# **Currículo de Referência**

Tecnologia da Informação   
com Ênfase em Segurança da Informação

# 

Sumário

[**Currículo de Referência**](#_2juv47ezg1zh) **1**

[**1. Apresentação do Curso**](#_56tr6tlrrsw) **3**

[1.2 Contexto](#_bq78v0f51qjf) 4

1.3 Perfil do Profissional Egresso 5

[1.3.1](#_kawd1eime7d0) Competências Gerais 5

1.4 Princípios e Diretrizes Pedagógicas 7

[1.4.1](#_kawd1eime7d0) Sobre as Metodologias Ativas 8

1.4.2 Requisitos para o Corpo Docente 10

[**2. Perfil Curricular**](#_e3hdgp36ybu3) **11**

[2.1 Caracterização do Curso](#_vxu3akic7s4) 11

[2.2 Organização Curricular](#_657rqz3393c7) 12

[2.3 Sistemática de Avaliação](#_wfmxurfshcxg) 14

[**3. Ementário**](#_ph5lr88au1p4) **16**

3.1 Disciplinas do Eixo Básico 16

Introdução à Computação 16

Arquitetura e Organização de Computadores 17

Redes e Conectividade 18

Introdução à Segurança da Informação 19

Banco de Dados 20

[Introdução à Programação](#_2dtpdao8j3zo) 21

Fundamentos da Análise Quantitativa 22

Estrutura de Dados 23

[3.2 Disciplinas do Eixo 1:](#_bavzfs3i0y45) Segurança Defensiva 24

Gestão de Risco 24

Operações de Segurança 25

Gestão da Identidade e Controle de Acesso (IAM) 26

Segurança, Proteção e Privacidade de Ativos 27

Gestão da Continuidade de Negócios 28

Modelagem de Ameaças 29

[3.3 Disciplinas do Eixo 2:](#_ofcvdqc016ne) Segurança Ofensiva 30

Gestão, Avaliação e Mitigação de Vulnerabilidades 30

Comunicação e Segurança de Rede 31

Avaliação e Testes de Segurança 32

[3.4 Disciplinas do Eixo 3:](#_s5xd0b7h9ya6) Desenvolvimento Seguro 33

Criptografia Aplicada 33

Segurança e Desenvolvimento de Software 34

Arquitetura e Engenharia de Segurança 35

[**Referências**](#_t0708npbrexu) **36**

# 

# 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 TI, 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 Segurança da Informação 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.

Além disso, o setor de Tecnologia da Informação 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 TI do país.

## 1.3 Perfil do Profissional Egresso

Profissionais de Segurança da Informação são responsáveis pela administração de segurança de uma ampla variedade de sistemas de TI em toda a empresa. Isso pode envolver a administração diária de ferramentas e dispositivos de segurança cibernética, bem como suporte de primeiro e segundo nível para informações de segurança e gerenciamento de eventos (SIEM). Como as obrigações de conformidade legal e regulatória continuam a crescer em impacto e importância no mundo, a função do administrador de segurança, incluindo o suporte de auditoria. Em algumas organizações, as tarefas de administração de segurança podem ser realizadas por uma equipe de administração de usuário e acesso, bem como uma equipe que lida com a configuração de segurança mais técnica e aspectos administrativos do trabalho. Para o desenvolvimento profissional, é essencial que um tecnólogo em segurança tenha um conhecimento profundo dos sistemas operacionais, corporativos e aplicativos de segurança, e ainda um conhecimento prático de protocolos e ferramentas de rede básicos.

### 1.3.1 Competências Gerais

O profissional egresso do curso de tecnólogo em **Tecnologia da Informação com Ênfase em Segurança da Informação** 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, deve se propor a desenvolver competências e habilidades digitais necessárias para o contexto de transformação digital, tais como: cultura digital, ser adaptativo às novas tecnologias, proficientes nos seus usos e trabalhar conectado em rede. Em linhas gerais, é esperado que saiba:

* Gerenciar e operar a Segurança da Informação, desde a autorização e monitoramento de acesso a instalações ou infraestrutura de TI, até a conformidade com a legislação pertinente;
* Auxiliar os usuários na definição de seus direitos e privilégios de acesso, bem como executar tarefas de administração de segurança não padrão e resolver problemas de administração de segurança;
* Garantir que os registros de segurança sejam precisos e completos e que as solicitações de suporte sejam tratadas de acordo com os padrões e procedimentos estabelecidos;
* Monitorar a aplicação dos procedimentos de administração de segurança e analisar os sistemas de informação em busca de violações reais ou potenciais de segurança;
* Auxiliar na resolução de problemas relacionados a controles de acesso e sistemas de segurança, bem como garantir que todas as violações identificadas sejam completamente investigadas e que todas as alterações do sistema necessárias para manter a segurança sejam implementadas;
* Investigar violações de segurança de acordo com os procedimentos estabelecidos, recomendar as ações necessárias e apoiar / acompanhar para garantir que estas sejam implementadas;
* Manter os processos de administração de segurança e verificar se todas as solicitações de suporte são atendidas de acordo com os procedimentos acordados, fornecendo orientação na definição de direitos e privilégios de acesso;
* Interagir de perto com fornecedores de produtos e provedores de serviços, com pessoal de vários outros departamentos de TI, bem como com departamentos de negócios e administrativo;
* Contribuir para a criação e manutenção de políticas, padrões, normas, processos, documentação e diretrizes para a segurança física e eletrônica de sistemas automatizados, garantindo que sejam adequados ao propósito, atuais e corretamente implementados;
* Revisar novas propostas de negócios e fornecer consultoria especializada sobre questões e implicações de segurança.

## 

## 1.4 Princípios e Diretrizes Pedagógicas

O Curso de **Tecnologia da Informação com Ênfase em Segurança da Informação** 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 Segurança da Informação 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:

1. **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).

1. **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

1. **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.

#### 4, **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 Segurança da Informação.

## 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 Segurança da Informação |
| **Modalidade:** | Tecnólogo |
| **Carga Horária:** | 2.000 horas - 2400 |
| **Período Mínimo de Integralização:** |  |
| **Disciplinas Obrigatórias:** | A ser decidido por cada instituição |
| **Atividades complementares:** | A ser decidido por cada instituição |
| **Estágio Curricular:** | | A ser decidido por cada instituição | | --- | |
| **Trabalho de conclusão de curso:** | A ser decidido por cada instituição |

## 

## 2.2 Organização Curricular

O curso está organizado em quatro (04) eixos de formação:

* Eixo Básico: oito (08) disciplinas relacionadas à **Tecnologia da Informação** (Introdução à Computação; Arquitetura e Organização de Computadores; Redes e Conectividade; Introdução à Segurança da Informação; Banco de Dados; Introdução à Programação; Fundamentos de Análise Quantitativa; Estrutura de Dados);
* Eixo 1: seis (06) disciplinas relacionadas à **Segurança Defensiva** (Gestão de Risco; Operações de Segurança; Gestão da Identidade e Controle de Acesso (IAM); Segurança, Proteção e Privacidade de Ativos; Gestão da Continuidade de Negócios; Modelagem de Ameaças);
* Eixo 2: três (03) disciplinas relacionadas à **Segurança Ofensiva** (Gestão, Avaliação e Mitigação de Vulnerabilidades; Comunicações e Segurança de Rede; Avaliação e Testes de Segurança);
* Eixo 3: três (03) disciplinas relacionadas ao **Desenvolvimento Seguro** (Criptografia Aplicada; Segurança e Desenvolvimento de Software; Arquitetura e Engenharia de Segurança).

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 Segurança da Informação**

| **Eixo Formativo** | **1º Semestre** | **2º Semestre** | **3º Semestre** | **4º Semestre** | **5º Semestre** |
| --- | --- | --- | --- | --- | --- |
| **Eixo Básico** | Introdução à Computação | Estruturas  de Dados |  |  |  |
| Introdução à Programação | Arquitetura e Organização de Computadores | Fundamentos de Análise Quantitativa |  |  |
| Redes e Conectividade | Banco de Dados |  |  |  |
| Introdução à Segurança da Informação |  |  |  |  |
| **Eixo 1:**  **Segurança Defensiva** |  |  | Gestão de Risco | Gestão da Identidade e Controle de Acesso (IAM) | Gestão da Continuidade de Negócios |
|  |  | Operações de Segurança | Segurança, Proteção e Privacidade de Ativos | Modelagem de Ameaças |
| **Eixo 2:**  **Segurança Ofensiva** |  |  | Gestão, Avaliação e Mitigação de Vulnerabilidades | Avaliação e Testes de Segurança |  |
|  |  | Comunicações e Segurança de Rede |  |  |
| **Eixo 3:**  **Desenvolvimento Seguro** |  |  | Criptografia Aplicada | Segurança e Desenvolvimento de Software | Arquitetura e Engenharia de Segurança |
|  |  |  |  |  |  |

## 

## 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.

## 

### 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.

### 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. Porto Alegre: Bookman, 2021.
* WETHERALL / TANENBAUM. Redes de Computadores.6. ed, Porto Alegre: Bookman, 2011
* KUROSE, James F.; ROSS, Keith W. Redes de computadores e a internet: uma abordagem topdown. 8.ed. São Paulo: Addison Wesley, 2021.

### 

### 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.

### Banco de Dados

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Introdução a programação.

**Ementa:**

Modelo de dados. Modelagem e projeto de banco de dados. Sistemas de gerenciamento de bancos de dados (SGBD): arquitetura, segurança, integridade, concorrência, recuperação após falha, gerenciamento de transações. Linguagens de consulta. Gestão de banco de dados.

**Bibliografia** :

**Básica:**

* DATE, C. J. **Uma Introdução a Sistemas de Bancos de Dados**. 6a edição. São Paulo: Edgar Blücher, 1999.
* ROB, P.; CORONEL, C. **Sistemas de Banco de Dados**: Projeto, Implementação a Administração. 8a. Ed. Boston: Cengage Learning, 2010.

**Complementar:**

* ALVES, W. P. **Banco de Dados**: Teoria e Desenvolvimento. São Paulo: Editora Érica, 2009.
* MILLER, F. **Introdução à Gerência de Banco de Dados**: Manual de Projeto. Rio de Janeiro: Editora LTC, 2009.

### 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; EBERSPACHE, 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.

### Fundamentos de Análise Quantitativa

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

*Nenhum*

**Ementa:**

Estatística descritiva; elementos de probabilidade e de inferência estatística; base conceitual, métodos e aplicações da Estatística em Ciência e Tecnologia.

**Bibliografia** :

**Básica:**

* BUSSAB, Wilton O; MORETTIN, Pedro A. **Estatística básica**. 6. ed.. São Paulo: Saraiva, 2006.
* BUSSAB, Wilton O. **Estatística básica**: métodos quantitativos. 5. ed. São Paulo: Saraiva, 2002.

**Complementar:**

* TRIOLA, Mario F. **Introdução à estatística**. 9. ed. Rio de Janeiro: LTC, 2005.
* PAPOULIS, A; PILLAI, S. U. **Probability, Random Variables and Stochastic Processes**. 4a ed. New York (NY): McGraw-Hill, 2002.

### Estrutura de Dados

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

Introdução à Programação.

**Ementa:**

Construção e raciocínio sobre diferentes algoritmos para estruturas de dados lineares e hierárquicas; construção e implementação de algoritmos para problemas de ordenação e pesquisa; Análise sobre a complexidade dos algoritmos. Ao término da disciplina o aluno deverá conhecer e diferenciar as estruturas de dados: listas, filas, pilhas, conjuntos, árvores; Manipular estas estruturas de dados por meio de algoritmos; Aplicar algoritmos de ordenação e de pesquisa; Identificar e construir estruturas de dados adequadas para modelar aplicações.

**Bibliografia**:

**Básica:**

* CORMEN, T.; LEISERSON, C.; RIVEST, R.; STEIN, R. Algoritmos: teoria e prática. [Sl]: GEN LT, 2021.

**Complementar:**

* BHARGAVA, A.Y. Entendendo Algoritmos: um guia ilustrado para programadores e outros curiosos. [Sl]: Novatec Editora, 2017.

## 

## 3.2 Disciplinas do Eixo 1: Segurança Defensiva

### Gestão de Risco

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

Introdução à Segurança da Informação.

**Ementa:**

Esta disciplina buscará compreender como diferentes componentes de um plano de segurança devem ser combinados para a elaboração de um plano integrado de segurança da informação que englobe aspectos tecnológicos e humanos envolvidos nessa tarefa; elaborar planos de segurança da informação com confidencialidade, integridade, autenticidade, disponibilidade e não repúdio às informações sensíveis; e identificar pontos críticos nos planos de segurança da informação de um ambiente e propor soluções. Dentre os temas a serem abordados, estão a construção de um plano de Gestão de Segurança da Informação; o modelo de plano gerencial e cenários de ambientes computacionais; o histórico, conceitos e definições de riscos e da análise de riscos; e os métodos e técnicas para análise de riscos.

**Bibliografia:**

**Básica:**

* MCCARTHY, N. K. **Resposta a Incidentes de Segurança em Computadores**: Planos para Proteção de Informação em Risco. Porto Alegre: Bookman, 2014.

**Complementar:**.

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

### Operações de Segurança

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Introdução à Computação;

Introdução à Segurança da Informação.

**Ementa:**

O domínio desta disciplina oferece uma visão do plano de operações com investigações, monitoramento e técnicas de proteção para segurança da informação. Ainda, discute conceitos relacionados ao suporte à investigações de incidentes segurança. Dentre os principais temas e domínios desta disciplina, serão tratados as noções básicas sobre investigações de incidentes (técnicas, coleta, manuseio e ferramentas de forense digital); requisitos internacionais para categorias de investigação; análise de registros (logs) e atividades de monitoramento; inventário, configurações e gerenciamento de ativos; conceitos básicos para operações de segurança; e técnicas de proteção de recursos.

**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:**.

* DIÓGENES, Yuri. **Certificação Security+**: da prática para o exame SY0-401. Rio de Janeiro: Editora Novaterra, 2015.

### 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.

### 

### Segurança, Proteção e Privacidade de Ativos

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

Introdução à Segurança da Informação;

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, 2015.

### 

### Gestão da Continuidade de Negócios

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

Operações de Segurança.

**Ementa:**

Nesta disciplina são apresentados os princípios de gerenciamento de continuidade de negócios, incluindo a identificação de riscos, ameaças e vulnerabilidades. A disciplina visa estabelecer os conceitos da condução de uma análise de impacto nos negócios e o desenvolvimento de planos de continuidade abrangentes. Serão introduzidas, também, as técnicas para desenvolver e avaliar programas de continuidade. Dentre os principais temas e domínios desta disciplina, serão tratados a gestão de incidentes; implantação e testes de planos de recuperação de desastres; design do processo e de teste para recuperação de desastres (DR); avaliação da segurança física; planejamento e testes de continuidade de negócios; e gestão da segurança física; gestão da segurança da informação e proteção do pessoal.

**Bibliografia**:

* MANOEL, Sergio Silva. **Sistema de Gestão de Continuidade de Negócios**: Esteja preparado para salvar a sua vida e os negócios em caso de um incidente ou desastre. 1a ed. Rio de Janeiro: Editora Brasport, 2019.
* MCCARTHY, N. K. **Resposta a Incidentes de Segurança em Computadores**: Planos para Proteção de Informação em Risco. Porto Alegre: Bookman, 2014.
* 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.

### Modelagem de Ameaças

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

Gestão de Risco.

**Ementa:**

Esta disciplina aborda as etapas básicas na criação de um modelo de ameaça, decompondo o processo etapa a etapa. A disciplina visa introduzir guias básicos de análise de ameaças, identificar quando implementar táticas de mitigação e compreender como validar a saída do modelo de ameaça. A disciplina primeiramente trará conceitos, tipos e metodologias de modelagem de ameaças; e em seguida, irá abordar as etapas básicas de análise de ameaças. A disciplina irá então apresentar a validação de ameaças, tipos e táticas de mitigação; avançando com a apresentação das Árvores de Ataque e Caminho Crítico.

**Bibliografia** :

**Básica:**

* SHOSTACK, Adam. **Threat Modeling**: Designing for Security. 1a ed. Hoboken (NJ): John Wiley & Sons, 2014.

**Complementar:**

* c

## 3.3 Disciplinas do Eixo 2: Segurança Ofensiva

### Gestão, Avaliação e Mitigação de Vulnerabilidades

## **Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Introdução à Computação;

Arquitetura e Organização de Computadores.

**Ementa:**

Esta disciplina visa introduzir os controles, processos e ferramentas de controle de vulnerabilidades, e sua aplicação na proteção de sistemas de informação. A disciplina se concentrará na avaliação e mitigação de vulnerabilidades, bem como nas arquiteturas de segurança em projetos de sistemas móveis, sistemas baseados na web e sistemas embarcados. Por fim, a disciplina se aprofunda na aplicação e implementação de princípios e controles locais de segurança.

**Bibliografia** :

**Básica:**

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

**Complementar:**

* MCCLURE, S; SCAMBRAY, J; KURTZ, G. **Hacking Exposed 7**: Network Security Secrets & Solutions. 7a ed. New York (NY): McGraw-Hill, 2012.
* KENNEDY, D; O’GORMAN, J; KEARNS, D. **Metasploit**: The Penetration Tester’s Guide. 1a ed. São Francisco (CA): No Starch Press, 2011.

### Comunicações e Segurança de Rede

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Introdução à Computação;

Arquitetura e Organização de Computadores;

Redes e Conectividade.

**Ementa:**

O domínio desta disciplina consiste no conhecimento de componentes de rede, princípios e implementação de comunicações seguras. A disciplina iniciará com o estudo dos princípios de design seguro na implementação de arquiteturas de rede: Protocolos; Modelos de implementação (ISO/OSI - IP); SDNs; Redes sem Fio. Em seguida, serão apresentados os componentes de segurança de rede: Hardwares de interconexão (firewall, switches, etc); Meios de transmissão; Dispositivos NAC; Segurança de endpoints. Por fim, a disciplina irá explorar a segurança de canais de comunicação por padrão (by default): Acesso remoto; Redes virtualizadas; e Comunicação de Dados.

**Bibliografia** :

**Básica:**

* VERAS, Manoel. **Computação em Nuvem**: Nova Arquitetura de TI. 1a ed. Rio de Janeiro: Editora Brasport, 2015.
* VERAS, Manoel. **Arquitetura de Nuvem**: Amazon Web Services (AWS). 1a ed. Rio de Janeiro: Editora Brasport, 2013.

**Complementar:**

* MCCLURE, S; SCAMBRAY, J; KURTZ, G. **Hacking Exposed 7**: Network Security Secrets & Solutions. 7a ed. New York (NY): McGraw-Hill, 2012.
* KENNEDY, D; O’GORMAN, J; KEARNS, D. **Metasploit**: The Penetration Tester’s Guide. 1a ed. São Francisco (CA): No Starch Press, 2011.

### Avaliação e Testes de Segurança

**Carga Horária:**

60 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Introdução à Programação;

Gestão, Avaliação e Mitigação de Vulnerabilidades.

**Ementa:**

Esta disciplina trata do design, implementação, avaliação de desempenho, e testes do sistema de auditoria. Dentre os principais temas e domínios desta disciplina, serão tratados as estratégias de auditoria interna, externa e de terceiros; a avaliação de testes dos controles de segurança; a coleta de dados do processo de segurança; a análise de resultados de teste e relatórios; e as auditorias de segurança.

**Bibliografia** :

**Básica:**

* WEIDMAN, Georgia. **Testes De Invasão**: Uma Inovação Prática Ao Hacking. São Paulo: Novatec Editora, 2014.
* MCCLURE, S; SCAMBRAY, J; KURTZ, G. **Hacking Exposed 7**: Network Security Secrets & Solutions. 7a ed. New York (NY): McGraw-Hill, 2012.

**Complementar:**

* VELHO, Jesus Antônio (org.). **Tratado de Computação Forense**. 1a ed. Campinas: Millennium, 2016
* SIKORSKI, Michael; HONIG, Andrew. **Practical Malware Analysis**: The Hands-On Guide to Dissecting Malicious Software. 1a ed. São Francisco (CA): No Starch Press, 2012.
* KENNEDY, D; O’GORMAN, J; KEARNS, D. **Metasp60loit**: The Penetration Tester’s Guide. 1a ed. São Francisco (CA): No Starch Press, 2011.

## 3.4 Disciplinas do Eixo 3: Desenvolvimento Seguro

### 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.

### 

### Segurança e Desenvolvimento de Software

**Carga Horária:**

60 horas.

**Pré-Requisitos:**

Introdução à Computação;

Introdução à Programação;

Arquitetura e Organização de Computadores;

Introdução à Segurança da Informação.

**Ementa:**

Esta disciplina fornece conceitos, aplicações, e modelos de implementações para segurança de software. Dentre os principais temas e domínios desta disciplina, serão tratados a compreensão e implementação da segurança no Ciclo de Vida de Desenvolvimento de Software (SDLC) por completo; a execução de controles de segurança em ambientes de desenvolvimento; a eficácia da segurança do software (auditoria, registro, análise de risco e mitigação); a avaliação do impacto de segurança; e a definição e aplicação de normas, diretrizes e boas práticas de codificação segura.

**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.

### Arquitetura e Engenharia de Segurança

**Carga Horária:**

70 horas;

Sugestão de 20 horas práticas adicionais em laboratório.

**Pré-Requisitos:**

Estruturas de Dados;

Redes e Conectividade;

Criptografia Aplicada;

Segurança e Desenvolvimento de Software.

**Ementa:**

O domínio desta disciplina inclui implementações de engenharia utilizando princípios de design seguro, bem como modelos e avaliação de competências na arquitetura organizacional da segurança. A disciplina se inicia com a exploração de conceitos fundamentais utilizados em modelos de segurança e, em seguida, irá apresentar o projeto de sistemas baseados em componentes e recursos de segurança de sistemas de informação. Finalmente, a disciplina mostrará como revisar a segurança da plataforma tecnológica.

**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.

### 

.

# 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.