

## Plano de Ensino – Atividades Remotas Emergenciais – 2020/2

Código	DCC831
Disciplina	TTECC: Cibersegurança
Turma	P10
Professor	Leonardo Barbosa e Oliveira

### Ementa.

Princípios de segurança da informação, Cibersegurança, vulnerabilidades, Common Vulnerability Scoring System

### Programa

Aula	Data	Conteúdo previsto	Modalidade	Interação
1	2ª's e 4ª's	Apresentação do curso	Síncrona	MS Teams
2		Introdução à segurança da informação	Síncrona	MS Teams
3		Introdução à segurança da informação	Síncrona	MS Teams
4		Princípios de Segurança de Software	Síncrona	MS Teams
5		Princípios de Segurança de Software	Assíncrona	Vídeo
6		Seminários	Síncrona	MS Teams
7		Lab de Princípios de Segurança de Software	Assíncrona	Vídeo
8		Introdução ao CVSS	Síncrona	MS Teams
9		Seminários	Síncrona	MS Teams
10		Prólogo de classificação de vulnerabilidade	Assíncrona	Vídeo
11		Lab de classificação de vulnerabilidade	Assíncrona	Moodle
12		Seminários	Síncrona	MS Teams
13		Classificação de vulnerabilidade	Assíncrona	Vídeo
14		Lab de classificação de vulnerabilidade	Assíncrona	Moodle
15		Seminários	Síncrona	Remoto
16		Predição de risco de vulnerabilidade	Assíncrona	Vídeo
17		Lab de previsão de risco de vulnerabilidade	Assíncrona	Moodle
18		Seminários	Síncrona	MS Teams
19		Predição de risco de vulnerabilidade, parte 2	Assíncrona	Vídeo
20		Lab de predição de risco de vulnerabilidade, parte 2	Assíncrona	Moodle
21		Seminários	Síncrona	MS Teams
22		Classificação de vulnerabilidade com NN	Assíncrona	Vídeo
23		Classificação de vulnerabilidade com NN lab	Assíncrona	Moodle
24		Seminários	Síncrona	MS Teams
25		Classificação de vulnerabilidade com NN parte 2	Assíncrona	Vídeo
26		Lab Classificação de vulnerabilidade com NN parte 2	Assíncrona	Moodle
27		Seminários	Síncrona	MS Teams
28		Classificação de vulnerabilidade com NLP	Assíncrona	Vídeo
29		Lab de Classificação de vulnerabilidade com NLP	Assíncrona	Moodle
30		Seminários	Síncrona	MS Teams

## Bibliografia

### Digital Security

Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte, The Shellcoder's Handbook: Discovering and Exploiting Security Holes

Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications

Michael T. Goodrich & Roberto Tamassia, Introduction to Computer Security

Jon Erickson, Hacking The Art of Exploitation

Pfleeger and Pfleeger, Security in Computing

Ross Anderson, Security Engineering

[Charu C. Aggarwal, Outlier Analysis](#)

S1 [I/A] A Large-Scale Empirical Study of Security Patches  
<https://dl.acm.org/doi/abs/10.1145/3133956.3134072>

S2 [I] VulPecker: an automated vulnerability detection system based on code similarity analysis  
<https://dl.acm.org/doi/abs/10.1145/2991079.2991102>

S3 [I] Predicting Vulnerable Software Components via Text Mining  
<https://ieeexplore.ieee.org/document/6860243>

S4 [I] Automated identification of security issues from commit messages and bug reports  
<https://dl.acm.org/doi/abs/10.1145/3106237.3117771>

S5 [I] Cross-Project Transfer Representation Learning for Vulnerable Function Discovery  
<https://ieeexplore.ieee.org/document/8329207>

S6 [I] VCCFinder: Finding Potential Vulnerabilities in Open-Source Projects to Assist Code Audits  
<https://dl.acm.org/doi/abs/10.1145/2810103.2813604>

S7 [A] Learning to Catch Security Patches  
<https://arxiv.org/abs/2001.09148>

S8 [I] When a Patch Goes Bad: Exploring the Properties of Vulnerability-Contributing Commits  
<https://ieeexplore.ieee.org/abstract/document/6681339>

S9 [A] SPAIN: Security Patch Analysis for Binaries Towards Understanding the Pain and Pills  
[https://ieeexplore.ieee.org/abstract/document/7985685?casa\\_token=a-khXG6WCyEAAAAA:4a9WpbBy-](https://ieeexplore.ieee.org/abstract/document/7985685?casa_token=a-khXG6WCyEAAAAA:4a9WpbBy-)

[Lb6FOvUiHpXrq318PWPUIgQxuDWARVUEgYbQISqpvXJpKmg9JpilpegMiHmr  
pJXla0](#)

S10 [A] Historical Analysis of Exploit Availability Timelines

<https://www.usenix.org/system/files/cset20-paper-householder.pdf>

S11 [A] Patch Based Vulnerability Matching for Binary Programs

[https://dl.acm.org/doi/pdf/10.1145/3395363.3397361?casa\\_token=JaxScrN2Ni8  
AAAAA:yq65mBxi72UD2gRDzJtL0ICFQJZIDOA8\\_xjuMiP0pggQCzS7LjU6v8q  
O8SHxCCPr\\_jGBw33P9RWyzA](https://dl.acm.org/doi/pdf/10.1145/3395363.3397361?casa_token=JaxScrN2Ni8AAAA:yq65mBxi72UD2gRDzJtL0ICFQJZIDOA8_xjuMiP0pggQCzS7LjU6v8qO8SHxCCPr_jGBw33P9RWyzA)

### **Avaliações**

1	Laboratórios: 50 pts	50 pontos	assíncrono
2	Seminários: 25 pts	25 pontos	síncrono
3	Leitura/participação: 25 pts	25 pontos	Assíncrono/síncrono

## **Definições**

**Modalidade:** tipo de atividade didática, sempre remota. Exemplos: reunião virtual, video, exercícios, avaliação.

**Interação:** forma de interação prevista para exposição de conteúdo, discussões, esclarecimento de dúvidas, promoção de debates, resolução de exercícios.

**Videos (aulas):** conteúdo expositivo preparado em vídeo, com utilização dos slides disponíveis e outros recursos. Tópicos serão divididos em vários vídeos curtos para melhor acompanhamento e para facilitar a produção.

**Reunião virtual:** Reunião virtual no horário de aula, para discussões e esclarecimento de dúvidas.