



Curso	SEGURANÇA CIBERNÉTICA			Núcleo Temático	FUNDAMENTOS DE SEGURANÇA	Etapa	4
Comp. Curricular	Exploração de Aplicações Web e Mobile					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			
	Assíncrono			Prática como CC			Sim
EaD	4			Outras Modalidades			
						Creditação da Extensão	Percentual %
Ementa							
Conceitos de aplicações web segura. Reconhecimento e Varredura para Web. Ataques de injeção em aplicações Web. Ataques de quebra de autenticação e gerenciamento de sessão em aplicações Web. Ataques no cliente de aplicação web. Ataque de desserialização insegura. Ataques Mobile. <i>Web Capture the flag (web CTF)</i> .							
Bibliografia básica							
PAULI, J. Introdução ao Web Hacking: Ferramentas e técnicas para invasão de aplicações web . Novatec Editora, 2020.							
STUTTARD, D. PINTO, M. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws , 2nd Edition. Willey, 2011.							
WEIDMAN, G. Testes de Invasão: uma Introdução Prática ao Hacking . 1ª edição. Novatec Editora, 2017.							
Bibliografia Complementar							
BASTA, A., et al. Segurança de computadores e teste de invasão . Cengage Learning, 2014.							
HARPER, A.; LINN, R.; SIMS, S.; BAUCOM, M.; FERNANDEZ, D.; TEJEDA, H.; FROST, M. Gray hat hacking: the ethical hacker's handbook . McGraw-Hill Education, 2022.							
KIM, P. The Hacker Playbook 3: Practical Guide To Penetration Testing . 1st edition. Independently published, 2018.							
MORENO, D. Pentest em Aplicações web . 1ª edição. Novatec, 2017.							
SEITZ, J.; ARNOLD, T. Black Hat Python: Python Programming for Hackers and Pentesters . No starch press, 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	4		
Comp. Curricular	Respostas a Incidentes de Segurança						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			
				Específico			X			
Online	Síncrono			Optativo			X	Sim		
	Assíncrono			Prática como CC						
EaD	4			Outras Modalidades				Percentual	0	%
Ementa										
Entender os fundamentos ao tratamento de incidentes cibernéticos. Compreender o ambiente de <i>Computer Emergency Response Team (CSIRT)</i> . Conhecer o código de conduta de âmbito internacional. Identificar a informação crítica, ataques de <i>e-mails</i> , códigos maliciosos e agentes maliciosos na rede para análise de incidentes. Aprender a tratar, monitorar e reportar a detecção de incidentes e o uso de ferramentas específicas. Compreender a forma de colaboração com o poder judiciário.										
Bibliografia básica										
ANSON, S. Applied Incident Response . 1st Edition. Wiley, 2020.										
LUTTGENS, Jason T. et al. Incident Response & Computer Forensics . 3rd Edition. McGraw-Hill Education, 2014.										
MCCARTHY, N. K. Resposta a Incidentes de Segurança em Computadores. Planos para proteção de informação em risco . Bookman, 2013.										
Bibliografia Complementar										
CERT.BR. Recomendações para Notificações de Incidentes de Segurança . 2022. Disponível em: < https://cert.br/docs/whitepapers/notificacoes/ >										
CERT.BR. Criando um Grupo de Respostas a Incidentes de Segurança em Computadores: Um Processo para Iniciar a Implantação . 2004. Disponível em< https://cert.br/certcc/csirts/Creating-A-CSIRT-br.html >										
CERT Coordination Center, “CERT/CC Vulnerability Note Database. Software Engineering Institute Disponível em: http:// https://www.kb.cert.org/vuls/bypublished/desc/ .										
HOEPERS, C; STEDING-JESSEN, K; CHAVES, M. Projeto e desenvolvimento de um sistema de controle e acompanhamento de notificações de spam . Disponível em < https://www.cert.br/docs/papers/spamctl-ssi2003.pdf >										
INPE. Honeynets Applied to the CSIRT Scenario . Presented at 15th Annual FIRST Conference on Computer Security Incident Handling, (Ottawa, Canada), June, 2003. Disponível em: < https://cert.br/docs/papers/hnbr-first2003.pdf >										
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	4
Comp. Curricular	Projeto Aplicado em Segurança Cibernética I					Código	
Componente Curricular (CC)	Carga horária (horas)		63,33	EIXO		Projeto	
	Créditos			Universal		Não	
Presencial	Teórica			Comum		Sim	X
	Prática			Específico	X	Não	
Online	Síncrono			Optativo		Sim	
	Assíncrono			Prática como CC		X	
EaD	4			Outras Modalidades		Percentual	100 %
Ementa							
Desenvolvimento de um projeto utilizando as ferramentas e conceitos aprendidos durante o curso. O tema dos projetos pode variar a cada semestre. O projeto deve conter as seguintes etapas: análise de viabilidade, descrição detalhada do problema, especificações do sistema a ser desenvolvido, arquitetura da proposta e análise dos resultados. Cada projeto deve ter um cronograma a ser seguido ao longo do semestre. A finalização do projeto será realizada na continuidade deste componente – Projeto Aplicado em Segurança Cibernética II.							
Bibliografia básica							
LUTTGENS, Jason T. et al. Incident Response & Computer Forensics . 3rd Edition. McGraw-Hill Education, 2014.							
PAULI, J. Introdução ao Web Hacking: Ferramentas e técnicas para invasão de aplicações web . Novatec Editora, 2020.							
SIKORSKI, M.; HONIG, A. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software . 1st Edition. No Starch Press, 2012.							
Bibliografia Complementar							
BASTA, A., et al. Segurança de computadores e teste de invasão . Cengage Learning, 2014.							
BELL, L.; SMITH, R.; BRUNTON-SPALL, M.; BIRD, J. Agile Application Security . O'Reilly Media, 2017.							
HOEPERS, C; STEDING-JESSEN, K; CHAVES, M. Projeto e desenvolvimento de um sistema de controle e acompanhamento de notificações de spam . Disponível em < https://www.cert.br/docs/papers/spamctl-ssi2003.pdf >							
MCGRAW, G. Software security. Building security in . Addison-Wesley Professional; 1ª edição, 2006.							
MORENO, D. Introdução ao Pentest . 2ª edição. Novatec, 2019.							
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	4
Comp. Curricular	Desenvolvimento de Software Seguro					Código	
Componente Curricular (CC)	Carga horária (horas)		63,33	EIXO		Projeto	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							
Conceitos de software seguro. Requisitos de software seguro. Arquitetura e design de software seguro. Implementação segura de software. Teste de software seguro. Gerenciamento seguro do ciclo de vida do software. Implantação, operações e manutenção de software seguro. Cadeia de suprimentos de software seguro.							
Bibliografia básica							
MEAD, N. R.; ALLEN, J.H.; BARNUM, S.; ELLISON, R.J.; MCGRAW, G.R. Software security engineering: a guide for project managers . Addison-Wesley Professional, 2004.							
MEAD, N. R.; WOODY, C. Cyber security engineering: A practical approach for systems and software assurance . Addison-Wesley Professional, 2016.							
VAN WYK, K.R.; GRAFF, M.G.; PETERS, D.S.; BURLEY, D. L. Enterprise Software Security: A Confluence of Disciplines . Addison-Wesley Professional, 2014.							
Bibliografia Complementar							
BELL, L.; SMITH, R.; BRUNTON-SPALL, M.; BIRD, J. Agile Application Security . O'Reilly Media, 2017.							
BOYENS, J.; PAULSEN, C.; MOORTHY, R.; BARTOL, N.; STEPHANIE, A.S. Supply chain risk management practices for federal information systems and organizations . NIST Special publication 800, no. 161 (2015): 32.							
HSU, T. H. Hands-On Security in DevOps: Ensure continuous security, deployment, and delivery with DevSecOps . Packt Publishing Ltd, 2018.							
RANSOME, J.; MISRA, A. Core software security: Security at the source . CRC press, 2018.							
MCGRAW, G. Software security. Building security in . Addison-Wesley Professional; 1ª edição, 2006.							
Coordenador do Curso	Fabio Silva Lopes			Diretor da Unidade	Daniela Vieira Cunha		
Coordenador Adjunto	Leandro Carlos Fernandes						



Curso	SEGURANÇA CIBERNÉTICA			Núcleo Temático	TECNOLOGIAS E INFRAESTRUTURA		Etapa	4		
Comp. Curricular		Segurança em Sistemas Operacionais II					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										
Análise de Vulnerabilidades em sistemas operacionais, segurança de servidores, monitoramento de ambientes, controle de usuários, segurança de arquivos, e práticas para mitigação de ataques em sistemas operacionais.										
Bibliografia básica										
GOODRICH, M.T.; TAMASSIA, R. Introdução à Segurança de Computadores . Bookman, 2013.										
SILBERSCHATZ, A., GALVIN, P.B, GAGNE, G. Fundamentos de Sistemas Operacionais: princípios básicos . 9ª ed. Rio de Janeiro: LTC, 2015.										
TANENBAUM, A. S. Sistemas Operacionais Modernos . 4ª ed. São Paulo: Pearson, 2016.										
Bibliografia Complementar										
BITTENCOURT P. H. M., Ambientes Operacionais . 2ªed Editora Pearson, 2019.										
DEITEL, H.M.; DEITEL, P.J.; CHOFFNES, D.R. Sistemas operacionais . 3. ed. São Paulo: Pearson Prentice Hall, 2010.										
MACHADO, F.B.; MAIA, L.P. Arquitetura de sistemas operacionais . 5ª. ed. Rio de Janeiro: LTC, 2013.										
OLIVEIRA, R. S.; TOSCANI, S. S. Sistemas Operacionais . 4ª ed. Porto Alegre: Bookman, 2010.										
STALLINGS, W. Operating systems: internals and design principles . 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								