



INSTITUTO FEDERAL

Ceará

Campus Tabuleiro do Norte

**DEPARTAMENTO DE ENSINO
COORDENAÇÃO DO CURSO
PROGRAMA DE UNIDADE DIDÁTICA – PUD**

DISCIPLINA: FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO	
Código: ADS504	
Carga Horária Total: 40h	CH Teórica: 30h CH Prática: 10h CH PPS: 0h CH Extensão: 0h
Número de Créditos: 2	
Pré-requisitos: -	
Semestre: 5	
Nível: Superior Tecnológico	
EMENTA	
Princípios e conceitos em segurança da informação. Análise e tratamento de riscos. Regulamentações Legais e Padrões de Segurança da Informação. Segurança de aplicações, de base de dados e de comunicações	
OBJETIVO	
Objetivo geral Utilizar os princípios e métodos de segurança necessários para projetar, implementar e implantar sistemas de software. Objetivos específicos - Implementar soluções em segurança da informação; - Planejar e apresentar políticas para controle de riscos com análise de risco em ativos; - Avaliar e propor melhorias no controle de acesso através de normas de segurança e leis de proteção; - Propor segurança em aplicações e em bases de dados; - Desenvolver um perfil adequado de profissional de sistemas de informação.	
PROGRAMA	
PRINCÍPIOS E CONCEITOS EM SEGURANÇA DA INFORMAÇÃO • Conceitos básicos de segurança em TI; • O ciclo de vida de uma informação e sua segurança; • Classificação e controle dos ativos de informação; • Segurança no ambiente físico e lógico; • Ataques à segurança e ameaças.	

ANÁLISE E TRATAMENTO DE RISCOS

- Riscos;
- Identificação e análise e tratamento de riscos de segurança;
- Visão geral das normas NBR ISO/IEC 27005 e 15999;
- Firewall, IDS, IPS e WAF;
- Técnicas de defesa.

REGULAMENTAÇÕES LEGAIS E PADRÕES DE SEGURANÇA DA INFORMAÇÃO

- Normas de segurança da informação;
- Normas NBR ISO/IEC 27001;
- Normas NBR ISO/IEC 27002;
- Lei Geral de Proteção de Dados (LGPD);
- Aspectos que impactam o desenvolvimento de software.

SEGURANÇA DE APLICAÇÕES, DE BASE DE DADOS E DE COMUNICAÇÕES

- Softwares maliciosos;
- Sistemas de backup;
- Testes de penetração;
- Análise de logs;
- Rede privada virtual;
- Conceitos de criptografia e a PKI.

IMPLEMENTAÇÕES DE CÓDIGO PARA SOFTWARE SEGURO

- Exemplos e aplicações.

METODOLOGIA DE ENSINO

Aulas teóricas:

- As estratégias de aprendizado farão uso de aulas expositivas, a fim de apresentar o conjunto de conhecimentos sistêmicos acerca da Segurança da informação, contextualizando com as vivências práticas do conteúdo em sala de aula, oportunizando os discentes a vivenciar o processo de implementação de segurança em corporações focado nas etapas do desenvolvimento. Além disso, os discentes devem conhecer sobre as legislações que envolvem o desenvolvimento de software e o cliente. Reconhecendo as diferentes aptidões e experiências dos estudantes, deve-se ter atenção às dificuldades distintas apresentadas pelos discentes e estimular experiências complementares de aprendizagem que atendam, mais proximamente, às necessidades particulares de comunicação do(a) aluno(a). Como recursos de apoio, tem-se a utilização do quadro branco, projetor de slides e livro(s) de referência(s).

Aulas práticas:

- Atividades práticas serão conduzidas nos Laboratórios de Informática e CAD, com o apoio de desktops e softwares específicos disponibilizados, visando a consolidação dos conceitos vistos em sala de aula, por meio do uso e melhoramento de suas habilidades de trabalho ativo, onde a ênfase está na reflexão sobre o que se faz, provocando o encontro de significados no que for visto na aula teórica.
- Como recursos de apoio, tem-se a utilização de equipamentos de redes e cabos, simuladores de plataformas online de ensino aprendizagem de redes de computadores e trabalhos dirigidos à implementação de redes funcionais;
- Uso da aprendizagem baseada em resolução de problemas com foco na interdisciplinaridade para projetar softwares seguros.

AValiação

A avaliação se dará de forma contínua, considerando aspectos qualitativos e quantitativos, em conformidade com as diretrizes estabelecidas no Regulamento da Organização Didática (ROD). Considerando seu caráter formativo, os instrumentos de avaliação deverão prever retorno aos estudantes sobre seus progressos e orientações para sanar dificuldades. Os instrumentos de avaliação serão diversificados e deverão estimular a análise e implementação de recursos de segurança. Os instrumentos de avaliação a serem adotados serão realização de trabalhos, apresentações, individuais e em grupo, visitas técnicas para análise e elaboração de política de segurança entre outros. A escolha dos instrumentos deve considerar o perfil da turma e ser um facilitador do processo de ensino e aprendizagem. Durante toda a continuidade do processo ensino-aprendizagem, sugere-se a promoção, em alta frequência, de avaliações formativas capazes de proporcionar ao docente um feedback imediato de como estão as interferências pedagógicas em sala de aula, e permitindo ao aluno uma reflexão sobre ele mesmo, exigindo autoconhecimento e controle sobre a sua responsabilidade, frente aos conteúdos já vistos em aula, privilegiando a preocupação com a satisfação pessoal do aluno e juntando informações importantes para mudanças na metodologia e intervenções decisivas na construção de conhecimento dos discentes, inclusive com subsídios para propostas de atividades de recuperação paralela na(s) reunião(es) de colegiado de curso, coordenadoria de curso e demais setores ligados ao ensino.

BIBLIOGRAFIA BÁSICA

- [1] HANS BAARS; KEES HINTZBERGEN; JULE HINTZBERGEN; ANDRÉ SMULDERS. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Editora Brasport. Livro. (0 p.). ISBN 9788574528670.
- [2] VISACRO, Alessandro. **A Guerra na era da informação**. Contexto. Livro. (226 p.). ISBN 9788552000433.
- [3] GALVÃO, Michele da Costa (organização). **Fundamentos em Segurança da Informação**. São Paulo: Pearson Education do Brasil, 2015. Livro. (128 p.). ISBN 9788543009452.

BIBLIOGRAFIA COMPLEMENTAR

- [1] MACHADO, Felipe Nery R. **Segurança da informação - princípios e controle de ameaças - 1ª edição - 2014**. Editora Saraiva, 2014. E-book. ISBN 9788536531212. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788536531212/>. Acesso em: 23 de fev. 2023.
- [2] BARRETO, Jeanine dos S.; ZANIN, Aline; MORAIS, Izabelly Soares de; VETTORAZZO, Adriana de S. **Fundamentos de segurança da informação**. Grupo A, 2018. E-book. ISBN 9788595025875. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788595025875/>. Acesso em: 23 de fev. 2023.
- [3] MORAIS, Izabelly Soares de; GONÇALVES, Glauber Rogerio B. **Governança de tecnologia da informação**. Grupo A. E-book. ISBN 9788595023437. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788595023437/>. Acesso em: 23 de fev. 2023.
- [4] GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9786555060164/>. Acesso em: 23 de fev. 2023.
- [5] TERADA, Routo. **Segurança de dados**. Editora Blucher, 2008. E-book. ISBN 9788521215400. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788521215400/>. Acesso em: 23 de fev. 2023.

Coordenador do Curso

Setor Pedagógico