# **Currículo de Referência**

Tecnologia da Informação

com Ênfase em Cibersegurança

# 

Sumário

**Currículo de Referência 1**

**1. Apresentação do Curso 3**

1.2 Contexto 4

1.3 Perfil do Profissional Egresso 6

Competências Gerais 6

1.4 Princípios e Diretrizes Pedagógicas 8

[1.4.1](#_kawd1eime7d0) Sobre as Metodologias Ativas 9

1.4.2 Requisitos para o Corpo Docente 11

[**2**](#_e3hdgp36ybu3)**. Perfil Curricular 12**

2.1 Caracterização do Curso 12

2.2 Organização Curricular 13

2.3 Sistemática de Avaliação 15

**3. Ementário 17**

3.1 Disciplinas do Eixo Básico 17

Introdução à Computação 17

Introdução à Segurança da Informação 18

Segurança, Proteção e Privacidade de Ativos 19

Sistemas Operacionais 20

Introdução à Computação em Nuvem 21

Criptografia Aplicada 22

Arquitetura e Organização de Computadores 23

Arquitetura de Segurança 24

Análise e Testes de Segurança (Defesa) 25

3.2 Disciplinas do Eixo 1: Gestão da Operação 26

Redes e Conectividade 26

Gestão da Identidade e Controle de Acesso (IAM) 27

3.3 Disciplinas do Eixo 2: Segurança Defensiva 28

Forense Computacional 28

Gerenciamento de Incidentes 29

3.4 Disciplinas do Eixo 3: Segurança Ofensiva 30

Testes de Invasão (PenTesting & Ethical Hacking) 30

Exploração e Desenvolvimento de Ameaças 31

3.5 Disciplinas do Eixo 4: Desenvolvimento Seguro 32

Introdução à Programação 32

Análise de Código (Estático/Dinâmico) 33

**Referências 34**

# 

# 1. Apresentação do Curso

Este documento apresenta propostas de currículos para a área de Tecnologia da Informação no que tange ao programa de Educação Tecnológica no nível de graduação. De acordo com a resolução do conselho Nacional de Educação (CNE, 2020), vários princípios precisam ser observados nessa formação, principalmente: articulação com o setor produtivo na construção de itinerários formativos; incentivo à pesquisa como princípio pedagógico de formação para um mundo em permanente transformação, integrando competências cognitivas e socioemocionais; indissociabilidade entre saberes e fazeres, conhecimento e prática social.

De acordo com a resolução do CNE (2021, p.4), o objetivo da formação técnica e tecnológica é desenvolver Competências Profissionais, definidas como:

A capacidade pessoal de mobilizar, articular, integrar e colocar em ação conhecimentos, habilidades, atitudes, valores e emoções que permitam responder intencionalmente, com suficiente autonomia intelectual e consciência crítica, aos desafios do mundo do trabalho.

O grande desafio é a formação dessas competências em médio prazo para atender às demandas reprimidas em diversos setores de TIC, dentre eles: 25% em **Internet das Coisas**, 11% em **Segurança**, 10% em **Big Data,** 6% em **Cloud Computing** e 2% em **Inteligência Artificial (BRASSCOM, 2021).**

O itinerário formativo em Cibersegurança contido neste documento é baseado no cruzamento de informações dos cursos mais bem conceituados nos Rankings acadêmicos, grandes empresas de mercado e pesquisas setoriais de instituições como a BRASSCOM.

## 1.2 Contexto

Segundo a pesquisa "Profissões Emergentes na Era Digital" (CNI, 2021), realizada pelo SENAI e a Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, os atuais centros de formação profissional não são capazes de atender às demandas da indústria por profissionais de Tecnologia da Informação e da Comunicação. Cursos técnicos ou universitários também não conseguem desenvolver competências e habilidades requeridas para esses profissionais, com o nível de profundidade necessária para o atual mercado de trabalho. Por isso, 80% das empresas que participaram da pesquisa informaram que possuem academias corporativas para *upskilling* de seus profissionais.

A pesquisa ainda aponta as principais profissões emergentes, onde dentre elas podemos destacar o especialista em cloud, analista de segurança, especialista em inteligência artificial e o cientista de dados. Estas mesmas áreas, segundo o "Relatório Setorial 2020 Macrossetor de TIC" (BRASSCOM, 2021) têm perspectivas de receber investimentos na ordem de bilhões e continuar crescendo de 2021 a 2024.

De acordo com a International Data Corporation (IDC, 2021) o Brasil precisará investir em tecnologias relacionadas à infraestrutura de conectividade e redes, crescimento do 5G, fibra óptica e atualização das empresas. A previsão do crescimento do setor de Telecomé de 2% para 2021, sendo 10% de crescimento para o mercado corporativo.

A inovação tecnológica demanda profissionais atualizados e com perfis diferentes dos currículos antigos que desconsideram o avanço da transformação digital nas corporações e a necessidade de visão sistêmica dessas tecnologias nos negócios.

A formação profissional exige conhecimentos em Cloud Computing, Internet das Coisas, Sistemas Analíticos, NFV (Network Functions Virtualization), SDN (Software Defined Networking) , ou seja, capacidade de relacionar Tecnologia da Informação, Conhecimento de Cloud Computing e Telecom.

Além disso, o setor de Tecnologia da Informação e Comunicação como um todo vem se descobrindo como uma atividade que envolve um significativo esforço de interação sociotécnica, de modo que o desenvolvimento de competências técnicas, apenas, não é suficiente para assegurar o sucesso de profissionais ou otimizar o sucesso dos projetos nos quais eles irão atuar. Por isso, competências socioemocionais vem sendo consideradas tão, ou ainda mais importantes, do que as competências técnicas, para a formação integral de profissionais preparados para atuação no mercado de trabalho contemporâneo.

Competência é aqui compreendida de maneira genérica como a mobilização de conhecimentos, habilidades, atitudes e valores, responsivos às demandas complexas da vida. Competências são desenvolvidas por meio de experiências em ambientes complexos onde o conhecimento não pode ser separado das habilidades e das atitudes. As Competências Socioemocionais, por sua vez, referem-se a aspectos individuais que se manifestam nos modos de pensar, sentir e nos comportamentos ou atitudes para se relacionar consigo mesmo e com os outros. A perspectiva de desenvolvimento de competências exige a compreensão de que o seu trajeto de construção se estende ao processo de formação continuada, sendo, portanto, um instrumento norteador do desenvolvimento profissional permanente. Além disso, este currículo de referência reflete diversas alternativas de como competências podem ser trabalhadas, praticadas e aprendidas no contexto da formação tecnológica, e estão relacionadas ao desenvolvimento de outras competências, como as competências cognitivas nos contextos de aprendizagem formais e informais.

Segundo o relatório da **Organização para Cooperação e Desenvolvimento Econômico (2021), o Brasil precisa atingir quatro grandes objetivos na Educação Tecnológica:**

1. Expandir a Educação com qualidade**;**
2. Promover treinamento na prática aos estudantes (Aprendizagem baseada em trabalho)**;**
3. Envolver o setor produtivo:
4. Avaliação, envolvendo o mercado de trabalho com feedbacks e sugestões de melhorias durante a formação e atualização curricular.

Neste contexto, o objetivo principal é construir um currículo referencial que considere as necessidades de mercado, em termos das competências profissionais e socioemocionais, e que sirva como instrumento de aperfeiçoamento do perfil dos egressos dos tecnólogos em Comunicação do país.

## 

## 1.3 Perfil do Profissional Egresso

O tecnólogo em Cibersegurança está apto a identificar vulnerabilidades e apresentar solução para proteção de sistemas, ambientes e dispositivos; Fazer a gestão de ambientes computacionais e definir a arquitetura tecnológica; Definir tecnologias para a proteção de ambientes críticos; Executar procedimentos, políticas e normas de segurança da Informação; Criar estratégias de prevenção e defesa contra ameaças do ciberespaço a partir de uma compreensão situacional; Estabelecer procedimentos, práticas e tecnologias que visam a segurança digital contra práticas ilícitas e danos aos computadores, redes, programas e dados; Atuar de forma a evitar perda parcial ou total de dados, roubos de senhas, identidade, dados bancários, a disseminação de SPAM, o suborno para resgate de informações sigilosas, dentre outras; Auxiliar outros profissionais no desenvolvimento de uma política de segurança interna da informação; Monitorar aspectos relacionados à segurança dos sistemas e redes de uma empresa ou negócio; Assegurar que os dados estejam guardados e protegidos, conforme premissas e normativas vigentes, como a Lei Geral de Proteção de Dados Pessoais.

### 1.3.1 Competências Gerais

O profissional egresso do curso de tecnólogo em **Tecnologia da Informação com Ênfase em Cibersegurança** precisa ter competências e habilidades para apoiar equipes, resolver problemas, bem como, ser proativo para implementar soluções, gerenciar atividades e permanecer em constante processo de aprendizagem. Precisam desenvolver competência e habilidades socioemocionais para dar suporte a todas essas atividades. O curso, também, se propõe a desenvolver competências e habilidades digitais necessárias para o contexto de transformação digital, como: cultura digital, ser adaptativo às novas tecnologias, proficientes nos seus usos e trabalhar conectado em rede. De acordo com cada eixo formativo, em linhas gerais, é esperado que saiba:

**Formação Básica**

* Identificar vulnerabilidades e apresentar solução para proteção de sistemas, ambientes e dispositivos;
* Administrar ambientes computacionais e definir a arquitetura tecnológica visando a segurança cibernética .
* Definir tecnologias para a proteção de ambientes críticos;
* Assegurar que os dados estejam guardados e protegidos, conforme premissas e normas vigentes i
* Identificar diferentes métodos criptográficos, protocolos, algoritmos, assinaturas e certificados digitais e o uso da criptografia como componente de serviços de autenticação e controle de acesso;
* Conhecer padrões para Implementar, monitorar e proteger sistemas operacionais, equipamentos, redes, aplicativos e controles usados para permitir vários níveis de confidencialidade, integridade e disponibilidade.

**Gestão da Operação**

* Estabelecer o conhecimento necessário para implantação dos processos de Gestão das Operações de Segurança em uma organização;
* Compor o skillset da função centralizada dentro de uma organização que emprega pessoas, processos e tecnologia para monitorar e melhorar continuamente sua postura de segurança;
* Promover ações para evitar, detectar, analisar e responder a incidentes de segurança cibernética.
* Competências-chave: Resposta a incidentes.

**Segurança Defensiva**

* Utilizar uma abordagem reativa à segurança que se concentra na prevenção, detecção e resposta a ataques;
* Definir um tipo de cibersegurança que visa proteger a organização em qualquer circunstância, desde a análise da rede atual, até proteger completamente a infraestrutura da rede;
* Conceber um plano de segurança que garanta a efetividade de quaisquer controles de segurança integrados;
* Competências-chave: Prevenção, monitoramento e reação.

**Segurança Ofensiva**

* Empregar uma abordagem proativa e antagônica para proteger sistemas de computador, redes e indivíduos contra ataques;
* Empregar uma abordagem proativa à segurança por meio do uso de testes de penetração e hacking ético;
* Promover medidas de segurança ofensivas focadas na busca dos atacantes por meio de suas próprias técnicas e, em alguns casos, na tentativa de desabilitar ou, ao menos, interromper suas operações;
* Fornecer o arcabouço técnico necessário para utilizar ferramentas, sistemas e processos na busca proativa de vulnerabilidades;
* Competências-chave: Ataques e testes de invasão.

**Desenvolvimento Seguro**

* Escrever códigos de software de forma que sejam protegidos de todos os tipos conhecidos de vulnerabilidades, ataques ou qualquer ação que possa causar danos ao software ou ao sistema que o utiliza (codificação segura);
* Empregar padrões e melhores práticas para proteger o software em todas as partes do ciclo de vida de desenvolvimento;
* Competências-chave: Segurança por Design; Segurança por Padrão.

1.4 Princípios e Diretrizes Pedagógicas

O Curso de **Tecnologia da Informação com Ênfase em Cibersegurança** envolve o desenvolvimento de competências técnicas e socioemocionais complexas. Por isso, de maneira mais ampla, sugerimos o uso de metodologias ativas, que instiguem a investigação com perguntas decorrentes do contexto profissional real. Fazem a diferença na aprendizagem aquelas atividades que proporcionam conceituações e categorizações de diferentes modelos; o uso de ferramentas digitais para que os estudantes mapeiem os conceitos e as suas aplicações práticas; fóruns de discussões em grupos virtuais,grupos de pesquisa, estudos de caso, atividades práticas em laboratórios e participação em competições,etc.

É fundamental trabalhar com exemplos e estudos de casos de cenários reais e atuais sobre o uso e as potencialidades da Cibersegurança e, ao mesmo tempo, levantar discussões de natureza Ética e Filosófica sobre o conhecimento. Os estudantes deverão demonstrar sua capacidade de articular o conhecimento teórico e propor modelos de soluções para diferentes problemas.

Aulas práticas podem também ser feitas no contexto online, de maneira síncrona ou assíncrona. O professor, após apresentar a teoria e os exemplos necessários à compreensão, poderá propor problemas ou desafios que façam sentido ao contexto dos estudantes. Sugerimos também o uso de aplicativos com ambientes gamificados para auxiliar na aprendizagem de aspectos técnicos. Como é o caso de exemplos da aprendizagem de lógica de programação com diversas ferramentas gamificadas, competições de IA no ***Kaggle*** ou em outros ambientes.

As competências socioemocionais são desenvolvidas de maneira intimamente conectada a um determinado contexto sociocultural, e por isso precisam de estratégias que articulem teoria e prática de maneira aglutinada e adaptada à realidade no qual os cursos estão inseridos. Quando falamos de competências socioemocionais estamos nos referindo a aspectos afetivo-emocionais que podem ter motivações e sistemas de recompensa diferentes, dependendo do contexto e cultura dos estudantes. Por isso, recomendamos que as estratégias pedagógicas para o desenvolvimento das competências socioemocionais sejam observadas e adaptadas continuamente, e sempre quando houver necessidade. As estratégias precisam estar sempre centradas nas experiências dos estudantes para que sejam emocionalmente significativas para eles, seja nos desafios individuais ou nos projetos em times.

Para as disciplinas que envolvem a expressão de conceitos, técnicas, ferramentas, e métodos cognitivos articulados, sugerimos que, além de aulas expositivas, tais disciplinas explorem a discussão crítica de casos; análise de textos de artigos, reportagens e documentários; produção textual dissertativo; investigação para resolução de problemas práticos e/ou criativos; e trabalhos em grupos.

Para aquelas disciplinas que demandam o domínio de competências fundamentalmente reflexivas e comportamentais, sugerimos a exploração de situações práticas de trabalho, em grupos, a comunicação oral por meio de seminários, clínicas coletivas, avaliações colaborativas e autoavaliações supervisionadas. É fundamental, nestes casos, a atuação presente do professor ou tutor treinado.

1.4.1 Sobre as Metodologias Ativas

As Metodologias de Ensino e Aprendizagem são essenciais para criar estratégias de aprendizagem, engajar o estudante e tornar a aprendizagem significativa conectada com um contexto profissional real.

“[...] diretrizes que orientam os processos de ensino e aprendizagem, que se concretizam em estratégias, abordagens e técnicas concretas, específicas e diferenciadas” (MORAN, 2018, p. 4).

As Metodologias ativas engajam os estudantes em atividades nas quais eles são proativos na construção das suas competências, habilidades e atitudes. As metodologias de ensino e aprendizagem acompanham os objetivos de cada formação. Como diz Moran (2013, p.15 ):

Se queremos que os alunos sejam proativos, precisamos adotar metodologias em que os alunos se envolvam em atividades cada vez mais complexas, em que tenham que tomar decisões e avaliar os resultados, com apoio de materiais relevantes. Se queremos que sejam criativos, eles precisam experimentar inúmeras novas possibilidades de mostrar sua iniciativa.

É importante para a trilha de aprendizagem do estudante, o professor considerar atividades que promovam a aprendizagem individual, a aprendizagem em pares ou grupos e a aprendizagem com orientação do professor, tutor ou alguém mais especializado.

Sugestão de algumas metodologias para o ensino e aprendizagem:

**Sala de Aula Invertida:**

Os estudantes fazem uma trilha de aprendizagem mais elementar sozinhos, acessam desafios, textos, e outros recursos, num ambiente estruturado pelo professor; em seguida participam de discussões e resoluções de problemas mais profundos sob a orientação deste. O professor propõe problemas que obriguem a contextualização, aplicação e ampliação da trilha básica de aprendizagem realizada pelo estudante (BERGMAN e SAM, 2020).

**Aprendizagem Baseada em Problemas:**

Propõe-se problemas a serem resolvidos para cada tema ou competência a ser construída. A ideia é desenvolver a capacidade de investigação, transdisciplinaridade do conhecimento, competências metacognitivas, como o aprender a aprender e as competências e habilidades socioemocional. Além disso, formação para os problemas reais das suas profissões.

De acordo com Barrows e Tamblyn ( 1980, p.48):

* Apresentam-se um determinado problema a um grupo de alunos, onde deverão organizar as ideias, solucionando os problemas com os seus conhecimentos prévios;
* Após a discussão, são levantados questionamentos nos quais eles não possuem conhecimento;
* Planejam os próximos passos da investigação definindo quem, como, quando e onde as questões serão investigadas.;
* Em um novo encontro, devem levantar as questões anteriores fazendo o novo planejamento para solução dos problemas com base nos novos conhecimentos adquiridos; e 5- finalizando o trabalho, os alunos avaliarão o processo e o desempenho de cada integrante do grupo

**Aprendizagem Baseada em Projetos**

Há várias modalidades de aprendizagem baseada em projetos, uma delas é o Projeto Integrador:

**Projeto Integrador:** Projeto transdisciplinar que deve ser bem estruturado em todas as suas etapas articulando teoria e prática de várias disciplinas.No planejamento do projeto integrar precisa deixar claro qual é a entrega final e o que será avaliado. O projeto integrador com bons desafios pode dar conta dos seguintes objetivos de aprendizagem:

* Contextualizar e articular os saberes;
* Desenvolver a capacidade de tomar decisão;
* Desenvolver a capacidade do discente de resolver problemas;
* Analisar, explicar e avaliar um determinado projeto de estudo, levando em conta a sociedade;
* Planejar ações;
* Estimular a oralidade;
* Desenvolver visão crítica;
* Desenvolver atitude empreendedora;
* Despertar interesse pela pesquisa;
* Melhorar a capacidade de administrar conflitos;
* Estimular a construção de conhecimento coletivo.

#### **Aprendizagem baseada em Trabalho:**

A OCDE (2021) recomendou às instituições envolvidas com Educação tecnológica desenvolver programas de inserção dos estudantes no contexto profissional.Pensar em benefícios para eles e as empresas. Isto, além das oportunidades de aprendizagem e trabalho, engaja as organizações. Alguns exigem que o curso ofertado garanta para todos os estudantes períodos nas empresas. Alguns países analisados pela OCDE tornaram o treinamento prático no trabalho obrigatório, e uma escola somente pode oferecer um curso de EPT se houver locais suficientes para o estágio dos alunos.

### 

### 

### 1.4.2 Requisitos para o Corpo Docente

Os requisitos para o corpo docente em cursos de Educação Profissional Tecnológica de Graduação estão estabelecidos nos termos do art. 66 da Lei 9.394/1996.

No artigo 57, determina que a formação dos educadores dos cursos tecnológicos requer um bom domínio dos saberes e competências profissionais, além de um bom domínio dos saberes pedagógicos necessários ao ensino e à aprendizagem. Estas formações são necessárias para que:

I - possa fazer escolhas relevantes dos conteúdos que devem ser ensinados e aprendidos, para que o formando tenha competências para responder, de forma original e criativa, aos desafios diários de sua vida profissional e pessoal, como cidadão trabalhador; II - tenha o domínio dos chamados conhecimentos disciplinares associados aos saberes pedagógicos e do conjunto dos conhecimentos da base científica e tecnológica da atividade profissional; e III - saiba fazer e saiba ensinar, estando o saber vinculado diretamente ao mundo do trabalho, no setor produtivo objeto do curso (CNE/CP, 2021, p.18).

Requer a graduação na área da sua atuação, experiência profissional e competência na área tecnológica do eixo em que atua.

# 

# 2. Perfil Curricular

A seguir a descrição da caracterização do curso em termos de habilitação, carga horária, disciplinas obrigatórias e horas dedicadas ao estágio. Além disso, a descrição de como foi pensado a organização do curso com ênfase em Cibersegurança.

## 2.1 Caracterização do Curso

Os cursos de tecnólogos do eixo Informação e Comunicação possuem carga horária que variam entre 2.000 e 2400 horas (CNCST, 2017).

| **Nome:** | Tecnologia da Informação |
| --- | --- |
| **Habilitação:** | Ênfase em Cibersegurança |
| **Modalidade:** | Tecnólogo |
| **Carga Horária:** | 2.000 horas - 2400 |
| **Período Mínimo de Integralização:** | 2 anos |
| **Disciplinas Obrigatórias:** | Definidas pela Instituição |
| **Atividades complementares:** | Definidas pela Instituição |
| **Estágio Curricular:** | Definidas pela Instituição |
| **Trabalho de conclusão de curso:** | 60 horas |

## 2.2 Organização Curricular

O curso está organizado em cinco (05) eixos de formação:

* Eixo Básico: nove (09) disciplinas relacionadas aos **Fundamentos** necessários para o aprofundamento no domínio do conhecimento de cibersegurança (Introdução à Computação; Sistemas Operacionais; Introdução à Segurança da Informação; Arquitetura e Organização de Computadores; Arquitetura de Segurança; Introdução à Computação em Nuvem; Segurança, Proteção e Privacidade de Ativos; Análise e Testes de Segurança, Criptografia Aplicada);
* Eixo 1: duas (02) disciplinas relacionadas à **Gestão da Operação** (Redes e Conectividade; Gestão da Identidade e Controle de Acesso (IAM));
* Eixo 2: duas (02) disciplinas relacionadas à **Segurança Defensiva** (Forense Computacional; e Gerenciamento de Incidentes);
* Eixo 3: duas (02) disciplinas relacionadas à **Segurança Ofensiva** (Testes de Invasão (PenTesting & Ethical Hacking); e Exploração e Desenvolvimento de Ameaças);
* Eixo 4: duas (02) disciplinas relacionadas ao **Desenvolvimento Seguro** (Introdução à Programação; e Análise de Código (Estático/Dinâmico)).

No que diz respeito ao desenvolvimento de competências Socioemocionais, notadamente existem aspectos que podem ser trabalhados de maneira disciplinar (por meio de componentes curriculares específicos), enquanto outros fazem mais sentido serem desenvolvidos de maneira transversal, por meio de atividades complementares e/ou não curriculares. Por isso, propomos a criação de um eixo curricular específico para Formação Socioemocional. Ao mesmo tempo, propomos a exploração de atividades práticas por meio de abordagens pedagógicas transversais ao longo de todas as outras disciplinas do curso, apontadas no ementário como a componente de “Prática Profissional”.

**Tabela 1 - Matriz Curricular do curso de Tecnologia da Informação**

**com Ênfase em Cibersegurança**

| **Eixo Formativo** | **1º Semestre** | **2º Semestre** | **3º Semestre** | **4º Semestre** | **5º Semestre** |
| --- | --- | --- | --- | --- | --- |
| **Eixo Básico** | Criptografia Aplicada | Arquitetura e Organização de Computadores |  |  |  |
| Introdução à Computação | Arquitetura de Segurança |  |  |  |
| Sistemas Operacionais | ​​Introdução à Computação em Nuvem |  |  |  |
| Introdução à Segurança da Informação | Segurança, Proteção e Privacidade de Ativos | Análise e Testes de Segurança |  |  |
| **Eixo 1:**  **Gestão da Operação** | Redes e Conectividade | Gestão da Identidade e Controle de Acesso (IAM) |  |  |  |
|
| **Eixo 2:**  **Segurança Defensiva** |  |  | Forense Computacional |  |  |
| Gerenciamento de Incidentes |
| **Eixo 3:**  **Segurança Ofensiva** |  |  |  | Testes de Invasão (PenTesting & Ethical Hacking) | Exploração e Desenvolvimento de Ameaças |
| **Eixo 4:**  **Desenvolvimento Seguro** |  |  | Introdução à Programação | Análise de Código (Estático/Dinâmico) |  |
|  |  |  |  |  |  |

2.3 Sistemática de Avaliação

A [Resolução CNE/CP nº 1, de 5 de janeiro de 2021](http://portal.mec.gov.br/index.php?option=com_docman&view=download&alias=167931-rcp001-21&category_slug=janeiro-2021-pdf&Itemid=30192), determina que:

*“Art. 45. A avaliação da aprendizagem dos estudantes visa à sua progressão contínua para o alcance do perfil profissional de conclusão, sendo diagnóstica, formativa e somativa, com prevalência dos aspectos qualitativos sobre os quantitativos, na perspectiva do desenvolvimento das competências profissionais da capacidade de aprendizagem, para continuar aprendendo ao longo da vida.”*

Uma avaliação contínua necessita de parâmetros e critérios de avaliação, a serem acompanhados no interior de cada disciplina e ao longo do curso. Neste sentido, uma das recomendações é a definição de rubricas por disciplina e uma síntese dessas para acompanhar o perfil do estudante em seu desenvolvimento global, ao longo do curso. As rubricas requerem clareza para os envolvidos no processo avaliativo sobre os indicadores e a evolução das competências no tempo das disciplinas.

Além disso, o conhecimento da matriz avaliativa pelo estudante permite o processo de autoconhecimento necessário a sua formação e direcionamento de estudos. A consciência de seu desenvolvimento, sua autoavaliação, facilita o profissional a migrar para uma perspectiva de aprendizagem ao longo da vida. Recomenda-se, portanto, que a matriz de rubricas seja também preenchida pelo estudante, sempre com possibilidade dele e o professor compararem as duas perspectivas.

A matriz de rubricas serve como um feedback para o estudante saber os aspectos que devem investir, e permitir uma maior confiabilidade a uma avaliação somativa, exigida pelo sistema educacional atual. É com base na matriz de rubricas de cada disciplina que a nota do estudante deve ser atribuída. Permite que o estudante identifique quais os conhecimentos avaliados, quais as habilidades e quais atitudes.

A avaliação da aprendizagem não destina-se apenas ao retorno para o estudante, serve também para pautar o repensar pelo professor de suas metodologias e ênfases tomadas ao longo da disciplina, em diferentes habilidades e competências. É nesse sentido que uma síntese das avaliações de rubricas de todos os estudantes de cada turma deve subsidiar cada professor e a coordenação do curso em um repensar contínuo de cada disciplina e uma avaliação periódica do curso, com sugestão a ser feita bi-anual.

Como determina a lei 9.694/96, que estabelece as diretrizes e bases da Educação Nacional, o processo avaliativo precisa ser:

* Constante: Deve estar inserido na relação planejamento, ensino e aprendizagem.
* Diverso: A avaliação deve ser materializada por meio de uma diversidade de instrumentos avaliativos;
* Democrático: O processo avaliativo precisa ser apresentado no começo de cada disciplina, discutido e negociado com os estudantes;
* Pertinente: De acordo com o componente curricular, o conteúdo trabalhado e os objetivos de aprendizagem do curso.

Quanto aos instrumentos de avaliação, estes se caracterizam pelos momentos e artefatos que o professor utiliza para a coleta de dados que subsidiam a sua avaliação. Os momentos e artefatos devem portanto ser variados: com produções individuais e coletivas, que permitam identificar resultados finais e processos, que possibilitem a avaliação de diferentes habilidades e competências pelo professor, em diferentes momentos da disciplina, com diferentes formas de expressão e produção. Recomenda-se como instrumentos de avaliação:

1. Resolução de problemas reais: exigindo as competências técnicas, cognitivas e socioemocionais das disciplinas do período;
2. Prova individual ou em grupo (com ou sem consulta): além da compreensão dos conceitos, com estudos de casos para avaliar o saber fazer:
3. Estudos de Casos: Contextualização e desafios para os solucionar;
4. Seminários: importantes para que sejam avaliados competências como comunicação, assertividade, organização do grupo, liderança, etc.
5. Autoavaliação : É uma das prerrogativas das competências socioemocionais, coloca o estudante como protagonista no gerenciamento da sua aprendizagem (aprender a aprender);
6. Trabalhos em grupos: Essencial para o desenvolvimento de competências requeridas no trabalho colaborativo e digital.

Além das avaliações formativas recomenda-se processos para diagnose do conhecimento do estudantes no início do processo de aprendizagem e as somativas ao término de cada ciclo de conhecimento.

Recomendações específicas são traçadas para o acompanhamento do desenvolvimento dos estudantes em relação às competências socioemocionais ao longo do curso. É importante que existam mecanismos específicos de avaliação para acompanhamento do desenvolvimento destas habilidades ao longo do curso. Recomendamos a utilização da abordagem de rubricas avaliativas, que podem ser elaboradas e modificadas com base em critérios previamente estabelecidos de acordo com os objetivos da aprendizagem. O mais importante é que a avaliação esteja sempre a serviço da aprendizagem.

# 

# 3. Ementário

## 3.1 Disciplinas do Eixo Básico

### Introdução à Computação

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

*Nenhum*

**Ementa:**

História da Ciência da Computação. Conceitos básicos. Bases numéricas. Sistemas de numeração em computação. Introdução à Ciência da Computação: a ciência, o curso e a profissão. Introdução às principais áreas da computação: redes, sistemas operacionais, segurança, inteligência artificial, banco de dados.

**Bibliografia** :

**Básica:**

* BROOKSHEAR, J. Glenn. **Ciência da Computação**: uma visão abrangente. 5a ed. Porto Alegre: Bookman, 2000.
* FEDELI, R. D.; POLLONI, E; PERES, F. **Introdução à Ciência da Computação**. São Paulo: Pioneira Thomson Learning, 2003.

**Complementar:**

* TURING, Dermot. **A História da Computação**: do ábaco à inteligência artificial. 1a ed. São Paulo: M. Books, 2019.

### 

### Introdução à Segurança da Informação

**Carga Horária:**

40 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

*Nenhum*

**Ementa:**

Esta disciplina deve abordar a descrição da arquitetura de segurança em nuvem e explora os princípios de design de segurança, padrões de design, padrões de boas práticas da indústria, e tecnologias habilitadoras que endereçam os requisitos de conformidade regulatória essenciais para projetar, implementar, entregar e gerenciar serviços seguros baseados em nuvem. A disciplina aprofunda os aspectos da arquitetura de nuvem segura com relação à identificação, gerenciamento de identidade de ponta a ponta e aspectos de controle de acesso, auditoria e atendimento de conformidade com os marcos regulatórios e da indústria. Esta disciplina se fundamenta nas diretrizes de segurança em nuvem estabelecidas pelo NIST, ISO, PCI-DSS e Cloud Security Alliance (CSA).

**Bibliografia** :

**Básica:**

* BAARS, Hans; HINTZBERGEN, Kees; HINTZBERGEN, Jule. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002. 1a ed. Rio de Janeiro: Editora Brasport, 2018.

**Complementar:**

* SAMANI, Raj; REAVIS, Jim; HONAN, Brian. **CSA Guide to Cloud Computing**: Implementing Cloud Privacy and Security. 1a ed. Amsterdam: Elsevier 2014.
* DOTSON, Chris. Practical Cloud Security: **A Guide for Secure Design and Deployment.** 1a ed. Sebastopol: O'Reilly, 2019.

### Segurança, Proteção e Privacidade de Ativos

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

Introdução à Computação;

Criptografia Aplicada.

**Ementa:**

O domínio desta disciplina se refere aos requisitos de proteção das informações para ativos (IAP) em uma organização. Ainda, a disciplina tratará desde propriedade intelectual, patentes, conhecimento científico, e/ou outros ativos intangíveis, até repositórios de dados, software, dispositivos de comunicação e armazenamento. Os principais tópicos a serem abordados em Segurança, Proteção e Privacidade de Ativos são: Identificação, classificação e propriedade de informações e de ativos; Proteção da privacidade; Retenção de ativos; Controles para segurança de dados; e Manuseio de ativos (dispositivos e informações). O objetivo dessa disciplina é capacitar o aluno a formular um programa de IAP, implementar uma estratégia baseada em mitigação de risco, e identificar potenciais lacunas de proteção.

**Bibliografia** :

**Básica:**

* KIM, David. **Fundamentos de Segurança de Sistemas de Informação.** 1. ed. Rio de Janeiro: LTC, 2014.

**Complementar:**

* PINHEIRO, Patrícia Peck (org.). **Segurança Digital**: Proteção de Dados nas Empresas. 1a ed. São Paulo: Atlas, 2020.
* VERAS, Manoel. **Computação em Nuvem**: Nova Arquitetura de TI. 1a ed. Rio de Janeiro: Editora Brasport, 2018.

### Sistemas Operacionais

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

*Nenhum*

**Ementa:**

Nesta disciplina será estudado o histórico, classificação e estrutura dos sistemas operacionais. Processos, sincronização e técnicas de escalonamento de processos; Threads; Gerência de memória em sistemas multiprogramados; Técnicas de gerência de memória real; Técnicas de gerência de memória virtual: paginação e segmentação; Sistemas de arquivos; Sistemas de E/S; Mono e Multiprogramação.Estudo de um sistema operacional real.

**Bibliografia** :

* TANENBAUM, Andrew S. MACHADO FILHO, Nery. **Sistemas operacionais modernos**. 2a ed. São Paulo: Prentice Hall, 2008.
* TANENBAUM, Andrew S. WOODHULL, Albert S. **Sistemas Operacionais: Projetos e Implementação**. Porto Alegre: Bookman, 2009.
* MACHADO, Francis Berenger; MAIA, Luiz Paulo. **Arquitetura de sistemas operacionais**. Rio de Janeiro: Editora LTC, 2013.
* DEITEL H. M.; DEITELl P. J.; CHOFFNESs D. R. **Sistemas Operacionais**. 3a ed. São Paulo: Prentice-Hall, 2005, ISBN 8576050110.

### Introdução à Computação em Nuvem

**Carga Horária:**

40 horas;

Sugestão de 10 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

*Nenhum*

**Ementa:**

Esta disciplina tem como objetivo introduzir o conhecimento sobre a terminologia e arquiteturas da nuvem, que servirá como base para a compreensão dos detalhes técnicos que irão habilitar o aluno a implantar e dar suporte a ambientes em nuvem. Para tanto necessita compreender as novas tecnologias e opções, modelos de serviço de computação em nuvem; Modelos de implantação em nuvem; Dados confidenciais, Virtualização e Criptografia, Auditoria e conformidade; Contratos de provedor de serviços em nuvem. Ao término da disciplina os estudantes precisam ter desenvolvido competências e habilidades para compreensão e identificação de diferentes modelos de implantação de serviços, auditorias e confidencialidade de dados.

**Bibliografia**:

* CHEE, Brian JS; FRANKLIN JÚNIOR, C. **Computação em nuvem**: cloud computing. tecnologias e estratégias. Trad. Mario Moro. São Paulo: M. Books do Brasil, 2013.
* VELVE, A. T.; ELSENPETER, T. J. **Cloud Computing**: Computação em Nuvem - Uma Abordagem Prática, Mei, GE. 2011.
* ERL, Thomas, PUTTINI, Ricardo, MAHMOOD, Zaigham. **Cloud Computing**: Concepts, Technology & Architecture. Prentice Hall, 2013. 528 p. ISBN 0133387526.
* SANTOS, Gerson, R. **Cloud Computing**. Data Center Virtualizado. Gerenciamento, Monitoramento, Segurança. Rio de Janeiro: Ciência Moderna, 2015.
* ANTÔNIO, Miguel Ferreira. **Introdução ao Cloud Computing**. IaaS, PaaS, SaaS, Tecnologia, Conceito e Modelos de Negócio. Lisboa: FCA, 2015.

### Criptografia Aplicada

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

*Nenhum*

**Ementa:**

Esta disciplina objetiva compreender a importância da criptografia como alternativa para implementação de confidencialidade, integridade, autenticidade ou não repúdio a informações armazenadas em computadores ou que trafegam em redes de computadores. Ainda, identificar diferentes métodos criptográficos, protocolos, algoritmos, assinaturas e certificados digitais e o uso da criptografia como componente de serviços de autenticação e controle de acesso; identificar a solução de criptografia mais adequada para cada implementação, de acordo com suas particularidades. Como os temas trabalhados na disciplinas, teremos a abordagem da utilização da criptografia para garantir requisitos de segurança de informações, sistemas e transações eletrônicas, abrangendo uma introdução à origem da criptografia; a importância da criptografia para a segurança de sistemas e informações, algoritmos criptográficos, assinaturas e certificados digitais; certificados de atributos; segurança de redes; mídias criptográficas; identificadores biométricos; cibersegurança; e impactos na sociedade contemporânea.

**Bibliografia**:

**Básica:**

* STALLINGS, W. **Criptografia e Segurança de Redes**: princípios e práticas. 6.ed. São Paulo: Prentice Hall, 2015.

**Complementar:**

* BURNETT, Steven; PAINE, Stephen. **Criptografia e Segurança**: o guia oficial RSA. Rio de Janeiro: Campus, 2002.
* SHOKRANIAN, Salahoddin. **Criptografia para iniciantes**. 2.ed. Brasília: Editora UNB, 2021.

### 

### 

### Arquitetura e Organização de Computadores

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

*Nenhum*

**Ementa:**

Esta disciplina é uma introdução à Arquitetura de Computadores que aborda a lógica digital, dados em nível de máquina a representação de instruções, conceitos de projeto de Unidade Lógica Aritmética (ALU), organização do caminho de dados, e controle do processador. Examina a análise de desempenho, hierarquia do sistema de memória, pipelining e comunicação. O foco da disciplina é fornecer uma compreensão básica dos componentes funcionais de um sistema de computador, suas características, seu desempenho e suas interações. Esta disciplina irá abranger os conceitos básicos de Arquitetura de Computadores, incluindo o controle da CPU e caminho de dados, sistemas de memória, incluindo cache e memória virtual, e subsistemas de entrada/saída.

**Bibliografia**:

* MONTEIRO, M. A. **Introdução à Organização de Computadores**. 6ª ed. LTC, 2013.
* STALLINGS, W. **Arquitetura e Organização de Computadores**. 10ª ed. Pearson, 2017.
* TANENBAUM, A. S. **Organização Estruturada de Computadores**. 7ª ed. Pearson, 2013.

### 

### Arquitetura de Segurança

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

Introdução à Segurança da Informação;

Redes e Conectividade.

**Ementa:**

O objetivo desta disciplina é fornecer os conceitos, princípios, estruturas e padrões usados para projetar, implementar, monitorar e proteger sistemas operacionais, equipamentos, redes, aplicativos e controles usados para permitir vários níveis de confidencialidade, integridade e disponibilidade. A disciplina irá trabalhar uma variedade de tópicos, dentre eles: princípios de design de processos seguros, conceitos fundamentais de modelos de segurança, seleção de controles com base nos requisitos de segurança do sistema, recursos de segurança dos sistemas de informação, vulnerabilidades de várias arquiteturas de segurança, elementos de design e soluções, criptografia, bem como segurança física, que seriam considerados por um profissional de segurança ao projetar, implementar e operar uma arquitetura de segurança para proteger os ativos mais preciosos de uma empresa: suas informações.

**Bibliografia**:

**Básica:**

* WILSON, Glenn. **DevSecOps**: A leader’s guide to producing secure software without compromising flow, feedback and continuous improvement. Sebastopol: O'Reilly, 2020.

**Complementar:**

* HSU, Tony Hsiang-Chih. **Practical Security Automation and Testing**: Tools and techniques for automated security scanning and testing in DevSecOps. Birmingham: Packt Publishing, 2019.

Análise e Testes de Segurança (Defesa)

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Gestão da Identidade e Controle de Acesso (IAM);

Arquitetura de Segurança.

**Ementa:**

Esta disciplina apresenta os conceitos e ferramentas para conduzir uma avaliação de vulnerabilidade técnica, bem como as técnicas utilizadas por abordagens práticas testadas ao longo do tempo. Essa disciplina também fornece o conhecimento e a prática necessários para proteger os sistemas de informação contra ataques como vírus, worms e outras fraquezas do sistema que representam um perigo significativo para os dados organizacionais. Ao empregar corretamente as abordagens de hacking ético e teste de penetração para descobrir técnicas comuns usadas por cibercriminosos para explorar vulnerabilidades do sistema, esta disciplina visa fornecer as perspectivas dos invasores e descobrir onde eles podem atacar em seguida.

**Bibliografia** :

**Básica:**

* WEIDMAN, Georgia. **Testes De Invasão**: Uma Inovação Prática Ao Hacking. São Paulo: Novatec Editora, 2014.
* ENGEBRETSON, Patrick. **The Basics of Hacking and Penetration Testing**: Ethical Hacking and Penetration Testing Made Easy. 2a ed. [SI]: Syngress Publishing, 2013

**Complementar:**

* FRAGA, Bruno. **Técnicas de Invasão**: Aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Editora Labrador, 2019.
* KENNEDY, D; O’GORMAN, J; KEARNS, D. **Metasploit**: The Penetration Tester’s Guide. 1a ed. São Francisco (CA): No Starch Press, 2011.
* FRAGA, Bruno; VANGLLER, Thompson. **Técnica de invasão**. Londres: Obra Pessoal, 2017.

## 

## 3.2 Disciplinas do Eixo 1: Gestão da Operação

### Redes e Conectividade

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

*Nenhum*

**Ementa:**

Esta disciplina apresenta os conceitos de rede em nuvem, incluindo terminologia e protocolos de rede, conectividade para, e entre, aplicativos e cargas de trabalho distribuídas em todas as variações de nuvens, serviços baseados em nuvem, data centers locais, redes de borda, e padrões de rede, com ênfase na segurança de implantações de nuvem e sistemas de informação. A disciplina se aprofunda na implementação de recursos de rede e conectividade, configuração de domínios e isolamento de rede, serviços DNS e entrega de conteúdo. Esta disciplina apresenta os conceitos de solução de problemas de conectividade de rede e automação de tarefas de implantação, administração e monitoramento da conexão entre os componentes distribuídos.

**Bibliografia**:

* TANENBAUM, Andrews S. **Redes de computadores**. 6.ed. Rio de Janeiro: Bookman, 2021.
* TANENBAUM, Andrew S; FEAMSTER, Nick; WETHERALL, David. **Redes de Computadores**. 6. ed, Rio de Janeiro: Bookman, 2021.
* KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet**: uma abordagem topdown. 8.ed. São Paulo: Addison Wesley, 2021.

### Gestão da Identidade e Controle de Acesso (IAM)

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Introdução à Computação;

Introdução à Segurança da Informação.

**Ementa:**

Esta disciplina irá explorar os fundamentos da criptografia, gerenciamento de identidade, princípios de controle de acesso e estratégias de confiança aplicadas à arquitetura e serviços baseados em infraestrutura em nuvem. Abordaremos técnicas de criptografia e gerenciamento de identidade para enfrentar os desafios dos aspectos de segurança de confidencialidade, integridade, disponibilidade, autenticação, autorização e responsabilidade. O curso fará uso de algoritmos criptográficos, mecanismos e tecnologias aplicadas projetadas para criptografar dados em trânsito, em uso e em repouso, para gerenciar o ciclo de vida de chaves criptográficas, na verificação e validação de identidades pessoais, de dispositivo e de host a partir da utilização de assinaturas digitais, reforçando o controle de acesso e políticas de autorização para recursos em nuvem, ferramentas para monitoramento, registro e proteção de trilhas de auditoria para atender às normas regulatórias e da indústria.

**Bibliografia** :

**Básica:**

* LIMA, Adriano Carlos. **Segurança na computação em nuvem** (Série Universitária). 1a ed. São Paulo: Editora SENAC, 2018.

**Complementar:**

* SAMANI, Raj; REAVIS, Jim; HONAN, Brian. **CSA Guide to Cloud Computing**: Implementing Cloud Privacy and Security. 1a ed. Amsterdam: Elsevier 2014.
* DIÓGENES, Yuri. **Certificação Security+**: da prática para o exame SY0-401. Rio de Janeiro: Editora Novaterra, 2015.
* LISDORF, Anders. **Cloud Computing Basics**: A Non-Technical Introduction. 1a ed. Berkeley, CA: Apress, 2021.

### 

## 

## 3.2 Disciplinas do Eixo 2: Segurança Defensiva

### Forense Computacional

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Introdução à Computação;

Sistemas Operacionais;

Introdução à Segurança da Informação;

Redes e Conectividade;

Introdução à Computação em Nuvem.

**Ementa:**

Esta disciplina irá abordar padrões, ferramentas e práticas de forense digitais que objetivam a coleta de evidências eletrônicas em rede, clientes e dispositivos móveis. Ainda, a discussão específica também incluirá o processo de introdução desta prova eletrônica em casos civis e criminais.

**Bibliografia** :

* EC-Concil. **Computer Forensics**: Investigating Network Intrusions and Cybercrime (CHFI). 2a ed. Boston (MA): Cengage Learning, 2016.
* LUTTGENS J. T.; PEPE, Matthew; MANDIA, Kevin. **Incident response & computer forensics**. 3a ed. New York (NY): McGraw-Hill, 2014.
* OETTINGER, William. **Learn Computer Forensics**: A beginner's guide to searching, analyzing, and securing digital evidence. 1a ed. Birmingham: Packt Publishing, 2020.
* DA SILVA, ELEUTÉRIO, Pedro Monteiro; MACHADO, Marcio Pereira. **Desvendando a computação forense**. São Paulo: Novatec Editora, 2019.
* VELHO, Jesus Antônio. Tratado de Computação Forense. Campinas: Millenium Editora, 2016.

### Gerenciamento de Incidentes

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Arquitetura de Segurança.

**Ementa:**

Esta disciplina introduz uma abordagem metódica para lidar com as consequências de uma violação de segurança (ou incidente). Ainda, oferece uma análise abrangente dos recursos de malware como um fator crítico para a capacidade de uma organização de obter inteligência sobre ameaças, responder a incidentes de segurança da informação e estabelecer defesas. A disciplina incluirá um aprofundamento nas ferramentas e processos necessários para se preparar e lidar com incidentes de forma que os danos sejam limitados e o tempo de recuperação seja ideal.

**Bibliografia** :

**Básica:**

* MURDOCH, D. W. Blue Team Handbook: incident response edition: a condensed field guide for the cyber security incident responder. [SI]: CreateSpace Independent Publishing, 2016.
* LUTTGENS J. T.; PEPE, Matthew; MANDIA, Kevin. Incident response & computer forensics. 3a ed. New York (NY): McGraw-Hill, 2014.

**Complementar**:

* GCIH A Complete Guide - 2021 Edition.

## 3.4 Disciplinas do Eixo 3: Segurança Ofensiva

### Testes de Invasão (PenTesting & Ethical Hacking)

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Arquitetura de Segurança;

Gerenciamento de Incidentes.

**Ementa:**

Esta disciplina irá abordar a busca e avaliação de redes e hosts alvo para busca de vulnerabilidades de segurança. Testes de penetração específicos e metodologias de hacking ético, serão discutidos e usados em dispositivos de rede, máquinas clientes e dispositivos móveis.

**Bibliografia** :

* ENGEBRETSON, Patrick. **The Basics of Hacking and Penetration Testing**: Ethical Hacking and Penetration Testing Made Easy. 2a ed. [SI]: Syngress Publishing, 2013.
* FRAGA, Bruno. **Técnicas de Invasão**: Aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Editora Labrador, 2019.
* WEIDMAN, Georgia. **Testes De Invasão**: Uma Inovação Prática Ao Hacking. São Paulo: Novatec Editora, 2014.
* PAULI, Josh. **Introdução ao Web Hacking:** Ferramentas e técnicas para invasão de aplicações web. São Paulo: Novatec Editora, 2020.
* KENNEDY, D; O’GORMAN, J; KEARNS, D. **Metasploit**: The Penetration Tester’s Guide. 1a ed. São Francisco (CA): No Starch Press, 2011.

### Exploração e Desenvolvimento de Ameaças

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Análise de Testes e Segurança;

Forense Computacional;

Testes de Invasão.

**Ementa:**

Esta disciplina oferece um estudo abrangente dos princípios e práticas de segurança de sistemas, incluindo segurança do sistema operacional, segurança de rede, segurança de software e segurança da web. A disciplina se concentrará em ameaças e vulnerabilidades comuns, junto com princípios e técnicas básicas de como projetar um sistema seguro. As práticas ajudarão a fornecer uma compreensão de como pensar como um adversário, como os ataques cibernéticos modernos e as defesas funcionam na prática e como avaliar as ameaças e os mecanismos de proteção.

**Bibliografia**:

* SIKORSKI, Michael; HONIG, Andrew. **Practical malware analysis**: the hands-on guide to dissecting malicious software. no starch press, 2012.
* SEITZ, Justin; ARNOLD, Tim. **Black Hat Python**: Python Programming for Hackers and Pentesters. No Starch Press, 2021.
* KENNEDY, David *et al*. **Metasploit**: the penetration tester's guide. No Starch Press, 2011.
* LIGH, Michael Hale *et al*. **The art of memory forensics**: detecting malware and threats in windows, linux, and Mac memory. John Wiley & Sons, 2014.

## 

## 3.5 Disciplinas do Eixo 4: Desenvolvimento Seguro

### Introdução à Programação

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

*Nenhum*

**Ementa:**

Introdução à computação; Noções de lógica; Conceitos e representação de algoritmos; Constantes e variáveis; Estruturas de controle; Vetores; Matrizes; Registros e uniões; Procedimentos, Funções com passagem de parâmetros por valor e referência; Recursividade; Introdução à linguagem de programação. Ao final desta disciplina o estudante deverá ser capaz de projetar algoritmos e de desenvolver programas.

**Bibliografia**:

**Básica:**

* FORBELLONE, André L.V; EBERSPACHER, Henri F. **Lógica de programação**: a construção de algoritmos e estruturas de dados. 3.ed. São Paulo: Pearson, 2005.

**Complementar:**

* MENEZES, Nilo Ney Coutinho. **Introdução à programação com Python:** Algoritmos e lógica de programação para iniciantes. 3a. ed. São Paulo: Novatec Editora, 2019.
* FURGERI, Sérgio. **Introdução à programação em Python**. São Paulo: Editora Senac, 2021.

### Análise de Código (Estático/Dinâmico)

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Análise e Testes de Segurança;

Introdução à Programação.

**Ementa:**

Esta disciplina irá introduzir o conhecimento necessário para construir a capacidade de analisar e revisar software e código, de forma dinâmica e estática. Descubra erros que levam diretamente a vulnerabilidades e exploração de segurança. A disciplina irá, então, aprofundar os conceitos de análise e revisão de código, oferecendo um guia completo para análise estática: como funciona, como integrá-la aos processos de desenvolvimento de software e como aproveitá-lo ao máximo durante a revisão do código de segurança. Esta disciplina também fornecerá uma visão aprofundada de conteúdo especializado, como análise de código estático, tratamento de erros, condições de corrida e mediação, manipulação de buffer e estouro de inteiro, manipulação de vulnerabilidades na programação da web e de banco de dados.

**Bibliografia** :

**Básica:**

* CHESS, Brian; WEST, Jacob. **Secure Programming with Static Analysis**. Addison-Wesley Professional, 2007.
* BLOKDYK, Gerardus. **Static Code Analysi**s: A Complete Guide. 1a ed. [SI]: 5STARCooks, 2021.

**Complementar:**

* SIKORSKI, Michael; HONIG, Andrew. **Practical Malware Analysis**: The Hands-On Guide to Dissecting Malicious Software. 1a ed. São Francisco (CA): No Starch Press, 2012.

# 

# Referências

BRASSCOM. Relatório Setorial 2020 Macrossetor de TIC. Abril de 2021. Disponível em: <https://brasscom.org.br/relatorio-setorial-2020-macrossetor-de-tic/>. Acesso em: 28 out. 2021.

CNI. Profissões Emergentes na Era Digital: Oportunidades e desafios na qualificação profissional para uma recuperação verde. Edição: julho/2021. Disponível em: <http://www.portaldaindustria.com.br/publicacoes/2021/7/profissoes-emergentes-na-era-digital-oportunidades-e-desafios-na-qualificacao-profissional-para-uma-recuperacao-verde/>. Acesso em: 28 out. 2021.

[CNST - Catálogo Nacional de Cursos Superiores de Tecnologia - 3ª Edição](http://portal.mec.gov.br/index.php?option=com_docman&view=download&alias=98211-cncst-2016-a&category_slug=outubro-2018-pdf-1&Itemid=30192)

BERGMANN, J; SAMS, A. Sala de Aula Invertida: Uma metodologia ativa de aprendizagem. 1. ed. Rio de Janeiro: LTC, 2020

BARROWS, H. S.; TAMBLYN, R. M. Problem-Based Learning: an approach to medical Education. New York: Springer Publishing Company, 1980.

MORAN, José. Metodologias ativas para uma aprendizagem profunda. In: MORAN, José; BACICH, Lilian (Org.). Metodologias ativas para uma educação inovadora: uma abordagem teórico-prática. Porto Alegre: Penso, 2018.

OCDE. Revisões da OCDE sobre Ensino Profissional e Técnico. Novembro, 2021.