domínio das práticas de ensino a distância permitem uma abordagem pedagógica que reconhece as particularidades dessa modalidade, adaptando o conteúdo e as metodologias para maximizar a eficácia do processo de ensino-aprendizagem. Isso inclui a habilidade de elaborar materiais didáticos digitais, realizar avaliações formativas e somativas online e promover uma interação construtiva com e entre os estudantes.

Dessa forma, o documento "Perfil do Corpo Docente" ressalta o compromisso da Faculdade ACADI-TI com a excelência educacional, assegurando que todos os professores estejam preparados para liderar o processo de aprendizagem em um contexto digital. Esse alinhamento entre a experiência docente na educação a distância e o perfil do egresso visa garantir uma educação de qualidade, preparando os alunos não apenas para enfrentar os desafios

da cibersegurança, mas também para prosperar em um ambiente de aprendizado online dinâmico e em constante evolução.

3.8.2 Avaliação da capacidade dos docentes na Educação a Distância

A capacidade dos docentes na Educação a Distância é um aspecto crucial para a qualidade do ensino oferecido pelo Curso Superior de Tecnologia em Defesa Cibernética. Essa capacidade é avaliada tanto pela gestão do curso quanto pela Comissão Própria de Avaliação (CPA), garantindo um alinhamento estratégico com os objetivos pedagógicos e o perfil do egresso estabelecidos neste Projeto Pedagógico do Curso (PPC). Esta abordagem dupla assegura uma análise abrangente e objetiva das competências dos professores no ambiente virtual, focando em sua expertise técnica e acadêmica, e em sua habilidade para engajar e transmitir conhecimentos de maneira eficaz em plataformas de ensino online.

Por meio desse processo de avaliação, a gestão do curso e a CPA colaboram para identificar oportunidades de desenvolvimento profissional contínuo para os docentes, bem como para implementar melhorias no desenho e na entrega dos cursos a distância. Esta avaliação contínua contribui para a elevação do padrão de qualidade da educação a distância oferecida, promovendo um ambiente de aprendizado rico, interativo e, acima de tudo, eficiente. A importância dada à capacidade docente na educação a distância reflete o compromisso da Faculdade ACADI-TI em fornecer uma experiência educacional excepcional, preparando os alunos para enfrentar com sucesso os desafios da área de Defesa Cibernética no cenário atual e futuro.

3.8.3 Uso dos resultados das avaliações para aprimoramento da prática docente

Este processo de avaliação tem como foco garantir a eficácia pedagógica dos professores em ambientes virtuais, assegurando que a transmissão do conhecimento e a interação com os alunos sejam realizadas de maneira eficiente e engajadora. A gestão do curso, em colaboração com a CPA, utiliza os resultados dessas avaliações para identificar áreas de fortalecimento e oportunidades de desenvolvimento profissional dos docentes, visando a melhoria contínua da qualidade de ensino.

Além disso, a Faculdade ACADI-TI emprega os resultados das avaliações para o aprimoramento da prática docente, estabelecendo um ciclo de feedback construtivo que permite

ajustes e melhorias nas metodologias de ensino e nas estratégias de aprendizagem. Esse processo de aprimoramento está alinhado ao perfil do egresso desejado, garantindo que os professores estejam equipados para atender às necessidades educacionais e profissionais dos alunos, preparando-os eficazmente para os desafios do campo de Defesa Cibernética. A utilização estratégica desses resultados enfatiza o compromisso da instituição com a excelência educacional e com a formação de profissionais qualificados e adaptados às demandas do mercado de trabalho.

3.8.4 Exerce a liderança e ter sua produção reconhecida

Os professores da ACADI-TI não só exemplificam a excelência em ensino dentro do campo da cibersegurança, mas também exercem uma influência significativa na produção e disseminação do conhecimento através de suas contribuições acadêmicas e publicações. Bruno Botelho, com sua especialidade em Cyber Security Architect e experiência como Professor de Hacking Ético, enriquece o campo com suas pesquisas sobre novas técnicas de ataque em sistemas web e um guia prático sobre Ethical Hacking, refletindo diretamente na prática e na educação em segurança da informação. Leonardo, focado em Cyber Security & Infrastructure Architect, complementa essa base com seus trabalhos sobre a importância da segurança de redes na era da Internet das Coisas, além de um guia completo para proteger infraestruturas digitais.

Ernest Gontijo, especializado em Forense Cibernética e Investigação Digital, contribui com guias práticos voltados para a investigação de crimes digitais, oferecendo uma visão detalhada dos procedimentos de perícia computacional. Leandro Mainardi, atuando como Diretor de Educação em Cibersegurança, traz para o público obras que democratizam o entendimento sobre cibersegurança e orientam sobre carreiras no setor, demonstrando um compromisso com a formação de profissionais qualificados e bem-sucedidos. Essas contribuições dos docentes da ACADI-TI não apenas solidificam a reputação da instituição como um centro de excelência em educação para cibersegurança, mas também reforçam seu papel ativo na vanguarda da pesquisa e inovação, impactando positivamente tanto a comunidade acadêmica quanto o mercado de trabalho nesse campo vital.

3.9 EXPERIÊNCIA NO EXERCÍCIO DA TUTORIA NA EDUCAÇÃO A DISTÂNCIA

3.9.1 Relatório de estudo que considera o perfil do egresso com o corpo tutorial

O Curso Superior de Tecnologia em Defesa Cibernética enfatiza a importância da experiência dos professores em educação a distância (EaD), conforme detalhado no documento "Perfil do Corpo Docente". Esse foco sublinha a necessidade de adaptar-se às modalidades educacionais contemporâneas e alinhar essa experiência com o perfil desejado do egresso. O relatório de estudo sobre a adequação da experiência na EaD com o perfil do egresso revela um processo de seleção criterioso, assegurando que todos os professores possuam a qualificação acadêmica necessária e uma comprovada experiência em educar por meio de plataformas digitais. Essa experiência é vista como fundamental para enfrentar os desafios inerentes ao ensino online, como manter o engajamento dos alunos, aplicar metodologias pedagógicas adaptativas, e utilizar eficazmente as tecnologias educacionais.

A capacidade dos docentes na Educação a Distância é considerada crucial para a qualidade do ensino oferecido. A gestão do curso e a Comissão Própria de Avaliação (CPA) colaboram para identificar oportunidades de desenvolvimento profissional contínuo para os docentes, além de implementar melhorias no design e na entrega dos cursos a distância. Este processo assegura uma educação de alta qualidade, promovendo um ambiente de aprendizado rico, interativo e eficiente.

Além disso, os tutores do curso, que desempenham um papel fundamental na Educação a Distância, são destacados por sua capacidade de identificar as dificuldades dos alunos, expor o conteúdo de maneira aderente às características da turma, apresentar exemplos contextualizados, e elaborar atividades específicas para promover a aprendizagem. Este suporte é complementado pelo uso de práticas inovadoras no contexto da EaD, destacando a preocupação constante da instituição com a interação entre tutores, docentes e coordenação, o que garante a mediação e articulação eficaz entre todos os atores do processo educacional.

3.9.2 Análise da relação entre experiência em tutoria EAD e desempenho do corpo tutorial

A Faculdade ACADI-TI, ao implementar seu Curso Superior de Tecnologia em Defesa Cibernética, ilustra um compromisso excepcional com a educação a distância (EaD),

especialmente no tocante à designação de disciplinas e atividades tutoriais. Este compromisso é exemplificado pela seleção criteriosa de professores com experiência destacada em áreas específicas de cibersegurança, garantindo que os alunos recebam instruções de especialistas altamente qualificados. Bruno Botelho, com sua especialidade em Cyber Security Architect Manager e experiência como professor de Hacking Ético, é um exemplo distinto. As publicações de Botelho, incluindo um guia prático para penetração e testes de vulnerabilidade, o posicionam como uma autoridade em técnicas avançadas de ataque em sistemas web, tornando-o ideal para tutorar disciplinas focadas em hacking ético e segurança de aplicações web.

Leonardo, especialista em Cyber Security & Infrastructure Architect e professor de Segurança de Redes, traz uma perspectiva essencial sobre a importância da segurança de redes na era da internet das coisas. Suas publicações, como um guia completo para proteger infraestruturas digitais, fornecem uma base sólida para a tutoria em cursos relacionados à segurança de redes e infraestrutura. Ernest Gontijo, com sua expertise em Forense Cibernética e Investigação Digital, oferece um conhecimento profundo sobre a investigação de crimes digitais, ideal para disciplinas focadas em forense digital e resposta a incidentes. Suas publicações servem como um recurso valioso para alunos interessados em aspectos legais e técnicos da cibersegurança.

Leandro Mainardi, Diretor de Educação em Cibersegurança, com suas publicações orientadas para o público geral e profissionais da área, destaca-se na promoção da conscientização sobre cibersegurança e no desenvolvimento de carreiras no campo. A experiência de Mainardi como educador em cibersegurança o torna particularmente apto para liderar módulos que abordem estratégias de defesa cibernética abrangentes e o desenvolvimento de habilidades profissionais no setor.

A Faculdade ACADI-TI, ao alinhar a experiência específica desses profissionais com as necessidades do curso, assegura não apenas a aderência às atividades propostas, mas também a formação de profissionais qualificados capazes de enfrentar os desafios contemporâneos da cibersegurança. Este alinhamento estratégico entre a expertise do corpo docente e as demandas do mercado reflete o compromisso da instituição em colocar as pessoas certas nos lugares certos, maximizando assim o impacto educacional e preparando os alunos para contribuições significativas no campo da defesa cibernética.

3.9.3 Capacidades do corpo tutorial avaliadas

No contexto do Curso Superior de Tecnologia em Defesa Cibernética da Faculdade ACADI-TI, a tutoria desempenha um papel vital na estrutura educacional, especialmente na modalidade de educação a distância (EaD). Essa importância é reconhecida e rigorosamente avaliada por meio de um processo contínuo de avaliação, conduzido tanto pela Comissão Própria de Avaliação (CPA) quanto pela gestão do curso. A CPA, um órgão institucional responsável pela autoavaliação da instituição, juntamente com a gestão do curso, analisa a eficácia das atividades tutoriais, focando em aspectos como a capacidade de identificar dificuldades dos alunos, a eficiência na exposição do conteúdo e a implementação de práticas inovadoras no contexto da EaD. Esse processo de avaliação assegura que os tutores não apenas atendam aos padrões acadêmicos e pedagógicos exigidos, mas também contribuam para uma experiência de aprendizado enriquecedora e eficaz para os alunos.

Além disso, o sucesso da tutoria, segundo avaliado pela CPA e pela gestão do curso, reflete diretamente no cumprimento da missão educacional da Faculdade ACADI-TI de formar profissionais qualificados, éticos e capazes de transformar vidas por meio da educação em cibersegurança. O processo avaliativo engloba não apenas a qualificação e a experiência profissional dos tutores, mas também sua habilidade em promover o engajamento dos alunos e facilitar o acesso ao conhecimento em um ambiente virtual. Esse mecanismo de avaliação contínua permite a instituição identificar áreas de melhoria, desenvolver estratégias pedagógicas mais eficazes e, consequentemente, aprimorar a qualidade do ensino ofertado. Desse modo, a ACADI-TI reafirma seu compromisso com a excelência educacional e com o desenvolvimento de um corpo discente bem-preparado para enfrentar os desafios do campo da cibersegurança.

3.9.4 Relacionamento com aluno e incremento no ensino aprendizagem

O perfil dos tutores no Curso Superior de Tecnologia em Defesa Cibernética destaca-se por abranger uma combinação essencial de conhecimentos sólidos em cibernética, segurança da informação, leis e regulamentos de cibersegurança, ética, compliance, e gestão de riscos cibernéticos, bem como investigações de incidentes cibernéticos, conforme já trabalhando no capítulo que trabalhemos sobre o Conhecimento, Atitudes, Habilidade dos tutores. Além disso,

é imprescindível que possuam expertise em metodologias de ensino a distância, tecnologias da informação e comunicação, e práticas de tutoria. A habilidade de se comunicar claramente, interagir positivamente promovendo aprendizagem colaborativa, resolver problemas que emergem durante o ensino, e gerir as atividades educacionais de maneira eficaz são atributos cruciais. As atitudes como disponibilidade, empatia, proatividade e resiliência complementam o perfil, assegurando uma abordagem ética e profissional às responsabilidades tutoriais.

Para estabelecer um relacionamento efetivo com os alunos e incrementar o ensino-aprendizagem, os tutores devem desenvolver um ambiente de confiança e respeito, onde os alunos se sintam confortáveis para expressar suas dificuldades e dúvidas. A proatividade na identificação e resolução de problemas, juntamente com a flexibilidade para adaptar estratégias de ensino às necessidades individuais dos alunos, é fundamental. Acompanhamento personalizado, seja através de atendimento individual por chats, e-mails ou videoconferências, ou por meio de atividades em grupo como fóruns de discussão e workshops, permite não apenas a transmissão do conhecimento, mas também a construção coletiva da aprendizagem. Este acompanhamento personalizado, juntamente com a avaliação contínua do desempenho dos alunos e fornecimento de feedback construtivo, são estratégias-chave para promover a compreensão dos conceitos, o desenvolvimento de habilidades práticas e aprimoramento das competências de comunicação e colaboração, conduzindo a um aprendizado mais eficaz e engajado.

3.9.5 Sugestão de atividades e leituras complementares

Na metodologia adotada pelo Curso Superior de Tecnologia em Defesa Cibernética está previsto que o tutor atue não apenas como um facilitador do processo de ensino-aprendizagem, mas também como um mentor para os alunos. Essa abordagem pedagógica ressalta a importância de ir além da mera transmissão de conteúdo previsto no material didático e no Plano de Ensino. Os professores tutores são encorajados a ampliar o escopo do aprendizado, introduzindo leituras complementares e recursos adicionais que enriqueçam a experiência educacional dos alunos. Isso implica numa prática educativa que valoriza a curiosidade intelectual, estimula o pensamento crítico e promove uma compreensão mais profunda das temáticas abordadas. Ao fazer isso, os tutores não apenas expandem o conhecimento dos alunos,

mas também os preparam para aplicar essas informações de maneira eficaz em contextos reais e desafiadores do campo da cibersegurança.

Esta abordagem é coerente com a filosofia educacional que permeia todo este Projeto Pedagógico do Curso, onde a aprendizagem é vista como um processo ativo e colaborativo. Ao incentivar os tutores a oferecer leituras complementares e recursos didáticos adicionais, a instituição reforça a ideia de que a educação deve ser adaptável e responsiva às necessidades e interesses dos alunos. Assim, o tutor, agindo como mentor, desempenha um papel crucial na modelagem de profissionais reflexivos, autônomos e preparados para enfrentar os desafios contemporâneos da área de defesa cibernética. Dessa forma, o curso de Defesa Cibernética assegura que a educação oferecida atenda às expectativas acadêmicas e profissionais, ao mesmo tempo que contribui para o desenvolvimento integral dos alunos, capacitando-os a se tornarem agentes de mudança na sociedade e no mercado de trabalho.

3.10 ATUAÇÃO DO COLEGIADO DE CURSO

3.10.1 Atuação do colegiado e representatividade do curso

A atuação do Colegiado do Curso (CONCUR) de Defesa Cibernética é planejada para assegurar sua institucionalização efetiva, refletindo um compromisso sério com a governança participativa e democrática. Este planejamento inclui a clara representatividade de diferentes segmentos da comunidade acadêmica, garantindo que as vozes de professores, alunos, funcionários, e demais stakeholders sejam ouvidas e consideradas nas decisões que afetam o curso e seus participantes. A estrutura do colegiado é projetada para promover uma comunicação aberta e eficaz, fundamentada na inclusão e na transparência, assegurando que todas as partes interessadas tenham um papel ativo no desenvolvimento e na melhoria contínua do programa de Defesa Cibernética.

A organização e realização de reuniões pelo CONCUR são estabelecidas com periodicidade semestral, criando um ritmo constante de avaliação e discussão sobre o curso. Essas reuniões são essenciais para o monitoramento do progresso, a identificação de áreas que necessitam de melhorias e a implementação de estratégias inovadoras que respondam aos desafios emergentes no campo da cibersegurança. A documentação e o registro de decisões são materializadas nas atas do CONCUR e fornecem um histórico valioso de deliberações e ações

que suportam a transparência e a responsabilidade, facilitando a comunicação interna e a compreensão das políticas e diretrizes do curso por todos os envolvidos.

Além disso, o CONCUR possui um fluxo claramente definido para o encaminhamento das decisões, garantindo que as resoluções tomadas sejam prontamente comunicadas e implementadas de maneira eficiente. Um sistema acadêmico está em lugar para registrar, acompanhar e executar processos e decisões, maximizando a eficácia operacional e promovendo uma gestão ágil do curso. Este sistema facilita a coordenação entre diferentes departamentos e setores da faculdade, assegurando que as iniciativas aprovadas pelo colegiado sejam implementadas de forma integrada e coerente com os objetivos educacionais e institucionais.

A realização de avaliações periódicas sobre o desempenho do CONCUR é um elemento crucial de seu funcionamento, permitindo a reflexão contínua sobre suas práticas de gestão e a identificação de oportunidades para inovação e aperfeiçoamento. Essas avaliações são fundamentais para adaptar as estratégias do colegiado às necessidades em evolução dos alunos, do corpo docente e do mercado de trabalho em cibersegurança. A composição diversificada do colegiado, com representantes de todos os segmentos da comunidade acadêmica, fortalece sua capacidade de tomar decisões informadas e relevantes, contribuindo significativamente para o sucesso e a relevância do Curso Superior de Tecnologia em Defesa Cibernética <.>

3.10.2 Fluxo determinado para o encaminhamento das decisões

O fluxo de decisões no Colegiado do Curso de Defesa Cibernética da Faculdade ACADI-TI segue um processo organizado e sistemático, que envolve várias etapas e atores específicos, assegurando transparência e eficácia na gestão e implementação das políticas e diretrizes do curso. Esse processo começa com o recebimento de propostas ou questões pela Secretaria, que atua como ponto de entrada para as solicitações ou sugestões vindas de membros da comunidade acadêmica ou externa. Uma vez recebida, a Secretaria encaminha a proposta ao Presidente do Colegiado, que tem a responsabilidade de incluir o item na pauta da próxima reunião, garantindo que as questões importantes sejam discutidas e avaliadas em tempo hábil.

Após a inclusão na pauta, a Secretaria distribui os detalhes da proposta entre os membros do Colegiado, fornecendo-lhes informações suficientes para uma apreciação informada. Durante a reunião do Colegiado, a proposta é apreciada, permitindo uma discussão aberta entre

os membros. Se necessárias, podem ser propostas emendas à proposta original, que são então discutidas e votadas pelo Colegiado. As emendas aprovadas passam a integrar a proposta principal, que é posteriormente submetida à votação final pelo Colegiado. Este processo democrático garante que todas as perspectivas sejam consideradas antes da tomada de uma decisão final.

Uma vez aprovada a proposta, a Secretaria é responsável pelo registro das decisões em ata, assegurando uma documentação detalhada do processo decisório. Os atos resultantes da decisão, como portarias, resoluções, memorandos ou informes, são preparados pelo Presidente do Colegiado, formalizando as diretrizes a serem seguidas. A Secretaria então publica esses documentos em murais e no site da instituição, além de realizar a correspondência aos interessados, quando aplicável, garantindo que a comunidade acadêmica e as partes interessadas estejam devidamente informadas das decisões tomadas.

O acompanhamento das decisões e do plano de implementação é uma etapa crucial, realizada pelo Presidente do Colegiado. Esse acompanhamento contínuo assegura não apenas a implementação efetiva das decisões, mas também permite avaliar o impacto das políticas adotadas e fazer ajustes conforme necessário. Essa estrutura de tomada de decisão e implementação promove a responsabilidade, a eficiência e a eficácia na gestão do Curso de Defesa Cibernética, contribuindo significativamente para o seu desenvolvimento contínuo e adaptação às necessidades dinâmicas da área de cibersegurança.

PROCESSO	
Processo	**Envolvidos**
Recebimento	Secretaria
Inclusão na pauta	Presidente do Colegiado
Distribuição entre os membros	Secretaria
Apreciação	Colegiado
Emendas (quando houver)	Colegiado
Votação das emendas (se aprovadas passarão a compor a proposta principal)	Colegiado
Votação da proposta	Colegiado
Ata (registro das decisões)	Secretaria
ATOS	
Processo	**Envolvidos**
Portarias, resoluções, memorandos ou informes	Presidente do Colegiado

PROCESSO	
Processo	**Envolvidos**
Publicação em murais e site	Secretaria
Correspondência aos interessados (se for o caso)	Secretaria
Acompanhamento das decisões	Presidente do Colegiado
Acompanhamento do plano	Presidente do Colegiado

3.10.3 Implementação de práticas de gestão conforme avaliações de desempenho do colegiado

O Colegiado do Curso de Defesa Cibernética adotará uma abordagem inovadora e reflexiva para a gestão e o desenvolvimento contínuo do programa, centrada na implementação de práticas de gestão baseadas nas avaliações de seu próprio desempenho. Este compromisso com a autoavaliação e melhoria contínua é um reflexo do desejo do colegiado de atender, e exceder os padrões de qualidade educacional, garantindo que o curso permaneça na vanguarda da educação em cibersegurança.

O processo de avaliação do desempenho do colegiado envolverá uma análise abrangente de suas operações, eficácia das decisões tomadas, e o impacto dessas decisões no desenvolvimento do curso e na experiência de aprendizado dos alunos. Através da coleta e análise de feedbacks de estudantes, professores, o colegiado poderá identificar pontos fortes, oportunidades de melhoria, e desafios enfrentados na implementação de políticas e iniciativas. Essas avaliações permitirão ao colegiado refinar suas práticas de gestão, ajustar estratégias e processos, e adotar novas abordagens que promovam a eficiência, a eficácia, e a inovação.

Ao se comprometer com a implementação de práticas de gestão baseadas em avaliações de desempenho, o colegiado demonstra um compromisso claro com a responsabilidade e a excelência educacional. Esse processo contínuo de reflexão e renovação assegurará que o Curso de Defesa Cibernética esteja sempre alinhado com as necessidades e expectativas da comunidade acadêmica e do mercado de trabalho em rápida evolução. Além disso, essa abordagem promove uma cultura de melhoria contínua, onde todos os membros da comunidade acadêmica são incentivados a contribuir ativamente para o sucesso e o desenvolvimento do programa. Dessa forma, o Colegiado do Curso de Defesa Cibernética estabelece um padrão de excelência e inovação, preparando seus alunos não apenas para enfrentar os desafios atuais da cibersegurança, mas também para liderar a evolução da disciplina no futuro.

3.11 TITULAÇÃO E FORMAÇÃO DO CORPO DE TUTORES DO CURSO

3.11.1 Formação dos tutores

O Curso Superior de Tecnologia em Defesa Cibernética da Faculdade ACADI-TI é apoiado por uma equipe dedicada de 9 tutores, cuidadosamente selecionados por suas competências e conhecimentos especializados no campo da cibersegurança. Dessa equipe, 5 tutores possuem qualificações de pós-graduação stricto sensu, refletindo um alto nível de especialização e pesquisa avançada na área. Os outros 4 tutores complementam o time com suas qualificações de pós-graduação lato sensu, trazendo uma rica diversidade de experiências práticas e conhecimentos aplicados. Esse equilíbrio entre teoria avançada e aplicação prática é fundamental para o curso, pois assegura uma abordagem de ensino abrangente que aborda tanto os aspectos conceituais quanto os desafios práticos da cibersegurança.

Mais importante, todos os tutores demonstram 100% de aderência às disciplinas para as quais estão alocados, garantindo que cada tutor esteja plenamente capacitado e em sintonia com os objetivos de aprendizagem e conteúdo específico de suas respectivas disciplinas. Essa aderência completa não só assegura a eficácia do processo de ensino-aprendizagem, mas também fortalece a integridade e a coesão do currículo do curso. Ao alinhar as habilidades e conhecimentos dos tutores com as necessidades das disciplinas, a Faculdade ACADI-TI promove um ambiente de aprendizado onde os alunos podem se beneficiar plenamente da expertise de seus instrutores. Esse comprometimento com a aderência total garante que os alunos recebam orientação de alta qualidade, personalizada para atender às exigências complexas e multifacetadas do campo da defesa cibernética.

3.11.2 Perfil dos tutores

O corpo de tutores do curso possui experiência em Educação a Distância permitindo que eles possam identificar as dificuldades dos discentes, expor o conteúdo em linguagem aderente às características da turma, respeitando as dificuldades individuais e **apresentando** exemplos contextualizados com os conteúdos dos componentes curriculares, de forma que os discentes consigam relacionar o saber acadêmico com a aplicação profissional.

Os tutores também são habilitados para **elaborar** atividades específicas, em colaboração com os docentes, para a promoção da aprendizagem de alunos com dificuldades.

Entre as práticas exitosas que serão adotadas está a utilização dos testes de aprendizagem no AVA ou em aplicativos como o kahoot e o socrative que permitem que o discente, o tutor e o docente conheçam os conteúdos em que há maiores dificuldades, fazendo com que o tutor e o docente direcionem as atividades específicas e complementares para estas temáticas.

Docente tutor	Formação	Titulação
Bruno Botelho	T.I	Especialista
Marlon Luís Petry	T.I	Especialista
Thiago Muniz	T.I	Especialista
Leonardo de la Rosa	T.I	Especialista
Josemar Monteiro Silva	Pedagogia	Doutor
Egberto Gomes Franco	Engenharia	Doutor
Fábio Cristiano de Moraes	Pedagogia	Doutor
Eduardo dos Santos Pereira	Exatas	Doutor
Victor de Andrade Machado	T.I	Mestre

3.12 EXPERIÊNCIA DO CORPO DE TUTORES EM EDUCAÇÃO A DISTÂNCIA

3.12.1 Capacidade dos tutores em identificar as dificuldades dos alunos

No Curso Superior de Tecnologia em Defesa Cibernética a seleção de tutores é um processo rigoroso e meticulosamente planejado, desenhado para assegurar que apenas os docentes mais capacitados façam parte da equipe de ensino. Este processo criterioso reflete o compromisso da instituição com a excelência educacional e o sucesso dos alunos. Os tutores selecionados possuem uma combinação única de formação acadêmica avançada e experiência prática relevante, o que lhes confere a capacidade excepcional de identificar e compreender as dificuldades enfrentadas pelos alunos. Essa capacidade é crucial, pois permite que os tutores forneçam suporte personalizado e intervenções pedagógicas eficazes, adaptadas às necessidades individuais de cada aluno.

A eficácia do processo de seleção de tutores está diretamente relacionada à qualidade da aprendizagem do aluno. Ao garantir que os tutores não só dominem o conteúdo de suas disciplinas, mas também possuam habilidades pedagógicas sólidas e uma sensibilidade aguçada para as nuances do ensino a distância, a Faculdade ACADI-TI cria um ambiente de aprendizado onde os alunos são apoiados em cada etapa de seu desenvolvimento acadêmico e profissional.

Esta abordagem garante que os alunos não apenas absorvam o conhecimento teórico necessário, mas também desenvolvam competências práticas e resiliência intelectual. O resultado é uma experiência de aprendizado enriquecedora que prepara os alunos para enfrentar os desafios do campo da cibersegurança com confiança e competência, evidenciando o papel vital que um processo de seleção de tutores rigoroso desempenha no sucesso educacional dos alunos

3.12.2 Exposição do conteúdo em linguagem aderente às características da turma

A habilidade dos tutores em expor o conteúdo de forma que seja aderente às características da turma é uma competência essencial, reconhecida e cultivada pela instituição. Esta capacidade facilita a compreensão dos alunos e promove um ambiente de aprendizagem mais inclusivo e adaptativo, que reconhece e respeita a diversidade de backgrounds e estilos de aprendizagem dos estudantes. Para garantir a eficácia e aprimoramento contínuo dessa habilidade entre os tutores, a Faculdade ACADI-TI implementou um programa de capacitação abrangente, destinado ao corpo docente e tutorial. Este programa aborda técnicas pedagógicas avançadas e estratégias de ensino adaptativo, e enfatiza a importância de uma comunicação eficaz, garantindo que os tutores estejam bem equipados para apresentar os conceitos complexos da cibersegurança de maneira clara e acessível.

Além disso, a efetividade dessas práticas pedagógicas é avaliada semestralmente, através de um processo de avaliação que considera feedback dos alunos, desempenho acadêmico e a própria autoavaliação dos tutores. Esta avaliação semestral serve como uma ferramenta de feedback valiosa, permitindo que os tutores reflitam sobre suas práticas de ensino e identifiquem áreas para desenvolvimento profissional contínuo. Ao colocar em prática essas avaliações, a Faculdade ACADI-TI assegura a manutenção de altos padrões de ensino, e demonstra seu compromisso com a melhoria constante e a adaptação às necessidades em evolução de seus alunos. Esse ciclo de capacitação e avaliação está alinhada ao esforço contínuo da instituição em promover a excelência educacional, preparando os alunos para os desafios e oportunidades no campo da defesa cibernética

3.12.3 Apresentação de exemplos alinhados aos conteúdos curriculares

A presença de tutores com vasta experiência de mercado no Curso Superior de Tecnologia em Defesa Cibernética enriquece significativamente o processo educativo, permitindo a apresentação de exemplos contextualizados que ligam diretamente os conteúdos dos componentes curriculares à realidade profissional da área de cibersegurança. Essa prática pedagógica facilita a compreensão e a retenção do conhecimento por parte dos alunos, e oferece insights valiosos sobre a aplicação prática de conceitos teóricos em cenários reais do mercado de trabalho. A capacidade dos tutores de trazer para a sala de aula desafios, soluções e casos de sucesso do mundo real, torna o aprendizado mais relevante e estimulante, incentivando os alunos a pensar criticamente e a aplicar seus conhecimentos de forma inovadora.

Além disso, os exemplos práticos e contextualizados também são colhidos de projetos multidisciplinares e estágios remunerados, componentes essenciais do currículo que promovem a integração de diferentes áreas do saber e proporcionam experiências práticas valiosas aos alunos. Esses projetos e estágios, ao colocarem os alunos em contato direto com o ambiente profissional, geram um rico acervo de situações reais que podem ser discutidas e analisadas em sala de aula. Essa sinergia entre a experiência de mercado dos tutores e as atividades práticas realizadas pelos alunos potencializa o processo de ensino-aprendizagem, preparando os estudantes para enfrentar os desafios da área de defesa cibernética, e se destacarem como profissionais competentes e inovadores no mercado de trabalho.

3.12.4 Elaboração de atividades para a promoção da aprendizagem de alunos com dificuldades

A elaboração de atividades pedagógicas destinadas a promover a aprendizagem de alunos com dificuldades é uma prática integralmente incorporada ao Projeto Pedagógico do Curso (PPC), alinhando-se ao Projeto Pedagógico Institucional (PPI) da faculdade. Este compromisso reflete a convicção de que a educação de qualidade é inclusiva e adaptativa, capaz de atender às necessidades individuais de cada aluno, promovendo assim um ambiente de aprendizado equitativo e acessível. A concepção dessas atividades pedagógicas é guiada por um entendimento profundo das barreiras que impedem a aprendizagem, incluindo desafios relacionados a métodos de ensino tradicionais, diferenças no estilo de aprendizagem e possíveis

lacunas no conhecimento prévio. Através da personalização do ensino e da implementação de estratégias diferenciadas, o curso visa superar essas barreiras, facilitando o acesso ao conhecimento e a participação ativa de todos os alunos no processo educativo.

A elaboração de atividades para a promoção e ampliação do repertório do aluno aborda as dificuldades de aprendizagem, e visa enriquecer a experiência educacional de todos os estudantes. Ao introduzir métodos de ensino inovadores, como projetos práticos, estudos de caso, simulações, e atividades colaborativas, os tutores são capazes de estimular o engajamento, fomentar o pensamento crítico e aprofundar a compreensão dos temas abordados. Essa abordagem holística, prevista no PPC e respaldada pelo PPI da ACADI-TI, garante que o aprendizado transcenda a mera aquisição de conhecimento técnico, promovendo o desenvolvimento de habilidades essenciais, como resolução de problemas, trabalho em equipe e comunicação eficaz. Desta forma, as atividades são cuidadosamente desenhadas para atender às necessidades específicas dos alunos com dificuldades, e para ampliar o repertório acadêmico e profissional de toda a turma.

Ademais, essa estratégia educacional ressalta o papel central do tutor como facilitador da aprendizagem, encorajando uma interação constante e significativa com os alunos para identificar suas necessidades e ajustar as abordagens pedagógicas conforme necessário. A constante avaliação das atividades de ensino e o feedback dos alunos são componentes cruciais desse processo, permitindo refinamentos contínuos e a adaptação das metodologias de ensino. Em última análise, ao priorizar a elaboração de atividades que promovem a aprendizagem inclusiva e a ampliação do repertório dos alunos, a Faculdade ACADI-TI assegura que seu curso de Defesa Cibernética cumpre com seus objetivos pedagógicos, e contribui para a formação de profissionais qualificados, criativos e socialmente responsáveis, alinhados com as demandas e desafios do século XXI.

3.12.5 Adoção de práticas inovadoras no contexto da modalidade a distância

O incentivo às práticas inovadoras para tutores, especialmente no contexto do curso de Defesa Cibernética, é uma prioridade que reflete o compromisso institucional com a excelência educacional. Esta abordagem inovadora nasce do Projeto Pedagógico Institucional (PPI) da faculdade, sendo cuidadosamente integrada ao Projeto Pedagógico do Curso (PPC), garantindo

que as práticas de tutoria não só atendam, mas também excedam os padrões de qualidade e as expectativas dos alunos. Reconhecendo a importância da personalização da aprendizagem, a instituição encoraja seus tutores a empregar ferramentas de análise de dados para criar uma experiência educacional adaptada a cada aluno, promovendo um ensino que respeita os ritmos e necessidades individuais e potencializa o engajamento e a compreensão dos conteúdos.

A Faculdade ACADI-TI também valoriza a interação e o engajamento como pilares fundamentais da aprendizagem na modalidade a distância. Através da implementação de dinâmicas interativas, como debates online e projetos colaborativos, a instituição promove o aprendizado ativo e incentiva a participação estudantil. Tutores são capacitados para criar e utilizar tutoriais em vídeo e podcasts, além de organizar webinars e lives interativas, enriquecendo o processo educativo com recursos que tornam o aprendizado mais dinâmico e acessível. Essas iniciativas refletem a orientação do PPI e são concretizadas no PPC, materializando-se na prática de tutoria e contribuindo para uma experiência de aprendizagem rica e engajadora.

O uso de ferramentas tecnológicas avançadas é outra dimensão chave incentivada pela Faculdade ACADI-TI. Os tutores são estimulados a explorar ambientes virtuais de aprendizagem, recursos de realidade virtual e aumentada, além de aplicativos e plataformas educacionais, visando criar experiências imersivas e interativas. Esta abordagem facilita a compreensão e retenção de informações por parte dos alunos, e prepara-os para as demandas tecnológicas do mercado de trabalho em cibersegurança. O compromisso com a inovação tecnológica na educação está alinhado com as diretrizes do PPI, assegurando que a prática de tutoria esteja em constante evolução e adaptada às tendências contemporâneas.

Além disso, a Faculdade ACADI-TI promove o desenvolvimento profissional contínuo dos tutores, incentivando sua participação em comunidades online, cursos de atualização e envolvimento em pesquisa. Este suporte ao aprimoramento contínuo dos tutores assegura a atualização de suas competências pedagógicas, e a incorporação de práticas inovadoras no processo de ensino. Ao adotar uma cultura de aprendizagem contínua e experimentação, a instituição fortalece o papel do tutor na oferta de uma educação de ponta, evidenciando que as práticas inovadoras são fundamentais para o sucesso do modelo educacional da Faculdade ACADI-TI e, por extensão, para o curso de Defesa Cibernética.

3.13 INTERAÇÃO ENTRE TUTORES, DOCENTES E COORDENADORES

A conexão entre professores e tutores, tanto presenciais quanto à distância, é fortalecida através de programas de desenvolvimento contínuo dentro da equipe de Educação a Distância (EaD), utilizando encontros presenciais e webconferências para sincronizar esforços na melhoria da educação a distância. A colaboração entre docentes, tutores e estudantes se manifesta em diversas plataformas digitais e, ocasionalmente, em reuniões presenciais.

3.13.1 Planejamento de interação

A Faculdade ACADI-TI está comprometida com a excelência educacional, e isso se torna claro no Projeto Pedagógico Institucional e neste Projeto Pedagógico do curso de Defesa Cibernética. Para isso, adotará uma série de ações estratégicas para fomentar a interação frequente entre tutores, docentes e coordenadores, reconhecendo a importância dessa sinergia para o sucesso do curso. Inicialmente, a instituição planeja estabelecer reuniões regulares, a serem realizadas mensalmente, alternando entre formatos presenciais e virtuais para acomodar as necessidades de todos os envolvidos. Esses encontros visam facilitar a discussão sobre progressos, desafios enfrentados, e estratégias para aprimorar o processo de ensino-aprendizagem, além de explorar a integração de novas tecnologias educacionais. Será criado também um espaço virtual dedicado para permitir a comunicação constante e o compartilhamento de recursos entre tutores, docentes e coordenadores fora das reuniões agendadas.

Uma iniciativa crucial que a Faculdade ACADI-TI adotará será a utilização do Microsoft Teams como sua plataforma central de comunicação e gestão de aprendizado. Este sistema avançado proporcionará um canal eficaz de comunicação e permitirá o acompanhamento contínuo do progresso dos alunos. Com o Teams, será possível facilitar a distribuição de material didático, a realização de avaliações e o compartilhamento de feedbacks. A plataforma oferecerá funcionalidades como fóruns de discussão e mensagens privadas, essenciais para sustentar a interação constante entre os profissionais envolvidos no curso. Além disso, a integração de ferramentas analíticas no Teams possibilitará à equipe pedagógica ajustar métodos e estratégias de ensino de maneira mais eficaz, atendendo às necessidades dos alunos de forma personalizada e elevando a qualidade da experiência educacional.

Por último, a Faculdade ACADI-TI investirá no desenvolvimento profissional contínuo de sua equipe pedagógica, por meio de workshops, seminários e cursos sobre as mais recentes práticas e tecnologias em educação a distância e defesa cibernética. Esse compromisso com a formação continuada atualizará a equipe sobre as tendências mais recentes no campo da cibersegurança e incentivará uma cultura de inovação e colaboração. Através dessas ações, a Faculdade ACADI-TI busca fortalecer a interação entre tutores, docentes e coordenadores ao mesmo tempo que assegura excelência educacional no curso de Defesa Cibernética, preparando profissionais altamente qualificados para os desafios do futuro.

3.13.2 Facilitação de condições para mediação e articulação

A Faculdade ACADI-TI adota uma abordagem inovadora ao implementar o Microsoft Teams para aprimorar a mediação e articulação entre tutores, docentes e coordenadores. Esta estratégia coloca o Teams no centro da comunicação e integração dos envolvidos no processo de ensino-aprendizagem. A plataforma oferece uma infraestrutura robusta que suporta a colaboração, servindo como um hub digital para toda a comunidade acadêmica. Através do Teams, será possível compartilhar ideias, materiais didáticos e feedbacks de forma eficiente, além de gerenciar projetos e promover o trabalho colaborativo, o que facilita a resolução de questões e cultiva um ambiente de aprendizado contínuo e suporte mútuo.

Além disso, a ACADI-TI planeja organizar workshops e encontros formativos utilizando o Teams para desenvolver habilidades de mediação e articulação. Estas sessões de capacitação focarão em métodos de comunicação eficaz, resolução de conflitos e planejamento colaborativo, enriquecendo a experiência de interação entre todos os participantes do curso e garantindo que os estudantes se beneficiem de um ambiente de aprendizado integrado. Este esforço sublinha o compromisso da instituição com o desenvolvimento profissional contínuo de sua equipe.

Para complementar, a instituição empregará o Teams na implementação de um sistema de feedback dinâmico. Esse sistema permitirá que tutores, docentes e coordenadores avaliem a eficácia das interações e sugiram melhorias. Essa abordagem baseada na plataforma facilitará a ACADI-TI a ajustar e aprimorar as estratégias de ensino de acordo com as necessidades emergentes. Utilizando estrategicamente o Microsoft Teams, a ACADI-TI busca elevar a

comunicação e colaboração interna, mantendo um padrão de excelência e inovação no curso de Defesa Cibernética

3.13.3 Previsão de avaliações periódica

Para assegurar a eficácia dos meios de integração entre professores, tutores e coordenadores implementados pela Faculdade ACADI-TI, propõe-se, junto com a CPA, um plano de avaliação detalhado que enfoca a identificação de áreas de melhoria e o fortalecimento da interação entre os participantes. Este plano inclui a realização de avaliações periódicas, envolvendo uma série de métodos e ferramentas para coletar feedback de forma estruturada e sistemática.

Primeiramente, a instituição realizará pesquisas de satisfação online semestralmente, utilizando a plataforma Microsoft Teams para distribuir os questionários. Essas pesquisas abordarão diversos aspectos da interação e colaboração, incluindo a eficácia da comunicação, a adequação das ferramentas de gestão de projetos, e a qualidade do suporte mútuo entre tutores, docentes e coordenadores. A análise dos resultados permitirá identificar tanto sucessos quanto desafios, orientando a implementação de melhorias.

Além disso, serão organizadas sessões de feedback em grupo, conduzidas virtualmente, para promover discussões abertas sobre experiências, expectativas e sugestões de todos os envolvidos. Essas sessões oferecerão insights valiosos sobre a dinâmica de trabalho colaborativo, permitindo que a instituição compreenda melhor as necessidades específicas de sua equipe pedagógica.

Para complementar, a instituição implementará um sistema de acompanhamento contínuo, através do qual professores, tutores e coordenadores poderão registrar observações e recomendações no decorrer do semestre. Essa abordagem permitirá a identificação rápida de problemas e a aplicação oportuna de correções, garantindo uma resposta ágil às necessidades educacionais que surgem.

Ao final de cada semestre, a equipe de coordenação do curso compilará os dados coletados pelas pesquisas, sessões de feedback e registros de acompanhamento, elaborando um relatório de avaliação. Esse relatório identificará padrões, destacará áreas de sucesso e recomendará ações específicas para melhorar a interação e colaboração. Este documento servirá de base para a revisão e planejamento estratégico das atividades de integração para o semestre

seguinte, assegurando que a Faculdade ACADI-TI continue a aprimorar seu ambiente educacional de maneira proativa e reflexiva.

3.14 PRODUÇÃO CIENTÍFICA, CULTURAL, ARTÍSTICA OU TECNOLÓGICA

A Faculdade ACADI-TI desempenha um papel essencial na promoção da produção científica, cultural, artística e tecnológica, adotando uma série de estratégias para estimular a produção acadêmica de seu corpo docente. A instituição reconhece a importância da pesquisa e do desenvolvimento profissional para o avanço do conhecimento e inovação, implementando ações direcionadas para apoiar seus professores de forma efetiva.

3.14.1 Apoio financeiro com orçamento dedicado

A Faculdade ACADI-TI estabeleceu uma dotação orçamentária específica para o financiamento de pesquisas, com valores reservados expressamente para bolsas de pesquisa, auxílios para publicação e custeio de projetos (PDI p.162 a 172). Este compromisso financeiro garante que os docentes tenham recursos suficientes para explorar novas áreas de estudo e aprofundar suas investigações. O investimento em infraestrutura, como laboratórios de ponta e bibliotecas atualizadas, complementa esse suporte, proporcionando um ambiente propício à inovação.

Priorizando a capacitação contínua, a ACADI-TI oferece uma gama de cursos, workshops e programas de pós-graduação. Essas oportunidades de aprendizado abrangem desde metodologias de pesquisa até o uso de novas tecnologias, visando ampliar as habilidades dos professores. A organização de eventos científicos promove a atualização profissional e o intercâmbio de conhecimentos, enriquecendo a comunidade acadêmica.

3.14.2 Cultura de Valorização e Metas de Produção

A instituição promove uma cultura que valoriza e reconhece o trabalho acadêmico, com políticas de progressão de carreira que consideram a produção científica dos docentes. A Faculdade se empenha em divulgar amplamente as contribuições de seus professores, elevando a visibilidade de seu trabalho. Além disso, estabeleceu a meta ambiciosa de garantir que ao

menos 50% dos docentes tenham, no mínimo, nove produções nos últimos três anos, demonstrando o compromisso com a excelência acadêmica.

3.14.3 Parcerias Estratégicas para Ampliação da Pesquisa

A instituição também valoriza parcerias estratégicas com empresas, governos e outras entidades educacionais para fomentar a pesquisa aplicada e a inovação. Essas colaborações oferecem aos docentes oportunidades valiosas de pesquisa e facilitam a transferência de conhecimento para a sociedade.

As iniciativas implementadas pela ACADI-TI já demonstram resultados positivos, com um aumento no número de publicações e reconhecimentos obtidos por seus projetos de pesquisa. A Faculdade se compromete com a constante revisão e aprimoramento de suas estratégias de apoio à produção docente, visando um ambiente cada vez mais estimulante e produtivo para a pesquisa.

A Faculdade ACADI-TI, através de seu compromisso com o apoio financeiro, desenvolvimento profissional, reconhecimento e parcerias estratégicas, estabelece um ambiente acadêmico que estimula a excelência e a inovação. A definição de metas claras para a produção acadêmica e o investimento em recursos evidenciam o papel da instituição como um pilar no avanço do conhecimento e na contribuição para o desenvolvimento científico, tecnológico e cultural da sociedade.

As comprovações das publicações do professores estão em pasta especifica

4. INFRAESTRUTURA

4.1 ESPAÇO DE TRABALHO PARA DOCENTES EM TEMPO INTEGRAL

4.1.1 Disponibilidade de espaços de trabalho adequados para docentes T.I.

O Curso Superior de Tecnologia em Defesa Cibernética dispõe de uma equipe composta por três docentes dedicados em regime de tempo integral. A instituição oferece um ambiente de trabalho espaçoso, projetado para acomodar até oito professores em tempo integral, evidenciando o compromisso da faculdade com a excelência acadêmica e o bem-estar de seu corpo docente.

4.1.2 Viabilização de ações acadêmicas

O espaço dedicado aos docentes em tempo integral está equipado com acesso à internet de alta velocidade e recursos tecnológicos avançados, que são fundamentais para o desenvolvimento de atividades acadêmicas, incluindo o planejamento didático-pedagógico. Esta infraestrutura é essencial para a viabilização de uma metodologia de ensino inovadora e eficaz, alinhada às demandas contemporâneas da área de defesa cibernética.

4.1.3 Atendimento às necessidades institucionais

Os espaços de trabalho disponibilizados para os docentes em tempo integral são integralmente alinhados às necessidades institucionais, fornecendo um ambiente propício à realização das atividades docentes. Essa estrutura reforça o comprometimento da instituição com a qualidade da educação oferecida, assegurando condições ideais para o exercício profissional dos professores.

4.1.4 Equipamento dos espaços com recursos de TICs adequados

A instituição assegura que todos os espaços de trabalho para os docentes em tempo integral estejam adequadamente equipados com os mais modernos recursos de tecnologias da informação e comunicação (TICs). Esta providência garante que os professores disponham das

ferramentas necessárias para a condução de suas atividades de ensino, pesquisa e extensão com a máxima eficiência.

4.1.5 Garantia de privacidade nos espaços de trabalho

A configuração dos espaços de trabalho dedicados aos professores em tempo integral foi cuidadosamente planejada para assegurar a privacidade necessária ao desempenho de suas funções. A privacidade é um elemento chave para a promoção de um ambiente de trabalho tranquilo e propício à concentração. Há áreas de atendimento em grupo e individual com total segurança e privacidade.

4.1.6 Segurança para a guarda de material e equipamentos.

A segurança é uma prioridade dentro dos espaços de trabalho designados aos docentes em tempo integral. A sala dos professores foi especialmente projetada para oferecer condições seguras para a guarda de equipamentos pessoais e materiais didáticos, refletindo o zelo da instituição pela proteção dos bens de seu corpo docente, em harmonia com a natureza sensível do curso de Defesa Cibernética.

4.2 ESPAÇO DE TRABALHO PARA O COORDENADOR

A sala do Coordenador é estrategicamente projetada para facilitar o desempenho eficiente das funções acadêmico-administrativas inerentes ao cargo. Este espaço reflete o compromisso da instituição com a qualidade e a eficácia do processo educativo, garantindo um ambiente adequado para o planejamento, execução e avaliação das atividades pedagógicas

4.2.1 Disponibilidade de espaço de trabalho adequado para o coordenador.

O espaço destinado ao Coordenador é adequado, tanto em termos de dimensão quanto de configuração, para suportar uma ampla gama de atividades pedagógicas e administrativas. Projetado para promover um ambiente de trabalho produtivo, o espaço é suficiente para atendimentos individuais e reuniões em grupo, garantindo a eficácia no cumprimento das tarefas administrativas e acadêmicas.

4.2.2 Viabilização das ações acadêmico-administrativas.

A sala do Coordenador é um ponto central para a viabilização de ações acadêmico-administrativas, permitindo a eficiente coordenação de projetos, a tomada de decisões estratégicas e o acompanhamento das atividades curriculares. Este espaço propicia um ambiente organizado e funcional, essencial para o desenvolvimento de um trabalho pedagógico alinhado às diretrizes institucionais e às expectativas do curso.

4.2.3 Equipamento adequado no espaço.

Equipada com recursos tecnológicos avançados, incluindo computador, acesso Wi-Fi e impressora, além de ferramentas off-line como uma lousa, a sala do Coordenador é preparada para atender a todas as necessidades operacionais do cargo. Esses recursos são fundamentais para o planejamento, a gestão acadêmica e a comunicação eficaz dentro e fora da instituição. Há um **Plano de avaliação dos Espaços e Manutenção**.

4.2.4 Atendimento às necessidades institucionais.

O espaço de trabalho do Coordenador é concebido para atender plenamente às necessidades institucionais, proporcionando as condições necessárias para a gestão efetiva do curso. A disponibilidade de ferramentas de gestão, como a conta no Trello para o gerenciamento de demandas, exemplifica o apoio dado pela instituição à organização e à execução das responsabilidades administrativas e pedagógicas.

4.2.5 Possibilidade de atendimento de indivíduos ou grupos com privacidade.

A configuração da sala do Coordenador permite a realização de atendimentos individuais e reuniões em grupo com total privacidade. Este aspecto é crucial para assegurar um espaço de diálogo confidencial, onde assuntos sensíveis podem ser tratados de maneira discreta e segura, respeitando a privacidade dos envolvidos.

4.2.6 Disponibilidade de infraestrutura tecnológica diferenciada.

A instituição compromete-se com a oferta de uma infraestrutura tecnológica diferenciada para o espaço do Coordenador, reconhecendo a importância de recursos tecnológicos de ponta na facilitação das tarefas administrativas e pedagógicas. Esta infraestrutura suporta uma gestão inovadora e eficaz, permitindo que o Coordenador explore novas possibilidades no ensino, na pesquisa e na extensão, contribuindo para o avanço acadêmico e institucional.

4.3 SALA COLETIVA DE PROFESSORES

4.3.1 Viabilização do trabalho docente

A Sala Coletiva de Professores na Faculdade ACADI-TI é projetada para atender de maneira eficiente às necessidades do trabalho docente em um ambiente acadêmico dinâmico. Com uma capacidade de acomodação de três a cinco tutores por noite, este espaço é estruturado para promover uma interação produtiva e o desenvolvimento profissional contínuo dos professores. Equipada com uma ampla mesa comunitária e quatro computadores com acesso à internet de alta velocidade, a sala possibilita a preparação de aulas, realização de pesquisas acadêmicas e a colaboração em projetos educacionais. A infraestrutura inclui também isolamento acústico, iluminação adequada, ventilação otimizada e mobiliário ergonômico, garantindo um ambiente de trabalho saudável e propício ao desenvolvimento pedagógico, refletindo o comprometimento da Faculdade com a excelência e o bem-estar dos docentes.

4.3.2 Recursos de tecnologias da informação e comunicação

A Sala Coletiva de Professores é dotada de recursos tecnológicos de ponta, incluindo computadores de última geração, acesso à internet de alta velocidade e uma diversidade de softwares educacionais. Estes recursos permitem aos professores adotar metodologias de ensino inovadoras, conduzir pesquisas avançadas e engajar-se em programas de ensino à distância. A integração dessas tecnologias facilita a elaboração de um currículo contemporâneo e a aplicação de técnicas pedagógicas modernas, posicionando a Faculdade ACADI-TI na vanguarda da inovação tecnológica educacional.

4.3.3 Descanso e atividades de lazer e integração

Adjacentes à sala dos professores, espaços de descanso e lazer são criteriosamente projetados para promover o bem-estar e a interação social entre os docentes. Uma área de relaxamento equipada com sofá, poltronas, pufes, televisão e uma cozinha compacta oferece um ambiente confortável para os momentos de pausa. Este espaço multifuncional não apenas enfatiza a importância do descanso e do bem-estar docente, mas também integra tecnologias de entretenimento, assegurando que os períodos de lazer contribuam para o enriquecimento da experiência profissional dos professores.

4.3.4 Apoio técnico-administrativo próprio

A acessibilidade e funcionalidade da Sala Coletiva de Professores são ampliadas pela presença de uma mesa próxima à entrada, destinada a um auxiliar de sala. Essa disposição sublinha o compromisso da Faculdade ACADI-TI com a acessibilidade, oferecendo suporte técnico e administrativo imediato aos professores. Essa iniciativa facilita a logística diária e assegura que os docentes possam dedicar-se integralmente às suas responsabilidades pedagógicas, contando com um apoio acessível e eficiente.

4.3.5 Espaço para a guarda de equipamentos e materiais

A Sala Coletiva de Professores na Faculdade ACADI-TI foi equipada com armários dedicados, proporcionando aos professores um espaço seguro e prático para guardar seus materiais didáticos, equipamentos eletrônicos e objetos pessoais. Esses armários, projetados para maximizar a organização e a acessibilidade, refletem o compromisso da instituição em criar um ambiente de trabalho que não só apoie as necessidades pedagógicas, mas também atenda às exigências práticas do dia a dia docente. A inclusão desses espaços de armazenamento personalizados assegura que os professores tenham à disposição um recurso conveniente para manter seus pertences seguros e ordenados, facilitando assim a manutenção de um espaço de trabalho limpo e eficiente, o que é vital para um ambiente acadêmico produtivo e estimulante. Há um **Plano de avaliação dos Espaços e Manutenção**.

4.4 SALAS DE AULA

4.4.1 Adequação das salas de aula às necessidades institucionais e do curso

As salas de aula da Faculdade ACADI-TI são meticulosamente planejadas e estruturadas, garantindo total adequação às atividades institucionais e às demandas específicas do curso de Defesa Cibernética. Esta adaptação estratégica permite a realização de uma ampla gama de atividades presenciais, incluindo provas e apresentações de trabalhos, essenciais para um aprendizado teórico e prático eficaz. A infraestrutura reflete um compromisso com a inclusão e acessibilidade, assegurando que todos os alunos se beneficiem igualmente dos recursos educacionais disponíveis. Tecnologias avançadas e recursos didáticos diferenciados enriquecem a experiência de ensino, preparando os alunos para os desafios profissionais na área de cibersegurança.

4.4.2 Realização de manutenção periódica nas salas de aula.

A manutenção periódica das salas de aula é uma prática institucionalizada na Faculdade ACADI-TI, com avaliações regulares realizadas semestralmente pela direção geral e acadêmica em conjunto com a equipe de manutenção. Há um **Plano de avaliação dos Espaços e Manutenção**. Este plano garante que as instalações físicas se mantenham em conformidade com os mais altos padrões de qualidade, conforto e tecnologia, sustentando um ambiente de aprendizado dinâmico e propício ao desenvolvimento de habilidades relevantes.

4.4.3 Conforto das salas de aula

As salas de aula da Faculdade são limpas diariamente e projetadas para proporcionar ótima iluminação natural e artificial, além de excelente ventilação natural e ventiladores de teto, criando um ambiente saudável e propício ao aprendizado. Atenção especial é dada à ventilação, iluminação, isolamento acústico, segurança, acessibilidade e conservação, garantindo um espaço de aprendizagem confortável e acolhedor para todos os alunos.

4.4.4 Disponibilidade de recursos de TIC's

Cada sala de aula está equipada com sistemas de som ambiente de alta qualidade, projetores, computadores para uso do professor, e acesso à internet de alta velocidade. Estes recursos tecnológicos são fundamentais para um ambiente de aprendizado multimídia envolvente e eficaz, apoiando a entrega efetiva do currículo e enriquecendo a experiência de aprendizado

4.4.5 Flexibilidade das salas de aula para diferentes situações de ensino-aprendizagem

A mobília nas salas de aula é deliberadamente solta e adaptável, permitindo reconfigurações flexíveis do espaço para facilitar diferentes métodos de ensino e aprendizagem. Esta flexibilidade é crucial para a implementação de metodologias ativas e facilita a formação de grupos ou outros arranjos necessários, promovendo um ambiente inclusivo e adaptável.

4.4.6 Presença de recursos pedagógicos inovadores.

A infraestrutura tecnológica da Faculdade ACADI-TI suporta a simulação prática e a aplicação de metodologias ativas, ferramentas pedagógicas chave para o curso de Defesa Cibernética. Estes recursos pedagógicos inovadores permitem que os alunos experimentem cenários do mundo real em um ambiente controlado e seguro, promovendo um aprendizado experiencial onde teorias são aplicadas em práticas, desenvolvendo habilidades cruciais de maneira efetiva.

4.5 Acesso dos Alunos a Equipamentos de Informática

4.5.1 Atendimento às necessidades institucionais e do curso

Os laboratórios de informática da Faculdade ACADI-TI são projetados para atender às demandas institucionais e pedagógicas, proporcionando suporte a uma variedade de atividades acadêmicas, desde aulas regulares a projetos de pesquisa avançados. A infraestrutura tecnológica, incluindo a disponibilidade de computadores adaptados para alunos com

deficiência, reflete o compromisso da instituição com a inclusão e o acesso igualitário à educação, atendendo às necessidades específicas dos cursos oferecidos.

4.5.2 Adequação em termos de disponibilidade de equipamentos no laboratório

Cada laboratório dispõe de cerca de 30 computadores de última geração, configurados para atender tanto às necessidades gerais dos alunos quanto às especificidades dos alunos com deficiência, garantindo a adequação e a acessibilidade do espaço. Além disso, na biblioteca da instituição, há 10 computadores de acesso livre disponíveis para uso dos alunos em qualquer turno, atendendo às necessidades institucionais e promovendo a disponibilidade dos equipamentos.

4.5.3 Conforto do espaço do laboratório de informática

A ACADI-TI assegura que seus laboratórios de informática sejam espaços seguros e confortáveis, com isolamento acústico eficiente, iluminação planejada, sistemas de ar-condicionado e mobiliário ergonomicamente projetado. Essas características contribuem para um ambiente de aprendizado avançado que promove a saúde e o bem-estar dos alunos, permitindo-lhes passar várias horas estudando ou realizando projetos com conforto.

4.5.4 Estabilidade e velocidade de acesso à internet e disponibilidade de rede sem fio

A faculdade investe na estabilidade e na velocidade de acesso à internet, incluindo a disponibilidade de rede sem fio, nos laboratórios de informática. Isso facilita o processo de aprendizado e permite que os alunos trabalhem com ferramentas e softwares de última geração, garantindo uma experiência educacional rica e sem interrupções.

4.5.5 Disponibilidade de hardware e software atualizados no laboratório.

A inovação e atualização tecnológica são constantes nos laboratórios de informática da ACADI-TI. A instituição mantém uma equipe qualificada responsável pela atualização de softwares e hardwares, garantindo que os equipamentos e programas sejam sempre os mais avançados e relevantes para as necessidades educacionais dos alunos e professores. Isso inclui softwares que garantem a acessibilidade, refletindo o compromisso com a inclusão.

4.5.6 Realização de avaliações periódicas

A avaliação dos laboratórios de informática é realizada tanto pela própria equipe da ACADI-TI, através de manutenção preventiva e corretiva, quanto por pesquisas da CPA, que produzem relatórios avaliando diversos espaços da instituição. Existe um **Plano de avaliação periódica.** Essas avaliações periódicas garantem que os laboratórios permaneçam em condições ótimas de uso, atendendo às necessidades em constante evolução dos alunos e dos cursos oferecidos pela faculdade.

4.6 BIBLIOGRAFIA BÁSICA POR UNIDADE CURRICULAR

4.6.1 Acervo está registrado em nome da IES

O acervo bibliográfico do curso de Defesa Cibernética, registrado em nome da IES, representa um pilar fundamental na sustentação das atividades de ensino, pesquisa e extensão da Faculdade ACADI-TI. Este registro assegura a legalidade e a legitimidade do acesso aos recursos informacionais, em conformidade com as normativas vigentes (Portaria 11/2017), garantindo assim a integridade acadêmica e o respeito aos direitos autorais. A inscrição do acervo sob o nome da instituição fortalece o compromisso com a qualidade educacional, oferecendo suporte atualizado e relevante às necessidades curriculares das unidades de ensino e aprendizagem. Através do contrato firmado com a Curatoria Editora, a Faculdade ACADI-TI assegura um acervo virtual diversificado, com acesso garantido aos títulos necessários para a formação em Defesa Cibernética, refletindo o alinhamento estratégico entre os recursos disponibilizados e os objetivos pedagógicos do curso.

4.6.2 Acervo da bibliografia básica adequado e atualizado

O acervo da bibliografia básica do curso de Defesa Cibernética, cuidadosamente selecionado e mantido atualizado, reflete um profundo compromisso com a excelência educacional e a preparação dos alunos para enfrentar desafios contemporâneos no campo. Através da análise das necessidades de cada disciplina, como evidenciado pela colaboração com a Curatoria Editora, a instituição assegura que o conteúdo disponibilizado esteja em consonância com os últimos desenvolvimentos tecnológicos e tendências do setor de segurança cibernética.

Este alinhamento não é apenas uma questão de conveniência, mas uma necessidade imperativa em um campo que evolui rapidamente, onde novas ameaças e tecnologias emergem constantemente. Por exemplo, a inclusão de recursos atualizados sobre criptografia avançada e segurança de redes em cursos específicos equipa os estudantes com conhecimentos práticos essenciais para a proteção de infraestruturas críticas contra ataques cibernéticos sofisticados.

Além disso, a disponibilização de periódicos especializados e acesso a bases de dados atualizadas complementa a formação teórica com insights valiosos sobre pesquisas atuais, práticas recomendadas na indústria e estudos de caso relevantes. Isso não só enriquece a experiência de aprendizagem, mas também promove uma cultura de educação contínua e adaptabilidade entre os alunos, preparando-os para se tornarem profissionais resilientes e inovadores em Defesa Cibernética.

A manutenção de um acervo bibliográfico adequado e atualizado é uma pedra angular na estrutura do projeto pedagógico do curso, garantindo que os alunos tenham acesso aos recursos necessários para alcançar excelência acadêmica e profissional na vanguarda da segurança cibernética.

4.6.3 Acervo referendado por relatório de adequação

O acervo está referendado por relatório de adequação, assinado pelo Núcleo Docente Estruturante (NDE), comprovando a compatibilidade, em cada bibliografia básica da UC, entre o número de vagas autorizadas. Ata número 05 NDE de 01 de março de 2024.

4.6.4 Garantia do acesso na IES dos títulos virtuais

Na Faculdade ACADI-TI, o acesso aos títulos virtuais é uma prioridade estratégica, refletindo um compromisso com a educação moderna e inclusiva. As salas de estudo em grupo são equipadas com tablets, permitindo aos alunos acessarem coletivamente o acervo digital e colaborarem em projetos e pesquisas. Nas salas de estudo individuais, computadores estão disponíveis para pesquisa e acesso aos títulos virtuais, oferecendo um espaço tranquilo para estudo aprofundado.

Adicionalmente, os laboratórios de informática se destacam como pontos de acesso aos livros virtuais, equipados com tecnologia de ponta para suportar tanto a aprendizagem teórica quanto a aplicação prática.

Esta infraestrutura é complementada por uma forte conexão à internet e ferramentas de acessibilidade, garantindo que todos os estudantes possam aproveitar os recursos oferecidos ao máximo. Este ecossistema tecnológico é um testemunho da dedicação da Faculdade ACADI-TI em fornecer um ambiente de aprendizado rico e adaptável às necessidades de uma formação em Defesa Cibernética.

4.6.5 Acervo de periódicos especializados

A presença de periódicos acadêmicos na biblioteca virtual da Faculdade ACADI-TI é fundamental para a excelência acadêmica e profissional em Defesa Cibernética. Estes periódicos são janelas para o progresso científico, oferecendo aos professores e alunos acesso imediato às últimas pesquisas, debates e inovações no campo. Além de enriquecer a bibliografia dos cursos com conteúdo atualizado, os periódicos estimulam a análise crítica e o pensamento inovador, essenciais para formar especialistas capazes de responder aos desafios emergentes na segurança cibernética com soluções baseadas em evidências e práticas de vanguarda. Este recurso transforma o aprendizado em uma experiência dinâmica e interativa, preparando os alunos não apenas para o mercado de trabalho atual, mas também para contribuir ativamente para o avanço da área.

4.6.6 Gerenciamento do acervo

O gerenciamento eficaz do acervo na Faculdade ACADI-TI é um componente crucial para assegurar a acessibilidade e a relevância dos materiais disponibilizados aos alunos e professores. Este processo envolve uma atualização constante da quantidade de exemplares e assinaturas de acesso, especialmente daqueles mais demandados pela comunidade acadêmica. A instituição adota um plano de contingência robusto, garantindo o acesso ininterrupto aos recursos, mesmo frente a possíveis desafios técnicos ou aumentos significativos na demanda. Este gerenciamento proativo e estratégico assegura que os recursos de aprendizagem estejam sempre alinhados com as necessidades curriculares e com as tendências mais recentes no campo da Defesa Cibernética, promovendo uma educação de alta qualidade e altamente adaptável

4.7 BIBLIOGRAFIA COMPLEMENTAR POR UNIDADE CURRICULAR

4.7.1 Acervo da bibliografia básica adequado e atualizado

O acervo da bibliografia complementar do curso de Defesa Cibernética é meticulosamente selecionado e mantido atualizado, refletindo um comprometimento profundo com a excelência educacional e a preparação dos alunos para enfrentarem os desafios contemporâneos no campo. Através da análise das necessidades de cada disciplina, evidenciado pela colaboração com a Curadoria Editora, a instituição assegura que o conteúdo disponibilizado esteja alinhado com os últimos desenvolvimentos tecnológicos e as tendências do setor de segurança cibernética.

Esse alinhamento não é somente uma conveniência, mas uma necessidade crítica em um campo que evolui rapidamente, onde novas ameaças e tecnologias emergem constantemente. Por exemplo, a inclusão de recursos atualizados sobre criptografia avançada e segurança de redes em cursos específicos equipa os estudantes com conhecimentos práticos essenciais para a proteção de infraestruturas críticas contra ataques cibernéticos sofisticados.

Além disso, a disponibilização de periódicos especializados e acesso a bases de dados atualizadas complementa a formação teórica com insights valiosos sobre pesquisas atuais, práticas recomendadas na indústria e estudos de caso relevantes. Isso não apenas enriquece a

experiência de aprendizado, mas também promove uma cultura de educação contínua e adaptabilidade entre os alunos, preparando-os para se tornarem profissionais resilientes e inovadores em Defesa Cibernética.

A manutenção de um acervo bibliográfico complementar adequado e atualizado é um pilar fundamental na estrutura do projeto pedagógico do curso, garantindo que os alunos tenham acesso aos recursos necessários para alcançar excelência acadêmica e profissional na vanguarda da segurança cibernética.

Exemplos da Adequação da Bibliografia Complementar à Disciplina:

1. **"Desafios estratégicos para segurança e defesa cibernética" (BARROS Otávio Santana Rêgo; et al.)**: Este livro aborda estratégias e desafios no âmbito da segurança e defesa cibernética, proporcionando aos estudantes uma visão ampla sobre políticas de segurança nacionais e internacionais, essencial para compreender o contexto geopolítico da cibersegurança.
2. **"Inteligência cibernética: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil" (WENDT Emerson)**: Oferece uma análise detalhada da evolução da ciberguerra e do cibercrime, contribuindo para a compreensão dos alunos sobre as ameaças cibernéticas contemporâneas e como elas afetam a segurança nacional.
3. **"Softwares de segurança da informação" (NOVO Jorge Procópio da Costa)**: Esse material é fundamental para os alunos que buscam conhecimentos práticos sobre ferramentas de segurança da informação, abordando desde conceitos básicos até técnicas avançadas de proteção de dados.

Esses exemplos ilustram como a bibliografia complementar é cuidadosamente selecionada para oferecer aos estudantes uma base sólida de conhecimento teórico e prático, indispensável para enfrentar os desafios no campo da Defesa Cibernética

4.7.2 Acervo referendado por relatório de adequação

O acervo da Bibliografia Complementar está referendado por relatório de adequação, assinado pelo Núcleo Docente Estruturante (NDE), comprovando a compatibilidade, em cada bibliografia complementar das Unidades Curriculares (UCs), entre o número de vagas autorizadas. Ata número 05 do NDE de 01 de março de 2024.

Este documento certifica que a seleção e a quantidade de materiais complementares disponíveis estão alinhadas com a capacidade de atendimento do curso e as necessidades específicas de aprendizado de cada UC. A inclusão desta bibliografia complementar é um reflexo do compromisso da instituição em fornecer recursos adicionais que enriquecem o conhecimento dos alunos, oferecendo-lhes uma perspectiva mais ampla e aprofundada dos temas tratados nas disciplinas. Este acervo complementar, cuidadosamente escolhido pelo NDE, assegura que os estudantes tenham acesso a uma gama de materiais atualizados e relevantes para sua formação, indo além do essencial e estimulando a pesquisa, a crítica e a inovação no campo de estudo.

4.7.3 Acesso físico e virtual garantido aos títulos virtuais:

Na Faculdade ACADI-TI, o acesso aos títulos da Bibliografia Complementar é uma prioridade estratégica, refletindo um compromisso com a educação moderna e inclusiva. As salas de estudo em grupo são equipadas com tablets, permitindo aos alunos acessarem coletivamente o acervo digital complementar e colaborarem em projetos e pesquisas. Nas salas de estudo individuais, computadores estão disponíveis para pesquisa e acesso aos títulos virtuais complementares, oferecendo um espaço tranquilo para estudo aprofundado.

Adicionalmente, os laboratórios de informática se destacam como pontos de acesso aos livros virtuais da bibliografia complementar, equipados com tecnologia de ponta para suportar tanto a aprendizagem teórica quanto a aplicação prática.

Esta infraestrutura é complementada por uma forte conexão à internet e ferramentas de acessibilidade, garantindo que todos os estudantes possam aproveitar os recursos oferecidos ao máximo. Este ecossistema tecnológico é um testemunho da dedicação da Faculdade ACADI-TI em fornecer um ambiente de aprendizado rico e adaptável às necessidades de uma formação em Defesa Cibernética, assegurando que os alunos tenham acesso fácil e imediato a uma vasta gama de recursos complementares que enriquecem sua educação e preparação para os desafios do campo.

4.7.4 Acervo de periódicos especializados

A biblioteca virtual da Faculdade ACADI-TI destaca-se pela sua coleção de periódicos especializados, um pilar vital para alcançar a excelência acadêmica e profissional no âmbito da

Defesa Cibernética. Estes periódicos atuam como portais para o avanço científico, proporcionando a docentes e discentes acesso direto às mais recentes pesquisas, discussões e inovações na área. Contribuem significativamente para complementar a bibliografia dos cursos com informações contemporâneas, incentivando a análise crítica e o desenvolvimento do pensamento inovador — habilidades imprescindíveis na formação de profissionais aptos a enfrentar os desafios novos da segurança cibernética com estratégias fundamentadas em dados atualizados e práticas avançadas. Este acervo transforma o processo de aprendizagem em uma jornada dinâmica e interativa, equipando os estudantes não só para o mercado de trabalho presente mas também para uma participação efetiva no progresso do setor.

4.7.5 Gerenciamento do acervo

O gerenciamento proativo do acervo na Faculdade ACADI-TI é essencial para manter a acessibilidade e atualidade dos recursos oferecidos a alunos e docentes. Esse processo inclui a renovação contínua do acervo, com especial atenção aos materiais e periódicos de alta demanda dentro da comunidade acadêmica. A instituição implementa um plano de contingência eficiente, assegurando acesso contínuo aos recursos educacionais, mesmo diante de eventuais desafios técnicos ou picos de demanda. Esta abordagem de gestão estratégica garante a sincronia dos materiais de aprendizado com os objetivos curriculares e as inovações mais recentes na área de Defesa Cibernética, fomentando um ensino de excelência e flexível às mudanças constantes do setor.

4.8 Laboratórios Didáticos de Formação Básica e Específica

4.8.1 Adequação dos laboratórios didáticos às necessidades do curso

Os laboratórios didáticos da Faculdade ACADITI são projetados para atender integralmente às exigências dos componentes curriculares do Curso Superior de Tecnologia em Defesa Cibernética, equipando os alunos com as tecnologias e habilidades necessárias para se destacarem no mercado profissional. Equipados com tecnologias de ponta, esses espaços

fomentam a inovação e a aplicação prática dos conhecimentos adquiridos em sala de aula. **Há um Plano de avaliação e manutenção dos espaços**.

4.8.2 Conformidade com as normas de funcionamento, utilização e segurança dos laboratórios

A Faculdade ACADITI segue rigorosos protocolos de segurança em todos os seus laboratórios, assegurando um ambiente seguro e propício ao aprendizado. Com extintores, sistemas de alarme, monitoramento por câmeras e treinamentos de segurança regulares, a instituição garante a conformidade com as normas de funcionamento e utilização dos espaços de aprendizado.

4.8.3 Conforto e manutenção periódica dos laboratórios didáticos.

Os laboratórios da ACADITI são submetidos a uma manutenção periódica para assegurar seu bom estado de conservação e funcionamento. Com uma infraestrutura que atende aos mais altos padrões de conforto, os laboratórios oferecem um ambiente de aprendizagem inclusivo, com dispositivos adaptados para pessoas com deficiências e outros recursos que promovem a acessibilidade.

4.8.4 Disponibilidade de serviços de apoio técnico nos laboratórios.

Para suportar as atividades práticas e o aprendizado dos alunos, a ACADITI disponibiliza serviços de apoio técnico nos laboratórios, incluindo profissionais qualificados para assistência e orientação no uso dos equipamentos e softwares.

4.8.5 Quantidade de insumos, materiais e equipamentos

Cada laboratório da ACADITI está adequadamente abastecido com insumos, materiais e equipamentos de primeira linha, assegurando que os estudantes tenham acesso às ferramentas necessárias para o desenvolvimento de suas competências. A instituição mantém um compromisso com a atualização constante de suas instalações e recursos tecnológicos.

4.8.6 Avaliação periódica dos espaços e uso dos resultados

A Faculdade ACADITI implementa um processo de avaliação constante de suas instalações, incluindo os laboratórios didáticos, para alinhar a infraestrutura às necessidades

acadêmicas e profissionais dos alunos. Utilizando os resultados dessas avaliações, a instituição continua a aprimorar e enriquecer a experiência educacional.

Adicionalmente, a ACADITI enfatiza a importância dos ambientes práticos de aprendizagem, oferecendo laboratórios de informática de última geração e ambientes como cenários de Ataque e Defesa Cibernéticas para que os alunos possam praticar suas habilidades em condições reais, sob a orientação de professores experientes. Mesmo sendo um curso na modalidade a distância, a ACADITI garante a disponibilidade de sua infraestrutura para os alunos que necessitam ou preferem o acesso presencial para o desenvolvimento de trabalhos e estudos, reforçando seu compromisso com uma formação acadêmica de qualidade.

O Curso Superior de Tecnologia em Defesa Cibernética a Faculdade ACADITI tem grande parte dos seus componentes curriculares dependente do laboratório de informática, por conta dos programas necessários ao desenvolvimento das competências e habilidade previstas neste PPC. Em tratando-se de um curso na modalidade a distância, os laboratórios serão desenvolvidos em programas específicos.

Vale ressaltar que a ACADITI oferece toda infraestrutura necessária de laboratório no campus para que os alunos, que assim julgar necessário, possa vir presencialmente desenvolver seus trabalhos e estudos.

4.9 Processo de Controle de Produção ou Distribuição de Material Didático (Logística)

4.9.1 Formalização e atendimento à demanda do processo

O processo de controle de produção e distribuição de material didático na Faculdade ACADI-TI envolve a formalização e a padronização de procedimentos para garantir a qualidade, uniformidade e acessibilidade do material aos alunos. Esse processo é mediado pela Equipe Multidisciplinar, como já tratamos páginas atrás, que atua desde a concepção até a disponibilização do material, garantindo que as demandas da disciplinas sejam atendidas de forma plena.

A formalização do processo o planejamento detalhado da demanda de disciplina para o curso de Defesa Cibernética (neste caso, mas seguirá o mesmo para outros eventuais cursos). Em fase de autorização, a Equipe Multidisciplinar preocupou com a disponibilização das disciplinas dos dois primeiros semestres, a saber: Matemática para Computação, Introdução à Informática, Lógica de Programação e Algoritmos, Fundamentos de Redes de Computadores, Princípios de Segurança da Informação, Gerenciamento de Projetos para Segurança Cibernética, Administração Segura de Sistema Linux, Administração Segura de Sistema Windows, Arquitetura de Segurança de Sistemas para Segurança Cibernética e Ética, Moral e Direitos Humanos em Tecnologia da Informação. Esses materiais foram fornecidos pelo Telesapiens, parceiro na produção de material didático.

Em seguida, começou a seleção de autores, a elaboração do projeto do material didático e a definição do formato final do material, que foi definido como essencialmente digital. Importante ressaltar que todo o material didático fica a disposição de forma online na biblioteca ou nos laboratórios de informática.

O papel da equipe multidisciplinar neste processo compreende o zelo pela qualidade pedagógica e técnica do material didático. Essa equipe trabalha na interface entre autores, revisores, editores e os responsáveis pela distribuição. A equipe multidisciplinar assegura que o conteúdo desenvolvido atenda aos objetivos pedagógicos e esteja alinhado com as necessidades e expectativas dos alunos e professores.

Na fase de produção, os autores desenvolvem o conteúdo conforme o projeto aprovado. Esse material passa por revisões especializadas para garantir sua qualidade e adequação pedagógica, além de ser editado para clareza, coesão e correção gramatical. A edição é uma etapa crítica para assegurar que o material didático seja compreensível e acessível para todos os alunos.

Após a produção e revisão, o material é preparado para distribuição. Isso incluir a impressão física do material didático como plano de contingência e/ou sua digitalização para formatos acessíveis online, ePubs. A equipe multidisciplinar trabalha para garantir que o material esteja disponível de maneira conveniente para os alunos, seja através de plataformas online, bibliotecas ou livrarias.

A disponibilização do material didático aos alunos é o último passo do processo. O acesso ao material é facilitado e há opções para atender às diferentes necessidades dos alunos,

incluindo considerações de acessibilidade para pessoas com deficiência. A equipe multidisciplinar monitora o processo de distribuição para identificar e resolver quaisquer problemas que possam surgir, garantindo que todos os alunos tenham o material necessário para o seu sucesso acadêmico.

4.9.2 Plano de contingência

O Plano de Contingência para o Material Didático do curso de Defesa Cibernética da Faculdade ACADI-TI foi elaborado para assegurar a continuidade operacional pedagógico diante de eventuais interrupções. O Plano delineia a abordagem proativa da ACADI-TI para identificar e mitigar riscos, bem como para estabelecer ações de recuperação e manutenção operacional, garantindo que o processo educacional não seja prejudicado por imprevistos.

Identificação de Riscos

A primeira etapa do plano envolve a identificação detalhada de potenciais riscos que podem afetar a operação pedagógica por falta de acesso ao material. Esse eventos incluem, mas não se limitam a: falta de disponibilidade de autores, atrasos na entrega de conteúdos, erros ou falhas nas fases de revisão e edição, problemas técnicos nos sistemas de digitalização e distribuição online, interrupções logísticas, além de falhas de comunicação interna ou com parceiros externos. Reconhecendo estes riscos, a Faculdade ACADI-TI se posiciona para responder de maneira eficaz a qualquer cenário adverso.

Estratégias de Mitigação

Para cada risco identificado, foram desenvolvidas estratégias específicas de mitigação. A instituição compromete-se, com seu credenciamento e autorização do curso de Defesa Cibernética, a manter uma rede ampla de autores e revisores, implementar sistemas de backup para as etapas digitais, estabelecer contratos de parceria com múltiplas empresas de produção de material didático, e manter uma comunicação clara e eficiente com todos os envolvidos.

Incidente	Resposta ao Incidente
Falta de disponibilidade de autores ou atrasos na entrega dos conteúdos	Ativar a rede de autores e revisores para substituições rápidas; realocar prazos e ajustar o cronograma de publicação conforme necessário.

Erros ou falhas na fase de revisão e edição	Acionar equipe de revisores adicionais para correção imediata; implementar sessões de revisão de emergência.
Problemas técnicos nos sistemas de digitalização e distribuição online	Ativar sistemas de backup; caso o problema persista, recorrer a plataformas de distribuição alternativas.
Interrupções na produção ou distribuição física	Estabelecer contratos com múltiplas gráficas e distribuidoras; utilizar rotas alternativas de distribuição física.
Falhas de comunicação interna ou com fornecedores e parceiros externos	Implementar protocolos de comunicação de emergência; reforçar a comunicação através de múltiplos canais (e-mails, mensagens instantâneas, reuniões de emergência).

Plano de Ação para Recuperação

Na ocorrência de um incidente, o plano prevê a identificação imediata e a avaliação de seu impacto sobre o processo de produção e distribuição. A comunicação rápida do incidente mobiliza a equipe de resposta, que pode substituir autores ou revisores, ativar sistemas de backup ou alterar fornecedores conforme necessário. Estratégias para implementação de rotas alternativas de distribuição física são previstas para minimizar interrupções logísticas.

Manutenção da Continuidade Operacional

Para garantir a sustentabilidade do processo educacional, a Faculdade ACADI-TI enfatiza a importância de realizar auditorias regulares nos sistemas de backup e de atualizar o plano de contingência com base no feedback e análises de incidentes. A manutenção de um estoque mínimo de material didático impresso, o desenvolvimento de uma plataforma robusta de EAD, a diversificação de canais de distribuição, e a formação de um comitê de gestão de crise são medidas essenciais para a manutenção da continuidade operacional.

4.9.3 Sistema informatizado de acompanhamento

O processo de controle de produção e distribuição de material didático é desenhado para antecipa desafios potenciais que possam impactar no processo de ensino e aprendizagem e estabelece um caminho claro para a mitigação de riscos e a recuperação de incidentes. A chave para este sucesso reside no emprego da Plataforma de Gestão Institucional, que centraliza o controle das demandas de produção, garantindo assim a qualidade e a continuidade no fornecimento do material didático essencial para o processo educacional.

Além disso há indicadores claros e bem definidos, fundamentais para o monitoramento e a avaliação da qualidade do material didático e da eficiência dos processos internos. Indicadores como o Tempo de Produção, Taxa de Correção na Revisão, e Satisfação dos Usuários servem como métricas de desempenho, e como ferramentas de diagnóstico que permitem à instituição identificar áreas de melhoria e adaptar-se proativamente às necessidades emergentes dos alunos e docentes. Este nível de detalhamento e foco em qualidade assegura que o material didático não só atenda, mas exceda as expectativas acadêmicas e pedagógicas.

Além da avaliação qualitativa, buscamos garantir da eficiência operacional, utilizando indicadores como Adesão aos Prazos e Disponibilidade do Sistema de Gestão para garantir que os processos de produção e distribuição sejam realizados sem atrasos ou interrupções. O monitoramento contínuo desses indicadores, facilitado pela Plataforma de Gestão Institucional, permite à Faculdade ACADI-TI uma resposta ágil a qualquer incidente, minimizando potenciais impactos negativos sobre a experiência de aprendizagem dos estudantes.

Para implementar e gerenciar esses indicadores eficazmente, a instituição se apoia em uma integração sofisticada de ferramentas dentro da Plataforma de Gestão Institucional. A criação de dashboards analíticos para a visualização em tempo real dos indicadores possibilita uma tomada de decisão informada e rápida pelos gestores, fortalecendo a capacidade da faculdade de adaptar-se às dinâmicas do ambiente educacional. Esse nível de integração e análise contribui significativamente para a manutenção da alta qualidade do material didático e para a satisfação geral dos alunos e docentes com o processo educacional.

Adicionalmente, a Faculdade ACADI-TI reconhece a importância do feedback contínuo dos usuários finais – alunos e professores – na avaliação e melhoria do material didático. Canais de feedback direto e sistemático são essenciais para entender as necessidades, percepções e sugestões de melhorias, contribuindo para uma cultura de melhoria contínua. A revisão e o ajuste periódicos dos indicadores e dos processos, com base nesse feedback e nas análises de incidentes, garantem que a instituição não apenas responda às necessidades atuais, mas também antecipe e se prepare para os desafios futuros. Este compromisso com a excelência e a inovação reflete a dedicação da Faculdade ACADI-TI em oferecer uma educação de alta qualidade, preparando os alunos de Defesa Cibernética para os desafios do século XXI.

Indicadores de Gestão de Produção e Qualidade do Material Didático para o Curso de Defesa Cibernética da Faculdade ACADI-TI

Indicador	Descrição	Meta	Fonte de Dados	Periodicidade	Responsável
Tempo de produção	Tempo médio para produção de cada módulo didático	4 semanas	Sistema de gestão de projetos	Trimestral	Coordenador Pedagógico
Custo de produção	Custo médio por módulo didático	R$2.000,00	Sistema de gestão financeira	Semestral	Coordenador Pedagógico
Satisfação do aluno	Nível de satisfação dos alunos com o material didático	NPS > 70	Pesquisa de satisfacão	Semestral	Coordenador Pedagógico
Atualização do conteúdo	Percentual de conteúdo atualizado em relação à última versão	80%	Revisão de conteúdo	Anual	Professor da disciplina
Adequação ao público-alvo	Nível de adequação do material didático ao nível de conhecimento e às necessidades dos alunos	80%	Avaliação por especialistas	Semestral	Coordenador Pedagógico
Clareza e objetividade	Nível de clareza e objetividade do texto	80%	Avaliação por especialistas	Semestral	Coordenador Pedagógico
Qualidade da linguagem	Nível de correção gramatical e ortográfica	100%	Revisão de texto	Semestral	Revisor
Qualidade das imagens e recursos visuais	Nível de qualidade e adequação das imagens e recursos visuais	80%	Avaliação por especialistas	Semestral	Coordenador Pedagógico
Acessibilidade	Nível de acessibilidade do material didático para alunos com deficiência	100%	Avaliação por especialistas	Anual	Coordenador Pedagógico
Utilização do material didático	Frequência de utilização do material didático pelos alunos	80%	Plataforma de ensino online	Semestral	Professor da disciplina

5. CONSIDERAÇÃO FINAIS

No contexto da construção de uma identidade institucional, a Avaliação versa sobre ações sistêmicas a partir de uma percepção que se arrola as propostas curriculares e pedagógicas desenvolvidas no bojo das instituições. Especificamente a partir da busca pelo ensino e da aprendizagem a partir da contribuição dos métodos de socialização institucional, a partir da discussão sobre seus resultados.

A partir da percepção da Comissão Própria de Avaliação da ACADITI a avaliação possui três objetivos profícuos, os quais são devidamente compartilhados com toda comunidade acadêmica. Tais percepções conclamam a investigação a partir de um processo que consolide um estudo detalhado da instituição sob a orientação do escopo preconizado ao processo avaliativo.

As funções da Avaliação, neste contexto, preconizam predominantemente os princípios maiêuticos e autopoiéticos a partir da discussão dos resultados obtidos por meio do estudo direcionado das dimensões da avaliação. Desse modo, devidamente elencadas, as funções do processo avaliativo compreendem em delimitar ações pedagógicas, funções inovadoras e funções de controle.

No vértice das funções pedagógicas, a Avaliação Institucional preconiza efeitos que se voltem, sobretudo, aos processos instrutivos, orientando metodologicamente a comunidade acadêmica nas atividades operacionais e de ensino; educativos, já que estão consubstanciados em uma relação participativa entre professores e acadêmicos e de ressonância, que busca a discussão de seus resultados sob a égide da estratégia a partir de uma orientação social, conhecendo os agentes participantes e delimitando a cada um responsabilidades convergentes.