



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
SUL-RIO-GRANDENSE
Campus Camaquã

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL SUL-RIO-GRANDENSE
CAMPUS CAMAQUÃ

PLANO DE ENSINO

1. DADOS DE IDENTIFICAÇÃO	
NOME DO CURSO: Técnico em Informática	TURMA: 47751 - TEC.3665
TURNO: Tarde	REGIME: Anual
PROFESSOR: Vinícius Alves Hax	
DISCIPLINA: Administração e Segurança em Redes de Computadores	
Vigência: Março a Dezembro de 2024	Período Letivo: 2024
Carga Horária Semanal: 3 h/a	Carga Horária Total: 90h
Ementa: Construção de saberes teóricos e práticos relacionados aos princípios de funcionamento da tecnologia cliente-servidor, proporcionando a implementação dos principais serviços presentes nas redes de comunicação, como o serviço de resolução de nomes (DNS), configuração automática dos parâmetros de rede (DHCP), serviço WEB, transferência de arquivos e serviço de diretórios. Estudo dos conceitos gerais que envolvem a segurança da informação. Busca da compreensão dos tipos de ameaças e os respectivos mecanismos usados para minimizar os riscos de tais ameaças.	

2. OBJETIVOS

2.1 Objetivos gerais

O objetivo geral da disciplina Administração e Segurança de Redes de Computadores é capacitar os alunos a adquirir conhecimentos teóricos e práticos relacionados aos princípios de funcionamento da tecnologia cliente-servidor e à implementação dos principais serviços presentes nas redes de comunicação. Além disso, visa proporcionar uma compreensão abrangente dos conceitos gerais que envolvem a segurança da informação, incluindo tipos de ameaças e os mecanismos utilizados para minimizar os riscos associados a essas ameaças.

2.2 Objetivos Específicos:

1. Compreender os princípios de funcionamento da arquitetura cliente-servidor e sua aplicação na implementação de serviços de rede.
2. Dominar a configuração e administração dos principais serviços presentes em redes de comunicação, tais como DNS, DHCP, serviço web, transferência de arquivos e serviço de diretórios.
3. Explorar os conceitos fundamentais relacionados à segurança da informação, incluindo a identificação e classificação dos tipos de ameaças que podem comprometer a integridade, confidencialidade e disponibilidade dos dados.
4. Conhecer os mecanismos e técnicas utilizados para minimizar os riscos de segurança da informação, incluindo políticas de acesso, criptografia, firewalls, detecção de intrusão, entre outros.
5. Desenvolver habilidades práticas para configurar e administrar medidas de segurança em redes de computadores, garantindo a proteção eficaz dos sistemas e dados contra ameaças cibernéticas.

3. CONTEÚDOS

UNIDADE I – Domain Name Server (DNS)

- 1.1 Funcionamento do serviço do DNS
- 1.2 Instalação e configuração do serviço de DNS
- 1.3 Ferramentas de consulta ao serviço de DNS

UNIDADE II – Dynamic Host Configuration Protocol (DHCP)

- 2.1 Funcionamento
- 2.2 Instalação e configuração do serviço DHCP
- 2.3 Configuração no cliente

UNIDADE III – Servidor WEB

- 3.1 Funcionamento
- 3.2 Instalação e configuração do servidor WEB

UNIDADE IV – Servidor de Domínio

- 4.1 Funcionamento
- 4.2 Instalação e configuração do servidor de domínio
- 4.3 Gerenciamento de Usuários
- 4.4 Inclusão de clientes ao domínio

UNIDADE V – Servidor de Arquivo

- 5.1 Conceitos
- 5.2 Instalação e configuração do serviço de compartilhamento de arquivos
- 5.3 Permissões

UNIDADE VI – Segurança em Redes de Computador

- 6.1 Conceitos Básicos
- 6.2 Ameaças Virtuais e técnicas de computacionais
- 6.3 Criptografia
- 6.4 Ferramentas de Segurança
 - 6.4.1 Antivírus
 - 6.4.2 Firewall

4. Metodologia:

A metodologia será composta por um misto das seguintes atividades:

1. Aulas expositivas: Apresentações teóricas dos princípios de funcionamento da tecnologia cliente-servidor, dos serviços de rede e dos conceitos gerais de segurança da informação, utilizando recursos visuais e exemplos práticos para facilitar a compreensão dos alunos.
2. Laboratórios práticos: Exercícios práticos em laboratório para permitir que os alunos configurem e administrem os principais serviços de rede, bem como implementem medidas de segurança, como firewalls, criptografia e políticas de acesso.
3. Estudos de caso: Análise e discussão de casos reais de incidentes de segurança, incluindo exemplos de ameaças cibernéticas e os mecanismos de defesa utilizados para mitigar essas ameaças.
4. Simulações e testes de segurança: Utilização de ferramentas e técnicas de simulação e teste de segurança para avaliar a eficácia das medidas de proteção implementadas e identificar possíveis vulnerabilidades nos sistemas e redes.
5. Trabalhos práticos individuais e em grupo: Realização de projetos práticos que envolvam a configuração, administração e segurança de redes de computadores, incentivando a aplicação dos conhecimentos adquiridos e a colaboração entre os alunos.

5. AVALIAÇÃO

Na primeira etapa serão desenvolvidos dois trabalhos de ordem prática, um deles individual e outro em grupo. Na segunda etapa será feita uma avaliação escrita individual e com consulta à material impresso e um trabalho de ordem prática em grupo.

Cada uma das avaliações terá peso 5,0.

A reavaliação de cada semestre aos alunos que não demonstrarem atingir as competências mínimas será feita na forma de uma prova escrita ao final do período letivo.

6. RELAÇÕES DAS DISCIPLINAS COM AS DEMAIS ÁREAS

As disciplinas de redes de computadores são importantes pois a maioria dos softwares hoje em dia faz uso da comunicação em rede. Especificamente a disciplina de Administração e Segurança de Redes permite que os alunos possam aprender mais como funciona a administração e instalação básica de ambientes computacionais do tipo cliente-servidor. Os alunos também aprendem alguns fundamentos de segurança que permita que os ambientes configurados sejam protegidos de alguns tipos de ataques.

7. OBSERVAÇÕES

Sem observações.

8. CRONOGRAMA DE CONTEÚDOS E ATIVIDADES

Semana	Conteúdos/Atividades	Quantidade de períodos
	Atividades síncronas	
07/03	Apresentação da disciplina	3
14/03	Revisão de Redes 2	3
21/03	Introdução à Segurança da Informação	3
28/03	Servidor Web: conceitos e configuração básica	3
27/06	Introdução ao uso de Docker e containers	3
04/07	Comandos básicos no Docker	3
11/07	Criando uma imagem Docker	3
18/07	Configuração de rede no Linux	3
25/07	DHCP: Conceitos e configuração básica	3
01/08	DNS: Conceitos e configuração básica	3
08/08	Instalação de outros serviços com Docker	3
15/08	Outras configurações de DNS	3
22/08	Segurança em Redes de Computador	3
24/08	Sábado letivo: Gincana	3
29/08	Criptografia	3
05/09	Ameaças virtuais e técnicas de ataque	3
12/09	Conselhos de classe	3
03/10	Atividade simulada prática de ataque de segurança	3
10/10	Ferramentas de segurança	3
17/10	Ferramentas de segurança (2)	3
24/10	Configuração de firewall	3
31/10	Revisão da matéria e exercícios	3
07/11	Avaliação	3
14/11	Cloud computing: teoria e prática	3

21/11	Servidor de domínio: conceitos e funcionamento básico	3
28/11	Instalação e configuração de servidor de domínio	3
05/12	Inclusão de clientes no domínio	3
12/12	Gerenciamento de usuários	3
19/12	Desenvolvimento de trabalho	3
30/01/25	Servidor de arquivos: conceitos e funcionamento básico	3
06/02/25	Instalação e configuração de servidor de arquivos	3
13/02/25	Desenvolvimento de trabalho	3
20/02/25	Encerramento da disciplina	3
27/02/25	Conselhos de classe	3
	Total de períodos síncronos	102
	Atividades assíncronas	
13/07	Análise do vídeo "O melhor sistema operacional para programação"	3
18/07	Análise do vídeo "O melhor sistema operacional para programação" (continuação)	3
08/08	Análise de vídeo sobre Segurança da Informação	3
14/11	Análise de vídeo sobre Cloud Computing	3
19/12	Análise de vídeo sobre Servidores Windows	3
08/02/25	Análise de vídeo sobre carreira na área de redes de computadores	3
	Total de períodos assíncronos	18
	Total de períodos	120
	Total de horas aula (Períodos x 0,75)	90 h.a.

9. Referências Bibliográficas Básicas

SCHMITT, Marcelo Augusto Rauh; PERES, André; LOUREIRO, César Augusto Hass. Redes de computadores: nível de aplicação e instalação de serviços. Porto Alegre, RS: Bookman, 2013. XII, 173 p. ISBN 9788582600931.

STANEK, William R. Windows Server 2012: guia de bolso. Porto Alegre: Bookman, 2014. XXIX, 678 p. ISBN 9788582601686.

NEMETH, Evi; SNYDER, Gary; HEIN, Trent R. Manual completo do Linux: guia do administrador. 2. ed. São Paulo, SP: Pearson Prentice Hall, 2007. 684 p. ISBN 9788576051121.

GOODRICH, Michael T.; TAMASSIA, Roberto. Introdução à segurança de computadores. Porto Alegre: Bookman, 2013. XVIII, 550 p. ISBN 9788540701922.

STALLINGS, William. Criptografia e segurança de redes. 6. ed. São Paulo: Pearson, 2014. 580 p. ISBN 9788543005898.

10. Referências Bibliográficas Complementares

PERES, André; SCHMITT, Marcelo Augusto Rauh; LOUREIRO, César Augusto Hass. Redes de computadores II: níveis de transporte e rede. Porto Alegre, RS: Bookman, 2014. 114 p. (Tekne). ISBN 9788582601471.

Assinatura Professor (a)

Data: 28/03/2024

Assinatura Supervisor Escolar

Data:-----/-----

Observações da Direção de Ensino e/ ou Supervisão: