Ministério da Educação
UNIVERSIDADE FEDERAL DO PARANÁ
Setor de Ciências Exatas
Departamento de Informática

# Ficha 2 (variável)

Execução da disciplina em Ensino Remoto conforme Resolução CEPE 22/21, Artigos 1º e 2º.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Disciplina: Segurança Computacional | | | | | | | Código: CI1007 |
| Natureza:<br>( x ) Obrigatória<br>( ) Optativa | ( x ) Semestral ( ) Anual ( ) Modular | | | | | | |
| Pré-requisito: | Co-requisito: | Modalidade: ( ) Presencial ( ) Totalmente EaD ( )____ *C.H.EaD | | | | | |
| **CH Total: 60**<br>**CH semanal: 4** | Padrão (PD): 60 | Laboratório (LB): 00 | Campo (CP): 00 | Estágio (ES): 00 | Orientada (OR): 00 | Prática Específica (PE): 00 | |
| Estágio de Formação Pedagógica (EFP): | Extensão (EXT): 00 | Prática como Componente Curricular (PCC): 00 | | | | | |

**Indicar a carga horária semestral (em PD-LB-CP-ES-OR-PE-EFP-EXT-PCC)**
***Indicar a carga horária que será à distância.**

## EMENTA (Unidade Didática)

Conceitos básicos.
Vulnerabilidades e ataques
Introdução à criptografia.
Autenticação e controle de acesso.
Segurança de sistemas e aplicações.
Segurança em redes e na Internet.
Mecanismos de proteção, gestão de riscos e auditoria

**PROGRAMA (itens de cada unidade didática)**

1. Conceitos básicos: princípios e propriedades fundamentais para segurança computacional; legislação sobre cibercrimes; ética em computação e segurança
2. Vulnerabilidades e ataques: Tipos de vulnerabilidades e classes ataques
3. Introdução à criptografia: cifragem simétrica e assimétrica; hashes; assinaturas digitais; certificados; infraestruturas de chaves públicas
4. Autenticação e controle de acesso: autenticação local, em rede e distribuída; políticas, modelos e mecanismos de controle de acesso
5. Segurança de sistemas e aplicações: ataques contra sistemas e mecanismos de defesa; segurança de sistemas; segurança em aplicações Web; desenvolvimento seguro
6. Segurança em redes: filtragem de pacotes; firewalls; DMZ; ataques contra redes; protocolos de segurança
7. Mecanismos de proteção, gestão de riscos e auditoria: gerenciamento de riscos e vulnerabilidades; logs; testes de invasão; detecção de intrusão; antivírus; análise de malware; perícia forense computacional

**OBJETIVO GERAL**

O aluno deve ser capaz de pensar criticamente sobre os problemas de segurança passíveis de ocorrer em um sistema ou rede, bem como possíveis soluções para mitigá-los. Deve também ser capaz de buscar formas de identificar ameaças e vulnerabilidades, planejar a implantação de mecanismos de defesa e gerenciar adequadamente o processo de manutenção de segurança em uma organização.

**OBJETIVO ESPECÍFICO**

1. Entender o que é segurança computacional e os princípios fundamentais que norteiam a área;
2. Identificar ameaças, vulnerabilidades e ataques contra sistemas, redes e informação;
3. Aprender conceitos introdutórios sobre criptografia, mecanismos que a implementam e suas aplicações em segurança;
4. Compreender os mecanismos utilizados para prover autenticação e controle de acesso em sistemas e redes;
5. Estudar ataques clássicos e modernos de forma a entender como são feitos, que vulnerabilidades exploram e por que funcionam;
6. Conhecer o funcionamento dos mecanismos de defesa utilizados em sistemas e redes;
7. Instalar e configurar mecanismos de defesa tradicionais para analisar sua eficácia, eficiência e limitações;

8. Implementar ferramentas para varredura de vulnerabilidades, automatização de ataques e/ou detecção de ameaças;
9. Utilizar ferramentas (defensivas e ofensivas) para gerenciamento de vulnerabilidades em um sistema/rede: configuração, instalação, execução, atualização, monitoramento;
10. Conhecer as normas e padrões que regem a segurança da informação e estudar conceitos éticos sobre pesquisa, desenvolvimento e atuação na área.

**PROCEDIMENTOS DIDÁTICOS**

A disciplina será desenvolvida mediante aulas expositivas para apresentação dos conteúdos curriculares teóricos ou demonstrações feitas pelo professor, e através de atividades de laboratório nas quais as ferramentas e mecanismos serão implementados ou instalados, bem como avaliados na prática em ambiente controlado (máquinas virtuais).

As aulas serão ministradas via ferramentas de vídeo-conferência (BBB, jitsi, Zoom ou Teams) e as atividades e testes serão disponibilizados via Moodle.

Cronograma: os assuntos listados no item “PROGRAMA” serão dados naquela ordem, em no máximo duas aulas síncronas de 2 horas (cada) por semana.

**FORMAS DE AVALIAÇÃO**

- P1 e P2: Prova de conhecimentos teóricos (conteúdo até a aula expositiva anterior à avaliação)
- S1: Apresentação de seminário (artigo a ser sorteado oportunamente)
- T1: Trabalho prático com implementação, instalação, configuração e/ou testes de mecanismos de segurança

**Média Final: 40% (P1+P2)/2, 25% (S), 35% (T)**

**BIBLIOGRAFIA BÁSICA (mínimo 03 títulos)**

[1] Ross J. Anderson.Security Engineering: A Guide to Building Dependable Distributed Systems. 1a.edição. Wiley Publishing, 2001.

[2] Willian Stallings.Criptografia e segurança de redes: princípios e práticas. 6a. edição. Pearson, 2015.

[3] Emilio Nakamura e Paulo Lício de Geus.Segurança de redes em ambientes cooperativos. Novatec,2010.

**BIBLIOGRAFIA COMPLEMENTAR (mínimo 05 títulos)**

[4] Michael T. Goodrich e Roberto Tamassia.Introdução à Segurança de Computadores. Bookman, 2013.

[5] David Kim e Michael G. Solomon.Fundamentos de segurança de sistemas de informação. LTC, 2014.

[6] Mark Stamp e N. J. Hoboken.Information Security: Principles and Practice. Wiley-Interscience, 2006.

[7] Ross J. Anderson.Security Engineering: A Guide to Building Dependable Distributed Systems. 2aed.Wiley Publishing, 2008.ISBN: 9780470068526.

[8] Matt Bishop.Computer Security: Art and Science. Addison-Wesley Professional, 2005.

**Professor da Disciplina:** André Ricardo Abed Grégio

**Assinatura:** _____

**Chefe de Departamento ou Unidade equivalente:** Fabiano Silva

**Assinatura:** _____

Ministério da Educação
UNIVERSIDADE FEDERAL DO PARANÁ
Setor de Ciências Exatas
Departamento de Informática

**CRONOGRAMA – PERÍODO ESPECIAL 2021/2021**

| Data | Conteúdo | Horas | Tipo Atividade |
|---|---|---|---|
| 21/09/2021 | Apresentação da disciplina | 2 | Aula online síncrona |
| 23/09/2021 | Princípios básicos de segurança | 2 | Aula online síncrona |
| 28/09/2021 | Vulnerabilidades e Ataques | 2 | Aula online síncrona |
| 30/09/2021 | Ataques avançados | 4 | Aula assíncrona |
| 05/10/2021 | Introdução à criptografia | 2 | Aula online síncrona |
| 07/10/2021 | Controle de acesso | 2 | Aula online síncrona |
| 12/10/2021 | | | |
| 14/10/2021 | Gerenciamento de riscos | 2 | Aula online síncrona |
| 19/10/2021 | Apresentação de seminários | 4 | Aula online síncrona |
| 21/10/2021 | Apresentação de seminários | 4 | Aula online síncrona |
| 26/10/2021 | Apresentação de seminários | 4 | Aula online síncrona |
| 28/10/2021 | Prova 1 | 3 | Prova no Moodle |
| 02/11/2021 | | | |
| 04/11/2021 | Segurança em profundidade | 2 | Aula online síncrona |
| 09/11/2021 | Firewalls & Antivírus | 2 | Aula online síncrona |
| 11/11/2021 | Análise de malware | 2 | Aula online síncrona |
| 16/11/2021 | Registros de auditoria (logs) | 2 | Aula online síncrona |
| 18/11/2021 | Sistemas de Detecção de Intrusão | 2 | Aula online síncrona |
| 23/11/2021 | Desenvolvimento seguro | 2 | Aula online síncrona |
| 25/11/2021 | Testes de invasão | 2 | Aula online síncrona |
| 30/11/2021 | Apresentação de Trabalhos | 4 | Aula online síncrona |
| 02/12/2021 | Apresentação de Trabalhos | 4 | Aula online síncrona |
| 07/12/2021 | Apresentação de Trabalhos | 4 | Aula online síncrona |
| 09/12/2021 | Prova 2 | 3 | Prova no Moodle |
| 14/12/2021 | Semana de estudos | | |
| 16/12/2021 | Exame Final | | |