MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL FLUMINENSE
REITORIA
RUA CORONEL WALTER KRAMER, Nº 357, PARQUE SANTO ANTONIO, CAMPOS DOS GOYTACAZES / RJ, CEP 28080-565
Fone: (22) 2737-5600

RESOLUÇÃO Nº 28/2022 - CONSUP/IFFLU, DE 2 DE JUNHO DE 2022

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FLUMINENSE - IFFLUMINENSE, no uso das atribuições legais que lhe conferem a Lei nº 11.892 de 29 de dezembro de 2008, a Portaria MEC nº 645, de 17 de agosto de 2021 e o Decreto Presidencial de 03 de abril de 2020, publicado no DOU de 06 de abril de 2020.

CONSIDERANDO:

- A 3ª Reunião Ordinária do Conselho Superior do Instituto Federal Fluminense, realizada em 02 de junho de 2022.

RESOLVE:

Art. 1º APROVAR o Projeto Pedagógico de Curso (PPC) do Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio do **Campus** Cabo Frio, conforme o anexo a esta Resolução.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

JEFFERSON MANHÃES DE AZEVEDO
Presidente do Conselho Superior

Documento assinado eletronicamente por:

- **Jefferson Manhaes de Azevedo**, **REITOR - CD1 - REIT**, **REITORIA**, em 02/06/2022 17:23:50.

Este documento foi emitido pelo SUAP em 02/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.iff.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 358535
Código de Autenticação: 58b6466348

PROJETO PEDAGÓGICO
CURSO TÉCNICO EM SEGURANÇA CIBERNÉTICA CONCOMITANTE AO ENSINO MÉDIO

CAMPUS CABO FRIO
2022

IDENTIFICAÇÃO INSTITUCIONAL

IFFLUMINENSE – *Campus*:	CABO FRIO
CNPJ:	10.779.511/0003-79
Endereço completo:	Estrada Cabo Frio - Búzios, s/nº - Baía Formosa - Cabo Frio - RJ CEP: 28909-971 Caixa Postal: 112015
Fone/Fax de contato:	(22) 2645-9500
E-mail de contato:	gabinetecf@iff.edu.br
Diretor Geral:	Victor Barbosa Saraiva
Número do Processo:	23317.005508.2021-79

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
CAMPUS CABO FRIO

REITOR
Jefferson Manhães de Azevedo

PRÓ-REITOR DE ENSINO
Carlos Artur de Carvalho Arêas

PRÓ-REITOR DE EXTENSÃO
Cátia Cristina Brito Viana

DIRETOR GERAL DO *CAMPUS* CABO FRIO
Victor Barbosa Saraiva

DIRETOR DOS CURSOS SUPERIORES
Renato Cerqueira de Carvalho

DIRETOR DOS CURSOS TÉCNICOS
Vagner Machado de Assis

COORDENADORES DO CURSO TÉCNICO EM SEGURANÇA CIBERNÉTICA
Ewerton Longoni Madruga (Inmetro)

ASSESSORAMENTO PEDAGÓGICO
Tatiana Claro dos Santos

MEMBROS DO GRUPO DE TRABALHO PPC CTSEGCIBER

Fabrício Barros Gonçalves, IFF
Tatiana Claro dos Santos, INMETRO
Flávia Paiva Agostini, INMETRO
Antônio Lacerda Júnior, INMETRO
Cristiano Gurgel de Castro, INMETRO
Paulo Roberto Mesquita Nascimento, INMETRO
Ewerton Longoni Madruga, INMETRO

COLEGIADO DE CURSO

Conforme acordado entre IFF e Inmetro, o colegiado será definido após aprovação do PPC e composto pela coordenação dos cursos e professores.

SUMÁRIO

1. INTRODUÇÃO

1.1 SOBRE O ACORDO DE COOPERAÇÃO TÉCNICA

Ao final de 2020 o Instituto Federal Fluminense (IFF) e o Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO) iniciaram uma aproximação, tendo em vista interesses mútuos em pesquisa, ensino e extensão, que culminou na assinatura de um Acordo de Cooperação Técnica[1] em outubro de 2021, conforme processo SEI Inmetro nº 0052600.005272/2021-73 (Anexo B).

A referida cooperação técnica traz como objeto o estabelecimento de uma parceria para projetos voltados ao desenvolvimento, implementação e oferta de cursos de educação profissional técnica de nível médio nas áreas da ciência, tecnologia e inovação, com ênfase nas áreas de metrologia, metrologia legal, avaliação da conformidade, biotecnologia, informática e segurança da informação.

Vale ressaltar que a parceria foi motivada, ainda, por diversas questões, entre as principais:

(1) O Plano Nacional de Educação (PNE) sob responsabilidade do Ministério da Educação (MEC), que apresenta como uma de suas principais metas triplicar as matrículas de educação profissional técnica de nível médio assegurando a qualidade da oferta e pelo menos 50% (cinquenta por cento) da expansão no segmento público (LEI N° 13.005/2014 de 25 de junho de 2014, Meta 11);

(2) Algumas estratégias presentes no PNE como: a) expandir as matrículas de educação profissional técnica de nível médio na Rede Federal de Educação Profissional, Científica e Tecnológica, levando em consideração a responsabilidade dos Institutos na ordenação territorial, sua vinculação com arranjos produtivos, sociais e culturais locais e regionais, bem como a interiorização da educação profissional; b) fomentar a expansão da oferta de educação profissional técnica de nível médio nas redes públicas estaduais de ensino; c) fomentar a expansão da oferta de educação profissional técnica de nível médio na modalidade de educação a distância, com a finalidade de ampliar a oferta e democratizar o acesso à educação profissional pública e gratuita, assegurado padrão de qualidade;

[1] O acordo de cooperação é o instrumento jurídico hábil para a formalização, entre órgãos e entidades da Administração Pública ou entre estes e entidades privadas sem fins lucrativos, de interesse na mútua cooperação técnica, visando à execução de programas de trabalho, projeto/atividade ou evento de interesse recíproco, da qual **não decorra obrigação de repasse de recursos entre os partícipes.**
A celebração de acordo de cooperação deve ser precedida de adequada instrução processual, que deve necessariamente conter plano de trabalho que contemple as informações elencadas nos incisos I, II, III e VI do parágrafo 1º do art. 116 da Lei nº 8.666/1993 e análise referente às razões de sua propositura, objetivos e de sua adequação à missão institucional dos órgãos e/ou entidades envolvidos, além da pertinência das suas obrigações, esclarecendo, inclusive, o motivo pelo qual a Administração deixou de atender a algum dos requisitos estabelecidos no art. 116, §1º, da Lei nº 8.666/1993, se for o caso.

(3) A política de extensão do IFF, que visa fortalecer e ampliar as atividades de extensão de cunho tecnológico estabelecendo relacionamento entre a instituição e seus diversos públicos e contribuindo para fortalecimento dos arranjos produtivos regionais;

(4) O Plano de Desenvolvimento Institucional do IFF (PDI 2018-2022), traz como objetivos estratégicos: 6 - Ampliar a abrangência de atendimento, diversificando a oferta de cursos, considerando a demanda social regional; 7 - Desenvolver pesquisa, inovação e extensão em articulação com outros atores; 8 - Promover o reconhecimento de saberes, certificação e qualificação profissional;

(5) A própria missão institucional do IFF em promover a Educação Profissional e Tecnológica nacional e suas relações com a educação básica e superior a partir das regiões noroeste, norte e baixadas litorâneas do estado do Rio de Janeiro, na perspectiva da formação integral dos jovens e trabalhadores e do desenvolvimento regional, articulando os atores sócio educacionais e econômicos, assumindo protagonismo na definição e execução de políticas de educação e trabalho;

(6) Que o IFF, para atingir o objetivo estratégico 7, e o indicador 7.4 (número de projetos de extensão desenvolvidos em parceria com entes externos) estabelecidos em seu Plano de Desenvolvimento Institucional (PDI 2018-2022) possui como iniciativa estratégica o "fortalecimento de ações na busca de parcerias com instituições e empresas";

(7) A missão institucional do INMETRO em "viabilizar soluções de infraestrutura da qualidade que adicionem confiança, qualidade e competitividade aos produtos e serviços disponibilizados pelas organizações brasileiras, em prol da prosperidade econômica e bem-estar da nossa sociedade", o que propicia uma circunstância favorável para os profissionais com formação no segmento de Metrologia, Biotecnologia e Segurança Cibernética;

(8) O desdobramento da missão do INMETRO, que definiu sete macroprocessos, entre eles "Formação e qualificação em infraestrutura da qualidade", que traz como proposta de valor "Preparar profissionais especializados para atuarem nas organizações brasileiras e para resolverem problemas de cunho tecnológico, em áreas nas quais os conhecimentos da Infraestrutura da Qualidade sejam um diferencial", o que reforça e ratifica o cenário favorável para formação de profissionais nas áreas de Metrologia, Biotecnologia e Segurança Cibernética.

(9) A oferta, desde 1998, pelo INMETRO do Curso Técnico em Metrologia (o primeiro da América Latina e o quarto curso do gênero no mundo) e, desde 2011, do Curso Técnico em Biotecnologia, ambos executados por meio de Acordo de Cooperação com a Secretaria Estadual de Educação do Rio de Janeiro (SEEDUC-RJ), em regime de intercomplementaridade, tendo formado quase 500 profissionais nas duas áreas;

(10) A oferta pelo INMETRO do Curso de Qualificação Profissional em Segurança Cibernética, por iniciativa própria, tendo em vista a enorme demanda que vem sofrendo para disseminar competência na área de segurança cibernética, mais especificamente ligadas às questões de avaliação de segurança da informação do software embarcado em sistemas de medição.

(11) O histórico de sucesso das formações profissionalizantes do INMETRO, por meio do impacto social e econômico na região onde está localizado o Instituto (Distrito de Xerém/Município de Duque de Caxias/RJ), mas principalmente pela inserção de profissionais altamente capacitados no setor produtivo.

Dessa cooperação técnica culminam três planos de trabalho, voltados para realização de Cursos Técnicos em Metrologia, em Biotecnologia e Segurança Cibernética que, em sintonia com a consolidação e o fortalecimento dos arranjos produtivos locais, pretendem estimular a pesquisa aplicada, a produção cultural, o empreendedorismo e o cooperativismo, apoiando processos educativos que levem à geração de trabalho e renda.

As atribuições de cada instituição podem sem consultadas no texto do Acordo de Cooperação, assim como nos três planos de trabalho. Os documentos encontram-se anexos a este PPC.

1.2. SOBRE O PROJETO PEDAGÓGICO DE CURSO

Este documento tem por objetivo nortear as funções e atividades que devem ser planejadas para o desenvolvimento e implementação do **Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio**, articulando as bases legais e princípios norteadores explicitados pela Lei de Diretrizes e Bases da Educação Nacional (LDB) – Lei nº 9.394/1996 (BRASIL, 2006) –, o conjunto de leis, decretos, pareceres, referências e diretrizes curriculares para a Educação Profissional Técnica de Nível Médio que normatizam a Educação Profissional no sistema de ensino brasileiro, o Plano de Desenvolvimento Institucional (PDI) do IFF (BRASIL, 2018b), a Regulamentação Didático-Pedagógica do IFF (BRASIL, 2011b) e o Planejamento Estratégico do Inmetro (BRASIL, 2021c).

Encontram-se aqui expressos os principais parâmetros para a ação educativa do referido curso. Organizado na perspectiva de uma gestão estratégica e participativa, este projeto representa a sistematização das diretrizes filosóficas e pedagógicas tecidas para a otimização do processo educacional. Assim sendo, sua construção coletiva entre representantes do IFF e do Inmetro reafirma o fortalecimento das instâncias institucionais, bem como dos agentes sociais envolvidos no desenvolvimento das atividades.

Considerando a importância da articulação e do diálogo entre a gestão acadêmica, pedagógica e administrativa do curso com a gestão institucional, em um primeiro momento, neste projeto, serão apresentados brevemente os objetivos, características e finalidades das instituições envolvidas, caracterizando a gênese, a missão e a identidade institucional, para, a seguir, em um segundo momento, focalizar a identidade do curso, incluindo a justificativa, objetivos e perfil do curso, organização curricular, atividades, metodologia adotada e processo avaliativo.

Por fim, convém ressaltar que o PPC, como qualquer instrumento de planejamento, deve estar em permanente construção, sendo elaborado, reelaborado, implementado e avaliado de maneira contínua.

1.3. HISTÓRICO, IDENTIDADE E MISSÃO INSTITUCIONAL

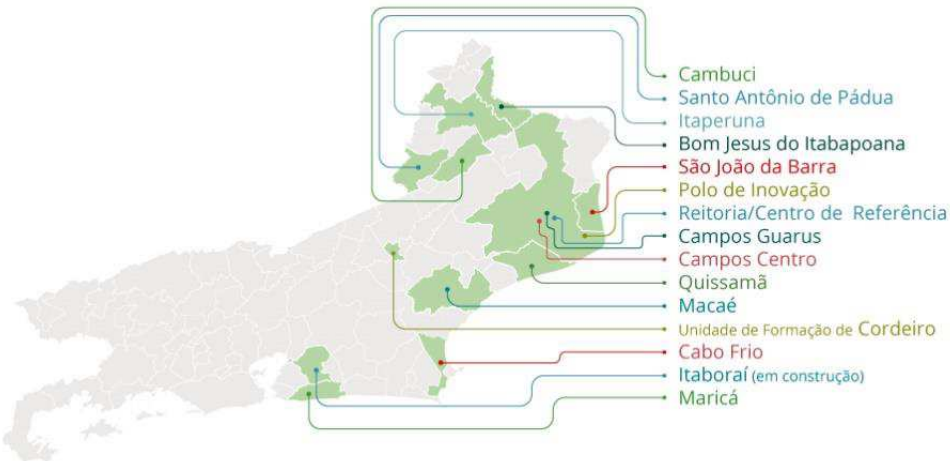
Neste item apresentaremos o histórico, a identidade e a missão das duas instituições parceiras, corresponsáveis pelo Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio: IFF e Inmetro.

1.3.1 O INSTITUTO FEDERAL FLUMINENSE – IFF

Formado a partir do Centro Federal de Educação Tecnológica de Campos dos Goytacazes, o Instituto Federal de Educação, Ciência e Tecnologia Fluminense é um dos trinta e oito institutos criados por meio da Lei n° 11.892 de 29 de dezembro de 2008, pelo Governo Federal, como fruto de uma política pública de expansão da Rede Federal de Educação Profissional. Desde sua criação, ainda como Escola de Aprendizes e Artífices, datada de 23 de setembro de 1909, ao longo de mais de um século de história, diversas foram suas transformações – de Escola de Aprendizes e Artífices para Escola Técnica Industrial (1945); de Escola Técnica Industrial para Escola Técnica Federal (1959); de Escola Técnica Federal para Centro Federal de Educação Tecnológica (1999); e de Centro Federal de Educação Tecnológica para Instituto Federal de Educação, Ciência e Tecnologia (2008) –, as quais foram, gradualmente, redimensionando a filosofia, os objetivos, o perfil e a própria organização e escopo de atuação institucional.

No movimento de territorialização, o Instituto Federal Fluminense encontra-se em 11 municípios, com uma malha espacial que alcança 12 campi, um Polo de Inovação, um Centro de Referência em Tecnologia, Informação e Comunicação na Educação e a Reitoria. Este desenho tem como base os municípios de Bom Jesus do Itabapoana, Itaperuna, Cambuci e Santo Antônio de Pádua na região Noroeste Fluminense; de Campos dos Goytacazes, São João da Barra, Quissamã e Macaé na região Norte Fluminense; na região das Baixadas Litorâneas, o de Cabo Frio; e os municípios de Itaboraí e Maricá na região Metropolitana. A representatividade territorial do IFFluminense ainda conta com os Polos de Educação a Distância nos municípios de Casimiro de Abreu, Bom Jardim, Porciúncula e Miracema; que se somam aos municípios onde há , constituindo, assim, uma verdadeira rede.

Figura 1: Mapa da Abrangência Regional do IFFluminense



Audiodescrição: mapa político do Estado do Rio de Janeiro em cinza claro, com destaque em verde para os municípios. De cada uma das regiões do mapa sinalizada em verde saem linhas quebras colorida que levam à coluna direita com lista indicativa da região de abrangência do IFFluminense: De cima para baixo da lista: Cambuci; Santo Antônio de Pádua; Itaperuna; Bom Jesus de Itabapoana; São João da Barra; em Campos dos Goytacazes têm-se: Polo Inovação, Reitoria/Centro de Referência, Campos Guaru, Campos Centros; Na sequência da lista, Quissamã; Macaé; Unidade de Formação Cordeiro, Cabo Frio, Itaboraí (em construção); Maricá. Fim da audiodescrição[2].

Disponível em: https://portal1.iff.edu.br/conheca-o-iffluminense/conheca-o-iffluminense. Acesso: 28 abr. 2022.

Esse novo desenho traz outra dimensão ao trabalho institucional, que, além de transformar a estrutura do IFFluminense em uma instituição de abrangência em quase todas as mesorregiões do estado do Rio de Janeiro, tem por missão:

i. ofertar educação profissional e tecnológica em todos os seus níveis e modalidades, formando e qualificando cidadãos com vistas à atuação profissional nos diversos setores da economia;
ii. desenvolver a educação profissional como processo educativo e investigativo de geração e adaptação de soluções técnicas e tecnológicas às demandas sociais e peculiaridades regionais;
iii. promover a integração e a verticalização da educação básica à educação profissional e educação superior, otimizando a infraestrutura física, os quadros de pessoal e os recursos de gestão;
iv. qualificar-se como centro de referência na oferta do ensino de Ciências, em geral, e de Ciências aplicadas, em particular, atuando, inclusive na capacitação técnica e atualização pedagógica dos docentes das redes públicas de ensino;
v. desenvolver programas de extensão e de divulgação científica e tecnológica;
vi. realizar e estimular a pesquisa aplicada, a produção cultural, o empreendedorismo, o cooperativismo e o desenvolvimento científico e tecnológico;
vii. e, por fim, promover a produção, o desenvolvimento e a transferência de tecnologias sociais, notadamente as voltadas à preservação do meio ambiente.

Por isso, no âmbito da Educação Profissional e Tecnológica, o IFFluminense, em cumprimento aos objetivos da educação nacional, integra seus cursos aos diferentes níveis e demais modalidades de educação e às dimensões do trabalho, da Ciência, da tecnologia e da cultura, tendo por objetivo primordial a formação e qualificação de profissionais na perspectiva de promover o desenvolvimento humano sustentável local e regional, por meio da tríade: ensino, pesquisa e extensão. Os cursos do Instituto, em suas diversas modalidades, estão agrupados em eixos conforme suas características científicas e tecnológicas e concorrem para a mudança da realidade do Norte e Noroeste Fluminense, das Baixadas Litorâneas e da região Metropolitana do Rio de Janeiro.

[2] Audiodescrição produzida pela audiodescritora Loide Aragão e pelo consultor Renato Ferreira da Costa.

Pensando na possibilidade de oferecer educação continuada e constante ao educando, com vistas à democratização do acesso, os cursos regulares oferecidos estão, atualmente, agrupados nas seguintes modalidades e formas de oferta:

I - Educação Presencial:

a) Para concluintes do Ensino Fundamental: Cursos Técnicos Integrados ao Ensino Médio

b) Para estudantes matriculados no Ensino Médio ou concluintes em outras instituições: Cursos Técnicos Concomitantes ao Ensino Médio

c) Para estudantes concluintes do Ensino Médio: Cursos de Graduação

II - Educação a Distância:

a) Para concluintes do Ensino Médio: Curso Técnico Subsequente ao Ensino Médio

b) Para estudantes concluintes do Ensino Médio: Cursos de Graduação

O *Campus* Cabo Frio

Tendo em vista o Acordo de Cooperação Técnica entre IFF e Inmetro, o *campus* de oferta do curso será Cabo Frio, também responsável pelo registro de vagas nos sistemas educacionais, como o SISTEC.

O *campus* Cabo Frio surgiu da implantação da Unidade de Ensino da Rede Federal de Educação Tecnológica na Região das Baixas Litorâneas em junho de 2007, como parte do Plano de Expansão da Rede Federal de Educação Tecnológica - FASE II. O município de Cabo Frio foi escolhido de acordo com o conceito de cidade-polo, pois apresenta como referência o conjunto de municípios na abrangência da região das Baixadas Litorâneas, na perspectiva de aproveitar o potencial de desenvolvimento, a proximidade com Arranjos Produtivos Locais (APL), a possibilidade de parcerias e infraestrutura existentes.

A área de abrangência do *Campus* Cabo Frio é composta por treze municípios e atende a uma população de aproximadamente 801.535 habitantes distribuídos em uma área de 5.415Km2, sendo o município mais distante o de Cachoeira de Macacu (144 km do *Campus*).

Em 2009, no *campus* Cabo Frio, foram implantados os cursos técnicos de nível médio integrados nas áreas de Petróleo e Gás, e Hospedagem e os cursos na modalidade concomitante em Eletromecânica e na modalidade subsequente em Guia de Turismo. Nesse mesmo ano, houve a inserção do Curso de Nível Superior – Licenciatura em Física, na Área Básica de Ciências da Natureza – para formar professores habilitados em Física. No período de 2010-2011, foram implantados os cursos concomitantes de técnicos em Cozinha e em Eventos. Ademais, os cursos de Licenciatura em Química e Biologia, Pós-Graduação Latu Sensu em Ensino de Ciências e de Educação Ambiental foram implantados em atendimento ao Programa de Integração da Educação Básica com a Educação Profissional e ao compromisso de formação de professores. Em 2013, foi implantado o Curso Técnico Concomitante em Química, e o Curso Superior de Tecnologia em Hotelaria em 2015.

A proposta estruturada no *campus* Cabo Frio configura-se nos seguintes objetivos:

- Organizar as atividades de ensino, pesquisa e extensão como expedientes fundamentais ao processo de ensino e de aprendizagem, nas modalidades de ensino ofertadas, em atendimento às novas demandas da sociedade que, por sua vez, exige uma formação que articule a competência científica e técnica com a inserção política e a postura ética.
- Buscar um padrão de trabalho que possa ser referência na educação profissional tecnológica, em seu compromisso com o desenvolvimento local e regional.
- Discutir permanente e sistematicamente com os campi do IFFluminense no sentido da implantação e implementação de uma metodologia de trabalho que integre propostas de atuação no ensino, pesquisa e extensão.
- Incentivar a participação dos discentes em projetos de iniciação científica e em outros programas de pesquisa, por meio de ampliação de bolsas e outros.
- Atuar em diferentes níveis e modalidades de formação na perspectiva da verticalização do ensino, estimulando a criação de linhas de pesquisa relacionadas aos cursos ofertados pelo *campus* Cabo Frio.
- Estabelecer diálogo permanente com o setor produtivo e a sociedade, especialmente de abrangência local e regional, oferecendo mecanismos para a educação continuada, na perspectiva de aprimoramento das propostas de formação profissional técnica e tecnológica.
- Reafirmar a política nacional de aperfeiçoamento profissional de professores, atuando nas licenciaturas e especialização de professores (em especial da Área de Ciências Naturais - Física, Química e Biologia).
- Trabalhar no sentido da criação de novos espaços de modo que o estudo das ciências aconteça de forma mais viva e integrada.
- Intensificar as iniciativas no campo da pesquisa, buscando responder aos editais de órgão de fomento.
- Consolidar convênios e cooperação técnica com empresas e órgãos governamentais.
- Estabelecer convênios com órgãos e movimentos sociais voltados para Tecnologias Sociais, Conservação Ambiental e Patrimônio Cultural.

Respeitando a legislação em vigor, especificamente a dos Institutos Federais de Educação, Ciência e Tecnologia, a organização curricular que sustenta a proposta pedagógica no *campus* Cabo Frio envolve os conceitos de interdisciplinaridade, contextualização, flexibilidade e atualização permanente, apresentados nos princípios estabelecidos na Carta de Cabo Frio (IPHAN/2008) para o IFFluminense em consonância às Diretrizes Curriculares Nacionais.

1.3.2 O INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA - INMETRO

O Instituto Nacional de Metrologia, Qualidade e Tecnologia - Inmetro - é uma autarquia federal, vinculada à Secretaria Especial de Produtividade, Emprego e Competitividade, do Ministério da Economia. O Instituto atua como Secretaria Executiva do Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (Conmetro), colegiado interministerial, que é o órgão normativo do Sistema Nacional de Metrologia, Normalização e Qualidade Industrial (Sinmetro).

Objetivando integrar uma estrutura sistêmica articulada, o Sinmetro, o Conmetro e o Inmetro foram criados pela Lei 5.966, de 11 de dezembro de 1973 (BRASIL, 1973), cabendo a este último substituir o então Instituto Nacional de Pesos e Medidas (INPM) e ampliar significativamente o seu raio de atuação a serviço da sociedade brasileira.

No âmbito de sua ampla missão institucional, o Inmetro objetiva fortalecer as empresas nacionais, aumentando sua produtividade por meio da adoção de mecanismos destinados à melhoria da qualidade e da segurança de produtos e serviços.

A autarquia possui uma ampla gama de atribuições, se constituindo numa instituição multidisciplinar, atuando nas áreas de Metrologia Científica e Industrial, Metrologia Legal, Avaliação da Conformidade, no credenciamento de laboratórios de ensaios e de calibração, sendo o organismo credenciador oficial do Brasil. É também o organismo credenciador de organismos de certificação de produtos e serviços, de organismos de inspeção, de organismos de certificação de pessoal, dentre outros.

Dentre as competências e atribuições do Inmetro destacam-se:

- Executar as políticas nacionais de Metrologia e da Qualidade;
- Verificar e fiscalizar a observância das normas técnicas e legais, no que se refere às unidades de medida, métodos de medição, medidas materializadas, instrumentos de medição e produtos pré-medidos;
- Manter e conservar os padrões das unidades de medida, assim como implantar e manter a cadeia de rastreabilidade dos padrões das unidades de medida no País, de forma a torná-las harmônicas internamente e compatíveis no plano internacional, visando a sua aceitação universal e a sua utilização com vistas à qualidade de bens e serviços;
- Fortalecer a participação do País nas atividades internacionais relacionadas com Metrologia e Avaliação da Conformidade, promovendo o intercâmbio com entidades e organismos estrangeiros e internacionais;
- Prestar suporte técnico e administrativo ao Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (Conmetro) e aos seus comitês assessores, atuando como sua secretaria executiva;
- Estimular a utilização das técnicas de gestão da qualidade nas empresas brasileiras;
- Planejar e executar as atividades de Acreditação de Laboratórios de Calibração e de Ensaios, de provedores de ensaios de proficiência, de Organismos de Avaliação da Conformidade e de outros necessários ao desenvolvimento da infraestrutura de serviços tecnológicos no País;
- Coordenar, no âmbito do Sistema Nacional de Metrologia, Normalização e Qualidade Industrial (Sinmetro), a atividade de Avaliação da Conformidade, voluntária e compulsória de produtos, serviços, processos e pessoas;
- Planejar e executar as atividades de pesquisa, ensino, desenvolvimento tecnológico em Metrologia e Avaliação da Conformidade; e
- Desenvolver atividades de prestação de serviços e transferência de tecnologia e cooperação técnica, quando voltadas à inovação e à pesquisa científica e tecnológica em Metrologia e Avaliação da Conformidade.

Por seu caráter multidisciplinar, o Inmetro – desde sua criação – apresenta forte vocação à produção e respectivo compartilhamento do conhecimento científico. Contudo, foi em 2011, quando a Lei nº 12.545 (BRASIL, 2011a) reformulou as atribuições do Inmetro, que outrora chamava-se "Instituto Nacional de Metrologia, Normalização e Qualidade Industrial", passando a se chamar Instituto Nacional de Metrologia, Qualidade e Tecnologia. Com a iniciativa, o governo pretendia melhorar a atuação do órgão no apoio à inovação do setor produtivo e controlar a entrada de produtos estrangeiros que não atendiam aos requisitos técnicos avaliados pelo Instituto.

Entre as funções do Inmetro definidas na nova lei estão a de planejar e executar atividades de pesquisa, ensino e desenvolvimento científico e tecnológico em Metrologia, avaliação da conformidade e áreas afins; conceder bolsas de pesquisa científica e tecnológica para o desenvolvimento de tecnologia, de produto ou de processo, de caráter contínuo, diretamente ou por intermédio de parceria com instituições públicas ou privadas.

Em 2021 o Inmetro elabora seu novo Planejamento Estratégico (BRASIL, 2021c), definindo como missão institucional "viabilizar soluções de infraestrutura da qualidade que adicionem confiança, qualidade e competitividade aos produtos e serviços disponibilizados pelas organizações brasileiras, em prol da prosperidade econômica e bem-estar da nossa sociedade".

A partir do desdobramento de sua missão, o Instituto definiu sete macroprocessos, entre eles "Formação e qualificação em infraestrutura da qualidade", que traz como proposta de valor "Preparar profissionais especializados para atuarem nas organizações brasileiras e para resolverem problemas de cunho tecnológico, em áreas nas quais os conhecimentos da Infraestrutura da Qualidade sejam um diferencial". Esse cenário reitera, certamente, uma circunstância favorável à formação de profissionais nos segmentos de atuação da referida autarquia.

Ensino, Pesquisa e Extensão no Inmetro

O Inmetro mantém ações contínuas e consistentes na formação de conhecimento em Metrologia, Biotecnologia e avaliação da conformidade. São cursos de pós-graduação *stricto sensu*, cursos técnicos, qualificação profissional e capacitações que favorecem a disseminação da cultura metrológica no Brasil e no exterior.

Essa ampla atuação assegura ao Inmetro uma posição de destaque entre os órgãos congêneres no exterior, reforçando a alta capacidade do País em contribuir para o constante avanço da Metrologia, sua aplicação nos diversos setores produtivos e, em última instância, para toda a sociedade.

As ações de ensino no Inmetro são gerenciadas pelo Centro de Capacitação, em consonância com as diretrizes do Conselho Acadêmico do Inmetro.

O Centro de Capacitação do Inmetro é a unidade responsável por promover a formação, a capacitação, o aperfeiçoamento e a profissionalização em Metrologia, Biotecnologia, avaliação da conformidade e áreas afins. Mantém o Programa de Pós-Graduação em Metrologia e Qualidade, o Programa de Pós-Graduação em Biotecnologia, o Curso Técnico em Metrologia, o

Curso Técnico em Biotecnologia e o curso de Segurança Cibernética (qualificação). As capacitações compõem outra importante frente de atuação, sendo voltadas para os públicos interno e externo, incluindo os órgãos delegados da Rede Brasileira de Metrologia e Qualidade - Inmetro. As capacitações podem ser ministradas presencialmente ou a distância. O Centro faz parte do Sistema de Escolas de Governo da União.

O Conselho Acadêmico do Inmetro é um órgão de assistência direta ao Presidente do Inmetro para tratar das questões referentes à formação de recursos humanos em caráter técnico-científico em Metrologia, Biotecnologia, avaliação da conformidade e áreas afins. Entre suas atribuições se destacam a proposição de diretrizes de formação técnica-científica, a promoção de atividades de desenvolvimento científico-tecnológico junto a organizações congêneres e a homologação de novos cursos e/ou ajustes nos programas de pós-graduação e no ensino técnico. Compõem o Conselho Acadêmico os diretores das unidades do Inmetro, os coordenadores de cursos e o Coordenador do Centro de Capacitação, a quem compete a execução das deliberações.

***Campus* do Inmetro – Xerém/RJ**

Além de sedes administrativas em Brasília e no Centro da cidade do Rio de Janeiro, o Inmetro possui um extenso *campus* localizado no distrito de Xerém, no município de Duque de Caxias (RJ). Dispondo de 2,3 milhões de metros quadrados, o *Campus* Dr. Armênio Lobo da Cunha Filho sedia o maior complexo laboratorial de Metrologia da América Latina e teve sua atuação estendida para áreas como a Nanometrologia e a Biotecnologia.

Figura 2: *Campus* de Laboratórios do Inmetro – Xerém/RJ

Audiodescrição: fotografia panorâmica de cima do *Campus* de Laboratórios do Inmetro, localizado no distrito de Xerém, Município de Duque de Caxias, Estado do Rio de Janeiro, Brasil. No canto esquerdo e na parte superior, vegetação local com árvores, arbusto e gramados. No canto superior esquerdo, pequeno quadro com a letra I em branco com a letra N por cima com fundo transparente, abaixo em letras pequenas brancas: INMETRO. Ao centro, tomando quase toda extensão da figura, largo terreno dividido em blocos de tamanhos irregulares com gramados, construção de diferentes tamanhos, não muito altas, aparentando ter mais ou menos de dois andares. Vias asfaltadas cortam os blocos. No canto superior, dois blocos, com uma construção cada, transpassados por vias na horizontas e na vertical. À frente da via horizontal, dois blocos com gramados e com torres de eletricidade. Descendo a via na vertical, tem-se um bloco largo horizontal, que leva a vias menores intercaladas por pequenos canteiros retangulares arborizados, lembrando um estacionamento. Na mesma dimensão do canteiro, tem-se uma passagem coberta de telhas que leva para um prédio baixo branco de tamanho médio de formato em O com pátio interno descoberto. Ao final da via horizontal tem-se uma rotatória. Seguindo a via vertical, à esquerda bloco com dois prédios, uma em formato em O, com pátio interno descoberto e outro em formato de I. À frente, campo largo horizontal com pequena construção em L. Descendo a rotatória, à direita, via que

leva para outro bloco, com pequeno prédio à esquerda e prédio maior localizado na parte de posterior em formato de O com pátio interno descoberto. Seguindo a mesma via, mais a esquerda, há outra via que leva para um bloco, ao centro com prédio em formato de U, com pequeno prédio à frente. No canto esquerdo, seguido a via que sai do prédio pequeno, tem-se um bloco com prédio pequeno em formato O com pátio interno descoberto. No canto inferior esquerdo, outro prédio menor retangular. No canto direito, vegetação, com árvores e gramado, transpassados por pequenas vias e calçadas. Em letras brancas "*Campus* de Laboratórios de Inmetro", abaixo em letras brancas menores "Xerém, Duque de Caxias – Rio de Janeiro – RJ". Fim da audiodescrição[3]

Disponível em: https://asmetro.org.br/portalsn/2019/05/20/45-anos-de-historia-campus-do-inmetro-xerem-e-denominado-dr-armenio-lobo-da-cunha-filho-2/ Acesso: 28 abr. 2022.

Localizado no Prédio 32 do *Campus* de Laboratórios do Inmetro, em Xerém, o Centro de Capacitação possui estrutura com salas de aula, ambiente virtual de aprendizagem, laboratórios, auditório e secretaria que atendem aos seus alunos, professores e parceiros vinculados aos diversos programas educacionais ali desenvolvidos.

Tendo em vista o Acordo de Cooperação Técnica entre IFF e Inmetro, as aulas do curso serão ministradas no referido *campus*, onde localiza-se o Centro de Capacitação, além de laboratórios e biblioteca.

Cursos Técnicos

Desde 1998 o Inmetro oferta o Curso Técnico em Metrologia, sendo o primeiro da América Latina e o quarto curso do gênero no mundo. Desde 2011 também oferece o Curso Técnico em Biotecnologia, ambos integrados ao Ensino Médio e executados por meio de Acordo de Cooperação com a Secretaria Estadual de Educação do Rio de Janeiro (SEEDUC-RJ), em regime de intercomplementaridade tendo formado quase 500 profissionais nas duas áreas.

Em 2019 o INMETRO iniciou, ainda, a oferta do Curso de Qualificação Profissional em Segurança Cibernética, por iniciativa própria, tendo em vista a enorme demanda que vem sofrendo para disseminar competência na área de segurança cibernética, mais especificamente ligadas às questões de avaliação de segurança da informação do software embarcado em sistemas de medição.

Nesse contexto, o Inmetro também tem se distinguido por ser um órgão socialmente responsável e, ao longo dos anos, vem buscando delinear um novo modelo de participação como forma de promover a redução das desigualdades sociais. Adicionalmente, a educação de qualidade desponta como um dos principais mecanismos de redução permanente da desigualdade social.

Dentro deste contexto se inserem os cursos técnicos e de qualificação profissional, que podem ser conceituados como uma das ações sociais realizadas pelo Inmetro de maior impacto e sucesso junto aos moradores da comunidade de Xerém e outras comunidades vizinhas ao *Campus*, tornando-se um curso de referência na região, podendo ser ainda considerado como um instrumento de renovação e ampliação do quadro de profissionais das referidas carreiras.

[3] Audiodescrição produzida pela audiodescritora Loide Aragão e pelo consultor Renato Ferreira da Costa.

2. IDENTIFICAÇÃO DO CURSO

2.1. APRESENTAÇÃO DO CURSO

O presente Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio é fruto de uma parceria entre o Inmetro e o IFF que culminou com a assinatura de um Acordo de Cooperação Técnica em outubro de 2021 (publicado no DOU N.º 15/2021, seção 3, página 43**,** ISSN 1677-7069 Nº 210, terça-feira, 9 de novembro de 2021) e visa atender, entre outros, a jovens interessados nos diferentes aspectos especializados ou multidisciplinares da ciência e tecnologia.

O curso proposto neste PPC será ofertado pelo IFF *Campus* Cabo Frio, que fará toda a tramitação acadêmica dos estudantes conforme estabelecido como competência do IFF no Acordo de Cooperação Técnica. Contudo, as aulas serão ministradas utilizando o corpo docente, a infraestrutura de salas de aula e laboratorial do Inmetro, na cidade de Duque de Caxias, no *Campus* do Inmetro – Xerém/RJ. O referido curso terá a duração de 2 anos e está organizado em 4 semestres.

A região metropolitana do Rio de Janeiro, onde o *campus* do Inmetro está situado, abriga uma das maiores áreas industriais do País, contando com indústrias químicas, aeroespaciais, navais etc. e apresenta uma demanda consistente por profissionais da área metrológica. Apesar de industrializada e próspera, a região apresenta baixo Índice de Desenvolvimento Humano (IDH) e escassas opções de ensino profissionalizante gratuito e de qualidade. Nesse sentido, a formação no Curso Técnico em Segurança Cibernética se apresenta como um diferencial para que a população dessa região consiga se inserir nesse mercado de trabalho especializado, operando uma transformação nas vidas de muitas famílias locais.

A ausência de Cursos Técnicos em Segurança Cibernética no país motivou o Inmetro a oferecer um curso de qualificação profissional nesta área do conhecimento a partir do ano de 2019. Nesse sentido, o Curso Técnico em Segurança Cibernética atende uma demanda em todo o espectro de empresas no mercado nacional. Em empresas de pequeno e médio porte, normalmente existem recursos mais reduzidos para a contratação de pessoal. Ali, sua experiência com sistemas seguros permite que auxilie o departamento de tecnologia da informação com a implantação de serviços, em cargos que podem ser de operador até analista júnior. Em empresas de grande porte, o técnico traz uma bagagem profissional que permite iniciar uma carreira em um enquadramento funcional inicial na hierarquia da empresa, como operador do centro de operações de segurança.

Ao implantar este curso, ambas as instituições Inmetro e IFF estarão novamente atuando na vanguarda da educação profissional no país. Este será o primeiro curso técnico em todo o Brasil nesta área tecnológica, a Segurança Cibernética. Para a implantação do curso, representantes de ambas as instituições já estão formalizando-o junto ao Governo Federal. No momento de elaboração deste plano pedagógico, estes representantes já estão contribuindo com o Ministério de Educação – MEC para inclusão do currículo deste novo curso no Catálogo Nacional de Cursos Técnicos (CNCT), atuando em um grupo de trabalho específico, liderado pelo Pró-Reitor de Ensino, do Instituto Federal Fluminense, por ocasião da elaboração deste plano pedagógico, Prof. Carlos Artur de Carvalho Arêas.

2.2 *CAMPUS*

Tendo em vista o Acordo de Cooperação Técnica entre os dois institutos, o registro dos estudantes será realizado pelo IFF *Campus* Cabo Frio, que fará toda a tramitação acadêmica dos estudantes conforme estabelecido como competência do IFF no ACT. Contudo, as aulas serão ministradas utilizando a infraestrutura de salas de aula e laboratorial do INMETRO, na cidade de Duque de Caxias, no *Campus* do Inmetro – Xerém/RJ.

2.3 DADOS DO CURSO

DADOS DA IDENTIFICAÇÃO DO CURSO		
1.	**Denominação do Curso**	Técnico em Segurança Cibernética Concomitante ao Ensino Médio
2.	**Área de Conhecimento ou Eixo Tecnológico**	Informação e Comunicação
3.	**Nível**	Médio
4.	**Modalidade de Ensino**	A Distância
6.	**Bases Legais**	Constituição Federal/1988; Lei Nº 5.966, de 11 de dezembro de 1973; Lei Nº 8.060/1990, suas alterações e regulamentos; Lei Nº 9.394/1996; Lei no 11.788/2008; Lei Nº 11.645/2008; Lei Nº 11.892/2008; Lei Nº 12.545, de 14 de dezembro de 2011 Lei Nº13.005/2014; Lei 13.145/2015; Decreto Nº 4.281/2002; Decreto Nº 5.154/2004; Decreto Nº 7.234/2010; Resolução CNE/CP Nº 01/2012; Resolução CNE/CP Nº 02/2012; Resolução CNE/CEB Nº 3/2018; Resolução CNE/CP Nº 1/2021; Portaria Inmetro Nº 2, de 4 de janeiro de 2017; Portaria Nº 2, de 4 de janeiro de 2017; Catálogo Nacional de Cursos Técnicos – 4a edição/2020; Regulamentação Didático-Pedagógica do IFF/2011; Projeto Político-Pedagógico Institucional (PPI) do IFF/2018; Resolução IFFluminense Nº 20/2015; Resolução IFFluminense Nº 34/2016; Resolução IFFluminense Nº 39/2016; Resolução IFFluminense Nº 23/2017; Resolução IFFluminense Nº 40/2017; Resolução IFFluminense Nº 43/2018; Instrução Normativa IFFluminense Nº 3/2021; Instrução Normativa IFFluminense Nº 2/2021. Portaria IFFluminense Nº 1.917/ 2017; Deliberação IFFluminense Nº 10/2017.
7.	**Unidade Ofertante**	Cabo Frio Local das aulas: *Campus* Inmetro – Duque de Caxias/Xerém, RJ
8.	**Público-Alvo**	Estudantes que estejam cursando o 2º ou 3º anos do Ensino Médio em qualquer Instituição de Ensino, pública ou privada.
9.	**Número de vagas oferecidas**	Até 30 (conforme edital)
10.	**Periodicidade da oferta**	Anual

11.	**Forma de oferta**	Concomitante ao Ensino Médio
12.	**Requisitos e formas de acesso**	Processo seletivo/Transferência Interna e Externa – Conforme Regulamentação Didático Pedagógica
13.	**Regime de matrícula**	Semestral
14.	**Turno de funcionamento**	Vespertino
15.	**Carga horária total do curso**	1200 horas
16.	**Total de horas-aula**	1200 horas
17.	**Carga horária específica da parte profissionalizante**	1200 horas
18.	**Estágio Curricular Supervisionado**	Não Obrigatório
19.	**Tempo de duração do curso**	Dois anos
20.	**Tempo de integralização do curso**	**Mínimo**: 2 anos e **Máximo**: não se estabelece período máximo para que a integralização se efetive, em conformidade com a Regulamentação Didático Pedagógica do IFFluminense.
21.	**Título acadêmico conferido**	Técnico em Segurança Cibernética
22.	**Coordenação do curso**	Inmetro: Ewerton Longoni Madruga, Ph.D. Pesquisador Tecnologista - Inmetro Doutor em Engenharia de Computação elmadruga@inmetro.gov.br
23.	**Início do Curso**	2º semestre letivo de 2022
24.	**Trata-se de**	(X) Apresentação Inicial de PPC ( ) Reformulação de PPC

2.4 JUSTIFICATIVA DE OFERTA DO CURSO

Com o mundo funcionando cada vez mais on-line, a questão da segurança cibernética tornou-se ainda mais urgente. Sinal disso, por exemplo, é o aumento de ataques e exposição de dados de empresas e de internautas, como informa a mídia especializada, que tem acompanhado o crescente uso da internet nesses tempos de isolamento social. Nesse cenário, especialistas em recrutamento e seleção já indicam que o profissional de segurança cibernética é uma das profissões em destaque no momento atual e que seguirá em alta após a pandemia.

2.4.1 – O QUE É SEGURANÇA CIBERNÉTICA?

Há muitas décadas, no surgimento da então nova área de segurança da informação, como concebida para o fluxo de informação processada por computadores, foi cunhada uma sigla que definia os fundamentos em questão. Esta é a sigla C.I.D., que são as iniciais de Confidencialidade, Integridade e Disponibilidade. A confidencialidade pressupõe que a informação deva ser privada apenas aos agentes que devem ter acesso a ela, servindo como sinônimo para o conceito de privacidade neste contexto. A integridade determina que uma vez concebida a informação, esta não pode ser modificada por terceiros. Finalmente, a disponibilidade determina que à informação terão acesso os agentes no momento determinado, sem possibilidade que terceiros criem obstáculos para este acesso. Esta tríade C.I.D. foi proposta ainda no início da década de 1970 (ANDERSON, 1972) como sendo aquela que definia os pilares para construção daquela que era uma nova área então.

Cinquenta anos depois, esta tríade, embora válida e referenciada em várias publicações atualmente, mostrou-se insuficiente para definir com clareza o espectro de atividades envolvidas quando o objetivo é prover segurança (HAM, 2021) nos dias atuais. Na década de 1970, computadores não estavam conectados entre si e sequer existia a Internet. O contexto no qual computadores são usados hoje em dia evoluiu drasticamente. De computadores isolados, que ocupavam salas inteiras para sua operação, nós hoje circulamos pelas ruas com vários computadores em pastas e bolsos do casaco que automaticamente se conectam em rede quando são ligados e colocados em operação.

A rotina do dia a dia está cada vez mais dependente de um sem-fim de ‘dispositivos’, móveis ou não e dos mais diversos tipos e tamanhos. Com o advento dos 'smartphones', acessando a Internet de qualquer lugar e à qualquer hora, e o fato inevitável de que estes aparelhos de uso privado são trazidos rotineiramente para dentro das empresas, políticas de proteção à informação concebidas lá atrás não são mais viáveis.

Muitas décadas mais tarde, agora tem-se um entendimento muito melhor dos riscos envolvidos quando o assunto é segurança cibernética. Como uma visão mais ampla do problema (HAM, 2021), a abordagem proposta pelo NIST, órgão de padronização e tecnologia do governo norte-americano, é uma daquelas que se destacam (NIST, 2018). Ali, define-se que a área da segurança cibernética é aquela compreendida por cinco atividades diferentes:

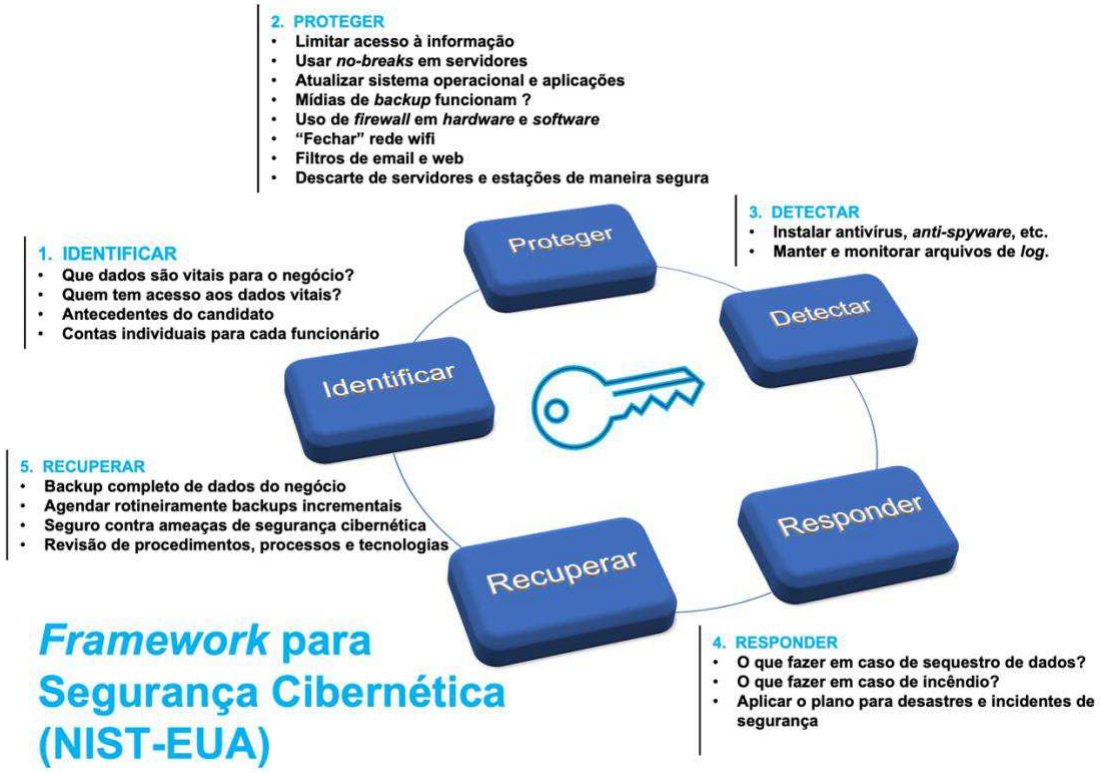
1) **Identificar**: listar os ativos mais importantes de uma organização que devem permanecer seguros;
2) **Proteger**: definir e implementar medidas de proteção dos ativos identificados;
3) **Detectar**: posicionar sensores e implantar processos para sinalizar quando a proteção implantada foi suplantada;
4) **Responder**: definir processos de resposta a incidentes detectados;

5) **Recuperar**: desenvolver planos de resiliência na organização, assim como mecanismos de recuperação.

Com a atividade de identificação, todos os ativos de uma empresa que devem estar seguros estarão devidamente listados. Esta lista será de conhecimento de todos os agentes responsáveis pela segurança destes ativos. Um ativo pode ser uma planilha Excel com dados de movimentação de produtos, um grupo de estações de trabalho do departamento de Marketing ou o celular dos executivos da empresa.

A atividade de proteção é apenas uma das atividades de segurança cibernética e não o foco único. Esta abordagem em atividades relevantes proposta pelo NIST coloca as medidas protetivas como uma parte do processo como um todo, e menos como o objetivo central.

Figura 3: O Framework de Segurança Cibernética, de acordo com o *National Institute for Standards and Technology* (NIST-EUA)



Audiodescrição: Imagem vertical que demostra as cinco atividades que compõem o ciclo em que consiste a segurança cibernética. Cada atividade traz consigo uma lista de exemplos de tarefas que são características daquela atividade. A atividade número um é identificar; a atividade número dois é proteger; a atividade número três é detectar; a atividade número quatro é responder; e a atividade número cinco é recuperar. Fim da audiodescrição.

Adaptado de: https://www.nist.gov/news-events/news/2018/05/mep-centers-aid-manufacturers-cybersecurity. Acesso em: 25 maio 2022.

As atividades de detecção, resposta e recuperação nos ajudam com o fato de que segurança não é algo absoluto. A proteção para riscos mais complexos pode ser economicamente inviável para a organização, e devem ser mitigados pela detecção, resposta e recuperação de incidentes. Estas 3 atividades nos fazem compreender que segurança nunca é perfeita - o analista que trabalha assumindo ter um ativo 100% seguro pode ver-se sem seu emprego no dia seguinte. Medidas devem ser sempre planejadas para o pior caso, na falha das medidas protetórias, para que as consequências negativas de um incidente não sejam devastadoras para o futuro da organização. Para melhor ilustração, a Figura 3 acima traz exemplos de tarefas associadas a cada atividade do ciclo.

O uso cada vez mais amplo da internet fez propagar as chamadas ameaças cibernéticas, capazes de causar grandes danos às empresas, governos e sociedade em geral. Infelizmente, o Brasil ainda é um país vulnerável e pouco preparado para lidar com essas ameaças.

A segurança cibernética no Brasil é uma área que ainda está em construção, sendo necessária uma maior disseminação da cultura da segurança e o envolvimento de todos os atores sociais. É através de políticas públicas que são estabelecidas regras e ações visando proteger e controlar o ambiente virtual no país.

Através do Decreto Nº 10222, o Presidente da República aprovou em 5 de fevereiro de 2020 a Estratégia Nacional de Segurança Cibernética – E-Ciber, conforme o disposto no inciso I do art. 6º do Decreto nº 9.637, de 26 de dezembro de 2018. A E-Ciber, criado no âmbito do Gabinete de Segurança Institucional (GSI) do executivo federal, além de preencher importante lacuna no arcabouço normativo nacional sobre segurança cibernética, estabelece ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto. Uma destas ações é na área da Educação.

O rápido avanço tecnológico, acompanhado da transformação digital proposta para a sociedade moderna, tornou imprescindível o desenvolvimento de ações educacionais e pedagógicas para a formação em prol do uso criterioso, seguro e responsável das tecnologias. Nesse sentido, considera-se que a prioridade de investimentos em programas de educação relacionados à segurança cibernética é um pilar essencial para reduzir os riscos às empresas e à sociedade.

No contexto da formação, a abordagem da segurança cibernética nas escolas brasileiras ainda é muito incipiente, quando não, inexistente. No âmbito da educação superior, a segurança cibernética, como disciplina ou programa de estudo, ainda é de difícil acesso aos alunos. A segurança cibernética, em geral, não é um tópico acadêmico isolado, mas parte do currículo do curso de graduação de Ciência da Computação, sendo um tema em constante mudança, que requer treinamento e educação constantes. Entretanto, ressalta-se que já existem iniciativas de ensino em áreas correlatas à segurança cibernética, como a recente criação do curso superior de Tecnologia em Defesa Cibernética, no Catálogo Nacional de Cursos Superiores de Tecnologia.

Atualmente, universidades e instituições não formam especialistas em número suficiente em segurança cibernética para atender às crescentes necessidades do setor; entretanto, o tema tornou-se de tamanha relevância que não pode permanecer restrito àquelas entidades, mas deve ser de conhecimento e de domínio de todos os níveis de ensino.

Assim, o E-Ciber, no Decreto Nº10222/2020, recomenda que seja dada ênfase em segurança cibernética nos currículos de cursos técnicos, nos níveis de ensino médio e de ensino superior, e nos currículos da modalidade de ensino "educação tecnológica e formação profissional". As maiores dificuldades das empresas no processo de contratação no Brasil são a ausência de habilidades técnicas (33%), seguida pela falta de experiência (23%) e pela carência de habilidades interpessoais (19%). A primeira tem a ver com as lacunas educacionais brasileiras. A segunda se relaciona com a resistência de recrutadores de dar oportunidade a novatos. E a terceira relaciona-se a competências comportamentais, que não são inatas, sendo possível desenvolvê-las. Tais dificuldades para a contratação demonstram o descompasso existente entre a situação dos profissionais existentes e as necessidades do mercado de trabalho.

Nessa direção, tal cenário, assim como a ausência de Cursos Técnicos em Segurança Cibernética no país motivaram o Inmetro a oferecer um curso de qualificação profissional nesta área do conhecimento a partir do ano de 2019. Ao implantar este curso, ambas as instituições, Inmetro e IFF, estarão novamente atuando na vanguarda da educação profissional no país.

Convém destacar, conforme anteriormente apontado, que para a implantação do curso, representantes de ambas as instituições já estão formalizando-o junto ao Governo Federal. No momento de elaboração deste plano pedagógico, estes representantes já estão contribuindo com o Ministério da Educação – MEC para inclusão do currículo deste novo curso no Catálogo Nacional de Cursos Técnicos (CNCT), atuando em um grupo de trabalho específico, liderado pelo Pró-Reitor de Ensino, do Instituto Federal Fluminense, por ocasião da elaboração deste plano pedagógico, Prof. Carlos Artur de Carvalho Arêas.

2.5. OBJETIVOS DO CURSO

2.5.1 – GERAL

O Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio, do Instituto Nacional de Metrologia, Qualidade e Tecnologia - Inmetro, com a parceria do Instituto Federal Fluminense - IFF, tem como objetivo geral formar profissionais em Informática, com capacidade de investigação e resolução de problemas, aplicando conhecimentos específicos de Segurança Cibernética, bem como utilizando soluções inovadoras.

Ademais, deseja-se que o aluno seja formado para integrar equipes com o perfil dos profissionais atuais da área de Tecnologia da Informação, caracterizado pela crescente busca por conhecimento e novas tecnologias e pela intensa conectividade. Ainda, o curso deve viabilizar a inserção desses profissionais em atividades na área de metrologia e da avaliação da conformidade em laboratórios acreditados pelo Inmetro e outras empresas de atuação análoga.

2.5.2 – ESPECÍFICOS

O curso terá como objetivos específicos:

- Qualificar profissionais para que possam contribuir nas tarefas de complexidade baixa à intermediária no Centro de Operação de Segurança (Security Operations Center – SOC) de empresas nacionais e internacionais;
- Preparar o profissional para instalação e configuração de equipamentos e serviços com a perspectiva da segurança cibernética sempre presente;
- Estimular o profissional a entender a ética envolvida quando é necessário desempenhar uma atividade típica de um consultor de segurança (white hat hacker);
- Conscientizar o aluno sobre a necessidade de buscar continuamente o conhecimento, aplicá-lo com criatividade em novas situações e produzir novos conhecimentos e tecnologias a partir do domínio de modelos, técnicas e informações;
- Incentivar o comprometimento e o trabalho em equipe, exercitando a ética, a capacidade de iniciativa e a solidariedade;
- Incentivar a produção e inovação científico-tecnológica;
- Cultivar o pensamento reflexivo, a autonomia intelectual, a capacidade empreendedora e a compreensão do processo tecnológico.

3. ORGANIZAÇÃO DIDÁTICO-PEDAGÓGICA

3.1. PERFIL DO CURSO

O Curso de Técnico em Segurança Cibernética forma um egresso consciente de seu papel transformador junto à sociedade, tendo como base uma formação ampla na área de Segurança da Informação. Ao mesmo tempo, o curso está formatado para prover uma formação científica, humanista, crítica, reflexiva e cidadã, de modo que o aluno possa absorver e desenvolver tecnologias de forma crítica, criativa e ética. Para tanto, o curso dota esse egresso com habilidades e competências adquiridas a partir de uma formação que integra conhecimentos e saberes do Ensino Médio e da sua área de atuação profissional, de modo que ele possa se inserir no mundo do trabalho de maneira compromissada com o desenvolvimento local, regional e nacional, integrando os saberes de segurança cibernética às novas tecnologias relacionadas à indústria 4.0, à liderança de equipes e à solução de problemas.

3.2. PERFIL PROFISSIONAL DO EGRESSO

O Curso Técnico em Segurança Cibernética está estruturado para garantir formação tecnológica e empreendedora, ofertando um conhecimento amplo em Informática e áreas afins, concedendo subsídios para reconhecer, definir e aplicar a melhor solução para o desenvolvimento de sistemas de medição, além de possibilitar a absorção de novas tecnologias, de acordo com a dinâmica profissional e empresarial.

Esse curso possibilita que o aluno adquira competências para solucionar problemas de vulnerabilidade no acesso a informações. O egresso do curso é capaz de:

- Desenvolver atividade como operador no sistema de incidentes do Centro de Operações de Segurança Cibernética (SOC) da organização onde trabalha;
- Levantar informações de vulnerabilidades existentes em aplicações Web;
- Administrar sistemas operacionais que ficam em um datacenter ou na nuvem;
- Extrair dados para análise de brechas de segurança em sistemas computacionais;
- Identificar alternativas quanto à métodos que garantam integridade, confidencialidade e autenticação de sistemas de informação seguros;
- Prover suporte para escolha de políticas de controle de acesso: senhas, certificados, etc.;
- Utilizar ferramentas para implementar serviços com confidencialidade, integridade e disponibilidade (IPSEC, openSSL, openVPN, entre outras).

3.2.1. QUAIS SÃO AS ÁREAS DE ATUAÇÃO DESTE PROFISSIONAL?

Como mencionado anteriormente, o técnico em Segurança Cibernética atende demanda em todo o espectro de empresas no mercado nacional. Em empresas de pequeno e médio porte, normalmente existem recursos mais reduzidos para a contratação de pessoal. Ali, sua experiência com sistemas seguros permite que auxilie o departamento de tecnologia da informação com a implantação de serviços, em cargos que podem ser de operador até analista júnior.

Em empresas de grande porte, o técnico traz uma formação profissional que permite iniciar uma carreira em um enquadramento funcional mais simples, como operador de SOC. É importante ressaltar que empresas maiores estão em geral melhor estruturadas e possuem diferentes times para atuação em diferentes áreas de segurança cibernética, como:

- Resposta a Incidentes;
- Varredura de Ameaças (*Threat Hunting*);
- Testes de Invasão;
- Analista Forense;

Com oportunidades de treinamento na empresa contratante, o profissional que aprecia a área em que atua poderá ser gradualmente promovido para analista júnior em alguma das áreas acima. Com alguns anos de capacitação e aprendizado profissional adicionais, poderá tornar-se um analista sênior ou um consultor na área de segurança cibernética.

4. ORGANIZAÇÃO CURRICULAR

A organização curricular compõe-se basicamente de disciplinas de diferentes áreas de Ciência de Computação (como programação, redes de computadores e sistemas operacionais) voltadas à formação técnico-profissional diferenciada do estudante, e estruturadas de modo a oferecer um encadeamento lógico na sequência do aprendizado e formação do perfil de atuação no mercado de trabalho do egresso.

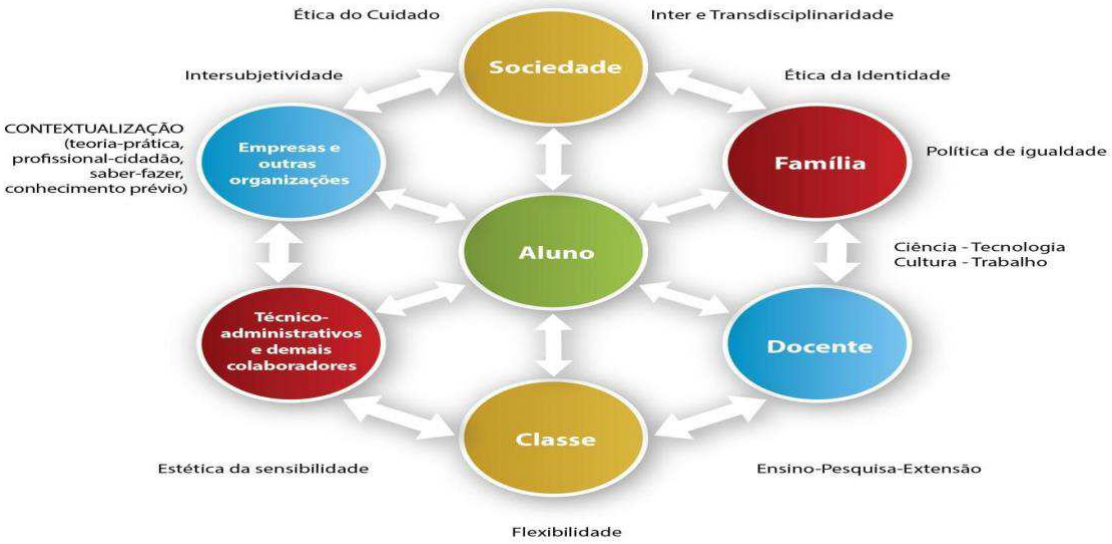
Desta forma, pretendemos apresentar um curso que rompe com a tradicional dicotomia e segmentação dos saberes, e ofertar uma aprendizagem que destaca a inter-relação entre os saberes de diferentes áreas e busca a compreensão global do conhecimento, oportunizando uma formação profissional de qualidade, articulada com as demandas educacionais da sociedade vigente e com os constantes avanços da Ciência e da tecnologia, permitindo, assim, a inserção dos indivíduos no mundo do trabalho que exige cada vez mais um conhecimento plural dos formandos.

São metas do Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio, promover uma metodologia problematizadora, investigativa e multidisciplinar, que desperte aptidões e vocações dos discentes e incentive o desenvolvimento de habilidades e competências tais como criatividade, empreendedorismo, autonomia, conduta ética, responsabilidade ambiental e social, além da capacidade de trabalho em equipe e respeito à diversidade e individualidade de cada ser. Com isso, busca-se não somente o cumprimento dos programas, mas o envolvimento dos estudantes, sua participação ativa no processo de construção do conhecimento, oportunizando o desenvolvimento de novas competências e habilidades aliando teoria e prática, por meio de técnicas/práticas variadas articuladas entre si e ao conteúdo/conhecimento selecionado e utilizado pelo docente.

Trabalhar a interdisciplinaridade, nessa linha de pensamento, permite a criatividade, a autonomia do educador e as especificidades conceituais inerentes aos diversos componentes curriculares, reconstruindo-os sob a perspectiva da discussão coletiva e do trabalho interativo entre diferentes atores sociais – para além do docente e do estudante, a família, sua classe, a escola, a sociedade – onde cada um aporta conhecimentos, habilidades e valores permitindo a compreensão do objeto de estudo em suas múltiplas relações.

Os princípios da concepção pedagógica que permeiam o curso são apresentados na Figura 4.

Figura 4: Princípios da Concepção Pedagógica do Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio.



Audiodescrição: Imagem vertical colorida de Fluxo de relação central dos Princípios da Concepção Pedagógica do Curso. Ao centro em um círculo verde: Aluno. A sua volta, setas duplas direcionam para seis círculos: dois amarelos, dois vermelhos e dois azuis, cada um com textos em letras brancas. Entre os círculos, setas duplas. No círculo amarelo, acima do círculo verde: Sociedade. No sentido horário, seta dupla. Do lado externo direito, próximo a ponta esquerda: Inter e Transdisciplinaridade; na ponta direita: Ética da Identidade. Círculo vermelho: Família. Do lado externo direito: Política de Igualdade. Seta dupla, Do lado externo direito: Ciência – Tecnologia; Cultura – Trabalho. Círculo Azul: Docente. Seta dupla. Do lado externo direito: Ensino-pesquisa-Extensão. Círculo amarelo: Classe. Do lado externo inferior: Flexibilidade. Seta dupla. Do lado externo esquerdo: Estética da sensibilidade. Círculo vermelho: Técnico-administrativos e demais colaboradores. Seta dupla. Círculo Azul: Empresas e outras organizações. Do lado externo esquerdo CONTETUALIZAÇÃO (teoria-prática. profissional-cidadão, saber-fazer, conhecimento prévio). Seta dupla. Do lado externo esquerdo: Intersubjetividade. Círculo amarelo reinicia o ciclo. Fim da audiodescrição[4].

Disponível em: https://portal1.iff.edu.br/nossos-campi/itaperuna/cursos/cursos-tecnicos/projetos-pedagogicos-dos-cursos-tecnicos/ppc-do-curso-tecnico-em-quimica/projeto-pedagogico-do-curso-tecnico-concomitante-em-quimica-turmas-ingressantes-a-partir-de-2020/view Acesso: 28 abr. 2022.

Nessa perspectiva, o estudante, bem como o professor, revela o seu repertório de conhecimentos prévios, a partir de suas experiências de vida e de seu conhecimento de mundo, trazendo consigo crenças e modelos mentais acerca daquilo que ele considera a sua realidade, quando diante das atividades escolares. Se tais atividades são construídas na trama das atividades sociais e coletivas, transgredindo o aspecto individual, isto justifica a importância que tem a influência decisiva da família, dos amigos, da classe e de todos os sujeitos do ambiente escolar – dos técnicos-administrativos e demais colaboradores aos docentes, os quais interagem na transformação da escola enquanto um espaço de multiplicidades, onde diferentes valores,

[4] Audiodescrição produzida pela audiodescritora Loide Aragão e pelo consultor Renato Ferreira da Costa.

experiências, concepções, culturas, crenças e relações sociais se misturam e fazem do cotidiano escolar uma rica e complexa estrutura de conhecimentos e de sujeitos.

Nesse contexto de interação – estudante-estudante, estudante-família, estudante-docente, estudante-empresas, estudante-servidores, etc. – as representações coletivas do educando expressam sua forma de pensamento elaborado, resultante de suas relações com os objetos que afetam. Portanto, é necessário destacar que, na medida em que os estudantes interagem, ocorre reflexão de significados sendo estes compartilhados. Frente a isso, pensamos a sala de aula como um ambiente de aprendizagem social e sociável, possível de configurar uma cultura escolar interacionista, onde todos os sujeitos envolvidos formam e transformam seu conhecimento, ampliando suas redes de significados acerca de suas realidades, e produzindo uma estrutura organizada para construção de novos conhecimentos.

Na verdade, a própria seleção e organização dos componentes e conteúdos curriculares são também produtos da atividade e do conhecimento humano registrados socialmente, o que se torna ainda mais visível quando se trata do ensino profissionalizante, o qual, no âmbito das relações entre escola, empresa e sociedade, destaca a necessidade de uma educação também pautada no atendimento das necessidades da sociedade, no que se refere à exigência de organizar o currículo com base nas demandas socioeconômicas, científicas e tecnológicas da região em que cada curso encontra-se inserido.

No que diz respeito, por fim, à relação do estudante consigo mesmo, visamos estimular a autonomia e a construção de uma consciência crítica, política e reflexiva, podendo pensar e construir uma sociedade plural com vistas à melhoria da qualidade de vida das pessoas e do sistema. Busca-se, desta forma, através das múltiplas relações estabelecidas entre os sujeitos atuantes nas atividades escolares, (i) otimizar o processo de ensino-aprendizagem, e (ii) sistematizar os fundamentos, as condições e as metodologias na realização do ensino e do saber, associando-os à extensão e à pesquisa, e convertendo os objetivos sociopolíticos e pedagógicos em objetivos de ensino, ou seja, selecionando conteúdos e métodos em função desses objetivos.

Todas essas relações, em verdade, são interdependentes e se interpenetram, e só fazem sentido na medida em que dialogam e agem, simultaneamente, umas sobre as outras, encontrando-se permeadas pelas diretrizes que norteiam as práticas acadêmico-pedagógicas institucionais, presentes no Plano de Desenvolvimento Institucional (PDI) vigente.

4.1. METODOLOGIA

As práticas pedagógicas a serem adotadas no Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio tem clara orientação para integração entre teoria e prática nos ambientes de aprendizagem e partem da compreensão do discente como um agente ativo em seu processo de aprendizagem, de forma a assumir o protagonismo na busca do saber com ajuda de sua própria capacidade de avaliação e senso crítico.

Nesse cenário, busca-se não somente o cumprimento da matriz curricular e seus programas, mas o envolvimento dos discentes, sua participação ativa no processo de construção do conhecimento, oportunizando, assim, o desenvolvimento de competências e habilidades para a vida profissional e pessoal.

Em consonância a tal perspectiva, cabe ao corpo docente oferecer propostas ativas, que aliem a problematização e as atividades de prática profissional aos conteúdos teóricos ministrados em cada componente curricular, favorecendo o discente a “aprender a aprender”.

Em acréscimo, as práticas pedagógicas devem ser igualmente pautadas nos princípios pedagógicos presentes no Projeto Político-Pedagógico Institucional do IFF, a saber:

(1) A indissociabilidade Ensino, Pesquisa e Extensão
(2) A Pesquisa como Princípio Pedagógico
(3) O Trabalho como Princípio Educativo
(4) O Respeito à Diversidade
(5) Interdisciplinaridade

As práticas pedagógicas orientam-se para atividades que conduzem o estudante para o perfil profissional esperado, a possibilidade de integração das atividades dos componentes curriculares e orientadas à formação do cidadão atuante e protagonista. Dentre essas práticas, destacam-se:

a) Aulas participativas: visam à introdução a um novo conteúdo e sua respectiva ampliação e contextualização por meio de construção interativa entre todos os participantes.

b) Projetos e/ou resolução de problemas: aos discentes, de acordo com a natureza das componentes curriculares e viabilidade de execução, são apresentadas atividades envolvendo papéis e cenários realistas, a fim de trabalhar a identificação de problemas, formulação de explicações, elaboração de questionamentos, busca de novas informações, construção de soluções e avaliação.

c) Debates: são realizados com objetivo de avaliar o grau de aquisição das competências e habilidades desenvolvidas pelos discentes;

d) Sala de Aula Invertida: São disponibilizados previamente materiais de estudo para serem trabalhados pelos alunos de maneira assíncrona em tempo fora do horário escolar. Essa atividade pode utilizar recursos digitais (vídeos, áudios, *podcasts*, games, textos, entre outros) ou físicos (textos impressos, leitura do livro-texto ou de um artigo científico, entre outros) e é conhecida como “sala de aula invertida”, pois há uma inversão da lógica do modelo tradicional de ensino. Dessa maneira, os discentes ganham autonomia em seu processo de aprendizagem, já que estudam os conceitos antes da aula e, em seguida, em encontros presenciais (ou síncronos), debatem, ampliam e contextualizam o conhecimento adquirido.

e) Exercícios: os discentes são estimulados a realizar exercícios com o objetivo de fixar as bases tecnológicas e científicas, tanto em sala de aula como fora dela, em todo o percurso formativo, bem como no uso de laboratórios, no sentido de incrementar a inter-relação teoria-prática;

f) Seminários: para melhor adequação e contextualização dos conteúdos propostos, são realizados seminários e palestra sobre assuntos pertinentes ao perfil profissional e ao conjunto de bases tecnológicas do período, com compartilhamento de conhecimento científico de outros profissionais do meio, permitindo que os discentes possam acompanhar os avanços tecnológicos específicos na área e ampliem sua rede de contato profissional;

g) Participação em projetos institucionais: os alunos são estimulados a participar de projetos de pesquisa, monitoria, apoio tecnológico e extensão, colocando em prática seus conhecimentos e adquirindo novas habilidades e competências;

h) Avaliações diversificadas: consistem na avaliação do processo de ensino-aprendizagem constituída de instrumentos com as seguintes funções: diagnóstica, formativa e somativa.

- A avaliação diagnóstica é aquela que ao iniciar um período letivo, dado a diversidade de saberes, o docente deve verificar o conhecimento prévio dos alunos com a finalidade de constatar os pré-requisitos necessários de conhecimentos ou habilidades imprescindíveis que os discentes possuem para o preparo de novas aprendizagens.
- A avaliação formativa é aquela realizada durante todo o decorrer do período letivo, com o intuito de verificar se os alunos estão atingindo os objetivos previstos. Nesse sentido, a avaliação formativa visa, basicamente, avaliar se o discente domina gradativamente e hierarquicamente cada etapa da aprendizagem, antes de prosseguir para uma outra etapa subsequente de ensino-aprendizagem.
- Por fim, a avaliação somativa tem por função básica a classificação dos alunos, sendo realizada em etapas bem definidas no decorrer das componentes curriculares, classificando os alunos de acordo com os níveis de aproveitamento previamente estabelecidos.

A autoavaliação também é uma importante ferramenta que pode ser empregada ao longo do curso e permite a reflexão do discente sobre o próprio desempenho. Quando bem conduzida, a autoavaliação se torna um meio eficiente de autorregulação, na qual o aluno aprende a identificar e corrigir seus erros.

i) Participação em atividades acadêmicas curriculares ou de extensão: os alunos são estimulados a participar de feiras, cursos, palestras, seminários, visitas técnicas, mantendo o discente em sintonia com o contexto da área e acompanhando a modernização do setor, de modo a ampliar os conhecimentos adquiridos.

Dentre as atividades de extensão, vale destacar a Jornada de Iniciação Científica e Tecnológica do Inmetro integrada à Jornada de Pós-graduação e a Semana Nacional de Ciência e Tecnologia. Tais eventos integram as produções dos alunos dos cursos técnicos, alunos de

iniciação científica e alunos da pós-graduação do Inmetro, no qual os discentes serão incentivados a participar e apresentar seus trabalhos acadêmicos e pesquisas, em um ambiente profícuo de troca de conhecimento. Na Semana Nacional de Ciência e Tecnologia, além da troca entre pares, ou seja, entre os atores envolvidos na produção do conhecimento científico, há a possibilidade da mobilização da comunidade do entorno para atingir o maior objetivo deste importante evento que é o de oportunizar que o público leigo conheça e discuta os projetos, resultados, relevância e impactos da pesquisa científico-tecnológica, principalmente daquelas realizadas no Brasil, e suas aplicações.

Salienta-se que as atividades de Pesquisa, Ensino e Extensão encontram-se indissociáveis e estão diretamente relacionadas com os conteúdos trabalhados durante o curso, preferencialmente de maneira interdisciplinar. Dessa forma, é possível notar a presença da tríade Ensino, Pesquisa e Extensão na estrutura do Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio, refletindo a interligação e indissociabilidade entre esses elementos

4.2. MATRIZ CURRICULAR DO CURSO

Campus: Cabo Frio					
EIXO TECNOLÓGICO: INFORMAÇÃO E COMUNICAÇÃO CURSO TÉCNICO EM SEGURANÇA CIBERNÉTICA CONCOMITANTE AO ENSINO MÉDIO					
Ano de Implantação: 2022					
Semestre	**Componentes Curriculares**	**Carga Horária (hora-aula = 45 minutos)**			
		Nº de Aulas Semanais	**CH Presencial**	**CH em EaD**	**Total de CH**
1º	Matemática para Informática	2	6	24	30
	Introdução à Programação de Computadores	4	12	48	60
	Fundamentos de Segurança Cibernética	6	18	72	90
	Fundamentos de Informática	4	12	48	60
	Fundamentos de Metrologia	2	15	15	30
	Língua Inglesa Aplicada à Tecnologia	2	6	24	30
	Subtotais	**20**	**60**	**240**	**300**
2º	Matemática para Criptologia	2	6	24	30
	Fundamentos de Redes de Computadores	4	12	48	60
	Banco de Dados	4	12	48	60
	Programação de Sistemas Embarcados	2	6	24	30
	Políticas de Segurança	2	6	24	30
	Algoritmos e Estrutura de Dados	2	6	24	30
	Sistemas Operacionais para Redes de Computadores	4	12	48	60
	Subtotais	**20**	**60**	**240**	**300**
3º	Fundamentos de Criptologia	2	6	24	30
	Programação de Aplicações Web	4	12	48	60
	Sistemas Embarcados e Aplicações Móveis	4	12	48	60
	Monitoramento de Redes de Computadores	2	6	24	30
	Segurança Defensiva	4	12	48	60
	Operações em Segurança Cibernética	4	12	48	60
	Subtotais	**20**	**60**	**240**	**300**
4º	Criptologia Aplicada	2	6	24	30
	Gestão e Planejamento Profissional	4	12	48	60
	Serviços de Redes de Computadores em Nuvem	4	12	48	60
	Segurança Ofensiva: Aplicações Web	4	12	48	60
	Empreendedorismo	2	6	24	30
	Inteligência Artificial Aplicada à Segurança Cibernética	4	12	48	60
	Subtotais	**20**	**60**	**240**	**300**
	Total				**1200**

4.3. REPRESENTAÇÃO GRÁFICA DO PERFIL DE FORMAÇÃO

4.4. COMPONENTES CURRICULARES

Os conteúdos abordados em cada uma das disciplinas pertencentes às etapas do curso estão descritos nos tópicos abaixo, separados por semestres. Os componentes curriculares foram planejados de forma a se complementarem e o aprendizado de cada um deles é interligado aos componentes seguintes, revisando, aprofundando e reforçando o aprendizado dos discentes, destacando a inter-relação entre os saberes das diversas áreas e sua importância para atuação profissional na sociedade atual.

Cabe ressaltar, ainda, que há componente curriculares obrigatórios e optativos, e temáticas ou transversalidades sugeridas pelas Resoluções CNE/CP Nº 1/2004 (Diretrizes Curriculares Nacionais para Educação das Relações Étnico- Raciais), CNE/CP N° 1/2012 (Diretrizes Nacionais para a Educação em Direitos Humanos) e Decreto Nº 4.281/2002 (Politicas de Educação Ambiental), que serão tratadas transversalmente nos componentes curriculares obrigatórios e nos eventos desenvolvidos no *Campus* do Inmetro, como a Semana do Meio Ambiente. Os itens relacionados às relações étnicos raciais e direitos humanos estão, ainda, previstos na grade curricular da disciplina “Gestão e Planejamento Profissional”.

4.4.1 – PRIMEIRO SEMESTRE

Matemática para Informática

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		Informação e Comunicação
Componente Curricular		**Ano de Implantação**
Matemática para Informática		2022
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30h	2 aulas semanais	Primeiro semestre

Ementa:

Sistema Numérico Decimal; Números Naturais; Números Inteiros; Números Racionais; Números Decimais; Números Irracionais; Números Reais; Conversão de unidades; Razão, proporção e regra de três; Porcentagem

Objetivos

Oferecer formação integrada articulando a teoria à prática, proporcionando aos estudantes conhecimentos técnicos e humanísticos, tornando-os capazes de contribuir para o desenvolvimento regional. Formar profissionais conscientes das responsabilidades com relação à ética profissional e ao meio ambiente, capazes de desenvolver trabalhos de iniciação científica, bem como proporcionar a inserção qualificada no âmbito profissional, desenvolver conhecimentos necessários para a organização da área tecnológica dos diversos setores produtivos da região, integrando o ensino ao trabalho, oportunizando o desenvolvimento das condições para a vida produtiva contemporânea.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Sistema Numérico Decimal
   - **a.** Ordens e classes
   - **b.** Numerais cardinais
2. Números Naturais
   - **a.** Operações básicas e suas propriedades
   - **b.** Noves-fora
   - **c.** Decomposição em somas e em produtos
   - **d.** Múltiplos e divisores
   - **e.** Números primos
   - **f.** MMC e MDC
   - **g.** Algoritmo de Euclides
   - **h.** Números primos entre si
   - **i.** Fatoração
   - **j.** Teste de primalidade
3. Números Inteiros
   - **a.** Inverso aditivo
   - **b.** Classificação
4. Números Racionais
   - **a.** Inverso multiplicativo
   - **b.** Tipos de frações
   - **c.** Frações irredutíveis
   - **d.** Operações com frações
5. Números Decimais
   - **a.** Operações com números decimais
   - **b.** Operações com potências de 10
   - **c.** Representação por frações
6. Números Irracionais
   - **a.** A irracionalidade de raiz de 2
   - **b.** Racionalização
7. Números Reais
   - **a.** A reta dos reais
   - **b.** Classificação e notação
8. Conversão de unidades
   - **a.** Prefixos decimais

9. Razão, proporção e regra de três
   a. Conceito
   b. Aplicações
10. Porcentagem
   a. Conceito
   b. Aplicações

Habilidades

1. Despertar a valorização da pesquisa;
2. Proporcionar condições para uma atitude crítica e objetiva diante de fatos e problemas científicos que exijam soluções e decisões;
3. Oferecer ao estudante, situações que tornem natural a interpretação dos fenômenos estudados;
4. Desenvolver no aluno o pensamento científico contribuindo para o seu desenvolvimento profissional;
5. Permitir que o aluno, compreenda a matemática como parcela do crescimento humano, essencial na formação e construção de uma visão de mundo necessária para desenvolver capacidades que serão exigidas ao longo da vida social e profissional;
6. Desenvolver habilidades de pensamento e raciocínio lógico através da diversidade de situações, relacionadas às demais áreas do conhecimento;
7. Identificar, ampliar e construir novos significados dos conjuntos numéricos e operações;
8. Operar no cotidiano porcentagem, grandezas e regra de três;

Atitudes

- Autoconfiante para entender assuntos mais complexos.
- Perseverante na busca da solução de problemas
- Investigativo na busca de ferramentas proporcionadas pela matemática para resolução de problemas cotidianos
- Discernimento na aplicação dos conceitos matemáticos para os problemas onde se aplicam
- Curioso e persistente para validação das respostas corretas
- Comunicativo para interação com colegas e professores para busca da solução de problemas mais complexos

Referências:

Bibliografia Básica:

MENDES, I. F. e KERSNOWSKY, I. **Aritmética Elementar**, Editora XYZ, 1ª edição, 2018.
LACERDA, J. C. A. **Praticando a Aritmética**, Editora XYZ, 1ª edição, 2018.
SANTOS, A. L. **Problemas Selecionados De Matemática**, Ciência Moderna, 1ª edição, 2006.

Bibliografia Complementar:

ZEGARELLI, M. **Matemática básica e pré-álgebra para leigos**, Alta Books; 2ª edição, 2019.
VASCONCELOS, L. **Matemática para Vencer**, Editora Ciência Moderna, 1ª edição, 2018.
VASCONCELOS, L. **O Algebrista**, Editora Ciência Moderna, 1ª edição 2019.
HALMOS, P. R., **Teoria Ingênua dos Conjuntos**, Ciência Moderna, 1ª edição, 2001.
RIBENBOIM, P. **Números Primos: Mistérios e Recordes**, Coleção Matemática Universitária, 1ª edição, 2001.

Introdução à Programação de Computadores

Campus: **Cabo Frio**		
Cursos		**Eixo Tecnológico**
Curso Técnico em Segurança Cibernética		Informação e Comunicação
Componente Curricular		**Ano de Implantação**
Introdução à Programação de Computadores		2022
Carga Horária	**Aulas por Semana**	**Período Letivo**
60h	4 aulas semanais	Primeiro semestre

Ementa

Algoritmos e linguagens de programação; Métodos de representação de algoritmos; Tipos, variáveis e constantes; Operações de entrada e saída; Expressões aritméticas e lógicas; Estruturas de desvio de fluxo; Estruturas de repetição; Modularização.

Objetivos

- Geral:
  - Desenvolver soluções para problemas simples através de algoritmos computacionais, utilizando uma linguagem de programação de alto nível.
- Específicas:
  - Representar algoritmos computacionais de forma descritiva e gráfica
  - Desenvolver algoritmos computacionais capazes de interagir com um usuário
  - Desenvolver algoritmos computacionais utilizando estruturas de controle para manipulação dos dados
  - Modularizar algoritmos computacionais utilizando funções para separar responsabilidades

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Algoritmos e linguagens de programação
   1. Tipos de linguagens de programação
   2. Compilador e interpretador
   3. Paradigmas de programação
2. Métodos de representação de algoritmos
   1. Descrição narrativa
   2. Fluxograma
   3. Pseudocódigo
3. Tipos, variáveis e constantes
   1. Tipos primitivos
   2. Declaração de variáveis e constantes
   3. Operador de atribuição
4. Operações de Entrada e Saída
   1. Comandos de saída de dados
   2. Comandos de entrada de dados
   3. Conversão de tipos
5. Expressões aritméticas e lógicas
   1. Operadores aritméticos
   2. Operadores relacionais
   3. Operadores lógicos e tabela-verdade
   4. Regras de precedência
6. Estruturas de desvio de fluxo
   1. Estrutura condicional simples
   2. Estrutura condicional composta
   3. Estrutura condicional aninhada
   4. Estrutura de seleção
7. Estruturas de repetição
   1. Estrutura de repetição controlada por condição
   2. Estrutura de repetição controlada por contador
   3. Contadores e acumuladores
8. Modularização
   1. Declaração de funções
   2. Parâmetros e argumentos

3. Retorno de uma função
Habilidades
● Descrever algoritmos em suas diferentes formas de representação ● Utilizar métodos de entrada e saída de dados para interação com o usuário ● Aplicar estruturas de controle, de forma adequada, em algoritmos computacionais ● Organizar e dividir algoritmos computacionais em módulos menores que possuam responsabilidades específicas
Atitudes
● Desenvolvimento do raciocínio lógico e criativo para resolução de problemas ● Autonomia para analisar problemas reais e desenvolver soluções computacionais ● Motivação e autonomia em aprofundar os conhecimentos em conceitos avançados de programação
Referências
Bibliografia Básica
PAES, R. B. **Introdução à Programação usando a Linguagem C**. Editora Novatec, 2017. BACKES, A. **Linguagem C: Completa e Descomplicada**, 2ª Edição. Editora GEN LTC, 2018. MANZANO, J.A. e OLIVEIRA, J.F. **Algoritmos: Lógica Para Desenvolvimento de Programação de Computadores**, 29ª Edição. Editora Érica, 2019.
Bibliografia Complementar
ASCENCIO, A. F. G.; DE CAMPOS, E. A. V. **Fundamentos da programação de computadores**: Algoritmos, Pascal, C/C++ (padrão ANSI) e Java. 3. ed. São Paulo: Pearson, 2012. MANZANO, J. A. N. G.; DE OLIVEIRA, J. F. **Algoritmos**: Lógica para Desenvolvimento de Programação de Computadores. 29. ed. São Paulo: Érica, 2019. FORBELLONE, A. L. V.; EBERSPÄCHER, H. F. **Lógica de Programação**: A Construção de Algoritmos e Estruturas de Dados. 3. ed. São Paulo: Pearson, 2005. SZWARCFITER, J. e MARKENZON, L. **Estrutura de Dados e seus Algoritmos**, 3ª Edição. Editora LTC, 2010. PEREIRA, S.L. **Estruturas de Dados em C: Uma Abordagem Didática**. Editora Érica, 2015.

Fundamentos de Segurança Cibernética

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Fundamentos de Segurança Cibernética		**2022**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
90h	6 aulas semanais	Primeiro semestre

Ementa:

O mundo da Segurança Cibernética; O cubo da Segurança Cibernética; Ameaças, vulnerabilidades e ataques à Segurança Cibernética; A arte da proteção de segredos; A arte de garantir a integridade; O conceito dos cinco noves; Proteção de um domínio de Segurança Cibernética; Como se tornar um especialista em Segurança Cibernética.

Objetivos

Geral:

- Desenvolver uma compreensão básica da segurança cibernética e como ela se relaciona com a segurança da informação e da rede.

Específicas:

- Entender os conceitos, o valor e a importância da informação e da segurança.
- Reconhecer os princípios de confidencialidade, integridade e disponibilidade nos estados de dados e segurança cibernética.
- Aplicar conhecimentos básicos de Segurança Cibernética.
- Identificar ameaças, ataques e vulnerabilidades.
- Estabelecer uma relação entre ameaças e riscos.
- Aplicar medidas físicas, técnicas e organizacionais.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. O mundo da Segurança Cibernética
    a. Domínios de Segurança Cibernética
    b. Criminosos da Segurança Cibernética versus especialistas da Segurança Cibernética
    c. Ameaças comuns
    d. Propagação de ameaças de Segurança Cibernética
    e. Criação de mais especialistas

2. O cubo da Segurança Cibernética
    a. As três dimensões do cubo de Segurança Cibernética
        i. Princípios de Segurança
        ii. Estados dos dados
        iii. Proteções da Segurança Cibernética
    b. Tríade CID
        i. Confidencialidade
        ii. Integridade
        iii. Disponibilidade
    c. Estados dos dados
        i. Dados em repouso
        ii. Dados em trânsito
        iii. Dados em processamento
    d. Contramedidas de Segurança Cibernética
        i. Tecnologias
        ii. Reconhecimento, educação e treinamento

iii. Políticas e procedimentos de segurança
e. Estrutura de gerenciamento de Segurança de TI
i. O modelo de Segurança Cibernética ISO
ii. Uso do modelo de Segurança Cibernética ISO

3. Ameaças, vulnerabilidades e ataques à Segurança Cibernética
   a. Malware e código malicioso
   b. Disfarce
   c. Ataques

4. A arte da proteção de segredos
   a. Criptografia
   b. Controle de Acesso
   c. Ofuscação de dados

5. A arte de garantir a integridade
   a. Tipos de controle de integridade de dados
   b. Assinaturas digitais
   c. Certificados digitais
   d. Integridade do banco de dados

6. O conceito dos cinco noves
   a. Alta disponibilidade
   b. Medidas para melhorar a disponibilidade
   c. Resposta a incidentes
   d. Recuperação de desastres

7. Proteção de um domínio de Segurança Cibernética
   a. Defesa de sistemas e dispositivos
   b. Codificação do servidor
   c. Codificação da rede
   d. Segurança física

8. Como se tornar um especialista em Segurança Cibernética
   a. Domínios de Segurança Cibernética
   b. Noções básicas sobre a ética do trabalho na Segurança Cibernética

Habilidades

- Identificar requisitos de qualidade necessários para garantir a segurança da informação em uma organização;
- Entender por que a análise de uma violação de dados fornece lições valiosas para melhorar as medidas de segurança e evitar violações futuras;
- Identificar os riscos associados aos requisitos de qualidade;
- Identificar e aplicar contramedidas necessárias para mitigar os riscos;
- Entender por que é fundamental desenvolver políticas, procedimentos e diretrizes para proteção contra riscos de segurança cibernética;
- Identificar e aplicar medidas para a garantia da continuidade do negócio em caso de um desastre;
- Identificar e relatar incidentes de segurança na organização.

Atitudes

- Autonomia e segurança para identificar, classificar e aplicar medidas de segurança da informação;
- Atitude crítica quanto à aplicação de diferentes medidas em problemas de segurança cibernética.

Referências:

Bibliografia Básica:

BAARS, H., HINTZBERGEN, K., HINTZBERGEN, J. e SMULDERS, A. **Fundamentos de Segurança da Informação com base na ISO 27001 e na ISO 27002**, Brasport, 2018.

KIM, D. SOLOMON, M. **Fundamentos de Segurança de Sistemas de Informação**, Editora GEN/LTC, 2014. MACHADO, F. **Segurança da informação: Princípios e controle de ameaças**, Editora Érica, 2014.
Bibliografia Complementar:
FILHO, Sócrates Teixeira. Segurança da Informação Descomplicada, Brasília, 2015. FERREIRA, Fernando; ARAÚJO, Márcio. Política de Segurança da Informação - Guia prático para elaboração e implementação, Editora Ciência Moderna, 2a edição, 2020, ABNT NBR ISO/IEC 27001:2013 – **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.** ABNT NBR ISO/IEC 27002:2013 – **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. ABNT NBR ISO/IEC 27005:2011 – **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.**

Fundamentos de Informática

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Fundamentos de Informática		**2022**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60h	4 aulas por semana	Primeiro semestre

Ementa:

História da Computação; Hardware; Software; Unidades de Medida; Sistemas Operacionais; Redes de Computadores

Objetivos

Geral:

Descrever, de forma eficaz e crítica, os principais conceitos acerca da informática e da computação, demonstrando compreender a organização e o funcionamento de sistemas de computação.

Específicas:

Descrever a história da computação.
Conhecer, distinguir e conceituar os componentes básicos de um computador e suas funções.
Definir e classificar os principais conceitos correlatos a sistemas operacionais.
Compreender a representação da informação, manipular os sistemas de numeração e a aritmética nestes sistemas.
Distinguir e classificar redes de computadores e seus componentes.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. História da Computação:
    a. Introdução;
    b. Origens e História da Computação.
2. Sistemas de Numeração e Representação de Dados:
    a. História dos Sistemas de Numeração;
    b. Sistemas de Numeração: Decimal; Binário; Octal; e Hexadecimal.
    c. Mudanças de Base.
3. Algoritmos:
    a. Conceito;
    b. Representação de Algoritmos.
4. Hardware:
    a. Processador;
    b. Memória Primária;
    c. Memória Secundária: Discos Magnéticos; Discos Flexíveis; Discos Ópticos.
    d. Dispositivos de Entrada/Saída: Barramentos; Terminais; Mouses; Impressoras; Equipamentos de telecomunicações;
5. Software:
    a. Software e Programa;
    b. Software Básico;
    c. Software de Aplicação;
6. Unidades de Medida:
    a. Processamento;
    b. Armazenamento;
    c. Comunicação.
7. Linguagens de Programação;
8. Sistemas Operacionais;
9. Redes de Computadores

a. Conceito;
b. Meios de Comunicação: Cabo Metálico; Sem Fio; Óptico.

10. Equipamentos de Rede;

Habilidades

1. Identificar e classificar, conforme a função, os componentes de um sistema computacional;
2. Identificar e categorizar, de acordo com a função, os componentes de hardware de um sistema computacional;
3. Categorizar, conforme a função, softwares presentes em um sistema computacional;
4. Ler e interpretar medidas de componentes de sistemas computacionais;
5. Definir e descrever recursos de hardware e software, conforme o uso pretendido de um sistema computacional.
6. Identificar e categorizar, de acordo com a função, redes de computadores e seus equipamentos.

Atitudes

- Autonomia e segurança para identificar, classificar e descrever componentes de um sistema computacional;
- Atitude crítica quanto ao uso de componentes na composição, configuração e segurança de um sistema computacional.

Referências:

Bibliografia Básica:

DELGADO, J., RIBEIRO, C. **Arquitetura de Computadores**. 5ª Edição. Rio de Janeiro, 2017.
TANENBAUM, A. S. **Organização Estruturada de Computadores**. 6ª Edição. Pearson, 2013.
STALLINGS, W. **Arquitetura e Organização de Computadores**. 10ª Edição. São Paulo: Pearson, 2017.

Bibliografia Complementar:

CARTER, N. **Arquitetura de Computadores**. Porto Alegre: Bookman, 2003.
MONTEIRO, M. A. **Introdução à Organização de Computadores**. 5ª Edição. Rio de Janeiro: LTC, 2007.
HENNESSY, J. **Organização e Projeto de Computadores**. 5ª Edição. São Paulo: Elsevier, 2017.
HENESSY, J. L., PATTERSON, D. A. **Arquitetura de Computadores. Uma Abordagem Quantitativa**. 5ª Edição. São Paulo: Elsevier, 2013.
WEBER, R. F. **Fundamentos de Arquitetura de Computadores**. 4ª Edição. Porto Alegre: Bookman, 2012.

Fundamentos de Metrologia

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Fundamentos de Metrologia		**2022**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30h	2 aulas semanais	Primeiro semestre

Ementa:

Introdução à Metrologia. Sistema Internacional de Unidades. Conceitos técnicos em Metrologia. O Inmetro e a Metrologia. Noções de avaliação da conformidade. Noções de acreditação. Noções de Metrologia Legal.

Objetivos

Geral:

Familiaridade com conceitos técnicos em Metrologia e Avaliação da Conformidade.

Específicas:

Noções gerais a respeito do Sistema Internacional de Unidades
Identificar expressões relevantes ao seu trabalho no Vocabulário Internacional de Metrologia
Noções gerais sobre a incerteza de medições
Identificar a importância de um Sistema de Qualidade para a estrutura de uma empresa

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Introdução à Metrologia
2. Sistema Internacional de Unidades
3. Conceitos técnicos em Metrologia
4. O Inmetro e a Metrologia
5. Noções de Avaliação da Conformidade
6. Noções de Acreditação
7. Noções de Metrologia Legal

Habilidades

1. Conhecer a história da metrologia;
2. Compreender a importância da metrologia para a sociedade;
3. Identificar as principais áreas e atividades que fazem parte da metrologia;
4. Compreender a definição do SI e sua importância para as transações econômicas e científicas
5. Estudar os conceitos de grandeza e de unidade
6. Entender como são feitas as conversões entre múltiplos e submúltiplo de uma unidade de medida;
7. Reconhecer algumas regras para expressão e grafia das unidades de medidas;
8. Compreender o conceito de medição;
9. Entender os principais fatores que influenciam a medição;
10. Estudar os instrumentos de medição, a incerteza de medição e os erros de medição;
11. Reconhecer as principais atividades desempenhadas pelo Inmetro;
12. Perceber de que forma o Sinmetro e o Conmetro se relacionam com o Inmetro;
13. Reconhecer a importância das atividades do Inmetro para a sociedade brasileira;
14. Compreender o conceito de avaliação da conformidade;
15. Identificar os sujeitos e funcionalidades da atividade de avaliação da conformidade;
16. Identificar os diferentes procedimentos para o processo de avaliação da conformidade;

17. Compreender a importância das atividades de normalização e regulamentação técnica para a avaliação da conformidade;
18. Entender como a avaliação da conformidade permeia todas as principais atividades do Inmetro;
19. Entender a atuação da Rede Brasileira de Metrologia Legal e Qualidade do Inmetro (RBMLQ-I) na avaliação da conformidade;
20. Entender o conceito de acreditação;
21. Conhecer os fóruns internacionais e regionais de acreditação;
22. Sintetizar o funcionamento do sistema de acreditação brasileiro;
23. Compreender a interação entre a atividade de acreditação na infraestrutura da qualidade;
24. Conhecer o conceito de metrologia legal;
25. Identificar os instrumentos considerados alvos de medição legal no país;

Atitudes

- Desenvolvimento do raciocínio lógico com foco em princípios metrológicos
- Autonomia para analisar problemas reais e desenvolver soluções com base em normas
- Aprender a observar processos sob a perspectiva da conformidade às normas

Referências:

Bibliografia Básica:

BRASIL. Instituto Nacional de Metrologia, Qualidade e Tecnologia. **Vocabulário Internacional de Metrologia: conceitos fundamentais e gerais e termos associados (VIM)**. Inmetro. Duque de Caxias, RJ: INMETRO, 2012. 94 páginas.
ABNT NBR ISO/IEC 17000:2005 – **Avaliação da Conformidade – Vocabulário e princípios gerais**.
BRASIL. Instituto Nacional de Metrologia, Qualidade e Tecnologia. **Vocabulário Internacional de Termos de Metrologia Legal (VIML 2016)**. Portaria Inmetro nº 150, de 29 de março de 2016.

Bibliografia Complementar:

BRASIL. Lei n. 5.966, de 11 de dezembro de 1973. **Institui o Sistema Nacional de Metrologia, Normalização e Qualidade Industrial, e dá outras providências**. Diário Oficial da União, Poder Executivo, Brasília, DF, 12 dez.1973.
SILVA NETO, J.C. **Metrologia e Controle Dimensional: Conceitos, Normas e Aplicações**. Ed. GEN LTC, 2018.
ALBERTAZZI, J. e SOUSA, A. **Fundamentos de Metrologia Científica e Industrial: Revisada, Atualizada e Ampliada**. Editora Manole, 2017.
MENDES, A. e ROSÁRIO, P.P. **Metrologia e Incerteza de Medição - Conceitos e Aplicações**. Editora LTC, 2019.
LIRA, F.A. **Metrologia dimensional: Técnicas de medição e instrumentos para controle e fabricação industrial.** Editora Érica, 2014.
SILVEIRA, N. **Avaliação da Conformidade: Ferramenta Estratégica no Comercio Internacional**. Editora Aduaneiras, 2006.

Língua Inglesa Aplicada à Tecnologia

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Língua Inglesa Aplicada à Tecnologia		**2022**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30	2 aulas semanais	Primeiro semestre

Ementa:

Reconhecimento de gêneros textuais; Objetivos da leitura e níveis de compreensão; Cognatos; Conhecimento prévio; *Skimming*; *Scanning*; Marcadores discursivos; Formas verbais; Apostos; O gênero acadêmico

Objetivos

Geral:

Leitura de diferentes gêneros textuais, com foco na construção do significado e das ideias transmitidas pelo texto de língua inglesa
Construção do significado de textos na língua inglesa através da linguagem do próprio texto;
Montagem de um processo ativo de construção de sentido que relaciona as novas informações contidas no texto em língua inglesa ao conhecimento adquirido ao longo da vida;
Construção do sentido do texto através do cruzamento de diferentes níveis de conhecimento, como o linguístico, textual, estratégico além do conhecimento prévio.

Específicas:

Reconhecimento de cognatos e grupos nominais
Reconhecimento de comparativos e superlativos
Reconhecimento de afixos, referência pronominal, apostos e formas verbais
Reconhecimento de diferentes gêneros textuais: layout, marcadores discursivos e palavras-chave
Uso de técnicas de inferência textual, *skimming* e *scanning* como estratégias para construção do significado

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Reconhecimento de gêneros textuais;
    a. Formato (*layout*)
    b. Recursos tipográficos
    c. Palavras características de cada gênero
    d. Figuras
2. Objetivos da leitura e níveis de compreensão;
    a. Compreensão geral
    b. Compreensão das ideias principais
    c. Compreensão detalhada
3. Cognatos;
    a. Identificando cognatos
4. Conhecimento prévio;
    a. Relacionando a ideia central com o cotidiano
    b. Exemplos de textos e sua relação com experiências de vida
5. *Skimming* e *Scanning*
    a. Detectando o assunto em uma rápida leitura
    b. Usar a estrutura linguística e gráfica do texto
6. Marcadores discursivos;
    a. Adição
    b. Contraste
    c. Causal/consequência
    d. Sequência cronológica
    e. Exemplificação

f. Conclusão
g. Ênfase
h. Comparação

7. Formas verbais;
   a. Tempos verbais
   b. Verbos modais
8. O gênero acadêmico
   a. Introdução, desenvolvimento e conclusão
   b. Quem escreveu o artigo?
   c. Qual o público-alvo?
   d. Qual é o assunto do artigo ?
   e. Quais são as principais ideias que embasam o artigo ?

Habilidades

1. Absorver o significado e as ideias contidas em textos de gêneros diferentes no idioma estrageiro
2. Desenvolver o conhecimento linguístico para identificar cognatos, grupos nominais e demais componentes relevantes
3. Dominar técnicas de inferência textual a partir de experiências próprias de vida
4. Utilizar estratégias diversas para construir o significado do texto lido na língua estrangeira, como a inferência textual, o *skimming* e o *scanning*.

Atitudes

- Disciplina para manutenção da gradual evolução no aprendizado da leitura na língua estrangeira
- Perseverança na busca desta evolução através da leitura de diferentes gêneros textuais
- Senso crítico na definição dos gêneros textuais mais relevantes para que seus objetivos sejam atingidos

Referências:

Bibliografia Básica:

SOUZA, Adriana G.S., ABSY, Conceição, et al ., **Leitura em Língua Inglesa: uma abordagem instrumental**. 2a Edição. Disal Editora, 2010.
GALLO, L.R. **Inglês Instrumental para Informática**, Editora Ícone, 2017.
GRIGOLETO, Mariza. **Ensino de Leitura em Língua Estrangeira: o que mais pode ser feito**? Contexturas, vol.1, Apliesp, 1992.

Bibliografia Complementar:

SCHUHMACHER, C. **Inglês na Tecnologia da Informação**, Editora Disal, 2019.
KLEIMAN, Ângela. **Leitura: Ensino e Pesquisa.** Ed.Pontes, 1996.
KLEIMAN, Ângela. **Oficina de Leitura: Teoria e Prática**. Ed. Pontes, 1992.
SIERRA, Teresa. **Espanhol Instrumental**. Ed. Planeta, 2004.
VALENZUELA, Sandra. **Manual Compacto de Gramática da Língua Espanhola**. Ed. Bicho Esperto, 2010.

4.4.2 – SEGUNDO SEMESTRE

Matemática para Criptologia

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		Informação e Comunicação
Componente Curricular		**Ano de Implantação**
Matemática para Criptologia		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30h	2 aulas semanais	Segundo semestre

Ementa:

Divisão Euclidiana; Critérios de divisibilidade; Bases Numéricas; Base binária; Noções de lógica; Funções Aritméticas; Aritmética Modular

Objetivos

Oferecer formação integrada articulando a teoria à prática, proporcionando aos estudantes conhecimentos técnicos e humanísticos, tornando-os capazes de contribuir para o desenvolvimento regional. Formar profissionais conscientes das responsabilidades com relação à ética profissional e ao meio ambiente, capazes de desenvolver trabalhos de iniciação científica, bem como proporcionar a inserção qualificada no âmbito profissional, desenvolver conhecimentos necessários para a organização da área tecnológica dos diversos setores produtivos da região, integrando o ensino ao trabalho, oportunizando o desenvolvimento das condições para a vida produtiva contemporânea.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Divisão Euclidiana
   a. Conceitos
   b. Aplicações
2. Critérios de divisibilidade
   a. Critérios com restos
   b. Critérios sem restos
3. Bases Numéricas
   a. Conceito
   b. Mudanças de base
   c. Bases mais utilizadas
4. Base binária
   a. Bits, bytes e nibbles
   b. Prefixos binários
5. Noções de lógica
   a. Operadores lógicos
   b. Tabelas-verdade
6. Funções Aritméticas
   a. Função Tau
   b. Função Sigma
   c. Função Totiente
7. Aritmética Modular
   a. Adição, subtração e multiplicação
   b. Explicação dos critérios de divisibilidade
   c. Inversos modulares
   d. PLD (Problema do Logaritmo Discreto)
   e. Teorema de Fermat
   f. Teorema de Euler

Habilidades

1. Despertar a valorização da pesquisa;
2. Proporcionar condições para uma atitude crítica e objetiva diante de fatos e problemas científicos que exijam soluções e decisões;

3. Oferecer ao estudante, situações que tornem natural a interpretação dos fenômenos estudados;
4. Desenvolver no aluno o pensamento científico contribuindo para o seu desenvolvimento profissional;
5. Permitir que o aluno, compreenda a matemática como parcela do crescimento humano, essencial na formação e construção de uma visão de mundo necessária para desenvolver capacidades que serão exigidas ao longo da vida social e profissional;
6. Desenvolver habilidades de pensamento e raciocínio lógico através da diversidade de situações, relacionadas às demais áreas do conhecimento;
7. Entender a importância do sistema binário no ramo da informática.

Atitudes

- Autoconfiante para entender assuntos mais complexos.
- Perseverante na busca da solução de problemas
- Investigativo na busca de ferramentas proporcionadas pela matemática para resolução de problemas cotidianos
- Discernimento para aplicação dos conceitos matemáticos para os problemas onde se aplicam
- Curioso e persistente para validação das respostas corretas
- Comunicativo para interação com colegas e professores para busca da solução de problemas mais complexos

Referências:

Bibliografia Básica:

MILIES, C. P. e COELHO, S. P. **Números: Uma Introdução à Matemática**, Editora da Universidade de São Paulo, 3ª Edição, 2006.
COUTINHO, S. C. **Números Inteiros e Criptografia RSA**, 2ª Edição, 2000.
CAETANO, P. A. S., SAMPAIO, J. C. V. **Introdução a teoria dos números - Um curso breve**, Ed. UFSCar, 1ª edição, 2021.

Bibliografia Complementar:

CARNEIRO, F. J. F. **Criptografia e Teoria dos Números**, Editora Ciência Moderna, 2016.
MOREIRA, C. G. T. de A., TENGAN E., SALDANHA, N. C., MARTINEZ, F. B., **Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro**, Editora IMPA, 5ª edição, 2018.
SANTOS, J. P. de O., FERREIRA, D. M, **Problemas em Teoria dos Números**, Ciência Moderna, 2017.
LANDAU, E. **Teoria Elementar dos Números**, Ciência Moderna, 1ª edição, 2021.
BENATII, K. A., BENATTI, N. C. da C. M., **Teoria dos Números**, InterSaberes, 1ª edição, 2019.

Fundamentos de Redes de Computadores

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Fundamentos de Redes de Computadores		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60h	4 aulas semanais	Segundo semestre

Ementa:

As redes de hoje; Switch Básico e Configuração de Dispositivo Final; Protocolos e Modelos; Camada Física; Sistemas de Números; Camada de Enlace de Dados; Comutação Ethernet; Camada de Rede; Resolução de Endereços; Configuração Básica do Roteador; Endereçamento IPv4; Endereçamento IPv6; ICMP; Camada de Transporte; Camada de Aplicação; O protocolo HTTP; Fundamentos de Segurança de Rede; Criação de uma Rede Pequena

Objetivos

- Criar redes locais simples;
- Realizar configurações básicas para roteadores e switches;
- Implementar esquemas de endereçamento IP.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. As redes de hoje:
    a. Redes afetam nossas vidas;
    b. Representações e topologias de rede;
    c. Tipos comuns de redes;
    d. Conexões com a Internet;
    e. Redes confiáveis;
    f. Tendências das redes;
    g. Segurança de redes;
    h. O profissional de TI

2. Switch básico e configuração de dispositivo:
    a. Acesso ao Cisco IOS; Navegação IOS;
    b. A estrutura de comandos;
    c. Configuração básica de dispositivos;
    d. Salvar configurações;
    e. Portas e endereços;
    f. Configurar endereços IP;
    g. Verificar a conectividade.

3. Protocolos e modelos:
    a. As regras;
    b. Protocolos;
    c. Conjuntos de protocolos;
    d. Empresas de padrões;
    e. Modelos de referência;
    f. Encapsulamento de dados;
    g. Acesso a dados

4. Camada física:
    a. Propósito da camada física;
    b. Característica da camada física;
    c. Cabeamento de cobre;
    d. Cabeamento UTP;
    e. Cabeamento de fibra óptica;

f. Meios sem fio.

5. Sistemas de números:
    a. Sistema de numeração binário;
    b. Sistema de numeração hexadecimal;

6. Camada de enlace de dados:
    a. Finalidade da camada de enlace de dados;
    b. Topologias;
    c. Quadro de enlace de dados.

7. Switching ethernet:
    a. Quadros ethernet;
    b. Endereços MAC ethernet;
    c. A tabela de endereços MAC;
    d. Métodos de encaminhamento e velocidade de switches

8. Camada de rede:
    a. Características da camada de rede;
    b. Pacote IPv4;
    c. Pacote IPv6;
    d. Como um host roteia;
    e. Introdução ao roteamento.

9. Resolução de endereços:
    a. MAC e IP; ARP;
    b. Descoberta de vizinhos de IPv6.

10. Configuração básica do roteador:
    a. Configurar definições iniciais do roteador;
    b. Configurar interfaces;
    c. Configurar o gateway padrão.

11. Endereçamento IPv4:
    a. Estrutura do endereço IPv4;
    b. Unicast, broadcast e multicast IPv4;
    c. Tipos de endereços IPv4;
    d. Segmentação de rede;
    e. Sub-rede uma barra 16 e um prefixo 8;
    f. VLSM;
    g. Projeto estruturado.

12. Endereçamento IPv6:
    a. Problemas do IPv4;
    b. Representação do Endereçamento IPv6;
    c. Tipos de endereços IPv6;
    d. Endereçamento dinâmico para GUAs IPv6;
    e. Endereços IPv6 Multicast;
    f. Sub-rede de uma rede IPv6;

13. ICMP:
    a. Mensagens ICMP;
    b. Testes ping e traceroute

.

14. Camada de transporte:
    a. Transporte de dados;
    b. Visão geral do TCP;
    c. Visão geral do UDP;
    d. Números de porta;
    e. Processo de comunicação TCP;
    f. Confiabilidade e controle de fluxo;

g. Comunicação UDP.

15. Camada de aplicação:
    a. Aplicação, apresentação e sessão;
    b. Ponto a ponto;
    c. Protocolos de e-mail e web;
    d. Serviços de endereçamento IP;
    e. Serviços de compartilhamento de arquivos

16. O protocolo HTTP
    a. Cliente x Servidor
    b. Interação com HTML, CSS e Javascript
    c. Mensagem GET
    d. Mensagem POST
    e. Respostas do servidor
    f. Cabeçalhos mais comuns
    g. Presença de 'cookies'

17. Fundamentos de segurança de rede:
    a. Ameaças à segurança e vulnerabilidades;
    b. Ataques à rede;
    c. Mitigações de ataque à rede;
    d. Segurança de dispositivos.

18. Criação de uma rede pequena:
    a. Dispositivos em uma rede pequena;
    b. Aplicações e protocolos de redes pequenas;
    c. Escalar para redes maiores;
    d. Verificar conectividade;
    e. Host e comandos IOS;
    f. Metodologias de soluções de problemas;
    g. Cenários de solução de problemas

Habilidades

1. Explicar os avanços em tecnologias de rede modernas.
2. Implementar as configurações iniciais, incluindo senhas, endereçamento IP e parâmetros de gateway padrão em um switch de rede e em dispositivos finais.
3. Explicar como os protocolos de rede permitem que dispositivos acessem recursos de rede locais e remotos.
4. Explicar como os protocolos de camada física, os serviços e a mídia de rede possibilitam as comunicações em redes de dados.
5. Calcular números entre sistemas decimal, binário e hexadecimal.
6. Explique como o controle de acesso à mídia na camada de enlace de dados suporta as comunicações entre redes.
7. Explicar como a Ethernet funciona em uma rede de switches.
8. Explicar como os roteadores usam protocolos e serviços de camada de rede para viabilizar a conectividade de ponta a ponta.
9. Explicar como ARP e ND possibilitam a comunicação em uma rede local.
10. Implementar as configurações iniciais em um roteador e em dispositivos finais.
11. Calcular um esquema de sub-redes IPv4 para segmentar a rede com eficiência.
12. Implementar um esquema de endereçamento IPv6.
13. Usar várias ferramentas para testar a conectividade de rede.
14. Compare a operação dos protocolos da camada de transporte no suporte à comunicação de ponta a ponta.
15. Explicar a operação da camada de aplicação para dar suporte às aplicações do usuário final.
16. Configurar switches e roteadores com recursos de proteção de dispositivo para aumentar a segurança.
17. Solucionar problemas de conectividade em uma rede pequena.

Atitudes
1. Ser autônomo e assertivo para realizar configurações básicas em dispositivos intermediários e finais de redes de computadores, levando em considerações aspectos de eficiência e segurança; 2. Ser ciente do funcionamento eficaz de uma rede de computadores do nível mais baixo ao nível mais alto de abstração; 3. Ser analítico, reflexivo, crítico e assertivo quanto ao uso de estratégias e ferramentas para resolução de problemas em redes de computadores; 4. Ser analítico, reflexivo, crítico e assertivo acerca do planejamento e implementação de sub-redes IPv4.
Referências:
Bibliografia Básica:
KUROSE, J., ROSS, K. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 6a Edição. Pearson, 2013. BRITO, S. **Laboratórios de Tecnologias Cisco em Infraestrutura de Redes**. 2ª Edição. Editora Novatec, 2014. CARISSIMI, A. S., ROCHOL, J. GRANVILLE, L. Z. **Redes de Computadores.** Porto Alegre: Bookman, 2017.
Bibliografia Complementar:
BUNGART, J.W. **Redes de Computadores: Fundamentos e Protocolos.** Editora SENAI-SP, 2017. MOTA FILHO, J.E. **Análise de Tráfego em Redes TCP/IP: Utilize *tcpdump* na Análise de Tráfegos em Qualquer Sistema Operacional.** Editora Novatec, 2013. FERNANDES, A. **Redes de Computadores: Fundamentos**. Editora Érica, 2020. TANENBAUM, A, FEAMSTER, N. e WETHERALL, D. **Redes de Computadores**, 6ª Edição. Editora Bookman, 2021. COMER, D. **Redes de Computadores e Internet**, 6ª Edição. Editora Bookman, 2016.

Banco de Dados

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Banco de Dados		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60h	4 aulas por semana	Segundo semestre

Ementa:

Conceituação sobre Banco de Dados. Identificação, análise e aplicação de um modelo de Banco de Dados. Linguagem de definição e manipulação de Banco de Dados.

Objetivos

Conceituar e aplicar modelos e técnicas de projeto e implementação de banco de dados.

Conteúdos, Habilidades e Atitudes

Conteúdos

1.Fundamentos Básicos
- 1.1.Evolução histórica de Banco de Dados
- 1.2.Conceito de Banco de Dados e Sistema Gerenciador de Banco de Dados

2. Modelo Entidade Relacionamento
- a. Entidade
- b. Atributos
- c. Relacionamentos
- d. Generalização
- e. Diagrama Entidade-Relacionamento

3. Modelo Relacional
- 3.1 Conceito: relações, atributos, tuplas, chave primária, relacionamentos, chave estrangeira
- 3.3.Restrições de integridade

4. Linguagem de Definição e Manipulação de Dados
- 4.1.Comandos DDL – Definição das estruturas de dados
- 4.2.Comandos DML – Consulta, Inserção, Atualização, Exclusão

Habilidades

1. Analisar, interpretar e modelar um banco de dados.
2. Diferenciar os tipos de modelos de banco de dados, apontando as diferenças entre os mesmos.
3. Implementar as estruturas modeladas..

Atitudes

- Autonomia e segurança para analisar, identificar, construir e manipular um banco de dados;

Referências:

Bibliografia Básica:

DATE, C. J. **Introdução a Sistemas de Banco de Dados**. 8ª Edição. São Paulo: , 2004.
HEUSER, C. A. **Projeto de Banco de Dados.** 6ª Edição. Porto Alegre: Bookman, 2008.
SILBERSCHATZ, A, KORTH, H. F. SUDARSHAN, S. **Sistema de banco de dados**. 6. ed. Rio de Janeiro, RJ: Elsevier, 2012.

Bibliografia Complementar:

CARDOSO, V., CARDOSO, G. **Sistemas de Banco de Dados.** São Paulo, 2012.
DATE, C. J., **Projeto de Banco de Dados e Teoria Relacional: Formas Normais e Tudo Mais**. São Paulo: Novatec, 2015.

MACHADO, F. N. R., ABREU, M. P. **Projeto de Banco de Dados: Uma Visão Prática**. 17ª Edição. São Paulo: Érica, 2012.
ROB, P., CORONEL, C. **Sistemas de Banco de Dados: Projeto, Implementação e Administração**. São Paulo: Cengage, 2010.
TEOREY, T., LIGHTSTONE, S., NARDEAU, T., JAGADISH, H. V. **Projeto e Modelagem de Dados**. 2ª Edição. São Paulo: Elsevier, 2013.

Programação de Sistemas Embarcados

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Programação de Sistemas Embarcados		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30h	2 aulas por semana	Segundo semestre

Ementa:

Algoritmo, Linguagem C, Variáveis, Controle de fluxo, Funções, Vetores e Matrizes, Compilação, Sistema Embarcado, Arduino, Internet das Coisas - IoT.

Objetivos

- **Geral:**
  - Compreender a sintaxe, a compilação e técnicas de desenvolvimento de software em Linguagem C para atuar na análise e avaliação de sistemas embarcados.
- **Específicas:**
  - Desenvolver, compilar e depurar software em linguagem C;
  - Identificar, classificar e descrever os principais componentes de sistemas embarcados;

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Linguagem C:
   a. Tipos de Dados;
   b. Controle de Fluxo (if-else, switch-case, for, while);
   c. Vetores e Matrizes;
   d. Strings;
   e. Funções.
2. Sistemas Embarcados:
   a. Arquitetura de Sistemas Embarcados;
   b. Simulação de Sistema Embarcado com Arduino e Tinkercad;
3. Internet das Coisas - IoT:
   a. Arquitetura de Dispositivos de IoT;
   b. Wireless Sensor Networking - WSN;
   c. Simulação de Sistema de IoT com a Plataforma Blynk

Habilidades

- Identificar os componentes de um sistema embarcado e de sistemas de Internet das Coisas;
- Analisar, depurar e desenvolver software em linguagem C;
- Executar simulações de sistemas embarcados com dispositivos de prateleira, como o Arduino;
- Utilizar plataformas disponíveis na internet para desenvolver sistemas de IoT

Atitudes

- Autonomia e segurança para identificar, classificar e descrever componentes de sistemas embarcados e de IoT;
- Capacidade de formar o raciocínio lógico e propor soluções para o desenvolvimento de softwares em linguagem C.

Referências:

Bibliografia Básica:
BACKES, André. **Linguagem C: completa e descomplicada**. Elsevier Brasil, 2013. SCHILDT, Herbert. **C The Complete Reference.** 4ª Edição, McGraw-Hill 2000. MCROBERTS, Michael. **Arduino básico**. Novatec Editora, 2015.
Bibliografia Complementar:
SEACORD, Robert C. **Secure Coding in C and C++**. 2ª Edição, Pearson Education, 2005. GUPTA, Aditya. **The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things**. Apress, 2019. OLIVEIRA, C.L.V., NABARRO, C.B.M. e ZANETTI, H.A.P. **Raspberry Pi Descomplicado**. Editora Érica, 2018. OLIVEIRA, S. **Internet das Coisas com ESP8266, Arduino e Raspberry Pi**, 2ª Edição, Editora Novatec, 2021. JAVEED, A. **Criando Projetos com Arduino Para a Internet das Coisas: Experimentos com Aplicações do Mundo Real – Um Guia Para o Entusiasta de Arduino ávido por Aprender**. Editora Novatec, 2017.

Políticas de Segurança

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Políticas de Segurança		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30h	2 aulas por semana	Segundo semestre
Ementa:		
A necessidade de Segurança Cibernética; Ataques, conceitos e técnicas; Proteção de dados e privacidade; Proteção da empresa; O futuro na Segurança Cibernética.		
Objetivos		

• **Geral:**

- Compreender conceitos básicos sobre a Segurança Cibernética, incluindo o impacto das ameaças e porque a segurança cibernética é uma profissão em crescimento.

• **Específicas:**

- Aplicar conhecimentos básicos de Segurança Cibernética para proteção da vida digital pessoal.
- Obter insights sobre os maiores desafios de segurança que empresas, governos e instituições educacionais enfrentam hoje
- Compreender o papel de profissionais de segurança cibernética na proteção e defesa da rede em uma organização.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. A necessidade de Segurança Cibernética
    a. Dados pessoais
    b. Dados organizacionais
    c. Invasores e profissionais da Segurança Cibernética
    d. Guerra Cibernética

2. Ataques, conceitos e técnicas
    a. Análise de um ataque cibernético
        i. Exploits e vulnerabilidades de segurança
        ii. Tipos de vulnerabilidades de segurança
        iii. Tipos de Malware e sintomas
        iv. Métodos de infiltração
        v. Negação de serviço
    b. A paisagem da Segurança Cibernética
        i. Ataque misto
        ii. Redução do impacto

3. Proteção de dados e privacidade
    a. Como proteger os dados
        i. Como proteger a rede e os dispositivos
        ii. Manutenção de dados
    b. Como proteger a privacidade on-line
        i. Autenticação forte

ii. Compartilhamento de informações

4. Proteção da empresa
   a. Firewall
      i. Tipos de firewall
      ii. Equipamentos de segurança
      iii. Detecção de ataques em tempo real
      iv. Detecção de Malware
      v. Práticas recomendadas de segurança
   b. Abordagem comportamental à Segurança Cibernética
      i. Botnet
      ii. Kill chain
      iii. Segurança baseada em comportamento
      iv. NetFlow e ataques cibernéticos
   c. Ferramentas para prevenção e detecção de incidentes

5. O futuro na Segurança Cibernética
   a. Questões de ética e jurídicas em Segurança Cibernética, treinamento e carreiras
      i. Questões jurídicas em Segurança Cibernética
      ii. Questões éticas em Segurança Cibernética
      iii. Empregos de Segurança Cibernética

Habilidades

- Compreender a importância de comportamentos on-line seguros;
- Compreender como as ameaças à segurança cibernética afetam a todos;
- Descrever diferentes tipos de malware e ataques;
- Reconhecer a evolução do cenário de ameaças cibernéticas;
- Descrever as estratégias de proteção usadas pelas empresas para proteção contra ataques.

Atitudes

- Autonomia e segurança para identificar e classificar ameaças à segurança cibernética e descrever possíveis estratégias de proteção.

Referências:

Bibliografia Básica:

BAARS, H., HINTZBERGEN, K., HINTZBERGEN, J. e SMULDERS, A. **Fundamentos de Segurança da Informação com base na ISO 27001 e na ISO 27002**, Brasport, 2018.
KIM, D. SOLOMON, M. **Fundamentos de Segurança de Sistemas de Informação**, Editora GEN/LTC, 2014.
MACHADO, F. **Segurança da informação: Princípios e controle de ameaças**, Editora Érica, 2014.

Bibliografia Complementar:

FILHO, Sócrates Teixeira. **Segurança da Informação Descomplicada**, Brasília, 2015.
FERREIRA, Fernando; ARAÚJO, Márcio. **Política de Segurança da Informação - Guia prático para elaboração e implementação**, Editora Ciência Moderna, 2a edição, 2020,
ABNT NBR ISO/IEC 27001:2013 – **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**.
ABNT NBR ISO/IEC 27002:2013 – **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.**
ABNT NBR ISO/IEC 27005:2011 – **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.**

Algoritmos e Estrutura de Dados

***Campus*: Cabo Frio**		
Cursos		**Eixo Tecnológico**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Algoritmos e Estrutura de Dados		**2023**
Carga Horária	**Aulas por Semana**	**Período Letivo**
30 hs	2 aulas por semana	Segundo semestre

Ementa

Algoritmos e estrutura de dados; Tipo abstrato de dados; Ponteiros; Alocação de memória; Recursão; Notação assintótica; Listas; Pilhas; Filas; Árvores; Ordenação; Pesquisa.

Objetivos

- Geral:
  - Conhecimento das estruturas básicas e de algoritmos para gerenciá-las.
- Específicas:
  - Adquirir entendimento sólido da linguagem C (alocação dinâmica de memória, ponteiros, uso de compilador e linker);
  - Compreender técnicas de manipulação de estrutura de dados;
  - Modelar e implementar algoritmos em C utilizando estrutura de dados.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Manipulação de ponteiros e alocação de memória
   1. Fundamento de ponteiros
   2. Alocação dinâmica de memória
   3. Ponteiros como parâmetros para funções
   4. Aritmética de ponteiros
   5. Ponteiros de funções
2. Organizar um programa em C
   1. Compilador gcc
   2. Pré-processamento
   3. Módulos e o arquivos header
3. Recursão
   1. Fundamentos de recursão
   2. Recursão de cauda
   3. Recursão e iteração
4. Tipo Abstrato de dados
5. Análise de algoritmos
   1. Análise de melhor casos (pior, melhor e médio)
   2. Notação O
   3. Complexidade computacional
6. Listas
   1. Listas lineares
   2. Implementação estática e dinâmica de listas ligadas
   3. Implementação dinâmica de listas circulares
7. Pilhas e Filas
   1. Conceitos básicos
   2. Implementação estática e dinâmica pilhas
   3. Implementação dinâmica de filas
8. Ordenação
   1. Conceitos (Inserção, seleção, troca, distribuição, intercalação)
   2. Mergesort
   3. Quicksort
   4. Heapsort
9. Pesquisa
   1. Pesquisa sequencial
   2. Pesquisa em árvore binária

● Utilizar abstrações para representar dados ● Implementar algoritmos de pesquisa ● Implementar algoritmos de organização ● Atuar de forma proativa;
Atitudes
● Desenvolvimento do raciocínio lógico e criativo para resolução de problemas ● Autonomia para analisar problemas reais e desenvolver soluções computacionais ● Motivação e autonomia em aprofundar os conhecimentos em conceitos avançados de programação
Referências
Bibliografia Básica
LOUDON, Kyle. **Dominando Algoritmos Com C**. " O'Reilly Media, Inc.", 2000. SEDGEWICK, R. "**Algorithms in C: Parts 1–4 Fundamentals Data Structures Sorting and Searching.**", 3rd Edição CORMEN, Thomas H., et al. "**Algoritmos: teoria e prática**." Terceira Edição. 2012
Bibliografia Complementar
CORMEN, T.H. **Desmistificando Algoritmos.** Elsevier, 2014. CORMEN, H., LEISERSON, C.E., RIVEST, R.L., STEIN, C. **Introduction to Algorithms**, 3rd ed., McGraw-Hill, 2001. TENENBAUM, A., AARON, M., LANGSAM, Y., e AUGENSTEIN, M.J. **Estruturas de dados usando C**. Pearson Makron Books, 2004 AHO, A., et al. **Data structures and algorithms**. USA: Addison-Wesley, 1983. MOURA GUIMARÃES, A., e LAGES, N.A.C. **Algoritmos e estruturas de dados**. Livros Técnicos e Científicos, 1994 BENTLEY, J. **Programming Pearls**, 2nd.ed., Addison-Wesley, 2000 BENTLEY, J. **More Programming Pearls**, Addison-Wesley, 1990.

Sistemas Operacionais para Redes de Computadores

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Sistemas Operacionais para Redes de Computadores		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60	4 aulas semanais	Segundo semestre

Ementa:

Introdução ao Linux; Acesso à Linha de Comando; Gerenciamento de Arquivos na Linha de Comando; Ajuda no Linux; Criação, Visualização e Edição de Arquivos de Texto; Gerenciamento de Usuários e Grupos Locais; Controle de Acesso de Arquivos; Monitoramento e Gerenciamento de Processos do Linux; Controle de Serviços e Daemons; Configuração e Proteção do SSH; Análise e Armazenamento de Logs; Gerenciamento de Redes; Arquivamento de Transferência de Arquivos; Instalação e Atualização de Pacotes de Software; Acesso a Sistemas de Arquivos Linux.

Objetivos

- **Geral:**
  - Instalar, configurar e operar uma distribuição do sistema operacional Linux, por meio de interfaces de linha de comandos e ferramentas de nível empresarial, a fim de realizar tarefas básicas de administração de sistema operacional para redes de computadores.
- **Específicas:**
  - Configurar, instalar e manter sistemas Linux, além de fazer upgrade deles, com procedimentos e padrões estabelecidos;
  - Oferecer suporte operacional;
  - Gerenciar sistemas para monitorar a disponibilidade e desempenho;
  - Gravar e implantar scripts para automação de tarefas e administração de sistemas.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Introdução ao Linux;
2. Acesso à Linha de Comando:
   a. Acesso à linha de comando
   b. Acesso à linha de comando usando a área de trabalho;
   c. Execução de comando usando o shell Bash;
3. Gerenciamento de Arquivos na Linha de Comando:
   a. Descrição de conceitos de hierarquia do sistema de arquivos Linux;
   b. Especificação de arquivos por nome;
   c. Gerenciamento de arquivos usando ferramentas de linha de comando;
   d. Criação de links entre arquivos;
   e. Correspondência de nomes de arquivos com expansões de shell;
4. Ajuda no Linux:
   a. Leitura de páginas no manual;
   b. Leitura da documentação de informação.
5. Criação, Visualização e Edição de Arquivos de Texto:
   a. Redirecionamento da saída para um arquivo ou um programa;
   b. Edição de arquivos de texto a partir do prompt shell;
   c. Alteração do ambiente shell.
6. Gerenciamento de Usuários e Grupos Locais:
   a. Descrição de conceitos de grupos;
   b. Obtenção de acesso de superusuário;
   c. Gerenciamento de contas de usuários locais;
   d. Gerenciamento de senhas de usuários;
7. Controle de Acesso a Arquivos:
   a. Interpretação das permissões do sistema de arquivos do Linux;

b. Gerenciamento de permissões do sistema de arquivos a partir da linha de comando;
c. Gerenciamento de permissões padrão e acesso ao arquivos;

8. Monitoramento e gerenciamento de processos do Linux:
   a. Listagem de processos;
   b. Controle de tarefas;
   c. Encerramento de processos;
   d. Monitoramento de atividade de processo.
9. Controle de serviços e daemons:
   a. Identificação de processos do sistema iniciados automaticamente;
   b. Controle de serviços do sistema;
10. Configuração e proteção do SSH:
   a. Acesso à linha de comando remoto com o SSH;
   b. Configuração de autenticação baseada em chaves SSH;
   c. Personalização e configuração do open SSH;
11. Análise e Armazenamento de Logs:
   a. Descrição da arquitetura de log do sistema;
   b. Análise dos arquivos do syslog;
   c. Análise das entradas do diário do sistema;
   d. Preservação do diário do sistema;
   e. Manutenção de hora precisa.
12. Gerenciamento de hora precisa:
   a. Descrição de conceitos de rede;
   b. Validação da configuração de rede;
   c. Configuração de redes usando a linha de comando;
   d. Edição de arquivos de configuração de rede;
   e. Configuração de nomes de host e resolução de nomes;
13. Arquivamento e transferência de arquivos:
   a. Gerenciamento de arquivos tar compactados;
   b. Transferência de arquivos entre sistemas com segurança;
   c. Sincronização segura de arquivos entre sistemas;
14. Instalação e Atualização de Pacotes de Software:
   a. Registro de sistemas;
   b. Explicação e investigação de pacotes de software;
   c. Instalação e atualização de pacotes de software;
   d. Ativação de repositórios de software;
   e. Gerenciamento de fluxos módulos de pacote.
15. Acesso a Sistemas de Arquivos Linux:
   a. Identificação de sistemas de arquivos e dispositivos;
   b. Montagem e desmontagem de sistemas de arquivos;
   c. Localização de arquivos no sistema.

Habilidades

- Fazer login em sistema linux e executar comandos simples por meio de uma interface de linha de comandos;
- Copiar, mover, criar, excluir e organizar arquivos utilizando uma interface de linha de comando;
- Solucionar problemas de ajuda de sistemas locais;
- Gerenciar arquivos de texto a partir da saída do comando ou em um editor de texto;
- Criar, gerenciar e excluir grupos e usuários locais e administrar políticas de senhas locais;
- Configurar as permissões de sistemas de arquivos Linux e interpretar os efeitos de segurança de diferentes configurações de permissões;
- Avaliar e controlar processos sendo executados em um sistema operacional Linux;
- Controlar e monitorar os serviços de rede e os daemons do sistema utilizando o systemd;
- Configure um serviço de linha de comando seguro em sistemas remotos usando OpenSSH;
- Localizar e interpretar logs de eventos de redes em servidores Linux;
- Armazenar arquivos e copiá-los de um sistema para outro;
- Fazer download, instalar, atualizar e gerenciar os pacotes de software;
- Acessar, inspecionar e usar sistemas de arquivos existentes no armazenamento vinculado ao servidor Linux;

Atitudes

- Autonomia e segurança quanto a instalação, configuração e operação de uma distribuição do sistema operacional Linux;
- Criticidade quanto à implementação de requisitos de segurança para acesso ao sistema operacional Linux;
- Motivação em aprofundar conhecimentos acerca do sistema operacional Linux;
- Criatividade para implementação de soluções de administração básica de um sistema operacional Linux.

Referências:

Bibliografia Básica:

NEGUS, C. **Linux - a Bíblia: o mais abrangente e definitivo guia sobre Linux**. Editora Alta Books, 2014.
RAMOS, A. **Administração de Servidores Linux**. Editora Ciência Moderna, 2013.
OLONCA, R. **Administração de Redes Linux: Conceitos e Práticas na Administração de Redes em Ambiente Linux**. Editora Novatec, 2015.

Bibliografia Complementar:

NEMETH, E. SNYDER, G. HEIN, T. **Manual Completo do Linux: Guia do Administrador**, Pearson Universidades, 2007.
NEVES, J.C. **Programação Shell Linux: Referência Definitiva da Linguagem Shell**. Editora Novatec, 2022.
GIAVAROTO,S.C**. Kali Linux: Introdução ao Penetration Testing**. Editora Ciência Moderna, 2014.
MESSIER, R. **Learning Kali Linux: Security Testing, Penetration Testing, and Ethical Hacking**, Editora O'Reilly, 2018.
CLINTON, D. e NEGUS, C. **Ubuntu Linux Bible**. Editora Wiley, 2020.

4.4.3 – TERCEIRO SEMESTRE

Fundamentos de Criptologia

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		Informação e Comunicação
Componente Curricular		**Ano de Implantação**
Fundamentos de Criptologia		2023
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30h	2 aulas semanais	Terceiro semestre

Ementa:

Segurança da Informação; Criptologia; Integridade; Confidencialidade; Criptografia Simétrica; Troca de Chaves; Criptografia Assimétrica; Assinatura Digital; Noções mais avançadas

Objetivos

Oferecer formação integrada articulando a teoria à prática, proporcionando aos estudantes conhecimentos técnicos e humanísticos, tornando-os capazes de contribuir para o desenvolvimento regional. Formar profissionais conscientes das responsabilidades com relação à ética profissional e ao meio ambiente, capazes de desenvolver trabalhos de iniciação científica, bem como proporcionar a inserção qualificada no âmbito profissional, desenvolver conhecimentos necessários para a organização da área tecnológica dos diversos setores produtivos da região, integrando o ensino ao trabalho, oportunizando o desenvolvimento das condições para a vida produtiva contemporânea.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Segurança da Informação
   a. Conceitos iniciais
   b. Tipos de fraudes
   c. Complexidade computacional
2. Criptologia
   a. História da Criptologia
   b. Conceitos iniciais
   c. Serviços
3. Integridade
   a. Conceitos
   b. Funções Hash
4. Confidencialidade
   a. Esteganografia
   b. Cifras X Códigos
   c. Cifras de Substituição
   d. Cifras monoalfabéticas
   e. Cifras polialfabéticas
   f. OTP
   g. Cifras de transposição
5. Criptografia Simétrica
   a. Algoritmo DES
   b. Algoritmo 3DES
   c. Algoritmo AES
6. Troca de Chaves
   a. Algoritmo DH
7. Criptografia Assimétrica
   a. Algoritmo RSA
   b. Algoritmo Elgamal
8. Assinatura Digital
   a. Algoritmo DSA
9. Noções mais avançadas
   a. Curvas elípticas
   b. Criptografia homomórfica

c. Criptografia pós-quântica

Habilidades

1. Despertar a valorização da pesquisa;
2. Proporcionar condições para uma atitude crítica e objetiva diante de fatos e problemas científicos que exijam soluções e decisões;
3. Oferecer ao estudante, situações que tornem natural a interpretação dos fenômenos estudados;
4. Desenvolver no aluno o pensamento científico contribuindo para o seu desenvolvimento profissional;
5. Permitir que o aluno, compreenda a matemática como parcela do crescimento humano, essencial na formação e construção de uma visão de mundo necessária para desenvolver capacidades que serão exigidas ao longo da vida social e profissional;
6. Desenvolver habilidades de pensamento e raciocínio lógico através da diversidade de situações, relacionadas às demais áreas do conhecimento;
7. Entender a importância do sistema binário no ramo da informática.

Atitudes

- Autoconfiante para entender assuntos mais complexos.
- Perseverante na busca da solução de problemas
- Investigativo na busca de ferramentas proporcionadas pela matemática para resolução de problemas cotidianos
- Discernimento para aplicação dos conceitos matemáticos para os problemas onde se aplicam
- Curioso e persistente para validação das respostas corretas
- Comunicativo para interação com colegas e professores para busca da solução de problemas mais complexos

Referências:

Bibliografia Básica:

STALLINGS, W. **Criptografia e Segurança de Redes: Princípios e Práticas**, Editora Pearson, 6ª Edição, 2014.
COUTINHO, S. C. **Números Inteiros e Criptografia RSA**, 2ª Edição, 2000.
BENATII, K. A., BENATTI, N. C. da C. M., **Teoria dos números**, InterSaberes, 1ª edição, 2019.

Bibliografia Complementar:

SIMON, S. **O Livro dos Códigos**, Editora Record, 9ª edição, 2001.
PAAR, C., PELZL, J., **Understanding Cryptography: A Textbook for Students and Practitioners**, 1ª edição, 2010.
YAN, S. Y., **Number Theory for Computing**, Springer, 2ª edição, 2002.
DIFFIE, W., HELLMAN, M. E., **New Directions in Cryptography**, artigo do IEEE Transactions on Information Theory, 1976.
RIVEST, R.; SHAMIR, A.; ADLEMAN, L. **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**, artigo de Communications of the ACM, 1978.

Programação de Aplicações Web

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Programação de Aplicações Web		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60h	4 aulas semanais	Terceiro semestre

Ementa:

Conhecendo o Javascript; Javascript e seus comandos básicos; Conhecendo o *Document Object Model* (DOM); Condições em Javascript; Repetições; Tratamento de eventos com funções

Objetivos

- Geral:
  - Desenvolver soluções para problemas simples através de algoritmos computacionais, utilizando uma linguagem de programação de alto nível aplicada ao ambiente Web.
- Específicas:
  - Representar algoritmos computacionais de forma descritiva e gráfica
  - Entender a interação de HTML, CSS e Javascript no ambiente Web
  - Entender a operação do Javascript dentro e fora do ambiente do navegador
  - Desenvolver algoritmos computacionais capazes de interagir com um usuário
  - Modularizar algoritmos computacionais utilizando funções para separar responsabilidades

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Conhecendo o Javascript;
   a. o que o Javascript é capaz de fazer?
   b. Dicas de aprendizagem;
   c. Javascript vs ECMAScript;
   d. Requisitos de Software;
   e. Primeiros scripts em Javascript;

2. Javascript e seus comandos básicos;
   a. Armazenando dados;
   b. Tratamento de dados;
   c. Operações com dados;

3. Conhecendo o DOM;
   a. Document Object Model;
   b. Árvore DOM e seus elementos;
   c. Manipulando a árvore DOM;

4. Condições em JS;
   a. Uso de condicional simples;
   b. Condicional composto;
   c. Condições aninhadas;

5. Repetições;
   a. Comando 'while';
   b. Controle do número de repetições;
   c. Comando 'for';

6. Avançando nos Estudos;
   a. Variáveis compostas;
   b. Uso de funções eventos;

c. Passagem de parâmetros;
d. Exercícios propostos;

Habilidades

- Descrever algoritmos em suas diferentes formas de representação em um ambiente Web
- Utilizar métodos de interação com o usuário utilizando HTML e CSS em conjunto com Javascript
- Aplicar estruturas de controle, de forma adequada, em algoritmos computacionais
- Organizar e dividir algoritmos computacionais em módulos menores que possuam responsabilidades específica

Atitudes

- Desenvolvimento do raciocínio lógico e criativo para resolução de problemas
- Autonomia para analisar problemas reais e desenvolver soluções computacionais
- Motivação e autonomia em aprofundar os conhecimentos em conceitos avançados de programação

Referências:

Bibliografia Básica:

IEPSEN, E. **Lógica de Programação e Algoritmos com JavaScript: uma Introdução à Programação de Computadores com Exemplos e Exercícios Para Iniciantes**. Editora Novatec, 2022.
DUCKETT, J. **HTML e CSS**: projete e construa websites. 1. ed. Rio de Janeiro: Alta Books, 2016.
DUCKETT, J. **Javascript e Jquery**: Desenvolvimento de Interfaces Web Interativas. 1. ed. Rio de Janeiro: Alta Books, 2016.

Bibliografia Complementar:

HOFFMAN, A. **Web Application Security: Exploitation and Countermeasures for Modern Web Applications**, Editora O'Reilly, 2020.
SILVA, M.S**. Fundamentos de HTML5 e CSS3**. Editora Novatec, 2015
SILVA, M.S**. CSS Grid Layout: Criando Layouts CSS Profissionais**. Editora Novatec, 2017
MELONI,J., KYRNIN,J. **HTML, CSS, and JavaScript All in One: Covering HTML5, CSS3, and ES6 (SAMS Teach Yourself)**, 3a Edição, Editora Pearson, 2018.
HAVERBEKE, M. **Eloquent Javascript**: **A Modern Introduction to Programming**, 3 edition, No Starch Press, 2018.
FLANAGAN, D. **Javascript: The Definitive Guide: Master the World's Most-Used Programming Language**. 7a Edição. Editora O'Reilly, 2020.

Sistemas Embarcados e Dispositivos Móveis

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Sistemas Embarcados e Dispositivos Móveis		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60h	4 aulas semanais	Terceiro semestre

Ementa:

Sistema Operacional Android para Dispositivos Móveis; Aplicativos; Root; Depuração; Monitoramento do tráfego de rede; Identificação de Superfícies de Ataques; Mitigação de Vulnerabilidades

Objetivos

- **Geral:**
  - Compreender os principais componentes da arquitetura de dispositivos móveis para atuar na identificação ataques e na mitigação de vulnerabilidades.
- **Específicas:**
  - Compreender o funcionamento de sistemas operacionais em dispositivos móveis e realizar a instalação ou remoção de aplicativos do dispositivo;
  - Rootear smartphones baseados em Android, habilitar modo de desenvolvimento, realizar depuração de aplicativos e monitorar transferência de dados por rede;
  - Identificar superfícies ataques à dispositivos móveis e utilizar boas práticas de segurança na defesa do dispositivo

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Sistema Operacional Android:
   a. Origens do Android;
   b. Arquitetura do Sistema;
   c. Sistema de usuários e permissões;
   d. Android Studio;
   e. Emulador de Dispositivos Android
2. Aplicativos Android:
   a. Estrutura de projeto de um aplicativo;
   b. Android Debug Bridge:
   c. OWASP Mobile
3. Root:
   a. Vantagens e desvantagens do roteamento de dispositivos móveis.

4. Ataques e Defesas:
   a. Identificação de superfícies de ataques;
   b. Monitoramento de tráfego de rede com Burp;
   c. Ataques a aplicativos Android e mitigações;
   d. Ataques Server-Side e mitigações;

Habilidades

- Identificar os componentes de um sistema móvel;
- Instalar e depurar aplicativos móveis em sistemas Android, assim como analisar seu comportamento dinâmico;
- Observar tráfego de rede, identificar ataques em dispositivos móveis e executar ações defensivas para evitar ou reduzir os danos causados pelos ataques;

- Executar emuladores com o sistema operacional Android e conseguir permissão de superusuário;
- Utilizar ferramentas para investigar o funcionamento do sistema operacional e de aplicativos de dispositivos móveis, assim como realizar análises do tráfego de rede.

Atitudes

- Autonomia e segurança para identificar, classificar e descrever falhas de segurança e ataques a dispositivos móveis;
- Atitude crítica quanto ao uso de ferramentas computacionais para investigar o comportamento de aplicativos para dispositivos móveis;
- Ética quanto ao uso do conhecimento em segurança cibernética de dispositivos móveis em relação à privacidade e uso de dados alheios.

Referências:

Bibliografia Básica:

MEIKE, G. B., SCHIEFER, L. **Inside the Android OS Building, Customizing, Managing and Operating Android System Services**, 1ª Edição, Addison-Wesley Professional, 2021.

KOTIPALLI, S.R. e IMRAN, M.A. **Hacking Android,** Packt Publishing, 2016

GUNASEKERA, S. **Android Apps Security -Mitigate Hacking Attacks and Security**, 2ª Edição, Breaches-Apress, 2020.

Bibliografia Complementar:

ERICKSON, J. **Hacking: The Art Of Exploitation**, 2ª Edição. 2008.

ELENKOV, E. **Android Security Internal**s. 1ª Edição, No Starch Press, 2015

DRAKE, J.J., FORA, P. e LANIER, Z. **Android Hacker's Handbook**. Editora Wiley, 2014.

GLAUBER, N. **Dominando o Android com Kotlin**. Editora Novatec, 2019.

HOFFMAN, A. **Web Application Security: Exploitation and Countermeasures for Modern Web Applications**, Editora O'Reilly, 2020.

Monitoramento de Redes de Computadores

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Monitoramento de Redes de Computadores		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30h	2 aulas semanais	Terceiro semestre

Ementa:

1. Introdução a monitoramento e dimensionamento de redes;
2. Protocolo SMNP;
3. Inventário de Hardware;
4. Servidores de Logs;
5. Monitoramento ativo e passivo;
6. Ferramentas de Monitoramento Open Source;

Objetivos

Oferecer formação integrada articulando a teoria à prática, proporcionando aos estudantes conhecimentos técnicos e humanísticos, tornando-os capazes de contribuir para o desenvolvimento regional. Formar profissionais conscientes das responsabilidades com relação à ética profissional e ao meio ambiente, capazes de desenvolver trabalhos de iniciação científica, bem como proporcionar a inserção qualificada no âmbito profissional, desenvolver conhecimentos necessários para a organização da área tecnológica dos diversos setores produtivos da região, integrando o ensino ao trabalho, oportunizando o desenvolvimento das condições para a vida produtiva contemporânea.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Introdução a monitoramento e dimensionamento de redes;
    a. Introdução a taxas de transferência e gerenciamento de hardware;
    b. Importância do dimensionamento de redes;
    c. Técnicas e protocolos de monitoramento de redes.
2. Protocolo SNMP;
    a. Ferramentas de administração SNMP;
    b. Configuração de Serviço SNMP;
3. Inventário de Hardware;
    a. Métodos de detecção de alteração de Hardware;
4. Servidores de Logs;
    a. Introdução à logs em sistemas operacionais Windows e Linux;
    b. Ferramentas de alerta e tratamento de incidentes.
5. Monitoramento ativo e passivo;
    a. Técnicas de monitoramento passivo e ativos;
    b. Protocolo span;
    c. IDS e IPS;
6. Ferramentas de Monitoramento;
    a. Ferramenta Cacti;
    b. OCS inventory;
    c. Squil e Elsa;
    d. WireShark;
    e. MRTG;
    f. Zabbix;

Habilidades

- Despertar a valorização da pesquisa;

- Proporcionar condições para uma atitude crítica e objetiva diante de fatos e problemas científicos que exijam soluções e decisões;
- Oferecer ao estudante, situações que tornem natural a interpretação dos fenômenos estudados;
- Desenvolver no aluno o pensamento científico contribuindo para o seu desenvolvimento profissional;
- Permitir que o aluno, que entenda como localizar o significado das diversas mensagens e notificações que ser originadas em softwares e equipamentos de redes ao longo da sua vida profissional como administrador de redes;
- Identificar, implementar e gerenciar estrutura básica de monitoramento de rede a nível de analista 1;
- Fazer o primeiro atendimento em incidentes em uma rede de computadores ;
- Dimensionar e sugerir equipamentos de rede de acordo com a demanda da infraestrutura;
- Entender e resolver problemas do dia a dia.

Atitudes

- Desenvolvimento do raciocínio lógico e criativo para resolução de problemas
- Autonomia para analisar problemas reais e desenvolver soluções computacionais

Referências:

Bibliografia Básica:

LIMA, J.R. **Monitorando com Zabbix**. Editora Brasport, 2020.
RAMOS, A. **Administração de Servidores Linux**. Editora Ciência Moderna, 2013.
OLONCA, R. **Administração de Redes Linux: Conceitos e Práticas na Administração de Redes em Ambiente Linux**. Editora Novatec, 2015.

Bibliografia Complementar:

NEGUS, C. **Linux - a Bíblia: o mais abrangente e definitivo guia sobre Linux**. Editora Alta Books, 2014.
NEMETH, E., SNYDER, G. e HEIN, T. **Manual Completo do Linux: Guia do Administrador**, Pearson Universidades, 2007.
LIEFTING,N. e BAEKEL B.V. **Zabbix 5 IT Infrastructure Monitoring Cookbook: Explore the new features of Zabbix 5 for designing, building, and maintaining your Zabbix setup**, Editora Packt Publishing, 2022.
MESSIER, R. **Learning Kali Linux: Security Testing, Penetration Testing, and Ethical Hacking**, Editora O'Reilly, 2018.
CLINTON, D. e NEGUS, C. **Ubuntu Linux Bible**. Editora Wiley, 2020.

Segurança Defensiva

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Segurança Defensiva		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60hs	4 aulas semanais	Terceiro semestre

Ementa:

Posturas quanto à Segurança; O processo de Resposta a Incidentes; O que é uma estratégia para Segurança Cibernética? Entendendo o 'Kill Chain' da Segurança Cibernética; Reconhecimento do terreno; Comprometendo o sistema; Atrás da identidade de algum usuário; Movimentos laterais; Elevação de privilégio; Política de segurança; Segmentação da rede; Sensores sempre ativos; Inteligência sobre ameaças; Investigando um incidente; Procedimento de recuperação; Gestão de vulnerabilidades; Análise de 'logs'

Objetivos

- Geral:
  - Elaboração de estratégia de segurança cibernética para pequenas empresas

- Específicas:
  - Conhece as portas TCP e UDP de todos os serviços expostos aos clientes da organização
  - Entende o funcionamento de um firewall e como é usado para isolar os sistemas em produção da organização
  - Identificar quais os ativos de TI que devem ser protegidos na organização
  - Elabora planos de contingência e recuperação para empresas pequenas.

Conteúdos, Habilidades e Atitudes

Conteúdos

1) Posturas quanto à Segurança;
   a) Ameaças atuais;
   b) Lidando com credenciais - autenticação e autorização;
   c) Aplicativos;
   d) Desafios para a Segurança Cibernética;
   e) Melhorando a postura com relação à segurança;
   f) O 'Red Team' e o 'Blue Team';

2) O processo de Resposta a Incidentes;
   a) Lidando com um incidente;
   b) Atividades pós-incidente;
   c) Respostas a incidentes em ambientes em nuvem

3) O que é uma estratégia para Segurança Cibernética?
   a) Qual a necessidade de uma estratégia?
   b) Como construir uma estratégia?
   c) Melhores estratégias de ataque ('Red Team');
   d) Melhores estratégias de defesa ('Blue Team')

4) Entendendo o 'Kill Chain' da Segurança Cibernética;
   a) Reconhecimento;
   b) Informação como arma de ataque;
   c) Elevação de privilégio;
   d) 'Exfiltration';
   e) Gestão do ciclo de vida de uma ameaça;

f) Ferramentas utilizadas em cada fase do 'Kill Chain'

5) Reconhecimento do terreno;
   a) Reconhecimento de fora do perímetro;
   b) Ferramentas de enumeração para serviços web;
   c) Reconhecimento de dentro do perímetro

6) Comprometendo o sistema;
   a) Analisando ataques atuais;
   b) 'Phishing';
   c) Explorando uma vulnerabilidade;
   d) 'Zero-Day';
   e) Seguindo um passo-a-passo para comprometer um sistema;
   f) Dispositivos móveis (ataques contra iOS e Android)

7) Atrás da identidade de algum usuário;
   a) Identidade como o novo perímetro;
   b) Estratégias para comprometer a identidade de um usuário;

8) Movimentos laterais;
   a) Infiltração;
   b) Mapeamento da rede;
   c) Evitando alertas;
   d) Realizando movimentos laterais;

9) Elevação de privilégio;
   a) Infiltração;
   b) Evitando alertas;
   c) Elevando o privilégio;
   d) Técnicas para elevação de privilégio;

10) Política de segurança;
   a) Revisando sua política de segurança;
   b) Educando o usuário final;
   c) Fiscalização da política;
   d) Monitoramento de conformidade;
   e) Contínuo melhoramento da postura de segurança através da política;

11) Segmentação da rede;
   a) Abordagem da defesa em profundidade;
   b) Segmentação física da rede;
   c) Blindando o acesso remoto à rede;
   d) Segmentação de redes virtuais;
   e) Rede de 'confiabilidade zero';
   f) Segurança de redes híbridas de nuvem

12) Sensores sempre ativos;
   a) Capacidade de detecção;
   b) Sistemas de detecção de intrusão;
   c) Sistemas de prevenção de intrusão;
   d) Análise comportamental no datacenter;
   e) Análise comportamental na nuvem;

13) Inteligência sobre ameaças;
   a) Ferramentas de código aberto;
   b) Alavancando inteligência para investigação de atividade suspeita

14) Investigando um incidente;
   a) Definindo o escopo do incidente;
   b) Investigação de um computador comprometido que é local;
   c) Investigação de um computador comprometido na nuvem;
   d) Investigação pro-ativa

15) Procedimento de recuperação;
    a) Plano para recuperação de desastres;
    b) Plano de contingência;
    c) Melhores práticas para um bom plano de recuperação e de contingência

16) Gestão de vulnerabilidades;
    a) Criando uma estratégia para gerência de vulnerabilidades;
    b) Ferramentas para gerência de vulnerabilidades;
    c) Melhores práticas;

17) Análise de 'logs';
    a) Correlação de dados;
    b) 'Logs' do sistema operacional;
    c) 'Logs' do firewall;
    d) 'Logs' do servidor web;
    e) 'Logs' dos sistemas na nuvem

18) Laboratório de Segmentação de Rede: instalação, configuração e teste de um firewall

19) Laboratório de Sensores: sistema de detecção de intrusão

20) Laboratório de Gerência de Vulnerabilidades: sistema de varredura de vulnerabilidades

Habilidades

- Sabe realizar uma configuração básica de um firewall em ambiente Linux
- Sabe configurar de forma básica um sistema de detecção de intrusão em ambiente Linux
- Sabe como realizar uma varredura por vulnerabilidades nos servidores web atuais
- Propõe estratégias de segurança cibernética para empresas de pequeno porte

Atitudes

- Procura contínua pelo aprendizado que toda nova ocorrência proporciona
- Humildade para reconhecer o limite dos seus conhecimentos
- Disposição para interagir e aprender com colegas mais experientes
- Disposição de ensinar o pouco que aprendeu para colegas mais novos
- Perseverança na busca das ferramentas corretas para validar problemas relatados
- Sempre alerta para informações que foram categorizadas de maneira errada no sistema de incidentes e eventos do centro de operações de segurança
- Interesse em conhecer diferentes formas de utilizar ferramentas de software para investigação e validação de relatos feitos ao centro de operações de segurança.

Referências:

Bibliografia Básica:

MURDOCH, D. **Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter**, 2019.
BAARS, H., HINTZBERGEN, K., HINTZBERGEN, J. e SMULDERS, A. **Fundamentos de Segurança da Informação com base na ISO 27001 e na ISO 27002**, Brasport, 2018.
KIM, D. SOLOMON, M. **Fundamentos de Segurança de Sistemas de Informação**, Editora GEN/LTC, 2014.

Bibliografia Complementar:

NEGUS, C. **Linux - a Bíblia: o mais abrangente e definitivo guia sobre Linux**. Editora Alta Books, 2014.
DIOGENES,Y. e OZKAYA, E. **Cybersecurity: Attack and Defense Strategies.** Second Edition. Editora Packt Publishers, 2019.
ABNT NBR ISO/IEC 27001:2013 – **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**.
ABNT NBR ISO/IEC 27002:2013 – **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.**
ABNT NBR ISO/IEC 27005:2011 – **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.**
MACHADO, F. **Segurança da informação: Princípios e controle de ameaças**, Editora Érica, 2014.

Operações em Segurança Cibernética

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Operações em Segurança Cibernética		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60hs	4 aulas semanais	Terceiro semestre

Ementa:

O perigo; Soldados na guerra contra o crime digital; Os sistemas operacionais Windows e Linux; Protocolos de Rede; Princípios de segurança da rede; O protocolo ARP; A camada de transporte; Serviços de rede; Dispositivos de comunicação de rede; Infraestrutura de segurança de rede; Invasores e suas ferramentas; Ameaças e ataques comuns; Observação da operação de rede; Ataques à base; Ataque ao trabalho; Noções básicas sobre defesa; Controle de Acesso; Inteligência de ameaças; Criptografia; Proteção de 'endpoints'; Avaliação de vulnerabilidades de 'endpoints'; Tecnologias e protocolos; Dados de segurança de rede; Avaliação de alertas; Como trabalhar com dados de segurança de rede; Computação forense digital e análise e resposta a incidentes.

Objetivos

- Geral:
  - Utilização do sistema central de incidentes e eventos de segurança do centro de operações de segurança em um nível de operador

- Específicas:
  - Interage com clientes internos e externos ao centro de operações de segurança
  - Sabe ouvir relatos de ocorrências e alimentar o sistema com os fatos relatados
  - Faz uma validação inicial de problemas relatados através de ferramentas básicas de investigação antes de alimentar o sistema com fatos relatados
  - Ouve e interage com colegas mais experientes para solução de ocorrências de natureza desconhecida
  - Aprende com cada novo tipo de ocorrência que é inserida no sistema
  - Estuda a solução encontrada por colegas mais experientes para incidentes mais complexos.

Conteúdos, Habilidades e Atitudes

Conteúdos

1) O perigo;
   a) Introdução;
   b) Histórias de guerra;
   c) Agentes de ameaças;
   d) Impacto das ameaças;
   e) O resumo dos perigos;

2) Soldados na guerra contra o crime digital;
   a) Introdução;
   b) O moderno centro de operações de segurança ;
   c) Como tornar-se um defensor;
   d) Resumo de soldados na guerra contra o crime digital

3) O sistema operacional Windows;
   a) Introdução;
   b) A história do Windows;
   c) Arquitetura e operações do Windows;
   d) Configuração e monitoramento do Windows ;
   e) Segurança do Windows;
   f) O resumo do sistema operacional Windows

4) Visão geral do Linux;
    a) Introdução;
    b) Noções básicas do Linux;
    c) Como trabalhar no Linux Shell ;
    d) Servidores e clientes do Linux ;
    e) Administração básica do servidor;
    f) O sistema de arquivos Linux;
    g) Como trabalhar com a GUI do Linux;
    h) Como trabalhar em um host do Linux ;
    i) Resumo dos conceitos básicos do Linux

5) Protocolos de rede;
    a) Introdução;
    b) Processo de comunicação de rede;
    c) Protocolos de comunicação;
    d) Encapsulamento de dados;
    e) Resumo dos protocolos de rede

6) Ethernet e IP;
    a) Introdução;
    b) Ethernet;
    c) IPv4;
    d) Noções básicas sobre endereçamento IP ;
    e) Tipos de endereços IPv4;
    f) O gateway padrão;
    g) Comprimento do prefixo IPv6;
    h) Resumo dos protocolos Ethernet e IP

7) Princípios da segurança de rede;
    a) Introdução ICMP;
    b) Utilitários Ping e Traceroute;
    c) Resumo da verificação de conectividade;

8) O protocolo ARP;
    a) Introdução;
    b) MAC e IP;
    c) ARP;
    d) Problemas do ARP;
    e) Resumo do protocolo ARP

9) A camada de transporte;
    a) Introdução;
    b) Características da camada de transporte;
    c) Estabelecimento das sessões da camada de transporte;
    d) Confiabilidade da camada de transporte ;
    e) O resumo da camada de transporte

10) Serviços de rede;
    a) Introdução;
    b) DHCP;
    c) DNS;
    d) NAT;
    e) Serviços de transferência e compartilhamento de arquivos;
    f) E-mail;
    g) HTTP;
    h) Resumo dos serviços de rede

11) Dispositivos de comunicação de rede;
    a) Introdução;
    b) Dispositivos de rede;
    c) Comunicações sem fio;
    d) Resumo dos dispositivos de comunicação de rede

12) Infraestrutura de segurança de rede;
    a) Introdução;
    b) Topologias de rede;
    c) Dispositivos de segurança;
    d) Serviços de segurança;
    e) Resumo da infraestrutura de segurança de rede

13) Invasores e suas ferramentas;
    a) Introdução;
    b) Quem está atacando nossa rede?
    c) Ferramentas dos agentes de ameaças;
    d) Resumo dos invasores e suas ferramentas

14) Ameaças e ataques comuns;
    a) Introdução;
    b) Malware;
    c) Ataques de rede comuns - reconhecimento, acesso e engenharia social;
    d) Ataques de rede – negação de serviço, saturação de buffer e evasão;
    e) Resumo de ameaças e ataques comuns

15) Observação da operação de rede;
    a) Introdução;
    b) Introdução ao monitoramento de rede;
    c) Introdução às ferramentas de monitoramento de rede;
    d) Resumo do monitoramento e das ferramentas de rede;

16) Ataque à base;
    a) Introdução;
    b) Detalhes da PDU IP;
    c) Vulnerabilidades de IP;
    d) Vulnerabilidades de TCP e UDP;
    e) Resumo do ataque à base

17) Ataque ao trabalho;
    a) Introdução;
    b) Serviços IP;
    c) Serviços corporativos;
    d) Resumo do ataque ao nosso trabalho

18) Noções básicas sobre defesa;
    a) Introdução;
    b) Defense-in-Depth;
    c) Políticas de segurança, regulamentos e padrões ;
    d) Resumo das noções básicas de defesa

19) Controle de acesso;
    a) Introdução;
    b) Conceitos de controle de acesso;
    c) Uso e operação de AAA;
    d) Resumo do controle de acesso

20) Inteligência de ameaças;
    a) Introdução;
    b) Fontes de informações;
    c) Serviços de inteligência de ameaças;
    d) Resumo da inteligência de ameaças

21) Criptografia;
    a) Introdução;
    b) Integridade e autenticidade;
    c) Confidencialidade;
    d) Criptografia de chave pública;

e) Autoridades e o sistema de confiança de PKI ;
f) Aplicações e impactos da criptografia;
g) Resumo da criptografia

22) Proteção de endpoints;
a) Introdução;
b) Proteção antimalware;
c) Prevenção contra invasões baseada em host;
d) Segurança de aplicativos;
e) Resumo da proteção do endpoint

23) Avaliação das vulnerabilidades de endpoint;
a) Introdução;
b) Perfil de rede e servidor;
c) Common Vulnerability Scoring System (CVSS);
d) Gerenciamento de dispositivo seguro;
e) Sistemas de gerenciamento de segurança da informação;
f) Resumo da avaliação das vulnerabilidades de endpoint;

24) Tecnologias e protocolos;
a) Introdução;
b) Protocolos comuns de monitoramento;
c) Tecnologias de segurança;
d) Resumo de tecnologias e protocolos;

25) Dados de segurança de rede;
a) Introdução;
b) Tipos de dados de segurança;
c) Registros de dispositivo final;
d) Registros de rede;
e) Resumo dos dados de segurança de rede

26) Avaliação de alertas;
a) Introdução;
b) Fonte de alertas;
c) Resumo da avaliação de alerta;
d) Resumo da avaliação de alertas;

27) Como trabalhar com dados de segurança de rede;
a) Introdução;
b) Uma plataforma de dados comum;
c) Investigação dos dados de rede;
d) Como melhorar o trabalho do analista de segurança cibernética;
e) Resumo do trabalho com os dados de segurança de rede

28) Computação forense digital e análise e resposta a incidentes;
a) Introdução;
b) Manipulação de evidências e atribuição de ataques;
c) A Cyber Kill Chain;
d) O modelo diamante da análise de invasão;
e) Resposta a incidentes;
f) Resumo da computação forense digital e análise e resposta a incidentes

Habilidades

- Sabe como realizar a configuração básica de servidores Windows ou Linux
- Entende o funcionamento de uma rede de computadores
- Entende como ocorrem os ataques mais comuns
- Coleta dados obtidos nos 'logs' e históricos de eventos ocorridos em diferentes 'endpoints'

Atitudes

- Procura contínua pelo aprendizado que toda nova ocorrência proporciona

- Humildade para reconhecer o limite dos seus conhecimentos
- Disposição para interagir e aprender com colegas mais experientes
- Disposição de ensinar o pouco que aprendeu para colegas mais novos
- Perseverança na busca das ferramentas corretas para validar problemas relatados
- Sempre alerta para informações que foram categorizadas de maneira errada no sistema de incidentes e eventos do centro de operações de segurança
- Interesse em conhecer diferentes formas de utilizar ferramentas de software para investigação e validação de relatos feitos ao centro de operações de segurança.

Referências:

Bibliografia Básica:

BAARS, H., HINTZBERGEN, K., HINTZBERGEN, J. e SMULDERS, A. **Fundamentos de Segurança da Informação com base na ISO 27001 e na ISO 27002**, Brasport, 2018.

KIM, D. SOLOMON, M. **Fundamentos de Segurança de Sistemas de Informação**, Editora GEN/LTC, 2014.

MACHADO, F. **Segurança da informação: Princípios e controle de ameaças**, Editora Érica, 2014.

Bibliografia Complementar:

NEGUS, C. **Linux - a Bíblia: o mais abrangente e definitivo guia sobre Linux**. Editora Alta Books, 2014.

DIOGENES,Y. e OZKAYA, E. **Cybersecurity: Attack and Defense Strategies.** Second Edition. Editora Packt Publishers, 2019.

ABNT NBR ISO/IEC 27001:2013 – **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**.

ABNT NBR ISO/IEC 27002:2013 – **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.**

ABNT NBR ISO/IEC 27005:2011 – **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.**

4.4.4 – QUARTO SEMESTRE

Criptologia Aplicada

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Criptologia Aplicada		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30h	2 aulas semanais	Quarto semestre

Ementa:

Modos de operação; Ataques à comunicação; Infraestrutura de chaves públicas; Criptologia aplicada à Metrologia; GPG; OpenSSL

Objetivos

Oferecer formação integrada articulando a teoria à prática, proporcionando aos estudantes conhecimentos técnicos e humanísticos, tornando-os capazes de contribuir para o desenvolvimento regional. Formar profissionais conscientes das responsabilidades com relação à ética profissional e ao meio ambiente, capazes de desenvolver trabalhos de iniciação científica, bem como proporcionar a inserção qualificada no âmbito profissional, desenvolver conhecimentos necessários para a organização da área tecnológica dos diversos setores produtivos da região, integrando o ensino ao trabalho, oportunizando o desenvolvimento das condições para a vida produtiva contemporânea.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Modos de operação
   a. Vetor de inicialização
   b. Classificação dos modos de operação
2. Ataques à comunicação
   a. Conceitos
   b. Tipos de ataques
3. Infraestrutura de chaves públicas
   a. Conceito
   b. Certificado digital
   c. ICP-Brasil
4. Criptologia aplicada à Metrologia
   a. Cadeia legalmente relevante
   b. Carga remota de software
5. GPG
   a. Criar chaves
   b. Cifrar e decifrar
   c. Assinar digitalmente
6. OpenSSL
   a. Comandos básicos
   b. Aplicações

Habilidades

1. Despertar a valorização da pesquisa;
2. Proporcionar condições para uma atitude crítica e objetiva diante de fatos e problemas científicos que exijam soluções e decisões;
3. Oferecer ao estudante, situações que tornem natural a interpretação dos fenômenos estudados;
4. Desenvolver no aluno o pensamento científico contribuindo para o seu desenvolvimento profissional;
5. Permitir que o aluno, compreenda a matemática como parcela do crescimento humano, essencial na formação e construção de uma visão de mundo necessária para desenvolver capacidades que serão exigidas ao longo da vida social e profissional;

6. Desenvolver habilidades de pensamento e raciocínio lógico através da diversidade de situações, relacionadas às demais áreas do conhecimento;
7. Entender a importância do sistema binário no ramo da informática.

Atitudes

- Autoconfiante para entender assuntos mais complexos.
- Perseverante na busca da solução de problemas
- Investigativo na busca de ferramentas proporcionadas pela matemática para resolução de problemas cotidianos
- Discernimento para aplicação dos conceitos matemáticos para os problemas onde se aplicam
- Curioso e persistente para validação das respostas corretas
- Comunicativo para interação com colegas e professores para busca da solução de problemas mais complexos

Referências:

Bibliografia Básica:

STALLINGS, W. **Criptografia e Segurança de Redes: Princípios e Práticas**, Editora Pearson, 6ª Edição, 2014.
COUTINHO, S. C. **Números Inteiros e Criptografia RSA**, 2ª Edição, 2000.
BENATII, K. A., BENATTI, N. C. da C. M., **Teoria dos números**, InterSaberes, 1ª edição, 2019.

Bibliografia Complementar:

SIMON, S. **O Livro dos Códigos**, Editora Record, 9ª edição, 2001.
PAAR, C., PELZL, J., **Understanding Cryptography: A Textbook for Students and Practitioners**, 1ª edição, 2010.
YAN, S. Y., **Number Theory for Computing**, Springer, 2ª edição, 2002.
DIFFIE, W., HELLMAN, M. E., **New Directions in Cryptography**, artigo do IEEE Transactions on Information Theory, 1976.
RIVEST, R.; SHAMIR, A.; ADLEMAN, L. **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**, artigo de Communications of the ACM, 1978.

Gestão e Planejamento Profissional

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Gestão e Planejamento Profissional		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60h	4 aulas por semana	Quarto semestre

Ementa:

Orientação quanto ao contexto do mercado de trabalho e suas implicações no planejamento de ações que ajudem na preparação e facilitem a construção do seu projeto de carreira em TI, seguindo nas linhas de Desenvolvimento profissional, plataformas de currículos digitais, redes sociais de negócios e networking.

Objetivos

- Geral:

  Utilizar ferramentas e plataformas de networking, negócios e trabalho;
  Entender o mercado e cenário atual de tecnologia;
  Analisar tendências do mercado de trabalho em TI;

- Específicas:

  Desenvolver competências e habilidades da carreira profissional;
  Elaborar currículos digitais de qualidade;
  Procurar e analisar posições de trabalho;
  Desenvolver técnicas de comunicação e networking para negócios e posições de trabalho.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Desenvolvimento profissional;
   a. Aquisição e organização de conhecimento
   b. Planejamento de carreira
   c. Transição de carreira
2. Plataformas de currículos digitais;
   a. Plataforma Lattes
   b. LinkedIn
3. Redes sociais de negócios e networking;
4. Melhores práticas em entrevistas;
5. Plataformas de trabalho independente (freelancers);
6. Trabalho remoto:
   a. Tecnologias de trabalho remoto
   b. Gestão do tempo
   c. Qualidade de vida e saúde no trabalho remoto
7. Networking e posicionamento de mercado
   a. Procura e análise de vagas
   b. Comunicação e estratégia

Habilidades

1. Identificar e aplicar para vagas na área de informática
2. Realizar networking de trabalho e negócios
3. Evoluir e entender cada aspecto da sua carreira;
4. Criar e disponibilizar currículos de qualidade;
5. Conhecer e utilizar ferramentas de trabalho remoto.

Atitudes

- Autonomia para ter sua primeira renda proveniente da área tecnológica;
- Atitude proativa no trabalho;
- Resiliência em momentos de incerteza no mercado;
- Autodidata no aprendizado de conteúdos de tecnologia

Referências:

Bibliografia Básica:

DUTRA, J. S. **Administração de Carreiras**: Uma proposta para Repensar a Gestão de Pessoas, São Paulo, Ed. Atlas, 1996.
JANKOVIC BARDUCHI, Ana Lúcia; BONILHA, Ana Paula (orgs.). **Desenvolvimento Pessoal e Profissional.** São Paulo: Pearson, 2007.
MORIN, E. M. **Os sentidos do trabalho**. RAE, jul/set 2007. São Paulo, v. 41, n. 3, p. 8- 19.
SARRIERA, J. C.; CÂMARA, S. G.; BERLIM, C. S. **Formação e orientação ocupacional:** manual para jovens à procura de emprego. Porto Alegre: Sulina, 2006.

Bibliografia Complementar:

CARVALHO-NETO, A.; SANT'ANNA, A. DE S. **Relações de Trabalho e Gestão de Pessoas, Dois Lados de Uma Mesma Moeda: vinculações sob a ótica do fenômeno da liderança.** Revista Gestão & Tecnologia, v. 13, n. 2, p. 2–20, 2013.
CHIAVENATO, I. **Recursos Humanos: o capital humano das organizações.** 8 ed. São Paulo: Atlas, 2006.
LUCCHIARI, D. H. P. S. **O que é escolha profissional.** 3 ed. São Paulo: Brasiliense, 1998.
MINARELLI, J. A. **Empregabilidade: como ter trabalho e remuneração sempre.** 15. ed. São Paulo: Gente, 1995.
SARRIERA, J. C.; ROCHA, K. B.; PIZZINATO, A. **Desafios do mundo do trabalho: orientação, inserção e mudanças**. Porto Alegre: EDIPUCRS, 2004.
SCHEIN, E. **Identidade Profissional.** Nobel: São Paulo, 1996.

Serviços de Rede de Computadores em Nuvem

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Serviços de Redes de Computadores em Nuvem		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60h	4 aulas semanais	Quarto semestre

Ementa:

Virtualização com containers e computação em nuvem; Administração de Docker containers; Configurando CPU e Memória de containers; Acessando volumes em um Docker container; Nuvem open-source e a arquitetura do OpenStack; Serviço de identificação de usuários no OpenStack; Neutron e o OpenStack networking; OpenStack Nova e a computação virtual; Serviço de imagens do OpenStack Glance; Volumes virtuais com o OpenStack Cinder; Armazenamento de Objetos com OpenStack Swift; Orquestração de containers com OpenStack Magnum

Objetivos

Familiaridade com as finalidades básicas da utilização de containers; Noções básicas de administração de ambientes privados de computação em nuvem; Configuração e lançamento de máquinas virtuais conectadas por uma rede virtual em máquinas físicas hospedeiras; Acesso remoto de serviços baseados em nuvem privada;

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Introdução:
    a. O que é um container?
    b. O que é computação em nuvem?
    c. História da tecnologia
    d. Nuvens privadas e públicas

2. O que é um Docker Container?
    a. Onde entra o Docker nessa história?
    b. Copy-On-Write (COW) e Docker;
    c. Storage drivers;
    d. Docker Internals;
    e. Namespaces (PID, Net, Mnt, IPC, UTS, User);
    f. Cgroups;
    g. Netfilter;
    h. Para quem serve o Docker ?

3. Executando e administrando containers Docker;
    a. Subindo containers;
    b. Derrubando containers;
    c. Monitorando o consumo de recursos;
    d. Eliminando containers

4. Configurando CPU e memória para os meus containers;
    a. Especificando a quantidade de memória;
    b. Especificando a quantidade de CPU;
    c. Eu consigo alterar CPU e memória dos meus containers em execução?

5. Entendendo volumes;
    a. Introdução a volumes no Docker;
    b. Criando volumes;
    c. Localizando volumes;
    d. Criando e montando um data-only container;
    e. Sempre é bom um backup...

6. Introdução ao OpenStack;
    a. A arquitetura OpenStack
    b. Instalação e sua validação
    c. O cliente OpenStack
    d. Configuração do cliente no Linux

7. Keystone: serviço de identificação do OpenStack;
    a. Criando domínios OpenStack com KeyStone
    b. Adicionando usuários e definindo seus 'roles'
    c. Configuração de grupos de usuários

8. Neutron: OpenStack Networking;
    a. Gerenciando redes, sub-redes e portas
    b. Configurando roteadores e endereços IP flutuantes
    c. Gerenciando 'security groups'
    d. Gerenciando balanceadores de carga

9. Nova: Computação virtual com OpenStack;
    a. Adicionando e suspendendo um 'host' para manutenção
    b. Agregando 'hosts' com Nova Scheduler
    c. Criando e removendo 'availability zones'
    d. Configurando 'flavors': limites de CPU e IOPS
    e. Iniciando e parando uma instância
    f. Criando 'snapshots' de instâncias
    g. Comparação com AWS EC2

10. Glance: serviço de imagens do OpenStack;
    a. Gerenciando imagens
    b. Usando 'snapshots' de imagens
    c. Proteção de imagens
    d. Desativação de imagens
    e. Comparação com AWS EC2 Image Builder

11. Cinder: serviço de disco virtual do OpenStack;
    a. Criando serviço de volumes com Cinder
    b. Vinculando um volume a uma instância
    c. Desvinculando um volume de sua instância
    d. Removendo volumes
    e. Gerando 'snapshots' de volumes
    f. Habilitando a criptografia de volumes
    g. Comparação com AWS EBS

12. Swift: Armazenamento de Objetos com OpenStack;
    a. Criando e removendo 'buckets' de objetos
    b. Alimentando 'buckets' com objetos pequenos e grandes
    c. Fazendo o 'download' de objetos
    d. Removendo objetos
    e. Comparação com AWS S3

13. Magnum: Orquestração de Containers do OpenStack;
    a. Escolhendo o ambiente de orquestração de containers
    b. Kubernetes ou Docker Swarm
    c. Monitoração de containers

Habilidades

- Criar um Docker container com serviço web;
- Testar a performance do serviço web no Docker container com diferentes níveis de RAM e CPU;
- Usar OpenStack Nova para criar uma máquina virtual com uma imagem fornecida pelo desenvolvedor;

- Usar OpenStack Glance para criar uma máquina virtual com uma imagem customizada com o Docker container criado;
- Levantar uma instância desta máquina virtual com serviço web;
- Levantar uma instância com serviço de armazenamento de objetos Swift oferecendo o Docker container criado;
- Testar a performance da máquina virtual e serviço com diferentes níveis de RAM, CPU e IOPS;
- Montar um volume remoto e um volume local na instância sendo executada;

Atitudes

- Desenvolvimento do raciocínio lógico e criativo para resolução de problemas com base nas tecnologias de containers e nuvem.
- Autonomia para analisar problemas reais e desenvolver soluções computacionais

Referências:

Bibliografia Básica:

VITALINO, J.F. e CASTRO, M.A. **Descomplicando o Docker**, 2a Edição, Editora Brasport, 2018.
JACKSON, K., et al. **OpenStack Cookbook**, Editora Packet Publishers, 2018.
FIFIELD, T. et al. **OpenStack Operations Guide: Set Up and Manage Your Openstack Cloud**. Editora O'Reilly, 2014.

Bibliografia Complementar:

COCHRANE, K.et al. **Docker Cookbook**, Editora Packet Publishers, 2018.
KANE, S. e MATTIAS, K. **Docker: Up & Running: Shipping Reliable Containers in Production**. Editora O'Reilly, 2018.
MOUAT, A**. Using Docker: Developing and Deploying Software with Containers**. Editora O'Reilly, 2015.
SILVERMAN, B. e SOLBERG, M. **OpenStack for Architects - Second Edition: Design production-ready private cloud infrastructure**, 2a Edição. Editora PacktPub, 2018.
KHEDER, O. e DUTTA, C. **Mastering OpenStack - Second Edition: Design, deploy, and manage clouds in mid to large IT infrastructures**. Editora PacktPub, 2017.

Segurança Ofensiva: Aplicações Web

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Segurança Ofensiva: Aplicações Web		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
60h	4 aulas por semana	Quarto semestre

Ementa:

Revisão de programação javascript; revisão do protocolo HTTP; projeto OWASP Top 10; Interceptação da comunicação Cliente/Servidor com *proxy*; Reconhecer e mitigar vulnerabilidades do tipo *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF), Injeção de código SQL; Auditar a segurança de sistemas de autenticação básicos em Aplicações Web

Objetivos

- Pesquisar quais são as vulnerabilidades mais comuns da atualidade em aplicações web, através do projeto OWASP Top 10
- Domínio básico no uso das ferramentas de desenvolvedores ('devtools') em um ou mais navegadores
- Explicar as vulnerabilidades do tipo *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF) e Injeção de código SQL
- Determinar se uma aplicação web é vulnerável a ataques de *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF) ou Injeção de código SQL
- Explicar as formas de autenticação mais seguras para aplicações web
- Determinar se um esquema básico de autenticação em aplicação web é implementado de forma segura

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Programar em *javascript* no contexto do navegador web
    a. Javascript & HTML básicos;
    b. Alteração de nodos na árvore DOM
    c. Ferramenta DevTool do Navegador;
        i. aba Console;
        ii. aba Network/Rede;
    d. comandos 'alert()' e 'print()' do *javascript*
2. Entender o protocolo HTTP
    a. Mensagens GET e POST
    b. Cabeçalhos no pedido do cliente
    c. Cabeçalhos na resposta do servidor
    d. Como um 'cookie' é representado
3. A Fundação OWASP e o Projeto OWASP Top 10
4. Reconhecer vulnerabilidades do tipo *Cross-Site Scripting* (XSS)
5. Reconhecer vulnerabilidades do tipo *Cross-Site Request Forgery* (CSRF)
6. Reconhecer vulnerabilidades do tipo Injeção de código SQL
7. Saber utilizar ferramentas de monitoração da comunicação Cliente/Servidor via interceptação com *proxy*
    a. configuração de navegador para operação com proxy;
    b. Proxies: ZAP proxy, da OWASP e Burp Suite, da PortSwigger
        i. 'Scanning' e 'Spidering'
        ii. Avaliando validação de dados lidos pela aplicação web
        iii. Emulando ataques ao cliente: 'clickjacking', injeção de HTML e execução de *javascript*
8. Auditar a segurança de sistemas de autenticação em Aplicações Web:
    a. Testando enumeração de contas e existência de contas previsíveis
    b. Testando a eficiência de mecanismos de suspensão de contas suspeitas
    c. Testando técnicas para burlar mecanismos de autenticação
9. Auditar o gerenciamento de 'token' de sessão:
    a. Avaliar a solidez do 'token' de sessão

b. Testando atributos de ‘cookies’
c. Verificar o vazamento de variáveis de sessão
d. Verificar a ocorrência de *Cross-Site Request Forgery* (CSRF)

Habilidades

1. Explicar a ferramenta para desenvolvedores disponibilizada em um navegador (‘devtool’) e seu uso para levantamento de informações e avaliação de vulnerabilidades de uma aplicação web.
2. Utilizar a aba ‘console’ na interface ‘devtool’ para verificar mensagens
3. Saber observar a troca de mensagens entre cliente e servidor na aba ‘network’ da interface ‘devtool’
4. Usar *javascript* para gerar uma janela de alerta no navegador com comando `alert()`
5. Usar *javascript* para gerar mensagens na console do navegador com comando `print()`
6. Usar *javascript* para modificar a estrutura DOM de um documento web.
7. Analisar a classificação das 10 principais vulnerabilidades em aplicações web, segundo o projeto OWASP Top 10
8. Explicar qual a diferença entre as vulnerabilidades *Cross-Site Scripting* (XSS) e *Cross-Site Request Forgery* (CSRF)
9. Explicar quais são os principais cabeçalhos a serem observados para isolamento de vulnerabilidades de diferentes tipos
10. Explicar a diferença entre os vários *proxies* disponíveis para interceptação de comunicação entre Cliente e Servidor
11. Instalar e configurar um *proxy* para interceptação de comunicação entre Cliente e Servidor
12. Preparar um relatório de vulnerabilidades potenciais a partir das informações coletadas pelo *proxy* de interceptação de comunicação entre Cliente e Servidor
13. Determinar se scripts SQL poderão ser explorados para teste de vulnerabilidade em uma aplicação web.

Atitudes

- Ser autônomo e assertivo para realizar configurações básicas em ferramentas *proxy*;
- Ser ciente do funcionamento eficaz de uma aplicação web de baixo volume de acesso;
- Ser analítico, reflexivo e crítico quanto ao uso de estratégias para mitigar vulnerabilidades web

Referências:

Bibliografia Básica:

DUCKETT, J. **HTML e CSS**: projete e construa websites. 1. ed. Rio de Janeiro: Alta Books, 2016.
DUCKETT, J. **Javascript e Jquery**: Desenvolvimento de Interfaces Web Interativas. 1. ed. Rio de Janeiro: Alta Books, 2016.
HAVERBEKE, M. **Eloquent Javascript**: A Modern Introduction to Programming, 3 edition, No Starch Press, 2018.

Bibliografia Complementar:

PRUTEANU, A. **Manual do Hacker: Aprenda a Proteger Aplicações web Conhecendo as Técnicas de Pentest Utilizadas Pelos Hackers**. Editora Novatec, 2019.
SILVA, M.S**. Fundamentos de HTML5 e CSS3**. Editora Novatec, 2015.
WEAR, N. **Burp Suite Cookbook**. PacktPub, 2018.
FLANAGAN, D. **JavaScript**: The Definitive Guide. 7. O’Reilly, 2020.
HOFFMAN, A. **Web Application Security: Exploitation and Countermeasures for Modern Web Applications**, Editora O’Reilly, 2020.

Empreendedorismo

Campus: Cabo Frio		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Empreendedorismo		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30h	2 aulas por semana	Quarto semestre

Ementa:

Conceitos e fundamentos do empreendedorismo. Técnicas e ferramentas para modelagem e concepção de uma ideia ou negócio.

Objetivos

- Planejar e executar projetos
- Realizar brainstorms
- Dimensionar recursos
- Definir e organizar metas
- Diagnosticar oportunidades
- Desenvolver soluções

Conteúdos, Habilidades e Atitudes

Conteúdos

Fundamentos do empreendedorismo;
Business Model Canvas
Fundamentos de um MVP
Criação prática de um MVP
Conceitos para criação de um negócio on-line

Habilidades

- Conhecer e aplicar a estratégia de Business Model Canvas
- Criar um MVP para resolução de um problema
- Elaborar uma estratégia de negócio on-line

Atitudes

- Autonomia para elaborar uma ideia de negócio;
- Atitude na descoberta e resolução de problemas;
- Resiliência em momentos de incerteza no mercado;
- Autodidata na busca de novos conhecimentos em empreendedorismo e TI

Referências:

Bibliografia Básica:

RIES, E. A startup enxuta. Editora Sextante, 2019
CAROLI, P. Lean Inception: Como alinhar pessoas e construir o produto certo. Editora Caroli, 2018
BROWN, T. Design Thinking. Editora Elsevier, 2010.

Bibliografia Complementar:

KNAPP, J.; ZERATSKY, J.; KOWITZ, B. Sprint. O Método Usado no Google Para Testar e Aplicar Novas Ideias em Apenas Cinco Dias. Editora Intrínseca, 2017.
SUTHERLAND, J. & SUTHERLAND, J.J. SCRUM: a arte de fazer o dobro do trabalho na metade do tempo. Editora Sextante, 2019.
OSTERWLADER, A. & PIGNEUR, Y. Business Model Generation: Inovação Em Modelos De Negócios. Editora Alta Books, 2011.
FINOCCHIO, J. J. Project Model Canvas. Editora Elsevier, 2013

Inteligência Artificial Aplicada à Segurança Cibernética

***Campus*: Cabo Frio**		
Curso:		**Eixo Tecnológico:**
Curso Técnico em Segurança Cibernética		**Informação e Comunicação**
Componente Curricular		**Ano de Implantação**
Inteligência Artificial Aplicada à Segurança Cibernética		**2023**
Carga Horária	**Aulas por Semana:**	**Período Letivo**
30h	2 aulas por semana	Quarto semestre

Ementa:

Introdução ao Aprendizado de Máquina; Detectando ameaças à Segurança; Protegendo informações sensíveis e ativos; Redes Adversárias Generativas; Ética na Inteligência Artificial.

Objetivos

• **Geral:**

- Descrever, de forma eficaz e crítica, conceitos básicos de Aprendizado de Máquina aplicados à Segurança Cibernética.

• **Específicas:**

- Compreender os conceitos básicos para seleção de modelo em tarefas de aprendizagem supervisionada e não supervisionada no contexto da segurança cibernética.
- Desenvolver algoritmos básicos de Aprendizado de Máquina para tarefas de Aprendizado Supervisionado e Não Supervisionado no contexto da Segurança Cibernética.
- Identificar e compreender meios de enfrentar os desafios legais e éticos que surgem da coleta de dados sobre seres humanos e de usá-los para construir modelos de aprendizado de máquina.

Conteúdos, Habilidades e Atitudes

Conteúdos

1. Introdução ao Aprendizado de Máquina
    a. Tipos de Aprendizado de Máquina
        i. Aprendizado Supervisionado
        ii. Aprendizado não Supervisionado
        iii. Aprendizado por Reforço
    b. Arquitetura do Aprendizado de Máquina
        i. Aquisição, limpeza e manipulação de dados
        ii. Escolha de atributos
        iii. Treinamento do modelo
        iv. Validação do modelo
    c. Aprendizado de Máquina no Contexto da Segurança Cibernética

2. Detectando Ameaças à Segurança com o Aprendizado de Máquina
    a. Detecção de ameaças à segurança em mensagens de email
        i. Técnicas de conversão de texto em valores numéricos
        ii. Detecção de Spam
        iii. Detecção de Phishing
    b. Detecção de Malware
        i. Análise de Malware
        ii. Estratégias de detecção de Malware
        iii. Agrupando Malware
    c. Detecção de Anomalias
        i. Técnicas de detecção de anomalias de rede

ii. Classificando ataques de rede
iii. Algoritmos de Aprendizado de Máquina para detecção de Botnets
iv. Desafios no uso de Aprendizado de Máquina para detecção de anomalias

3. Protegendo Informações Sensíveis e Ativos
    a. Prevenção de abusos na autenticação
    b. Prevenção de fraudes
    c. Redes Adversárias Generativas
        i. Envenenamento do Modelo
        ii. Ataques de Evasão
        iii. Ataques ao Reconhecimento Facial

4. Ética na Inteligência Artificial
    a. Modelos e limitações de algoritmos de inteligência artificial
    b. Equidade e Bias nos dados
    c. Privacidade e conveniência na inteligência artificial

Habilidades

- Detectar anomalias, incluindo violações, fraude e falha iminente de sistemas;
- Conduzir análises de malware extraindo informações úteis de binários de computador;
- Detectar invasores dentro de uma rede, encontrando padrões nos conjuntos de dados;
- Entender as ameaças que os invasores representam para o aprendizado de máquina;
- Compreender a equidade, transparência e explicabilidade em modelos de Aprendizado de Máquina de Segurança Cibernética

Atitudes

- Autonomia e segurança para identificar, classificar e descrever modelos de aprendizado de máquina aplicados à segurança cibernética;
- Atitude crítica quanto ao uso de diferentes modelos de aprendizado de máquina a problemas de segurança cibernética.

Referências:

Bibliografia Básica:

GÉRON, A.. **Mãos à Obra: Aprendizado de Máquina com Scikit-Learn & TensorFlow,** Alta Books, 2019.
NORVIG, P. e RUSSEL, S. **Inteligência Artificial**, Elsevier, 3a edição, 2013.
HARRISON, M. **Machine Learning – Guia de Referência Rápida: Trabalhando com dados estruturados em Python**, Novatec Editora, 2019.

Bibliografia Complementar:

HENKE, Marcia; SANTOS, Clayton; NUNAN, Angelo Eduardo; FEITOSA, Eduardo Luzeiro. **Aprendizagem de Máquina para Segurança em Redes de Computadores: Métodos e Aplicações**, em Livro de Minicursos do XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, pp.55-105, Capítulo 2, Novembro de 2011.
NETO, Amílcar; MACIEL, Francisco. **Python para Data Science e Machine Learning descomplicado**, Rio de Janeiro: Alta Books, 2021.
HAYKIN, Simon. **Redes Neurais: Princípios e Prática**, 2a edição, Porto Alegre: Bookman, 2007.
LUGER, George F. **Inteligência Artificial**, 6a edição, São Paulo: Pearson Education do Brasil, 2013.
TAULLI, Tom. **Introdução à Inteligência Artificial - uma abordagem não técnica,** Novatec Editora Ltda, 2020.

4.5. INDISSOCIABILIDADE ENTRE ENSINO, PESQUISA E EXTENSÃO

O princípio da indissociabilidade entre ensino, pesquisa e extensão reflete um conceito de qualidade do trabalho acadêmico favorecendo a aproximação entre instituição de ensino e sociedade, a autorreflexão crítica, a emancipação teórica e prática dos estudantes e o significado social do trabalho acadêmico. Tal conceito reflete a própria missão e as respectivas atividades do Inmetro, cuja natureza encontra-se na pesquisa, no compartilhamento do conhecimento e na ação conjunta que o Instituto desenvolve com a sociedade brasileira e internacional.

Dessa forma, no âmbito do Acordo de Cooperação entre o Inmetro e o IFFluminense, o ensino, pesquisa e extensão são indissociáveis, pois a articulação entre os mesmos fornece conhecimentos, propostas de investigação e espaços para diferentes programas, projetos e cursos, incluindo também a perspectiva da formação política. Logo, confere-se à pesquisa a premissa de transformar-se em elo entre as necessidades da sociedade (Extensão) e o conhecimento acadêmico (Ensino), conjugando o saber, fazer e transformar por meio das produções técnico-científicas do curso, tais como: relatórios técnicos, artigos (conferências e periódicos) e trabalhos de conclusão de curso, conforme preconizado com seu PPI.

Em consonância com o PPI, o Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio articula o ensino, pesquisa e extensão fornecendo conhecimentos, propostas de investigação e espaços para diferentes atividades. Tal articulação propicia a identificação de novos problemas e para a proposição de projetos, que articulem, de maneira interdisciplinar, a investigação, a apropriação de conhecimento e a intervenção social. Por meio disso, o curso busca estabelecer um diálogo contínuo e permanente com a comunidades com a comunidade e com órgãos

Nesse sentido, estimula-se a pesquisa como princípio pedagógico, de modo que discentes e docentes possam juntos ir além da descoberta científica, ou seja, se comprometendo com a humanidade acerca da conjugação do saber, do fazer e do transformar. Os novos conhecimentos produzidos pelas pesquisas deverão estar colocados a favor dos processos produtivos locais e regionais, buscando reconhecimento e valorização dos mesmos no plano nacional e global (IFFLUMINENSE, 2018a).

Do ponto de vista da especificidade, no referido curso, a indissociabilidade entre ensino, pesquisa e extensão terá como objeto a produção e divulgação de ciência e tecnologia que, por meio do emprego da segurança da informação, permitam o enfrentamento dos problemas locais e regionais. Dessa forma, pretende-se alcançar o potencial transformador do conhecimento enquanto promotor da qualidade de vida com a sustentabilidade e a democracia. Nesse contexto, insere-se o compromisso com a inovação, compreendida tanto como resultados em termos de processos e produtos que contribuam para o desenvolvimento local e regional, sem perder de vista a sustentabilidade e a inclusão, quanto como o desenvolvimento de novas soluções e, com isso, contribuindo com o desenvolvimento da ciência.

5. PRÁTICA PROFISSIONAL

O Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio traz em sua natureza a prática profissional, especialmente por ter como docentes pesquisadores do Inmetro, que em seu dia a dia atuam nos laboratórios do instituto. Portanto, a Prática Profissional encontra-se presente nos mais diversos componentes curriculares em que se aplica, devendo ser desenvolvida ao longo de todo o curso.

A prática profissional compreende diferentes situações de vivência, aprendizagem e trabalho, com atividades específicas em ambientes especiais, empresas e outros, bem como investigação sobre atividades profissionais, projetos de pesquisa, extensão e/ou intervenção, visitas técnicas, simulações, observações, planejamento e execução de projetos concretos e experimentais característicos da área, participação em seminários, palestras, oficinas, minicursos e feiras técnicas, que promovam o contato real ou simulado com a Prática Profissional pretendida pela formação técnica, as quais serão fomentadas, também, por meio do componente curricular Prática Profissional, sob supervisão da Coordenação do Curso (Ver Figura 5).

Figura 5: A Prática Profissional no Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio.

Audiodescrição: Imagem vertical de pirâmide segmentada, tipo um quebra-cabeça colorido de triângulo equilátero. São quatro peças com contorno branco de cores diferentes, com uma palavra ao centro escrita em branco. Ao centro, peça verde com Segurança Cibernética; acima, peça vermelha com Ensino; na base direita, peça azul com Pesquisa; na base esquerda, peça amarela com Extensão. Fim da audiodescrição[5].

Adaptado de: https://portal1.iff.edu.br/nossos-campi/itaperuna/cursos/cursos-tecnicos/projetos-pedagogicos-dos-cursos-tecnicos/ppc-do-curso-tecnico-em-quimica/projeto-pedagogico-do-curso-tecnico-concomitante-em-quimica-turmas-ingressantes-a-partir-de-2020/view Acesso em: 28 abr. 2022.

[5] Audiodescrição produzida pela audiodescritora Loide Aragão e pelo consultor Renato Ferreira da Costa.

6. ESTÁGIO SUPERVISIONADO NÃO OBRIGATÓRIO

Não há estágio obrigatório para o Curso Técnico em Segurança Cibernética Concomitante ao Ensino Médio. Consideramos que o estudante, a partir do relacionamento entre teoria e prática, compartilhada em aulas laboratoriais, visitas técnicas, seminários, palestras, e, sobretudo, por meio da disciplina Prática Profissional, estará em condições de contextualizar e colocar em ação o aprendizado, razão pela qual optamos por ofertar o estágio não-obrigatório.

O estágio não-obrigatório poderá ser realizado após o estudante perfazer, no mínimo 50% (cinquenta por cento) da carga horária total do curso, como atividade opcional, acrescida à carga horária regular, desde que o estudante esteja matriculado. A carga horária, duração e jornada de estágio, a serem cumpridas pelo aluno, devem sempre ser compatíveis com sua jornada escolar, de forma a não prejudicar suas atividades escolares.

O estágio visa ao aprendizado de competências próprias da atividade profissional e à contextualização curricular, objetivando o desenvolvimento do educando para a vida cidadã e para o trabalho.

O estágio-não obrigatório não acarreta vínculo empregatício de qualquer natureza e deve ser realizado no próprio Inmetro ou, ainda, em empresas ou instituições de direito público ou privado, devidamente conveniadas com o IFF, que apresentem condições de proporcionar complementação à aprendizagem.

Caso o aluno opte por realizar o estágio, será́ designado um professor responsável pela orientação do aluno e articulação com os laboratórios do próprio Inmetro nos quais o estágio se realizará. O aluno terá́ a carga horária deste registrada no seu histórico escolar. Em consonância com a Resolução CNE/CEB 01/2004, a carga horária do estágio profissional não poderá́ exceder seis horas diárias, perfazendo 30 horas semanais, e poderá́ ser realizado a partir da demanda do aluno e/ou de organizações da comunidade.

A Resolução do Conselho Superior Nº 34, de 11 de março de 2016 apresenta o Regulamento Geral de Estágio do IFFluminense e aponta que, para a realização do estágio supervisionado, obrigatório ou não obrigatório, devem ser observados os seguintes requisitos:

I. o estudante deve estar matriculado e frequentando um dos cursos indicados no Artigo 1º

II. o estudante deverá ter cumprido uma carga horária mínima do curso, caso esteja definida no plano pedagógico do curso;

III. a celebração do termo de compromisso de estágio (TCE) entre o estudante, a instituição de ensino e a concedente do campo de estágio;

IV. a compatibilidade entre as atividades desenvolvidas no estágio e aquelas previstas no plano de atividades de estagiário (PAE) contido no TCE;

V. contratação em favor do estagiário de seguro contra acidentes pessoais.

7. PROGRAMAS DE EXTENSÃO, DE INICIAÇÃO CIENTÍFICA E PROJETOS DE PESQUISA

As atividades de extensão realizadas pelo Inmetro são indissociáveis à pesquisa e ao ensino. Procuram integrar o curso técnico com a comunidade local por meio de cursos, palestras, visitas, suporte e orientação técnica e educacional. Assim, busca-se atuar no contexto local e do mercado de trabalho, não só por meio da formação de mão de obra, mas intervindo nos problemas e buscando soluções que possam contribuir para ofertar qualidade de vida e acesso à arte, à cultura, à informação e à formação.

Os programas e projetos de extensão também propiciam a oportunidade de tornar a escola mais viva e vibrante. Se o conhecimento é considerado um valor inestimável, colocar esse conhecimento em prática e disseminá-lo é compartilhar com outros aquilo que se tem de mais valioso e, ao mesmo tempo, multiplicar esse mesmo bem.

Nessa direção, todos os estudantes do Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio poderão pleitear bolsas no IFF, uma vez que possua o perfil estabelecido para tal. Alternativamente, o INMETRO poderá ofertar bolsas para os estudantes deste curso realizado em parceria, sendo tal ação, da competência do mesmo.

O Inmetro, por meio do Programa Nacional de Apoio ao Desenvolvimento da Metrologia, Qualidade e Tecnologia (Pronametro), realiza concessão de bolsas para especialistas, técnicos e estudantes que contribuam para projetos nas áreas de pesquisa e desenvolvimento científico, tecnológico e institucional.

As bolsas Pronametro são concedidas por meio de editais dos quais podem participar desde estudantes técnicos de nível médio até pesquisadores com títulos de doutor. O processo de seleção avalia a formação do candidato, suas competências e sua aptidão à execução de projetos de pesquisa do interesse do Inmetro. Os selecionados podem realizar seus trabalhos em outras instituições, incluindo empresas públicas e privadas – por meio de Acordo de Cooperação com o Inmetro. A implementação das bolsas consta na Lei 12.545, de 14 de dezembro de 2011.

O Inmetro também participa do Programa Institucional de Bolsas de Iniciação Científica para o Ensino Médio (PIBIC-EM) do CNPQ, que tem por objetivo de despertar vocação científica e incentivar jovens talentos provenientes do ensino médio mediante sua participação em atividades de pesquisa científica ou tecnológica, envolvendo-os com os desafios atuais da Ciência e com a metodologia do trabalho científico, sob a orientação de pesquisadores do Inmetro. Por meio de editais, são ofertadas vagas aos discentes dos cursos técnicos, oportunizando o desenvolvimento do senso crítico e a interação com pesquisadores do Inmetro, de maneira única e direta, possibilitando a construção coletiva do conhecimento aos alunos dos cursos técnicos.

Pretende-se, ainda, que à medida que o novo curso amadureça, propor um conjunto de práticas a serem implementadas, de modo a contribuir para o desenvolvimento da sociedade, constituindo um vínculo que estabeleça troca de conhecimentos e experiências, com permanente avaliação e evolução da extensão e da pesquisa.

8. OFERTA DE COMPONENTES CURRICULARES POR EAD

O Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio prevê a oferta de seus componentes curriculares na modalidade a distância, nos quais a mediação didático-pedagógica nos processos de ensino e aprendizagem ocorre por meio de Tecnologias de Informação e Comunicação (TIC), com estudantes e profissionais da educação desenvolvendo atividades educativas em lugares e tempos diversos. Contudo, o curso prevê a carga horária presencial de 20%, conforme previsto na Resolução CNE/CEB nº 6/2012. Na matriz curricular deste PPC está definida a carga horária a distância e presencial de cada componente curricular.

Entende-se que a oferta do curso na modalidade a distância auxilia na flexibilidade do estudo, dando maior autonomia para que o estudante que realiza um a formação técnica concomitante à formação básica em outra instituição de ensino. No mais, a própria natureza e temática do curso – Segurança Cibernética – já favorece a adoção do uso de TICs no processo de ensino e aprendizagem.

A oferta de componentes curriculares a distância inclui métodos e práticas de ensino e aprendizagem que incorporem o uso integrado de TICs e de um ambiente virtual de aprendizagem para a realização dos objetivos pedagógicos, bem como prever encontros presenciais e atividades de tutoria. Nesse sentido, propõe-se que conteúdos conceituais dos componentes curriculares em EAD sejam ofertados por meio de videoaulas, *podcasts*, aulas interativas *on-line*, textos e resolução de questões. Em seguida, em encontro presenciais, professores e alunos debatem, ampliam e contextualizam o conhecimento, conforme definido no item “Metodologia” deste PPC.

Abaixo encontra-se o detalhamento da infraestrutura tecnológica e de interação. Cabe ressaltar que todo esse curso segue as orientações contidas na Instrução Normativa nº 2/2021 - PROEN/REIT/IFFLU, de 17 de agosto de 2021.

8.1. AMBIENTE VIRTUAL DE APRENDIZAGEM (AVA)

As atividades virtuais do Curso Técnico em Segurança Cibernética serão desenvolvidas utilizando-se primordialmente o ambiente virtual de aprendizagem *Modular Objected Distance Learning* – MOODLE e o *Google for Education*. O primeiro é um software de fonte aberta que viabiliza o gerenciamento de cursos a distância, orienta professores e alunos, oportunizando a realização das atividades propostas, possibilitando o acesso a um ambiente específico onde são realizados os estudos e procedimentos acadêmicos. O segundo é um ambiente proprietário de apoio ao *e-learning* da empresa Google, com a qual o INMETRO possui parceria.

O MOODLE é um AVA para a administração de cursos na Web, criação e participação que se sustenta na interação entre professores, tutores e alunos, representando ferramentas de comunicação síncrona e assíncrona. Ele destaca-se de outros AVAs devido a sua facilidade operacional e sua condição de *software* livre.

Os docentes e discentes podem se comunicar por meio dos fóruns, chat e mensagens no MOODLE, o que permite ao estudante esclarecer suas dúvidas, o tutor enviar comunicados entre outras funções. Os materiais, recursos, atividades e avaliações são disponibilizadas por meio das ferramentas citadas, assim como as notas são disponibilizadas pela ferramenta livro de notas.

Como AVA adicional, o Inmetro disponibiliza o *Google Classroom*, onde os professores podem publicar tarefas e acompanhar atividades, inserir comunicações no mural, inserir materiais de apoio e, em especial, agendar e realizar encontros síncronos. Por meio do *Google Classroom* ainda é possível a disponibilização de uma conta de e-mail institucional a cada integrante.

O acompanhamento da frequência do estudante deve ser avaliado por meio de atividades que demandem participação diferenciada das atividades presenciais. Para aprovação, o estudante deve, juntamente com o desempenho, possuir frequência mínima de 75% (setenta e cinco por cento) e será computada através da realização de atividades a distância disponibilizadas no AVA, em cada componente curricular ofertado na modalidade a distância.

Nas atividades presenciais dos componentes curriculares ofertados na modalidade a distância deste PPC o estudante deverá participar de, no mínimo, 75% (setenta e cinco por cento) para obter aprovação.

O material didático do curso, como videoaulas e apostilas, deve ser elaborado pelo professor do componente curricular com apoio da equipe técnica do Centro de Capacitação do Inmetro. O material é validado pela coordenação do curso, considerando sua abrangência, aprofundamento e coerência teórica, sua acessibilidade metodológica e instrumental e a adequação da bibliografia às exigências da formação, com linguagem inclusiva e acessível, com recursos comprovadamente inovadores. O material didático é disponibilizado aos discentes no MOODLE.

Caso seja necessária a distribuição de material impresso, o professor deverá entrar em contato com a coordenação do curso, a qual organizará as impressões à secretaria do curso, garantindo desta forma a continuidade de funcionamento do componente curricular.

8.2. ATIVIDADES DE TUTORIA

Considerando que nenhum componente curricular será ofertado totalmente a distância, a tutoria será desempenhada pelo próprio professor responsável pela disciplina, o qual deve prestar esclarecimentos aos estudantes em relação ao processo de ensino e aprendizagem e ao uso do ambiente virtual de aprendizagem, monitorar as atividades, realizar as avaliações e lançar as notas e frequências no ambiente virtual de aprendizagem e no Sistema Acadêmico Institucional.

O papel desempenhado pelo docente em componentes curriculares com carga horária EAD é de extrema relevância, devendo primar pela orientação dos processos de aprendizagem dos discentes. Nessa direção, todos os componentes curriculares híbridos preveem aulas e atividades presenciais, com o objetivo de interação entre discentes e professores, esclarecimentos de dúvidas, contextualização e ampliação dos saberes estudados a distância e avaliação da aprendizagem.

Para estabelecer comunicação efetiva com os estudantes, no início do semestre o docente deverá disponibilizar o calendário de aulas, apontando os dias e horários em que estará presencialmente no *Campus*. Além disso, deve proporcionar canais de comunicação virtuais e responder as mensagens em até dois dias úteis.

Um dos recursos mais valiosos na infra-estrutura tecnológica do curso é o portal educacional da Academia da Cisco, tradicional fabricante de software e equipamentos de rede de computadores e segurança cibernética.

Algumas das principais disciplinas do curso técnico utilizarão o material fornecido pelo portal educacional da Cisco. Permitirão o alinhamento da formação dos alunos ao perfil que o mercado procura nos jovens profissionais. Dentre os cursos do portal, algumas são preparatórias para exames de certificação profissional. Estes certificados são muito valorizados no mercado de trabalho, e estão ligados a uma formação inicial em Redes de Computadores e Segurança Cibernética.

Mais especificamente com relação a estas disciplinas preparatórias, a empresa Cisco exige que os instrutores façam curso de treinamento na plataforma de e-learning NetAcad, para que tenham contato com a plataforma em si assim como com todas as ferramentas da plataforma sob o ponto de vista de um aluno. Alguns dos docentes do curso, após treinamento intensivo, já estão acreditados pela empresa para treinamento preparatório para os exames de certificação profissional, como o *Cisco Certified Network Associate* – CCNA e *Cisco CyberOps Associate* – CBROPS.

Aos professores que não possuem formação específica para atuação em EAD, será ofertada uma Oficina ao início de cada ano letivo.

8.3 TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO (TIC) NO PROCESSO ENSINO-APRENDIZAGEM

Segundo a Instrução Normativa Nº 3 do IFFluminense (BRASIL, 2021b), as tecnologias de informação e comunicação (TIC) adotadas no processo de ensino e aprendizagem de

componentes curriculares EAD permitem a execução do projeto pedagógico do curso, garantem a acessibilidade digital e comunicacional, promovem a interatividade entre docentes, discentes e tutores, asseguram o acesso a materiais ou recursos didáticos a qualquer momento e lugar e possibilitam experiências diferenciadas de aprendizagem baseadas em seu uso.

No Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio, as TIC são capazes de oferecer experiências de aprendizagem que atendam diferentes necessidades e ritmos de aprendizagem, permitindo que os estudantes adequem melhor a rotina de estudo e trabalho. Além disso, as TIC estimulam novas habilidades nos discentes, como o gerenciamento e organização do estudo.

No Inmetro as tecnologias de informação e comunicação são constituídas por redes internas (Intranet), redes externas para acesso a pesquisa em websites, e-mails institucionais para servidores, equipamentos de videoconferência, computadores, impressoras e outros dispositivos e periféricos. Outras tecnologias utilizadas por servidores e docentes, por meio da parceria com o IFF, será o Sistema de Gestão Acadêmica.

Conforme já apontado, o Inmetro também oferta os AVAs MOODLE e Google Classroom, que funcionam como uma sala de aula on-line onde professores podem disponibilizar materiais didáticos e propor tarefas, como questionários e fóruns. Para os alunos, o ambiente facilita a troca de conhecimento e de arquivos multimídia.

O item deste PPC 14.4, Aplicação da Tecnologia da Informação e Comunicação apresenta maiores detalhes a respeito do uso das TICs e parcerias desenvolvidas para o Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio.

9. SISTEMAS DE AVALIAÇÃO

9.1. A AVALIAÇÃO DO ESTUDANTE

A avaliação do discente deve ser realizada de forma processual, ou seja, faz parte de todo o processo de ensino e de aprendizagem. Seu caráter é diagnosticador e formativo, com vista à formação integral do cidadão, sua preparação para o mundo do trabalho e a continuidade aos estudos. Propõe-se, portanto, a verificação do rendimento escolar por meio da avaliação contínua e cumulativa, sendo considerados aspectos qualitativos e quantitativos.

Considerada como um mecanismo intrínseco ao processo educativo, a avaliação dos estudantes deverá estar relacionada à concepção pedagógica do IFF e à natureza do componente curricular, circularizando os aspectos que devem ser a ela intrínsecos: processual, contínua, formativa, diagnóstica, inclusiva, democrática, dialógica e emancipatória.

A avaliação da aprendizagem deverá ser considerada em seu caráter permanente, acompanhar todo o processo educativo e ter seus registros em instrumentos avaliativos múltiplos e diversos, que não somente possibilitem o estágio de desenvolvimento dos estudantes, mas proporcionem aos profissionais da instituição a leitura do trabalho realizado para o necessário aperfeiçoamento do processo educativo.

No decorrer de cada disciplina, o professor realizará junto a turma avaliação diagnóstica a fim de verificar possíveis dificuldades e defasagem de conhecimentos prévios que são essenciais ao desenvolvimento dos conteúdos a serem abordados. Mediante este levantamento, o docente trabalhará para sanar as possíveis necessidades apresentadas pelo aluno.

Instrumentos avaliativos diversificados, conforme elencados abaixo, devem ser considerados no período letivo, a fim de traduzir o grau de desenvolvimento pessoal dos estudantes. Entre e outros instrumentos de avaliação, considerando o seu caráter progressivo, propõe-se:

a) observação diária dos estudantes pelos professores, durante a aplicação de suas diversas atividades;
b) trabalhos individuais e/ou coletivos;
c) fichas de observações;
d) provas escritas (com ou sem consulta);
e) provas práticas
f) provas orais;
g) seminários;
h) projetos interdisciplinares;
i) resolução de exercícios;
j) planejamento e execução de experimentos ou projetos;
k) relatórios referentes a trabalhos, experimentos ou visitas técnicas,
l) realização de eventos ou atividades abertas à comunidade;
m) autoavaliação descritiva.

9.1.1 CRITÉRIOS DE AVALIAÇÃO

a) Em relação ao aproveitamento

Os resultados obtidos pelos estudantes no decorrer do semestre letivo são considerados parte do processo de ensino e aprendizagem, no qual é esperado um aproveitamento mínimo de 60% (sessenta por cento) dos saberes previstos em cada componente curricular, em cada etapa. A frequência também é considerada como critério de promoção e, de acordo com as bases legais, é exigido o mínimo de 75% do total de horas letivas para aprovação.

b) Em relação à aplicação da avaliação

Devem ser aplicadas aos estudantes, por bimestre, no mínimo, 2 (dois) instrumentos avaliativos distintos, por componente curricular, sendo um individual, que corresponda entre 60% a 80% dos saberes previstos e pelo menos um deles, de elaboração coletiva.

Entende-se por "instrumento avaliativo de elaboração coletiva" trabalhos em grupos, pesquisas, jogos, seminários ou quaisquer outros que desenvolvam a convivência coletiva, a criação, a expressão oral, iniciativa e todos que colaborem para a formação do cidadão criativo e solidário.

c) Em relação ao registro de nota

A avaliação da aprendizagem deve acontecer no decorrer do processo bimestral e deve ser revertida em um único registro nota (numa escala de 0 a 10, com uma casa decimal) correspondente ao percentual de desenvolvimento dos saberes adquiridos.

O professor deverá registrar a nota bimestral no Sistema Acadêmico, observando os prazos constantes no Calendário Acadêmico do *Campus*. Já as atividades desenvolvidas, os conteúdos e a frequência dos estudantes a cada aula ministrada, deverão ser lançadas no Sistema Acadêmico.

d) Em relação à vista da avaliação

É direito do estudante ter acesso e posse aos instrumentos avaliativos logo após a correção.

e) Em relação à segunda chamada

O estudante que deixar de realizar um ou mais instrumentos avaliativos, no bimestre, terá direito à(s) atividade(s) avaliativa(s) que corresponda(m) ao percentual adotado nos outros instrumentos de avaliação que deixou de realizar, devendo justificar sua ausência à avaliação perante o professor/coordenação, preferencialmente acompanhado do(s) documento(s) que justifique(m) a ausência, conforme a Regulamentação Didático-Pedagógica do IFF.

f) Em relação à aprovação no componente curricular

Ao final do período letivo, é considerado APROVADO o aluno com um percentual mínimo de 75% (setenta e cinco por cento) de frequência da carga horária total trabalhada no módulo e um aproveitamento mínimo de 60% (sessenta por cento) dos saberes previstos em cada componente curricular. A média semestral corresponderá à média aritmética das notas do 1° e 2° bimestres e deverá ser maior ou igual a 6,0, seguindo a fórmula abaixo.

$$MS = (MB1 + MB2)/2 \geq 6,0$$

(Sendo, MS = Média Semestral; MB1 = Média do Bimestre 1; MB2 = Média do Bimestre 2.)

A partir do rendimento do estudante em cada um dos componentes curriculares, a situação de matrícula do período letivo assumirá uma das seguintes situações:

⇒ APROVADO: indicando que o estudante foi aprovado em todos os componentes curriculares tanto por nota quanto por frequência;

⇒ REPROVADO: indicando que o estudante foi reprovado em 01 (um) ou mais componente/s curricular/es no semestre letivo.

Convém ressaltar que o curso **NÃO prevê progressão parcial**, tendo em vista seu aspecto integrador. A ênfase será dada na recuperação paralela do discente, conforme descrito adiante, por meio de diversas estratégias de estudo e recuperação ao longo do semestre letivo.

g) Em relação à Recuperação Paralela

O professor deve promover, ao longo de todo período letivo, um processo de reconstrução dos saberes ao aluno que apresente dificuldades de aprendizagem durante a trajetória acadêmica, de forma contínua e paralela, objetivando alcançar seu melhor aproveitamento, sem a necessidade de esperar o fim do semestre letivo para tal.

Ao discente que não obtiver o rendimento mínimo de 60% no bimestre, será aplicada nova avaliação de recuperação, até o final de cada bimestre. A nota do bimestre terá peso 1 e a nota da recuperação terá peso 2 na composição da nova média bimestral, conforme fórmula abaixo.

$$NMB = [MB + (NRx2)]/3$$

(Sendo, NMB = Nova Média Bimestral; MB = Média do Bimestre; NR = Nota da Recuperação)

A Nova Média Bimestral substituirá a antiga Média do Bimestre, desde que a primeira seja maior que a última.

Essa avaliação de recuperação deve se dar no mínimo, uma semana após a divulgação do rendimento bimestral de cada componente curricular, no Sistema Acadêmico, observando o período de avaliações definido no Calendário Acadêmico. Para ter direito de participar do processo de recuperação do bimestre, o estudante deve ter, pelo menos, um registro de nota bimestral no componente curricular.

9.1.2 CRITÉRIOS DE AVALIAÇÃO DA APRENDIZAGEM PARA OS COMPONENTES CURRICULARES EM EAD

Os critérios de avaliação da aprendizagem para os componentes curriculares que ofereçam carga horária a distância são descritos na Instrução Normativa Nº 2 do IFFluminense, publicada em 2021 (BRASIL, 2021b).

Nos componentes curriculares a distância, deve ser garantida a equivalência de conteúdos e objetivos com os componentes curriculares presenciais, bem como o desenvolvimento das habilidades exigidas para a formação do estudante. Além disso, faz- se necessário que o professor do componente curricular elabore um calendário acadêmico, a ser publicado no AVA, contendo as datas das avaliações e atividades presenciais. A descrição das atividades deve ser descrita de forma clara nos Planos de Ensino de cada componente curricular.

Deve ocorrer, pelo menos, 1 (uma) avaliação presencial individual que represente, no mínimo, 60% (sessenta por cento) do valor total previsto para o componente curricular. Nos outros 40% (quarenta por cento), no máximo, a avaliação deve ocorrer por meio de atividades a distância.

Os componentes curriculares que realizarem atividades presenciais obrigatórias poderão utilizar avaliações referentes a estes momentos. Nesses casos, o somatório das avaliações das atividades presenciais com a avaliação presencial totalizará, no mínimo, 60% (sessenta por cento) do valor total do componente curricular.

O resultado do rendimento bimestral do aluno deve ser revertido em um único registro (numa escala de 0 a 10, com uma casa decimal). Ao final de cada semestre o estudante deve obter rendimento mínimo de 60%, calculado pela média aritmética dos rendimentos dos dois bimestres consecutivos que compõem o semestre letivo.

Ao final do período letivo, é considerado aprovado o aluno com um percentual mínimo de 75% (setenta e cinco por cento) de frequência da carga horária total trabalhada no período, e um aproveitamento mínimo de 60% (sessenta por cento) dos saberes previstos em cada componente curricular. A Média Anual para aprovação se obtém conforme já apontado no item 9.1.(Critérios de Avaliação), letra F.

Nos componentes curriculares ofertados na modalidade a distância, a frequência será computada por meio da da realização de atividades a distância disponibilizadas no AVA. Nas atividades presenciais desses componentes curriculares o estudante deverá participar de, no mínimo, 75% (setenta e cinco por cento) para obter aprovação.

O registro das atividades avaliativas deve ser realizado pelo professor, no AVA. Os resultados das etapas previstas no diário de classe também devem ser registrados pelo docente no Sistema Acadêmico Institucional.

9.2. AVALIAÇÃO DA QUALIDADE DO CURSO

O Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio utiliza-se dos seguintes mecanismos de avaliação:

9.2.1 AVALIAÇÃO DO PROJETO PEDAGÓGICO DO CURSO

Considerando o compromisso com a prestação de serviços de qualidade e a importância de uma avaliação contínua, o Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio será avaliado anualmente, utilizando o formulário de checagem, presente em anexo a este documento.

Os resultados serão utilizados não apenas para identificar as potencialidades e limitações do curso, mas também para aprimorá-lo continuamente.

9.2.2 CONSELHO DE CLASSE

O Conselho de Classe do Curso Técnico em Segurança Cibernética Concomitantes ao Ensino Médio será realizado em dois momentos: ao final do 1º bimestre e ao final do 2º bimestre. Nessa ocasião, reúnem-se o coordenador do curso, corpo docente, equipe pedagógica e representante do registro acadêmico com intuito de avaliar a aprendizagem dos estudantes e o processo de ensino.

O Conselho de Classe representa uma oportunidade para apontamento das dificuldades encontradas e das possíveis melhorias, favorecendo as estratégias mais adequadas à aprendizagem de cada turma e/ou estudante. Proporciona também uma avaliação conjunta por parte dos docentes em relação aos perfis das turmas, à adaptação e acompanhamento dos estudantes e à identificação e discussões em busca de soluções de situações pontuais que estejam prejudicando o rendimento escolar e a formação do aluno. Cabe ainda avaliar o trabalho educativo desenvolvido no período em questão, nos diferentes aspectos - discente, docente, metodológico – objetivando a construção e reformulação da prática educativa, em prol das necessidades curriculares e desenvolvimento do educando.

Vale ressaltar que, para o professor, a sua ausência deve ser justificada junto à Coordenação do Curso, dado o caráter de obrigatoriedade de participação.

Obs.: A análise da avaliação institucional do IFFluminense será considerada sempre que possível, visando identificar as fragilidades e potencialidades da instituição e seus cursos e nesse sentido, resultar na apresentação de propostas de melhorias.

9.3. AVALIAÇÃO DA PERMANÊNCIA DOS ESTUDANTES

A avaliação da permanência dos estudantes deve ser realizada em dois momentos. Inicialmente, avaliando o contexto imediato por meio de indicadores para tomada de decisão de curto e médio prazo. São eles: desempenho acadêmico dos discentes, participação de estudantes em projetos, evasão, retenção, trancamento de matrículas, número de estudantes cursando disciplinas em regime de progressão parcial e avaliação do corpo docente e da estrutura do curso pelo corpo discente.

Em um segundo momento, deve ser analisado o contexto amplo por meio de indicadores para avaliação de longo prazo. São eles: egressos aprovados em seleções de universidades e institutos públicos, empregados na iniciativa privada ou aprovados em concursos públicos, onde o diploma tenha proporcionado relevância no processo seletivo.

Em 2016, o IFFluminense realizou um estudo para investigar as principais causas de retenção e evasão, resultando no Plano Estratégico de Permanência e Êxito dos estudantes do Instituto Federal Fluminense 2017-2019, aprovado pela Portaria N° 23, de 06 de outubro de 2017 (BRASIL, 2017b). Este estudo propôs ações de intervenção em quatro dimensões, a saber:

1) Gestão

- Avaliação dos currículos escolares;
- Aprimoramento das metodologias de ensino;
- Aperfeiçoamento dos métodos avaliativos;
- Constituição de projetos pedagógicos de “resgate” de conteúdos escolares de fases anteriores.
- Promoção de monitorias observando os indicadores de retenção e os resultados avaliativos insatisfatórios.

2) Assistência estudantil

Criação de projetos de acompanhamento psicopedagógico e social dos estudantes;

Ampliação de projetos de assistência estudantil.

3) Orientação pedagógica ao acesso

- Divulgação dos cursos ofertados pelo instituto a comunidade para ajuste das expectativas de candidatos;
- Oferta de cursos que atendam a expectativa regional;
  pedagógica do processo ensino-aprendizagem
- Comunicação com a comunidade sobre as possibilidades de itinerários formativos ofertados na Instituição.

4) Vínculos entre o IFFluminense e a comunidade

- Aperfeiçoamento do diálogo: escola – poder público;
- Melhoria das relações: estudante-docente; estudante-coordenação/direção; estudante-setores administrativos da instituição;
- Aprimoramento das relações da escola – família;
- Aperfeiçoamento as relações entre escola – comunidade externa;

- Construção de calendários acadêmicos adaptados à realidade da comunidade.

As estratégias de intervenção devem ser planejadas a partir dos resultados dos indicadores e das ações do Plano Estratégico de Permanência e Êxito dos estudantes do Instituto Federal Fluminense e construídas coletivamente entre docentes, discentes e gestores. Além disso, será mantido diálogo com a Coordenação do Núcleo de Apoio ao Estudante (CONAE) e divulgado aos estudantes as ações realizadas por esse setor, tal como a bolsa de assistência estudantil e suporte psicológico.

10. CORPO DOCENTE

Conforme definido no Acordo de Cooperação Técnica entre IFF e Inmetro, os docentes do Curso Técnico em Segurança Cibernética concomitante ao ensino médio serão pesquisadores da Diretoria de Metrologia Científica do Inmetro, Diretoria de Metrologia Legal e de outras áreas do instituto.

Nome	Titulação	Regime de Trabalho	Área do Conhecimento de Atuação no Curso
Ana Carolina Pinto	Graduação	40h	Empreendedorismo
Antônio Lacerda Jr.	Mestrado	40h	Criptologia
Bruno Erthal	Mestrado	40h	Sistemas Embarcados e Programação de Sistemas
Carlos Eduardo Galhardo	Doutorado	40h	Segurança Defensiva e Programação de Sistemas
Cristiano Gurgel de Castro	Mestrado	40h	Sistemas Embarcados
Edson Seiti Miyata	Doutorado	40h	Empreendedorismo
Ewerton Longoni Madruga	Doutorado	40h	Segurança Ofensiva e Defensiva
Fernando Alves Rodrigues	Doutorado	40h	Programação de Sistemas
Flávia Paiva D'Agostini	Doutorado	40h	Políticas de Segurança e Inteligência Artificial
Paulo Roberto Mesquita Nascimento	Graduação	40h	Segurança Ofensiva e Tecnologias Móveis
Roberto Amaral	Graduação	40h	Sistemas Operacionais
Tatiana Claro dos Santos	Doutorado	40h	Metrologia
Wilson Mello Jr	Doutorado	40h	Criptologia e Redes de Computadores
Wladmir Chapetta	Doutorado	40h	Programação de Sistemas

11. SERVIDORES TÉCNICO-ADMINISTRATIVOS

NOME DO SERVIDOR	FORMAÇÃO	CARGO/FUNÇÃO
Luiz Fernando Rust da Costa Carmo	Doutor em Informática/Mestre em Mestrado em Engenharia de Sistemas e Computação/ Graduação em Engenharia Eletrônica	Especialista em Metrologia e Qualidade Sênior / Coordenador-Geral do Centro de Capacitação
Tatiana Claro dos Santos	Doutorado em Políticas Públicas e Formação Humana; Mestrado em Educação; Graduação em Pedagogia	Analista Executiva em Metrologia e Qualidade (Servidora) / Gestão Pedagógica dos Cursos
Beatriz P Guia	Mestrado em Educação, Arte e História da Cultura/ Graduação em Biblioteconomia	Analista Executiva em Metrologia e Qualidade (Servidora) / Bibliotecária
Giovanna Gomes Talon	Graduação em Biblioteconomia e Documentação	Técnica em Documentação I/ Bibliotecária

Cabe ressaltar que o Centro de Capacitação do Inmetro possui, ainda, 2 (dois) colaboradores (terceirizados) que atuam diretamente no apoio e secretaria dos cursos técnicos e 1 (uma) bolsista que atua no apoio ao laboratório didático.

No mais, os servidores do IFF - *Campus* Cabo Frio irão contribuir plenamente no que tange aos trâmites acadêmicos.

12. GRUPO DE TRABALHO

Visando a elaboração do projeto pedagógico do Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio, fruto da parceria do IFF e Inmetro, foram designados por meio da PORTARIA Nº 728/2021 - REIT/IFFLU, DE 6 DE OUTUBRO DE 2021, os seguintes membros:

- Fabrício Barros Gonçalves, IFF
- Tatiana Claro dos Santos, Inmetro
- Flávia Paiva Agostini, Inmetro
- Cristiano Gurgel de Castro, Inmetro
- Antônio Lacerda Júnior, Inmetro
- Paulo Roberto Nascimento, Inmetro
- Ewerton Longoni Madruga, Inmetro

13. GESTÃO ACADÊMICA DO CURSO (COORDENAÇÃO)

A coordenação do curso será realizada conjuntamente por um professor do IFF e uma servidora do Inmetro, possuindo, ainda uma coordenadora adjunta.

O coordenador do IFF será definido após a aprovação do PPC.

O Curso Técnico em Segurança Cibernética será coordenado, como representante do Inmetro, pelo Dr. Ewerton Longoni Madruga. O coordenador possui grau de Bacharel em Ciências de Computação pela Universidade Federal do Rio Grande do Sul (1990), mestrado em Computação pela Universidade Federal do Rio Grande do Sul (1994) e doutorado em Engenharia de Computação – University of California at Santa Cruz (2002). Atualmente é pesquisador do Instituto Nacional de Metrologia Normalização e Qualidade Industrial-RJ. Possui artigos publicados em revistas científicas e em anais de congressos internacionais. Suas áreas de interesse são sistemas móveis, sistemas multimídia para dispositivos móveis, computação em nuvem e segurança cibernética.

Informação Adicional	Link para acesso:
LinkedIn	https://www.linkedin.com/in/ewerton-madruga/
Currículo Lattes	http://lattes.cnpq.br/5597918477592415

14. INFRAESTRUTURA

14.1 CENTRO DE CAPACITAÇÃO

As aulas do Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio serão realizadas no *Campus* do Inmetro, em Xerém – Duque de Caxias, que conta com um dos melhores centros de pesquisa e tecnologia do Brasil, dispondo de 2,3 milhões de m² de área. Nele estão localizadas as salas de aula e laboratórios de pesquisa onde poderão ser realizadas visitas para contato com modernos equipamentos de pesquisa.

O Bloco F do Prédio 32, onde encontra-se o Centro de Capacitação, dispõe da seguinte infraestrutura para funcionamento do curso:

- 8 salas de aula, todas equipadas com ar, carteiras escolares, ar-condicionado tipo split e data show;
- 1 laboratório de informática;
- 1 auditório;
- 1 sala administrativa;
- 1 sala de reunião;
- 1 hall de convivência;
- Sanitários masculino e feminino; e
- 1 copa

14.2. BIBLIOTECA

A Biblioteca do Inmetro contribui com os Cursos Técnicos do Inmetro e Programas de Pós-Graduação, sendo uma extensão da sala de aula, capaz de prover: material bibliográfico especializado; subsídios para normalização dos trabalhos acadêmicos em geral; espaço de leitura, autoestudo, pesquisa e/ou orientação dos alunos pelos professores. Na Biblioteca, o aluno sempre poderá aprender, conhecer, estudar, pesquisar, consultar, referenciar.

Encontra-se instalada no 2º andar do prédio 6 do *Campus* do Inmetro e seu espaço divide-se entre os acervos bibliográficos, salas de estudo individuais e coletivas, salas de atividades técnico-administrativas, além de salão de leitura com 10 computadores para acesso à internet.

Entre suas atribuições, destacam-se:

- Adquirir, organizar, preservar e disponibilizar a produção científico-tecnológica do Inmetro, assim como materiais bibliográficos, referenciais e especiais adquiridos comercialmente;
- Prover pesquisa bibliográfica especializada;
- Disponibilizar salão de leitura, salas de estudo individuais/coletivas e acesso à internet para pesquisadores, alunos e visitantes;
- Elaborar fichas catalográficas nas publicações do Inmetro e trabalhos acadêmicos;
- Apoiar a normalização de trabalhos acadêmicos;
- Indexar artigos e legislação pertinente ao Inmetro;
- Prover acesso às normas técnicas nacionais, do Mercosul, estrangeiras e internacionais, por meio do Portal de Normas;
- Disponibilizar acesso ao Portal de Periódicos Capes;
- Emprestar materiais bibliográficos para o público interno, mediante cadastro;
- Disseminar informações/instruções quanto ao uso das bases de dados e sistemas da Biblioteca, para alunos, técnicos e pesquisadores;
- Gerenciar a Biblioteca On-line (catálogo de obras gerais) e o Repositório Institucional do Inmetro (Acervo Digital da Produção Intelectual do Inmetro).

A Biblioteca atende às comunidades interna e externa do Instituto, tendo acervos com características acadêmicas e técnico-científicas que cobrem a área de metrologia, avaliação da conformidade, qualidade, gestão, entre outras, conforme quadro abaixo:

Tipos de material do acervo da Biblioteca do Inmetro	**Quantidade de títulos**
Livros técnico-científicos	3.530
Livro de literatura (Clube do Livro)	299
TCC Curso técnico	460
Referência	309
Dissertações	407
Teses	46
CDs-ROM	176
E-books	35
Outras publicações	112
Total:	**5.374**

É possível consultar o acervo especializado pelo endereço eletrônico https://biblio.inmetro.gov.br/scripts/bnportal/bnportal.exe/index.

A Biblioteca também é responsável pelo **Repositório Institucional do Inmetro**, sendo possível consultá-lo no endereço eletrônico https://repositorio.inmetro.gov.br/xmlui/, para acessar a produção científica do Inmetro em formato digital, contando mais de 1.500 documentos.

O corpo funcional, entre bibliotecárias e atendentes, está disponível presencial ou remotamente, de 2ª a 6ª feira, das 8 às 16 h. O contato pode ser realizado por e-mail (biblioteca@inmetro.gov.br) ou por telefone (21-2679-9110).

14.3. INFRAESTRUTURA DE INFORMÁTICA

O Centro de Capacitação – Inmetro possui um laboratório com 21 estações de trabalho, sendo uma das estações posicionada para ser utilizada pelo(a) professor(a). Cada estação possui a seguinte especificação técnica:

Configuração de Estações de Trabalho	
Recurso	Especificação
CPU	Intel Core i7 de 8ª Geração, Seis Núcleos, 3.2 Ghz, 64 bits.
Memória RAM	16 Gb, DDR4 2400 Mhz
Disco Rígido	Interface SATA 3, 1 Tb
Placa de Vídeo	Controladora de vídeo integrado à placa-mãe com capacidade para controlar múltiplos monitores, possuindo um (01) conector do tipo DisplayPort e um (01) conector HDMI.
Monitor	23 polegadas, Full HD (1920x1080) a 60 Hz
Rede Wireless	Interface 802.11n
Rede Cabeada	Conector RJ-45, Ethernet, 1 Gbps
Sistemas Operacionais	Ubuntu 18.04 (Linux) e outros

As estações são configuradas para operar em vários sistemas operacionais, como no sistema operacional Linux, em regime de 'dual-boot'. Os recursos foram dimensionados para que sejam realizadas atividades de complexidade média, como usos de pacotes de software matemáticos para simulações, assim como edição de vídeos de curta duração e outros artefatos multimídia, sem prejuízo à atividade acadêmica sendo realizada em aula.

Cada estação está posicionada em uma mesa de trabalho, que comporta dois alunos (o que permite aulas práticas com até 40 alunos em modo presencial). Para apresentação de conteúdo, existe um quadro branco de 3 metros de largura e 1,5 metro de altura. Para as atividades multimídia, é disponibilizado um projetor multimídia, conectado à estação de trabalho do instrutor, e uma tela de projeção retrátil sobre o quadro branco.

14.4. APLICAÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Este projeto pedagógico foi concebido numa época muito incomum. Nunca se falou tanto em ensino remoto, e-learning, etc. como durante a pandemia de COVID-19. Durante um longo período, por conta das ameaças que a contaminação por este terrível vírus traz, as pessoas viram-se obrigadas a ficar em casa. As janelas de oportunidades profissionais ficaram mais abertas para aqueles trabalhadores familiarizados com tecnologias digitais. Quem não as dominava, precisou adaptar-se rapidamente.

A busca por tecnologia foi tamanha, que diversos fluxos passaram pelo processo de digitalização. De forma geral, o ser humano e a tecnologia nunca estiveram tão próximos. Esta tendência da digitalização de processos possivelmente continuará crescendo. E um dos setores que tem maiores condições de ser parcialmente digitalizado é o da educação. Existem barreiras para digitalização total em aula, sendo a execução da avaliação de alunos apenas uma delas.

Em consonância com esta tendência, para atender a demanda que se coloca a partir deste momento, o Curso Técnico em Segurança será lançado na modalidade à distância (EAD). Importante ressaltar a necessária observação da legislação vigente quanto ao tema, discutida anteriormente neste documento.

Emprego de e-learning e o EAD

O e-learning e o EAD não são excludentes, mas também não são sinônimos. EAD é a sigla que designa educação à distância. Ou seja, é o formato de ensino remotos que pode ser viabilizado por ferramentas digitais, inclusive pelas plataformas de e-learning. Já o e-learning, que geralmente é utilizado para EAD, é o ambiente de aprendizagem virtual.

Formatos de e-learning: síncrono vs. assíncrono

O e-learning, em geral, segue as seguintes características:

- ambiente virtual de aprendizagem;
- utilizado, em geral, para EAD;
- acessível via computadores, tablets e celulares.

O seu formato, porém, pode ser diferente conforme as estratégias. Por isso, antes de entender como o e-learning é utilizado no Curso Técnico em Segurança Cibernética, vale analisar os dois grandes meios de como ocorre esse método na prática. São eles: o e-learning síncrono e o e-learning assíncrono.

E-learning Síncrono

A grande diferença entre o e-learning síncrono e o assíncrono diz respeito, principalmente, ao espaço-tempo em que a aula ocorre. O e-learning síncrono ocorre quando o professor e o aluno estão em aula ao mesmo tempo. Geralmente, professor e aluno, neste format, encontram-se por videoconferências.

As vantagens do meio síncrono são a praticidade e o engajamento envolvidos quando o professor e o aluno estão ao vivo no mesmo espaço de tempo.

Nesse cenário, o professor pode realizar perguntas que devem ser respondidas ao vivo, aumentando o engajamento de alunos e alunas com a aula. E, o aluno ou a aluna, caso apresente dúvidas, pode saná-las imediatamente, contribuindo para um fluxo de aula mais dinâmico.

Além disso, muitos formatos síncronos permitem a interação entre alunos e alunas, não apenas com instrutores. Isto contribui para formar outras visões e multiplicar o conhecimento.

E-learning Assíncrono

O espaço-tempo da aula assíncrona é outro. Ao invés de ser realizada ao vivo, essa modalidade ocorre quando aluno e professor não se encontram on-line ao mesmo tempo. Esse tipo de aula costuma ocorrer através de vídeo-aulas ou, até mesmo, posts em blogs ou áudios, como podcasts.

Nessa modalidade, para compensar a falta de interação ao vivo, é possível criar ambientes virtuais de comunicação.

Fóruns on-line, por exemplo, conseguem ser uma ótima opção para solucionar a necessidade de contato. Além de ser um canal em que o professor pode passar, por escrito, uma quantidade maior de materiais de estudo que complementam a aula oferecida, os fóruns também podem ser um ambiente de troca constante entre o professor e o aluno e entre o aluno e seus colegas de classe.

Google for Education

Como previamente abordado, o Ambiente Virtual de Aprendizado conta com um dos ambientes mais utilizados nas instituições de educação no mundo: o Google for Education. Na sua versão mais simples, este ambiente permite o uso das seguintes aplicações web:

Aplicação	**Descrição**
Meet	Possibilita a reunião entre professor e alunos por video-conferência. Ferramenta importante para aulas síncronas.
Classroom	Funciona como um "mural" das atividades em aula.
Youtube	Alternativa para interação de professor e alunos, seja em tempo real como aula síncrona, ou seja como ferramenta para aula assíncrona, servindo como repositório de aulas gravadas.
Docs	Repositório de documentos elaborados por alunos e professores.
Sheets	Repositório de planilhas.
Slides	Repositório de aulas e apresentações.

De uma maneira geral, estas aplicações compõem a base das ferramentas utilizadas pelos professores do Curso Técnico em Segurança Cibernética para a administração das aulas à distância e distribuição do conteúdo. Porém, destas aplicações, as principais são o Google Classroom e o Youtube.

Google Classroom: mural de conteúdo e atividades

No Ambiente Virtual de Aprendizado à disposição de tutores do curso, o aplicativo Google Classroom é um dos mais utilizados para distribuição de conteúdo para os alunos.

A grande vantagem é que este aplicativo tem uma linha de tempo: as atividades, os documentos distribuídos ou os links para vídeos a serem assistidos ficam registrados ali no dia definido e permanecem até o final do módulo.

Desta forma, funciona como um mural de atividades, ao qual os alunos podem retornar sempre que precisam rever uma aula, buscar novamente um documento disponibilizado em outra aula, ou rever as notas de atividades avaliativas propostas previamente.

Youtube: E-Learning Síncrono e Assíncrono

Já há muito tempo, o Youtube é parte integrante da rotina dos jovens em todo o mundo. Muito atenta às enormes possibilidades para distribuição de conteúdo educacional multimeio, o Google disponibiliza um ótimo ambiente para criação de vídeos de aulas em formato assíncrono. Assim, antes de ter contato com o tutor, o aluno absorve o material de aprendizado criado pelo profissional conteudista do curso, faz suas anotações e coleta suas dúvidas.

Para um momento posterior, tutor e alunos se reúnem numa sala virtual on-line para que as dúvidas sejam discutidas e explicações adicionais sejam fornecidas a respeito do assunto daquela aula específica.

Ao final da aula, aquela aula fica gravada e disponível para que os alunos possam rever as explicações em um momento de preparação para avaliações de conhecimento, por exemplo.

Portanto, o Youtube é uma ferramenta valiosa tanto na aula em formato síncrono ou assíncrono. Particularmente neste último, a empresa tem sido muito atuante em incentivar a criação de conteúdo de qualidade. Estão disponíveis muitos canais no Youtube que falam a respeito de tecnologia e os docentes do curso usam também o material de qualidade produzidos por terceiros durante suas aulas.

Academia de Redes da Cisco

Em 1997, a Cisco Systems Inc. já era umas das maiores empresas globais. Tradicional fabricante de software e equipamentos de redes de computadores, sediada no Vale do Silício, na Califórnia, foi neste ano que criou a Cisco Network Academy. Também conhecida como Cisco NetAcad (http://www.netacad.com), esta academia é um valioso recurso para ensino de tópicos ligados à tecnologia e Internet.

Esta academia constitui-se em um portal repleto de recursos educacionais em diversas áreas ligadas diretamente ao setor de segurança da informação:

- Redes de Computadores
- Programação
- Sistemas Operacionais
- Segurança Cibernética

O portal NetAcad, da Cisco Systems, fornece amplo material de ensino para todas estas áreas. A espinha dorsal é um conteúdo completo em formato Web, que funciona como o livro-texto para os alunos. A compreensão deste conteúdo, aliado à parte prática, é exatamente o que é avaliado pela própria plataforma em cada unidade cursada. Além da parte teórica, existe

uma ênfase muito forte na parte prática, onde alunos recebem roteiros de estudo que devem ser cumpridos em laboratórios de maneira presencial ou remota.

No final do ano de 2021, o Inmetro foi acreditado pela empresa como uma Academia Cisco, e, portanto, pode ministrar vários dos cursos disponibilizados na plataforma.

Ainda com relação ao material para ensino, o conteúdo no portal é apresentado em formatos que vão além do texto, como em vídeo e interfaces interativas de avaliação de aprendizado. Para os instrutores e alunos são disponibilizadas apresentações na forma de slides. Pelo portal educacional, são fornecidos também roteiros de laboratório para a parte prática. No que diz respeito à avaliação do desempenho de alunos, existe um ambiente de criação de avaliação para instrutores que utiliza tanto as tradicionais perguntas de múltipla escolha como resultado de laboratórios práticos.

O Simulador *Packet Tracer*

No aprendizado de conceitos de segurança cibernética e redes de computadores é essencial a prática. Uma opção é a prática em equipamentos de redes de computadores fisicamente disponibilizados no laboratório de informática. Outra opção é o uso do simulador Packet Tracer, da plataforma NetAcad (https://www.netacad.com/pt-br/courses/packet-tracer). Este sistema é fornecido aos estudantes para que possam simular redes com escala de equipamentos e configurações que seriam teriam custo proibitivo para serem oferecidos para os estudantes do curso.

Algumas das principais disciplinas do curso utilizarão o material fornecido pelo portal educacional da Cisco. Permitirão o alinhamento da formação dos alunos ao perfil que o mercado procura nos jovens profissionais. Dentre as disciplinas do portal, algumas são preparatórias para exames de certificação profissional. Estes certificados são muito valorizados no mercado de trabalho, e estão ligados a uma formação inicial em Redes de Computadores e Segurança Cibernética.

Mais especificamente com relação a estas disciplinas preparatórias, a empresa Cisco exige que os instrutores façam curso de treinamento na plataforma de e-learning NetAcad, para que tenham contato com a plataforma em si assim como com todas as ferramentas da plataforma sob o ponto de vista de um aluno. Alguns dos docentes do curso, após treinamento intensivo, já estão acreditados pela empresa para treinamento preparatório para os exames de certificação profissional, como o Cisco Certified Network Associate – CCNA e Cisco CyberOps Associate – CBROPS.

15. POLÍTICAS DE APOIO AO ESTUDANTE

15.1. SERVIÇOS DIVERSOS GERAIS

Os estudantes do Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio, assim como qualquer outro aluno do IFF, poderão atendidos pelos serviços voltados para o atendimento e apoio ao estudante por meio do Núcleo de Atendimento ao Educando (NAE) do *Campus* Cabo Frio, composto por uma equipe multiprofissional formada por assistente social, pedagogo e psicólogo.

O NAE tem como função atender às demandas dos estudantes que emergem no espaço institucional no que diz respeito às dificuldades de aprendizagem, acesso e permanência, e à assistência social e psicológica. O núcleo ainda é responsável por selecionar e acompanhar os beneficiários de algumas modalidades de auxílios regulares, como Bolsa Permanência, Auxílio Transporte e Auxílio Moradia.

15.2. PROGRAMAS DE ASSISTÊNCIAS ESTUDANTIL

Os estudantes do Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio, assim como qualquer outro aluno do IFF, poderão ser inseridos no Programa de Assistência Estudantil do Instituto Federal Fluminense, aqui entendido como o conjunto de ações, serviços e projetos que visam possibilitar a democratização das condições de acesso, permanência e conclusão de curso pela minimização dos efeitos e impactos da desigualdade social estrutural na vida dos estudantes e suas famílias.

Esses efeitos e impactos podem se materializar de diversas formas, o que engloba dificuldades para satisfazer necessidades humanas básicas como comer, vestir-se, alimentar-se, morar, transitar e consumir bens e serviços fundamentais para o seu pleno desenvolvimento e participação social como cidadão. Importa destacar que, para satisfazer tais necessidades, pessoais e de seus familiares, muitos estudantes são impedidos de ingressar ou obrigados a interromper suas trajetórias escolares e acadêmicas para adentrar ou retornar ao mundo do trabalho, por vezes com atividades flexibilizadas e/ou informais.

É nesse sentido que o presente Programa, atendendo à perspectiva adotada nacionalmente pelos profissionais envolvidos com a Assistência Estudantil, apresenta um conjunto de mecanismos que visam atuar de forma preventiva em situações de retenção e evasão decorrentes de insuficiência financeira, desigualdades sociais e culturais que impactam diretamente na vida das classes populares. Dessa maneira, a implementação do Programa deve vir articulada com as áreas estratégicas de ensino, pesquisa e extensão, pilares que constituem a base de uma formação profissional cidadã̃ e de qualidade, na perspectiva da educação integral.

Considerando o exposto na Resolução IFF Nº 39/2016, são diretrizes do Programa de Assistência Estudantil do Instituto Federal Fluminense:

a) promover o acesso e a permanência dos estudantes com vistas à inclusão social e democratização do ensino; b) garantir a igualdade de oportunidades na perspectiva de direito social à educação de qualidade e exitosa;

c) proporcionar aos estudantes condições necessárias para a permanência com pleno desempenho acadêmico na Instituição;

d) contribuir para minimizar a retenção ou a evasão dos estudantes de maneira ascendente;

e) assegurar aos estudantes maior equidade de oportunidades no exercício das atividades acadêmicas;

f) garantir ao estudante com necessidades educativas específicas as condições necessárias para o seu desenvolvimento acadêmico;

g) contribuir para a formação integral dos estudantes, estimulando e desenvolvendo a criatividade, a reflexão crítica, a participação em atividades culturais, esportivas, artísticas, políticas, científicas e tecnológicas.

São objetivos do Programa de Assistência Estudantil do Instituto Federal Fluminense:

Objetivo geral:

Contribuir para a democratização do acesso, da permanência e da conclusão do curso dos estudantes do Instituto Federal Fluminense.

Objetivos específicos:

- promover o rendimento acadêmico dos estudantes inseridos no programa por meio de ações complementares de acompanhamento social, psicológico, acadêmico e de saúde;
- possibilitar que os estudantes em vulnerabilidade socioeconômica possam se dedicar integralmente aos estudos, evitando que eles tenham de se dividir entre a formação acadêmica e o mundo do trabalho;
- garantir um rendimento financeiro para que os estudantes com insuficiência financeira possam custear os gastos regulares com transporte, moradia, alimentação e demais necessidades para sua manutenção e conclusão do curso;
- reduzir as taxas de retenção e evasão dos estudantes;
- promover a articulação com as demais políticas sociais setoriais para um atendimento mais efetivo das necessidades dos estudantes.

O Programa Nacional de Assistência Estudantil (PNAES) é normatizado pelo Decreto Nº 7.234/2010, o qual reafirma a importância de que os recursos repassados às instituições federais de ensino devem ser destinados às modalidades de ações, projetos e serviços que contemplem as seguintes áreas, conforme Art. 3o §1o “as ações de assistência estudantil do PNAES deverão ser desenvolvidas nas seguintes áreas:

I. Moradia estudantil;
II. Alimentação;
III. Transporte;
IV. Atenção à saúde;
V. Inclusão digital;
VI. Cultura;
VII. Esporte;
VIII. Creche;

IX. Apoio pedagógico; e
X. Acesso, participação e aprendizagem de estudantes com deficiência, transtornos globais do desenvolvimento e altas habilidades e superdotação."

Em relação aos critérios para se definir os discentes que serão público prioritários das ações de assistência estudantil, o PNAES estabelece em seu Art. 5o que "os estudantes oriundos da rede pública de educação básica ou com renda familiar per capita de até um salário mínimo e meio, sem prejuízo de demais requisitos fixados pelas instituições federais de ensino superior". Não obstante, importa destacar que o termo "prioritariamente" se refere exatamente a dar atendimento primeiro, "acima de", "antes de".

Todas as ações dos Programas de Assistência Estudantil serão realizadas em parceria pela equipe pedagógica do Inmetro com a equipe do *Campus* Cabo Frio, decidindo, conforme a demanda, a melhor forma de atendimento aos discentes.

Uma vez selecionados, os estudantes passarão a integrar o Programa de Assistência Estudantil do Instituto Federal Fluminense, o que necessariamente implica o seu acompanhamento social e acadêmico pela Coordenação de Apoio ao Estudante ou setor equivalente. Os discentes deverão ser acompanhados regularmente em rendimento e frequência, tendo como condicionalidade para a manutenção nas bolsas e nos auxílios a participação em todas as atividades necessárias para a sua permanência e êxito escolar.

15.3 INFRAESTRUTURA DE ACESSIBILIDADE

Considerando a demanda de acessibilidade às pessoas com necessidades educativas específicas existente, o Inmetro vem nos últimos anos viabilizando e implementando adequações arquitetônicas que possibilitem não apenas o acesso, mas também a permanência das pessoas com necessidades educacionais específicas. Compreende-se que, eliminando as barreiras físicas, capacitando o pessoal docente e técnico para atuar com essa clientela e executando ações de conscientização, pode-se eliminar preconceitos e oportunizar a colaboração e a solidariedade entre colegas.

Nesse sentido, o IFF possui, em sua Resolução Nº 43/2018, que aprova o Plano de Desenvolvimento Institucional – PDI – do Instituto Federal Fluminense, seu Plano de acessibilidade", encontram-se as metas que são:

1. Implantação de piso tátil, direcional e alerta, em todos os campi;

2. Implantação de barras de apoio nos banheiros de todos os campi;

3. Implantação de corrimão, em duas alturas, em todas as escadas e rampas dos campi;

4. Garantir que todos os pavimentos dos diversos blocos sejam acessíveis em todos os campi.

Uma que vez que as aulas ocorrerão no Centro de Capacitação do Inmetro, a acessibilidade encontra-se garantida, por ser uma construção mais atual (2012), que possui andar único e térreo e foi planejada para oferecer condições de acesso para pessoas com deficiência e/ou mobilidade reduzida, contando com rampas e banheiros adaptados com barras de apoio. Contudo, melhorias contínuas podem ser realizadas, com apoio da Coordenação de Infraestrutura do Inmentro (Coinf), com a implantação de piso tátil.

15.4 AÇÕES INCLUSIVAS

Em atendimento à Lei Nº 13.146/2015, que Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência), e considerando o Decreto N.º 7611, de 17 de novembro de 2011, que dispõe sobre a educação especial, o atendimento educacional especializado e dá outras providências e o disposto nos artigos 58 a 60, Capítulo V, da Lei N.º 9394, de 20 de dezembro de 1996, será assegurado ao aluno com deficiência, transtornos globais do desenvolvimento e altas habilidades ou superdotados atendimento educacional especializado para garantir igualdade de oportunidades educacionais bem como prosseguimento aos estudos.

Nesse sentido, o IFF constituiu seu Núcleo de Acessibilidade, o NAPNEE, cujas atividades são regulamentadas pela Resolução Nº 33/2018. Constitui-se o público alvo das ações inclusivas do NAPNEE de cada *Campus* os estudantes com necessidades educacionais específicas que se originam em função de deficiência, transtornos globais do desenvolvimento e altas habilidades ou superdotação. Portanto, os estudantes do Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio, assim como qualquer outro aluno do IFF, poderão ser atendidos pelo NAPNEE, com mediação da equipe pedagógica do Inmetro.

São diretrizes do NAPNEE:

- Implementar as ações de inclusão do IFFluminense, de acordo com as Políticas Nacionais de Educação Inclusiva para a promoção da acessibilidade atitudinal, arquitetônica, comunicacional, instrumental, informacional, metodológica e procedimental;
- Incentivar, mediar e facilitar os processos de inclusão educacional e profissionalizante de pessoas com necessidades educacionais específicas na instituição;
- Implementar, participar e colaborar no desenvolvimento de parcerias com instituições que atuem com interesse na educação/atuação/inclusão profissional para PNEE;
- Promover a divulgação de informações e resultados de estudos sobre a temática, no âmbito interno e externo do *Campus*, articulando ações de inclusão em consonância com a Rede Federal de Educação Profissional, Científica e Tecnológica.
- Promover a cultura da educação para a convivência e aceitação da diversidade escolar, para que se desenvolva um sentimento de corresponsabilidade na construção da ação educativa de inclusão no IFFluminense.
- Promover capacitações relacionadas à inclusão de PNEE para a comunidade interna e externa.
- Estimular e apoiar o desenvolvimento de Projetos de Pesquisa e Extensão voltados para o ensino e melhoria da qualidade de vida e a autonomia das pessoas com necessidades educacionais específicas.
- Contribuir para a promoção da acessibilidade atitudinal, arquitetônica, comunicacional, instrumental, metodológica, procedimental e informacional.

A equipe pedagógica do Inmetro, com apoio do NAPNEE, atuará na orientação aos docentes sobre métodos, técnicas conteúdos e organização, assim como na elaboração de Planos Educacionais Individualizados (PEI), sempre que necessário for.

No caso de componentes curriculares que tenham aulas práticas e/ou de laboratório, os professores deverão, juntamente com o NAPNEE, decidir sobre as adaptações necessárias, tendo em vista as particularidades de cada limitação, dentre outras.

Tendo em vista o Acordo de Cooperação entre os dois institutos, no caso de identificação de pessoas com necessidades educacionais especiais, cabe ao Inmetro a contratação de profissionais de apoio, como mediadores, monitores e intérprete de libras, assim como a aquisição de materiais e equipamentos (caneta digita, scanner de voz, impressora Braille, softwares com recursos de acessibilidade, etc.), conforme demanda, sempre visando ao melhor atendimento aos estudantes.

16. CERTIFICADOS E/OU DIPLOMAS

Após a conclusão do Curso Técnico em Segurança Cibernética concomitante ao Ensino Médio é obrigatório o ato de Conferição de Grau, devendo o estudante concluinte apresentar à Coordenação de Registro Acadêmico do IFF, por intermédio da secretaria do Centro de Capacitação do Inmetro, o requerimento formal de conferição de grau, dentro do prazo estabelecido no Calendário Acadêmico.

Posteriormente a sua participação no ato de Conferição de Grau, o estudante deverá realizar o requerimento do diploma na Coordenação de Registro Acadêmico do IFF, por intermédio da secretaria do Centro de capacitação do Inmetro, onde deverá entregar todos os documentos solicitados, no caso de existir pendências.

Excepcionalmente, mediante justificativa, a aferição de grau fora do prazo estabelecido no calendário acadêmico deve ser autorizada pela Coordenação de Curso/Diretoria de Ensino.

17. REFERÊNCIAS

ANDERSON, J. **Computer Security Planning Study. Relatório Técnico ESD-TR-73-51.** Divisão de Sistemas da Força Aérea dos Estados Unidos da América, 1972.

BRASIL. **Lei Nº 5.966, de 11 de dezembro de 1973**. Institui o Sistema Nacional de Metrologia, Normalização e Qualidade Industrial, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5966.htm. Acesso: 08 dez. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [1988]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 mai. 2022.

BRASIL. **Lei nº 8.666, de 21 de junho de 1993**. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências. Diário Oficial da União, Brasília, DF, 22 jun. 1993. Acesso: http://www.planalto.gov.br/ccivil_03/leis/l8666cons.htm Acesso em: 10 mai. 2022.

BRASIL. **Lei Nº 9.394, de 20 de dezembro de 1996**. Estabelece as diretrizes e bases da educação nacional. Brasília, DF: Presidência da República, [1996]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 09 mai. 2022.

BRASIL. **Decreto Nº 4.281, de 25 de junho de 2002.** Regulamenta a Lei Nº 9.795, de 27 de abril de 1999, que institui a Política Nacional de Educação Ambiental, e dá outras providências. Brasília, DF: Presidência da República, [2004]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2002/d4281.htm. Acesso em: 09 mai. 2022.

BRASIL. **Decreto Nº 5.154, de 23 de julho de 2004.** Regulamenta o § 2o do art. 36 e os arts. 39 a 41 da Lei no 9.394, de 20 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional, e dá outras providências. Brasília, DF: Presidência da República, [2004]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5154.htm. Acesso em: 03 mai. 2022.

BRASIL. **Lei Nº 11.788, de 25 de setembro de 2008**. Dispõe sobre o estágio de estudantes. Brasília, DF: Presidência da República, [2008a]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11788.htm. Acesso: 04 mai. 2022.

BRASIL. **Lei Nº 11.892, de 29 de dezembro de 2008**. Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia e dá outras providências. Brasília, DF: Presidência da República, [2008b]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007- 2010/2008/lei/l11892.htm. Acesso: 9 mai. 2022.

BRASIL. **Decreto Nº 7.234, de 19 de julho de 2010**. Dispõe sobre o Programa Nacional de Assistência Estudantil – PNAES. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/decreto/d7234.htm. Acesso: 9 mai. 2022.

BRASIL. **Lei Nº 12.545, de 14 de dezembro de 2011**. Dispõe sobre o Fundo de Financiamento à Exportação (FFEX), altera o art. 1º da Lei nº 12.096, de 24 de novembro de 2009, e as Leis nºs

10.683, de 28 de maio de 2003, 11.529, de 22 de outubro de 2007, 5.966, de 11 de dezembro de 1973, e 9.933, de 20 de dezembro de 1999; e dá outras providências. 2011a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12545.htm. Acesso: 03 mai. 2022.

BRASIL. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. Instituto Federal de Educação, Ciência e Tecnologia Fluminense. **Regulamentação didático-pedagógica do Instituto Federal de Educação, Ciência e Tecnologia Fluminense**. Campos dos Goytacazes, RJ: Instituto Federal Fluminense, 2011b. Disponível em: https://portal1.iff.edu.br/ensino/legislacao-e-regulamentacoes/regulamentacao-didatico-pedagogica-iffluminense.pdf/view. Acesso em: 03 mai. 2022.

BRASIL. **Lei Nº 13.005, de 25 de junho de 2014.** Aprova o Plano Nacional de Educação - PNE e dá outras providências. Brasília, DF: Presidência da República, 2014a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l13005.htm. Acesso em: 10 mai. 2022.

BRASIL. **Lei Nº 13.145, de 6 de julho de 2015**. Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência). Brasília, DF: Presidência da República, 2015a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2015/lei/l13146.htm. Acesso em: 04 mai. 2022.

BRASIL. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. Instituto Federal de Educação, Ciência e Tecnologia Fluminense. Conselho Superior. **Resolução Nº 20, de 19 de junho de 2015.** Aprova a Regulamentação da Atividade Docente. Brasília, DF: Ministério da Educação, 2015b. Disponível em: http://cdd.iff.edu.br/documentos/resolucoes/2015/resolucao-no-20-de-19-de-junho-de- 2015. Acesso em: 08 mai. 2022.

BRASIL. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. Instituto Federal de Educação, Ciência e Tecnologia Fluminense. Conselho Superior. **Resolução Nº 34, de 11 de março de 2016.** Aprova o Regulamento Geral de Estágio do IFFluminense. Brasília, DF: Ministério da Educação, 2016a. Disponível em: http://cdd.iff.edu.br/documentos/resolucoes/2016/resolucao-no-034-de-11-de-marco-de-2016. Acesso em: 08 mai. 2022.

BRASIL. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. Instituto Federal de Educação, Ciência e Tecnologia Fluminense. Conselho Superior. **Resolução Nº 39, de 11 de março de 2016**. Aprova o Programa de Assistência Estudantil do Instituto Federal Fluminense. Brasília, DF: Ministério da Educação, 2016b. Disponível em: http://cdd.iff.edu.br/documentos/resolucoes/2016/resolucao-no-39-de-11-de-marco- de-2016. Acesso em: 06 mai. 2022.

BRASIL. **Portaria Nº 2, de 4 de janeiro de 2017**. Aprova o Regimento Interno do Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO. 2017a. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/20575325/Imprns_Nacional. Acesso: 06 mai. 2022.

BRASIL. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. Instituto Federal de Educação, Ciência e Tecnologia Fluminense. Conselho Superior. **Resolução Nº 23, de**

06 de outubro de 2017. Aprova o Plano Estratégico de Permanência e Êxito dos estudantes do Instituto Federal Fluminense 2017-2019. Brasília, DF: Ministério da Educação, 2017b. Disponível em: http://cdd.iff.edu.br/documentos/resolucoes/2017/resolucao-40. Acessado em: 27 abr. 2022.

Association for Computing Machinery (ACM), IEEE Computer Society. **Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity**, 2017c.

BRASIL. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. Instituto Federal Fluminense. **Projeto Político-Pedagógico Institucional (PPI).** 2018a. Disponível em: https://portal1.iff.edu.br/ensino/arquivos/ppi-2018-2022.pdf/@@download/file/PPI%202018-2022.pdf. Acesso em: 03 mai. 2022.

BRASIL. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. Instituto Federal Fluminense. **Resolução Nº 43, de 21 de dezembro de 2018**. Trata do Plano de Desenvolvimento Institucional 2018-2022. Brasília, DF: Ministério da Educação, 2018b. Disponível em: http://cdd.iff.edu.br/documentos/resolucoes/2018/resolucao-34. Acesso em: 04 mai. 2022.

National Institute for Standards and Technology (NIST). **Framework for Improving Critical Infrastructure Cybersecurity.**2018d. Disponível em: https://doi.org/10.6028/nist.cswp.04162018 Acesso: 08 mai. 2022.

BRASIL. Ministério da Educação. **Catálogo Nacional de Cursos Técnicos** – CNCT. 4. ed. Brasília, DF, 2020, 506 p. Disponível em: http://cnct.mec.gov.br/cnct-api/catalogopdf Acesso em: 05 mai. 2019.

BRASIL. **Resolução CNE/CP Nº 1, de 5 de janeiro de 2021**. Define as Diretrizes Curriculares Nacionais Gerais para a Educação Profissional e Tecnológica. Diário Oficial da União**:** edição 3, seção 1, Brasília, DF, p. 70, 6 jan. 2021. 2021a. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cne/cp-n-1-de-5-de-janeiro-de-2021-297767578. Acesso em: 09 mai. 2022.

BRASIL. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. Instituto Federal de Educação, Ciência e Tecnologia Fluminense. **Instrução Normativa Nº 3/2021 - PROEN/REIT/IFFLU, de 17 de agosto de 2021**. Institui as orientações para a elaboração de Projetos Pedagógicos de Cursos (PPCs) de Nível Médio e de Graduação, na modalidade presencial com previsão de carga horária a distância, no âmbito do Instituto Federal Fluminense. 2021b. Disponível em: https://portal1.iff.edu.br/ead/documentos . Acesso: 30 abr. 2022.

BRASIL. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. Instituto Federal de Educação, Ciência e Tecnologia Fluminense. **Instrução Normativa Nº 2/2021 - PROEN/REIT/IFFLU, de 17 de agosto de 2021**. Dispõe sobre as orientações para a elaboração de Projetos Pedagógicos de Curso (PPCs), de Nível Técnico e de Graduação, na modalidade a distância, no âmbito do Instituto Federal Fluminense. 2021b. Disponível em: https://portal1.iff.edu.br/ead/documentos . Acesso: 30 abr. 2022.

BRASIL. Ministério da Economia. Instituto Nacional de Metrologia, Qualidade e Tecnologia, **Planejamento Estratégico do Inmetro 2021 – 2023**. 2021c. Disponível em: https://www.gov.br/inmetro/pt-br/acesso-a-informacao/institucional/plano-estrategico-inmetro-2021-2023.pdf. Acesso: 04 abr. 2022.

HAM, J.V.D. **Toward a Better Understanding of Cybersecurity**. ACM Digital Threats: Research and Practice, Vol. 2, No. 3, Article 18, June 2021d.

BRAUM, D. e LAURENCE,F. **Cresce a Demanda por Segurança Cibernética: Brasil é alvo de mais de 3 bilhões de tentativas de ataques**. Jornal Valor Econômico, 26 de Agosto de 2021. 2021d. Disponível em: https://valor.globo.com/empresas/noticia/2021/08/26/cresce-a-demanda-por-seguranca-cibernetica.ghtml. Acesso: 05 set. 2021.

18. ANEXOS

ANEXO A – ACOMPANHAMENTO DO PROJETO PEDAGÓGICO DO CURSO

Acompanhamento da Execução do Projeto Pedagógico
1- A carga horária especificada no quadro de horários está de acordo com a carga horária prevista na matriz curricular?
2- As notas de cada disciplina estão sendo lançadas dentro dos prazos especificados no sistema adotado?
3- O Calendário Acadêmico está sendo cumprido na íntegra?
4- A frequência está sendo registrada no sistema adotado?
5- O conteúdo programático das disciplinas está sendo registrado no sistema adotado?
6- O conteúdo programático de cada disciplina está sendo ministrado?
7- As atividades avaliativas estão sendo cumpridas de acordo com o regulamento didático pedagógico?
8- As visitas técnicas estão ocorrendo conforme planejado?
9- Os projetos práticos são implementados?
10- Os recursos didático-pedagógicos estão atendendo às necessidades do curso (canetas, quadros, datashow, computadores)?
11- As salas de aula estão adequadas ao processo de ensino aprendizagem?
12- Os laboratórios estão atendendo às necessidades do curso?
13- As aulas das dependências estão sendo ministradas?
14- As visitas às comunidades de acordo com o eixo do curso estão sendo realizadas?
15- Os professores estão capacitados quanto aos princípios avaliativos do IFFluminense?
16- Os estudantes estão frequentando regularmente as aulas em cada disciplina?
17- Os estudantes estão aproveitando as oportunidades criadas pelo *Campus* Itaperuna com intuito de sanar os déficits de aprendizagem detectados (monitorias, aulas extras etc)?
18- Os estudantes desenvolvem as atividades complementares para fixação dos conteúdos (listas de exercícios, trabalhos etc.)
19- As coordenações encaminham os estudantes que apresentam deficiências psicossociais e pedagógicas ao setor responsável?
20- O setor de atendimento ao estudante tem criado mecanismos para solucionar os problemas que lhe são apresentados?
21- A equipe pedagógica tem dado o suporte aos professores?
22- Os PPCs estão sendo acompanhados e avaliados conforme o previsto?
23- Os Conselhos de Classe estão ocorrendo regularmente?
24- Os problemas detectados no Conselho de Classe são encaminhados ao setor responsável?
25- O acervo da biblioteca reflete os livros mencionados na bibliografia básica de cada disciplina?
26- As atividades que visam à interdisciplinaridade estão sendo executadas?
27- As atividades de integração entre Ensino, Pesquisa e Extensão estão sendo executadas?
28- As atividades que visam à aproximação teórico-prática estão sendo executadas?

ANEXO B – ACORDO DE COOPERAÇÃO TÉCNICA IFF E INMETRO

INMETRO

ACORDO DE COOPERAÇÃO TÉCNICA

ACORDO DE COOPERAÇÃO TÉCNICA QUE ENTRE SI CELEBRAM O INSTITUTO FEDERAL FLUMINENSE E O INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA - INMETRO PARA OS FINS QUE ESPECIFICA.

O **INSTITUTO FEDERAL FLUMINENSE**, doravante denominado **IFF,** com sede à Rua Dr. Walter Kramer 357, Parque Santo Antônio, Campos dos Goytacazes - RJ, inscrita no CNPJ/MF sob o nº. 10.779.511/0001-07, neste ato representado pelo Reitor JEFFERSON MANHÃES DE AZEVEDO, brasileiro, divorciado**, portador da identidade nº** [redacted], CPF nº [redacted], nomeado Reitor por meio do Decreto *de 03 de abril de 2020*, *publicado* no Diário Oficial da União em *06 de abril de 2020*.

O **INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA**, autarquia federal vinculada ao MINISTÉRIO DA ECONOMIA, criada pela Lei no 5.966, de 11/12/1973, com sede legal em Brasília, Distrito Federal, e com Unidades Técnicas na Avenida Nossa Senhora das Graças no 50, Distrito de Xerém, Município de Duque de Caxias, e SEPN-W3-Norte, Quadra 511, Bloco B - 4º andar, Brasília, Distrito Federal, inscrito no CNPJ sob o nº 00.662.270/0003-20, doravante designado **INMETRO**, representado neste ato por seu Presidente, MARCOS HELENO GUERSON DE OLIVEIRA JUNIOR, brasileiro, casado, portador de RG nº. [redacted], CPF [redacted].

Considerando: O Plano Nacional de Educação (PNE) sob responsabilidade do Ministério da Educação (MEC), que apresenta como uma de suas principais metas triplicar as matrículas de educação profissional técnica de nível médio assegurando a qualidade da oferta e pelo menos 50% (cinquenta por cento) da expansão no segmento público (LEI Nº 13.005/2014 de 25 de junho de 2014, Meta 11);

Considerando: Que o PNE inclui como estratégias: a) expandir as matrículas de educação profissional técnica de nível médio na Rede Federal de Educação Profissional, Científica e Tecnológica, levando em consideração a responsabilidade dos Institutos na ordenação territorial, sua vinculação com arranjos produtivos, sociais e culturais locais e regionais, bem como a interiorização da educação profissional; b) fomentar a expansão da oferta de educação profissional técnica de

nível médio nas redes públicas estaduais de ensino; c) fomentar a expansão da oferta de educação profissional técnica de nível médio na modalidade de educação a distância, com a finalidade de ampliar a oferta e democratizar o acesso à educação profissional pública e gratuita, assegurado padrão de qualidade;

Considerando: Que a política de extensão do IFF visa à fortalecer e ampliar as atividades de extensão de cunho tecnológico estabelecendo relacionamento entre a instituição e seus diversos públicos e contribuindo para fortalecimento dos arranjos produtivos regionais;

Considerando: Que o IFF, no seu Plano de Desenvolvimento Institucional (PDI 2018-2022), traz como objetivos estratégicos: 6 - Ampliar a abrangência de atendimento, diversificando a oferta de cursos, considerando a demanda social regional ; 7 - Desenvolver pesquisa, inovação e extensão em articulação com outros atores; 8 - Promover o reconhecimento de saberes, certificação e qualificação profissional;;

Considerando: Que o IFF possui em sua missão institucional promover a Educação Profissional e Tecnológica nacional e suas relações com a educação básica e superior a partir das regiões noroeste, norte e baixadas litorâneas do estado do Rio de Janeiro, na perspectiva da formação integral dos jovens e trabalhadores e do desenvolvimento regional, articulando os atores socio educacionais e econômicos, assumindo protagonismo na definição e execução de políticas de educação e trabalho;

Considerando: Que o IFF, para atingir o objetivo estratégico 7, e o indicador 7.4 (número de projetos de extensão desenvolvidos em parceria com entes externos) estabelecidos em seu Plano de Desenvolvimento Institucional (PDI 2018-2022) possui como iniciativa estratégica o "fortalecimento de ações na busca de parcerias com instituições e empresas";

Considerando: Que o INMETRO tem como missão institucional "viabilizar soluções de infraestrutura da qualidade que adicionem confiança, qualidade e competitividade aos produtos e serviços disponibilizados pelas organizações brasileiras, em prol da prosperidade econômica e bem-estar da nossa sociedade", o que propicia uma circunstância favorável para os profissionais com formação no segmento de Metrologia, Biotecnologia e Segurança Cibernética;

Considerando: Que desde 1998 o INMETRO oferta o Curso Técnico em Metrologia (o primeiro da América Latina e o quarto curso do gênero no mundo) e que desde 2011 também oferta o Curso Técnico em Biotecnologia, ambos concomitante ao Ensino Médio e executados por meio de Acordo de Cooperação com a Secretaria Estadual de Educação do Rio de Janeiro (SEEDUC-RJ), tendo formado quase 500 profissionais nas duas áreas;

Considerando: Que desde 2018 o INMETRO oferta o Curso de Qualificação Profissional em Segurança Cibernética, por iniciativa própria, tendo em vista a enorme demanda que vem sofrendo para disseminar competência na área de segurança cibernética, mais especificamente ligadas às questões de avaliação de segurança da informação do software embarcado em sistemas de medição.

E, por fim, o histórico de sucesso das formações profissionalizantes do INMETRO, por meio do impacto social e econômico na região onde está localizado o Instituto (Distrito de Xerém/Município de Duque de Caxias/RJ), mas principalmente pela inserção de profissionais altamente capacitados no setor produtivo.

RESOLVEM:

Firmar o presente ACORDO DE COOPERAÇÃO TÉCNICA, sujeitando-se os partícipes, no que couber, às disposições contidas nas leis correlatas, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1 Este Acordo de Parceria tem por objeto estabelecer a cooperação entre o INMETRO e o IFF, para projetos voltados ao desenvolvimento, implementação e oferta de cursos de educação profissional técnica de nível médio nas áreas da ciência, tecnologia e inovação, com ênfase nas áreas de metrologia, metrologia legal, avaliação da conformidade, biotecnologia, informática e segurança da informação;

1.2. As atividades serão direcionadas à comunidade acadêmica do IFF e do INMETRO, assim como à sociedade civil.

1.3. O presente Acordo de Cooperação Técnica prevê o compromisso entre as partes de atuar de maneira articulada e em parceria, proporcionando as decisões necessárias para as atividades conjuntas.

CLÁUSULA SEGUNDA – DA EXECUÇÃO

2.1. As atividades de que trata o objeto do presente Acordo de Cooperação serão exercidas pelo INMETRO e pelo IFF, de acordo com os projetos específicos aprovados pelos responsáveis das áreas competentes e conforme estabelecido em Planos de Trabalhos anexos a este instrumento.

CLÁUSULA TERCEIRA – DA COORDENAÇÃO

3.1. Cada partícipe designará um(a) servidor (a) de sua instituição que atuará como coordenador(a) responsável pela condução, acompanhamento e avaliação das atividades, além de eventuais necessidades de interlocução com outros parceiros, conforme previstos neste Acordo de Cooperação e respectivos Planos de Trabalho.

3.2. Competirá aos coordenadores:

a) Acompanhar e assegurar a realização das atividades desenvolvidas conforme os Planos de Trabalho, assim como representar sua instituição em reuniões voltadas para a execução dos mesmos;

b) Proceder a avaliação permanente deste Acordo de Cooperação Técnica, acompanhando seu detalhamento e operacionalização, em todos os seus aspectos, visando às melhorias e as correções que se façam necessárias;

c) Tomar as providências cabíveis visando à solução dos eventuais problemas de ordem técnica e/ou administrativa que surjam no decorrer do desenvolvimento dos projetos, observadas as normas vigentes de cada instituição e, quando for o caso, encaminhando a pendência à autoridade competente.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES DOS PARTÍCIPES

4.1 Aos partícipes, em conjunto, compete:

a) Zelar pelo cumprimento dos Planos de Trabalho, na medida de sua capacidade e em conformidade com os dispositivos legais e regimentares de cada instituição;

b) Construir, de forma coletiva e dialógica, os projetos pedagógicos de cursos (PPC) e as atividades que irão nortear as ações de ensino, pesquisa e inovação a serem desenvolvidas no âmbito deste instrumento;

c) Divulgar amplamente a realização das ações realizadas no presente, inclusive à sociedade civil;

d) Contribuir na elaboração de instrumentos de avaliação e relatórios referentes aos resultados das ações desenvolvidas;

e) Assumir ou transferir a responsabilidade pela execução do objeto, no caso de paralisação ou da ocorrência de fato relevante, de modo a evitar sua descontinuidade;

f) Observar e fazer observar, no âmbito de sua organização, e no que diz respeito aos assuntos sigilosos que, em decorrência deste Acordo de Cooperação, venham a ter conhecimento, as disposições legais e regulamentares concernentes à salvaguarda de assuntos sigilosos, particularmente as do Regulamento aprovado pelo Decreto no 7.845, de 14 de novembro de 2012.

Parágrafo único: Os empregados e/ou contratados de qualquer dos partícipes, que vierem a atuar na execução das atividades inerentes ao presente instrumento, não sofrerão qualquer alteração nas suas vinculações com a entidade de origem.

4.2. Ao INMETRO compete:

a) Executar os projetos pedagógicos de cursos (PPC) construídos conjuntamente pelos partícipes e em conformidade com os Planos de Trabalho;

b) Disponibilizar docentes para ministrar as aulas nos cursos de educação profissional técnica de nível médio, de qualificação profissional, de formação continuada e/ou de extensão nas áreas da ciência, tecnologia e inovação, com ênfase nas áreas de metrologia, metrologia legal, avaliação da conformidade, biotecnologia, informática e segurança da informação;

c) Disponibilizar equipe técnica e pesquisadores para o desenvolvimento de objetos de aprendizagem digitais para cursos a distância;

d) Disponibilizar os ambientes necessários para oferta dos cursos, incluindo laboratórios, ambientes tecnológicos e biblioteca com acervo especializado;

e) Oferecer material didático-pedagógico para desenvolvimento dos cursos;

f) Zelar pelo cumprimento dos projetos pedagógicos de cada curso e do calendário acadêmico propostos pelo IFF.

4.3. Ao IFF compete:

a) Prover apoio para a inclusão de novos cursos no Catálogo Nacional de Cursos Técnicos – MEC, a exemplo do Curso Técnico em Segurança Cibernética;

b) Elaborar, aprovar e publicar editais de processos seletivos para os cursos de educação profissional técnica de nível médio, de qualificação profissional, de formação continuada e/ou de extensão;

c) Planejar, organizar e realizar os procedimentos referentes às matrículas dos alunos em seus sistemas acadêmicos;

d) Planejar, organizar e realizar os procedimentos referentes à emissão de certificados para as ações de educação profissional técnica de nível médio, de qualificação profissional, de formação continuada e/ou de extensão.

CLÁUSULA QUINTA – DOS RECURSOS

5.1. Este Acordo de Cooperação Técnica não implica transferência de recursos entre as partes.

5.2. Os contratos específicos que envolverem compromissos de desembolso financeiro de quaisquer das partes signatárias terão a sua operacionalização vinculada à legislação pertinente, com definição prévia das condições de realização dos trabalhos e as atribuições e responsabilidades técnicas, administrativas e financeiras dos Contratantes, inclusive de terceiros participantes, investidos de funções executoras ou de outra natureza, os quais poderão ter a forma de contratos, termos de referência, ordens de serviços, programas, projetos aprovados e assinados pelos órgãos partícipes.

CLÁUSULA SEXTA – DO ACOMPANHAMENTO DA EXECUÇÃO

6.1. Os partícipes, por meio de servidor(a) especialmente indicado(a), conforme item 3.1 do presente instrumento, farão o acompanhamento, a supervisão e a avaliação do Acordo de Cooperação Técnica e emitirão parecer ANUAL acerca do atendimento aos objetivos.

CLÁUSULA SÉTIMA – DA AÇÃO PROMOCIONAL

7.1. Os resultados técnicos e todo e qualquer desenvolvimento decorrente de trabalhos realizados no âmbito do presente Acordo de Cooperação Técnica serão atribuídos ao IFF e ao INMETRO, com os respectivos créditos.

CLÁUSULA OITAVA – DA VIGÊNCIA, DA RENÚNCIA E DA RESCISÃO

8.1. O presente Acordo de Cooperação vigorará pelo prazo de 03 (três) anos, a contar da data de sua publicação no Diário Oficial da União, podendo ser prorrogado ou alterado mediante termo aditivo, bem como denunciado pelos partícipes e rescindido a qualquer tempo, mediante notificação por escrito, com antecedência mínima de 60 (sessenta) dias.

CLÁUSULA NONA – DA PUBLICAÇÃO

9.1. Constitui-se encargo do Inmetro a publicação de extrato deste Acordo de Cooperação, no Diário Oficial da União, após sua assinatura, conforme disciplinado no parágrafo único do artigo 61 da Lei nº 8.666/1993.

CLÁUSULA DÉCIMA – DAS ALTERAÇÕES

10.1. Quaisquer alterações aos termos do presente Instrumento serão efetivadas mediante celebração de Termos Aditivos que passarão a integrar o presente Acordo de Cooperação.

10.2. O Plano de Trabalho, parte integrante desse instrumento, poderá ser reformulado independentemente de Termo Aditivo, mediante troca de correspondência entre os partícipes, vedada à mudança do seu objeto.

10.3. Novos Planos de Trabalho, correspondente a este Acordo de Cooperação poderão ser formulados independentemente de Termo Aditivo, mediante troca de correspondência entre os partícipes, vedada à mudança do seu objeto.

CLÁUSULA DÉCIMA SEGUNDA – DOS CASOS OMISSOS

12.1. Os casos omissos serão resolvidos por conciliação entre os partícipes. As resoluções daí advindas poderão ser objeto de termo aditivo, na forma da cláusula décima.

12.2. As controvérsias intransponíveis por conciliação, oriundas da execução do presente Acordo de Cooperação serão solucionadas na forma prevista na Cláusula Décima Terceira deste Instrumento.

CLÁUSULA DÉCIMA TERCEIRA – DO FORO

13.1 Fica eleito o Foro da Cidade do Rio de Janeiro, para dirimir quaisquer questões oriundas deste termo e bem como de seus respectivos Termos Aditivos que vierem a ser firmados.

E, para validade do que pelos partícipes foi pactuado, firmou-se este Instrumento, na presença das testemunhas abaixo, a fim de que produza os efeitos jurídicos e legais, em juízo e fora dele.

DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO ART. 6º, § 1º, DO DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015 EM 07/10/2021, ÀS 17:15, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR

MARCOS HELENO GUERSON DE OLIVEIRA JUNIOR
Presidente

DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO ART. 6º, § 1º, DO DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015 EM 13/10/2021, ÀS 19:19, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR

JEFFERSON MANHÃES DE AZEVEDO
Usuário Externo

A autenticidade deste documento pode ser conferida no site https://sei.inmetro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1030424** e o código CRC **6150DAE1**.

ANEXO C – PORTARIA DE NOMEAÇÃO DO COORDENADOR DO CURSO TÉCNICO DE SEGURANÇA CIBERNÉTICA

Serviço Público Federal

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS - MDIC
INSTITUTO NACIONAL DE METROLOGIA , QUALIDADE E TECNOLOGIA - INMETRO

PORTARIAS DE 29 DE AGOSTO DE 2018.

O PRESIDENTE DO INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA – Inmetro, no uso das atribuições que lhe confere o parágrafo 3º do artigo 4º, da Lei nº 5.966, de 11 de dezembro de 1973, e tendo em vista o inciso V, do art. 18 da Estrutura Regimental da Autarquia, aprovada pelo Decreto nº 6.275, de 28 de novembro de 2007, com a redação alterada pelos Decretos nºs 7.938, de 19 de fevereiro de 2013, e 8.848, de 12 de setembro de 2016, **resolve:**

Nº 406 – Delegar competência a RODOLFO SABOIA LIMA DE SOUZA, matrícula Siape 2635453, para exercer o encargo de coordenador do Curso Técnico em Metrologia, compreendendo as seguintes responsabilidades: elaborar e executar o projeto pedagógico do curso; designar os professores do curso; manter contato permanente com professores e alunos, apresentando ao coordenador-geral do Cicma as propostas para solução dos problemas do curso; organizar e supervisionar os trabalhos pedagógicos de seu curso, assim como seus indicadores e resultados; acompanhar a fiel execução do regime didático, especialmente na observância dos programas e horários das atividades do curso com docentes e discentes; atestar a freqüência do pessoal docente de seu curso; cumprir as decisões do Cicma e/ou do Conselho Acadêmico do Inmetro; monitorar atividades de extensão entre docentes e discentes; e demais atividades atinentes ao perfil do encargo.

Nº 407 – Delegar competência a EWERTON LONGONI MADRUGA, matrícula Siape 1657795, para exercer o encargo de coordenador do Curso Técnico em Segurança Cibernética, compreendendo as seguintes responsabilidades: elaborar e executar o projeto pedagógico do curso; designar os professores do curso; manter contato permanente com professores e alunos, apresentando ao coordenador-geral do Cicma as propostas para solução dos problemas do curso; organizar e supervisionar os trabalhos pedagógicos de seu curso, assim como seus indicadores e resultados; acompanhar a fiel execução do regime didático, especialmente na observância dos programas e horários das atividades do curso com docentes e discentes; atestar a freqüência do pessoal docente de seu curso; cumprir as decisões do Cicma e/ou do Conselho Acadêmico do Inmetro; monitorar atividades de extensão entre docentes e discentes; e demais atividades atinentes ao perfil do encargo

Estas Portarias entram em vigor na data de sua publicação no Boletim de Serviço da Autarquia.

sei! DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO ART. 6º, § 1º, DO DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015 EM 06/09/2018, ÀS 16:33, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR:

CARLOS AUGUSTO DE AZEVEDO
Presidente

A autenticidade deste documento pode ser conferida no site http://sei.inmetro.gov.br/autenticidade, informando o código verificador **0159295** e o código CRC **86788306**.