



Curso	SEGURANÇA CIBERNÉTICA			Núcleo Temático	TECNOLOGIA E INFRAESTRUTURA		Etapa	3		
Comp. Curricular		Segurança em Redes					Código			
Componente Curricular (CC)		Carga horária (horas)		63,33		EIXO		Projetual	Não	X
		Créditos				Universal			Sim	
Presencial		Teórica	Prática	Ateliê	Comum		Creditação da Extensão	Não		
Online		Síncrono			Específico	X		X		
		Assíncrono			Optativo			Sim		
					Prática como CC					
EaD		4			Outras Modalidades		Percentual	0	%	
Ementa										
Introdução aos conceitos de segurança em redes. Segurança de conexões TCP: SSL/TLS. Redes privadas virtuais: IPsec e túneis seguros. Segurança em redes sem fio: 802.11. Firewalls.										
Bibliografia básica										
KUROSE, J. F.; ROSS, K.W. <b>Redes de computadores e a internet: uma abordagem top-down</b> . 8ª ed. São Paulo: Pearson Education do Brasil, 2021.										
MORAES, A. F., <b>Segurança em redes: Fundamentos</b> . São Paulo: Erica, 2012.										
STALLINGS, W. <b>Criptografia e Segurança de Redes: princípios e práticas</b> . Ed 6, 2015.										
Bibliografia Complementar										
COMER, D. E. <b>Redes de computadores e Internet</b> . 6. ed. Porto Alegre: Bookman, 2016.										
FOROUZAN A. B. <b>Comunicação de Dados e Redes de Computadores</b> . 4ª ed. Porto Alegre ArtMed, 2010.										
MORAES, A.F. <b>Redes de Computadores – Fundamentos</b> . 8a. Ed. Erica, 2020.										
RUFINO, Nelson M. de O. <b>Segurança em redes sem fio: aprenda a proteger suas informações em ambientes WI-FI e Bluetooth</b> . Editora Novatec. São Paulo, 2005.										
TANENBAUM, A.; FEAMSTER, N; WETHERALL, D, J, <b>Redes de Computadores</b> . 6º ed. Pearson, 2021.										
Coordenador do Curso		Fabio Silva Lopes				Diretor da Unidade		Daniela Vieira Cunha		
Coordenador Adjunto		Leandro Carlos Fernandes								



Curso	SEGURANÇA CIBERNÉTICA			Núcleo Temático	TECNOLOGIA E INFRAESTRUTURA			Etapa	3			
Comp. Curricular		Segurança em Sistemas Operacionais I						Código				
Componente Curricular (CC)		Carga horária (horas)		47,50		EIXO		Projetual	Não		X	
		Créditos			Universal		Sim					
		Teórica	Prática	Ateliê	Comum				Não			
Presencial					Específico	X		Creditação da Extensão	X			
Online	Síncrono				Optativo				Sim			
	Assíncrono				Prática como CC							
EaD		3			Outras Modalidades				Percentual	0	%	
Ementa												
Introdução ao conceito de segurança de sistemas operacionais, garantias de confidencialidade, integridade e disponibilidade de sistemas e programas, assim como mecanismo que controla o acesso de programas, processos ou usuários aos recursos do computador.												
Bibliografia básica												
GOODRICH, M.T.; TAMASSIA, R. <b>Introdução à Segurança de Computadores</b> . Bookman, 2013.												
SILBERSCHATZ, A., GALVIN, P.B, GAGNE, G. <b>Fundamentos de Sistemas Operacionais: princípios básicos</b> . 9ª ed. Rio de Janeiro: LTC, 2015.												
TANENBAUM, A. S. <b>Sistemas Operacionais Modernos</b> . 4ª ed. São Paulo: Pearson, 2016.												
Bibliografia Complementar												
BITTENCOURT P. H. M., <b>Ambientes Operacionais</b> . 2ªed Editora Pearson, 2019.												
DEITEL, H.M.; DEITEL, P.J.; CHOFFNES, D.R. <b>Sistemas operacionais</b> . 3. ed. São Paulo: Pearson Prentice Hall, 2010.												
MACHADO, F.B.; MAIA, L.P. <b>Arquitetura de sistemas operacionais</b> . 5ª. ed. Rio de Janeiro: LTC, 2013.												
OLIVEIRA, R. S.; TOSCANI, S. S. <b>Sistemas Operacionais</b> . 4ª ed. Porto Alegre: Bookman, 2010.												
STALLINGS, W. <b>Operating systems: internals and design principles</b> . 4th ed. Upper Saddle River: Prentice-Hall, 2001.												
Coordenador do Curso		Fabio Silva Lopes				Diretor da Unidade		Daniela Vieira Cunha				
Coordenador Adjunto		Leandro Carlos Fernandes										



Curso		SEGURANÇA CIBERNÉTICA			Núcleo Temático		ALGORITMOS E PROGRAMAÇÃO		Etapa		3					
Comp. Curricular		Programação Segura								Código						
Componente Curricular (CC)		Carga horária (horas)		63,33		EIXO		Projetual		Não		X				
		Créditos			Universal		Sim									
		Teórica		Prática		Ateliê		Comum		Creditação da Extensão		Não				
Presencial						Específico		X				X				
Online	Síncrono						Optativo					Sim				
	Assíncrono						Prática como CC									
EaD		4						Outras Modalidades				Percentual		0 %		
Ementa																
Entender o conceito de programação segura. Definir requisitos de segurança para desenvolvimento de <i>software</i> no ciclo de vida do projeto. Conhecer os tipos de vulnerabilidades em <i>softwares</i> . Aprender a projetar <i>software</i> para atender aos requisitos de segurança e reduzir os riscos de segurança. Verificar o <i>software</i> de terceiros. Aprender a criar código-fonte aderindo às práticas de codificação segura. Analisar o código para identificar vulnerabilidade para mitigação e tempo de resposta eficiente.																
Bibliografia básica																
DELAMARO, Marcio. <b>Introdução ao Teste de Software</b> . Grupo GEN, 2016. E-book. ISBN 9788595155732. Disponível em: <a href="https://app.minhabiblioteca.com.br/#/books/9788595155732/">https://app.minhabiblioteca.com.br/#/books/9788595155732/</a> .																
PRESSMAN, Roger S.; MAXIM, Bruce R. <b>Engenharia de software</b> . Grupo A, 2021. E-book. ISBN 9786558040118. Disponível em: <a href="https://app.minhabiblioteca.com.br/#/books/9786558040118/">https://app.minhabiblioteca.com.br/#/books/9786558040118/</a> .																
SOMMERVILLE, Ian. <b>Engenharia de Software</b> . 10º ed. - São Paulo. Pearson Education do Brasil, 2018. Disponível em: <a href="https://plataforma.bvirtual.com.br/Leitor/Publicacao/168127/pdf/0">https://plataforma.bvirtual.com.br/Leitor/Publicacao/168127/pdf/0</a> .																
Bibliografia Complementar																
GOOGLE. <b>OWASP best practices to protect your APIs from security vulnerabilities</b> . Disponível em: <a href="https://www.youtube.com/watch?v=TEndXv_AkrA">https://www.youtube.com/watch?v=TEndXv_AkrA</a>																
NIST. <b>Secure Software Development Framework (SSDF)</b> . Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. Disponível em: <a href="https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf">https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf</a> .																
MARTIN, Robert C. <b>Código limpo: Habilidades práticas do Agile Software</b> . Editora Alta Books, 2009. E-book. ISBN 9788550816043. Disponível em: <a href="https://app.minhabiblioteca.com.br/#/books/9788550816043/">https://app.minhabiblioteca.com.br/#/books/9788550816043/</a> .																
OWASP. <b>OWASP API Security Project</b> . Disponível em: <a href="https://owasp.org/www-project-api-security/">https://owasp.org/www-project-api-security/</a> .																
RODRIGUES, João P; CORDOVIL, Kleverton R. et al. <b>Investigação das práticas proativas de desenvolvimento de software seguro adotadas por pequenos times de desenvolvimento</b> . SBC, 2021. Disponível em: <a href="https://sol.sbc.org.br/index.php/semish/article/view/15828/15669">https://sol.sbc.org.br/index.php/semish/article/view/15828/15669</a> .																
Vetorazzo, A.S. <b>Engenharia de Software</b> . Grupo A, 2018.																
Coordenador do Curso		Fabio Silva Lopes						Diretor da Unidade		Daniela Vieira Cunha						
Coordenador Adjunto		Leandro Carlos Fernandes														



Curso	SEGURANÇA CIBERNÉTICA			Núcleo Temático	FUNDAMENTOS DE SEGURANÇA	Etapa	3
Comp. Curricular	Detecção de Intrusão					Código	
Componente Curricular (CC)	Carga horária (horas)		63,33	EIXO		Projetual	Não X
	Créditos			Universal		Sim	
Presencial	Teórica	Prática	Ateliê	Comum		Não	
				Específico	X	X	
Online	Síncrono			Optativo		Sim	
	Assíncrono			Prática como CC			
EaD	4			Outras Modalidades		Percentual	%
Ementa							
Introdução à Detecção de Intruso. Análise de Pacotes. Planejamento da Coleta de Dados. Plataforma de Sensores. Dados de Sessão. Captura de Pacotes. Detecção Baseada em Assinatura. Detecção Baseada Anomalias. Detecção de Intruso baseado em host.							
Bibliografia básica							
BEJTICH, R. <b>The Practice of Network Security Monitoring: Understanding Incident Detection and Response</b> . 1st Edition. No Starch Press, 2013.							
SANDERS, C.; SMITH, J. <b>Applied Network Security Monitoring: Collection, Detection, and Analysis</b> . Syngress, 2013.							
SANDERS, C. <b>Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems</b> . 3rd Edition. No Starch Press, 2017.							
Bibliografia Complementar							
DAVIDOFF, S.; HAM, J. <b>Network Forensics: Tracking Hackers through Cyberspace</b> . 1st Edition, Pearson, 2012.							
FEARNOW, M.; FEDERICK, K.; COOPER, M.; NORTHCUTT, S. <b>Intrusion Signatures and Analysis</b> , Sams, 2001.							
MOTA FILHO, J.E. <b>Análise de Tráfego em Redes TCP/IP: Utilize tcpdump na análise de tráfegos em qualquer sistema operacional</b> . Novatec Editora, 2013.							
NORTHCUTT, S.; NOVAK, J. <b>Network Intrusion Detection</b> . 3rd Edition. Sams Publishing, 2002.							
SANDERS, C. <b>Intrusion Detection Honeypots: Detection Through Deception</b> . Applied Network Defense., 2020.							
Coordenador do Curso	Fabio Silva Lopes			Diretor da Unidade	Daniela Vieira Cunha		
Coordenador Adjunto	Leandro Carlos Fernandes						



Curso	SEGURANÇA CIBERNÉTICA			Núcleo Temático	FUNDAMENTOS DE SEGURANÇA	Etapa	3
Comp. Curricular	Teste de Invasão					Código	
Componente Curricular (CC)	Carga horária (horas)		63,33	EIXO		Projetual	Não X
	Créditos			Universal			Sim
	Teórica	Prática	Ateliê	Comum			Não
Presencial				Específico	X		X
Online	Síncrono			Optativo			Sim
	Assíncrono			Prática como CC			
EaD	4			Outras Modalidades		Percentual	0 %
Ementa							
Conceitos de teste de invasão e hacker ético. Metodologias. Reconhecimento. Varredura e Enumeração. Análise de vulnerabilidades. Exploração de Falhas. Pós-exploração de falhas. Relatório dos testes de invasão. <i>Capture the flag (CTF)</i> .							
Bibliografia básica							
BASTA, A., et al. <b>Segurança de computadores e teste de invasão</b> . Cengage Learning, 2014.							
MORENO, D. <b>Introdução ao Pentest</b> . 2ª edição. Novatec, 2019.							
WEIDMAN, G. <b>Testes de Invasão: uma Introdução Prática ao Hacking</b> . 1a edição. Novatec Editora, 2017.							
Bibliografia Complementar							
HALTON, W.; WEAVER, B.; ANSARI, J.; KOTIPALLI, S.; IMRAN, M. <b>Penetration Testing: A Survival Guide</b> . Packt Publishing, 2017.							
HARPER, A.; LINN, R. SIMS, S.; BAUCOM, M.; FERNANDEZ, D.; TEJEDA, H.; FROST, M. <b>Gray hat hacking: the ethical hacker's handbook</b> . McGraw-Hill Education, 2022.							
KIM, P. <b>The Hacker Playbook 3: Practical Guide To Penetration Testing</b> . 1st Edition. Independently published, 2018.							
SEITZ, J.; ARNOLD, T. <b>Black Hat Python: Python Programming for Hackers and Pentesters</b> . No starch press, 2021.							
WYLIE, P. L.; CRAWLEY, K. <b>The Pentester Blueprint: Starting a career as an ethical hacker</b> . Wiley, 2021.							
Coordenador do Curso	Fabio Silva Lopes			Diretor da Unidade	Daniela Vieira Cunha		
Coordenador Adjunto	Leandro Carlos Fernandes						



Curso	SEGURANÇA CIBERNÉTICA			Núcleo Temático	FUNDAMENTOS DE SEGURANÇA	Etapa	3
Comp. Curricular	Engenharia Reversa II					Código	
Componente Curricular (CC)	Carga horária (horas)		63,33	EIXO		Projetual	Não X
	Créditos			Universal		Sim	
Presencial	Teórica	Prática	Ateliê	Comum		Não	
				Específico	X	X	
Online	Síncrono			Optativo		Sim	
	Assíncrono			Prática como CC			
EaD	4			Outras Modalidades		Percentual	0 %
Ementa							
Introdução à programas maliciosos e a engenharia reversa (vírus, worms, trojans, backdoors e rootkits). Assembly x86. Análise de Malwares em Máquinas Virtuais. Análise dinâmica. Análise Estática. Depuração. Codificação de Dados. Assinaturas de malwares.							
Bibliografia básica							
EAGLE, C. <b>The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler</b> . 2nd Edition. No Starch Press, 2011.							
EILAM, E. <b>Reversing: Secrets of Reverse Engineering</b> . 1st Edition. Wiley, 2005.							
SIKORSKI, M.; HONIG, A. <b>Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software</b> . 1st Edition. No Starch Press, 2012.							
Bibliografia Complementar							
ANDRIESSE, D. <i>Practical binary analysis: build your own Linux tools for binary instrumentation, analysis, and disassembly</i> . no starch press, 2018.							
DANG, B. et al. <b>Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation</b> . 1st Edition. Wiley, 2014.							
KUSSWURM, D. "Modern x86 Assembly Language Programming: 32-bit, 64-bit. SSE, and AVX", Berkley, CA: Apress (2014).							
LIGH, M.H. <b>The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory</b> . Wiley; 1st edition, 2014.							
MONNAPPA, K. A. <b>Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware</b> . Packt Publishing Ltd, 2018.							
Coordenador do Curso	Fabio Silva Lopes			Diretor da Unidade	Daniela Vieira Cunha		
Coordenador Adjunto	Leandro Carlos Fernandes						