



Curso	SEGURANÇA CIBERNÉTICA			Núcleo Temático	TECNOLOGIA E INFRAESTRUTURA		Etapa	5					
Comp. Curricular	Segurança em Hardware					Código							
Componente Curricular (CC)	Carga horária (horas)			31,67	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	2	Outras Modalidades					Percentual	0 %					
Ementa													
Análise de hardware, identificação e mitigação de eventuais vulnerabilidades de sistema. Vetores de Ataque, Metodologia de teste de sistemas, dispositivos e protocolos para mitigar riscos.													
<i>Bibliografia básica</i>													
CHANTZIS, Fotios, et.al. Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things. No Starch Press, 2021													
VALLE, Jean-Georges. Practical Hardware Pentesting. Editora O'Reilly, 2021													
MONTEIRO, Mário A. Introdução à organização de computadores. 5. ed. Rio de Janeiro, RJ: LTC, 2012. 698 p. ISBN 9788521615439.													
<i>Bibliografia Complementar</i>													
PATTERSON, David A; HENNESSY, John L. Organização e projeto de computadores: a interface hardware/software. Rio de Janeiro: GEN LTC, 2017. 1 ISBN 9788595152908.													
HENNESSY, John L; PATTERSON, David A. Arquitetura de computadores: uma abordagem quantitativa. 6.ed. Rio de Janeiro: GEN LTC, 2019. ISBN 9788595150669.													
NULL, Linda. Essentials of Computer Organization and Architecture. 5.ed. Jones & Bartlett Publishers, 2018. 821 p. ISBN 9781284123036.													
STALLINGS, William. Arquitetura e organização de computadores. 10.ed. Editora Pearson 2017 731 p. ISBN 9788543020532.													
TANENBAUM, Andrew S. Organização estruturada de computadores, 6.ed. Editora Pearson 2013 628 p. ISBN 9788581435398.													
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		Etapas	5	
Comp. Curricular	Governança de TIC					Código			
Componente Curricular (CC)	Carga horária (horas)			31,67	EIXO		Projetual	Não X	
	Créditos			Universal				Sim	
	Teórica	Prática	Ateliê	Comum				Não	
Presencial				Específico	X			X	
				Optativo			Creditação da Extensão	Sim	
				Prática como CC					
Online				Outras Modalidades			Percentual	%	
EaD	2								

**Ementa**

Entender o alinhamento de TIC nas organizações. Introdução à Governança Corporativa. Entender o conceito de estratégia e a sua aplicação no âmbito organizacional. Entender a importância da auditoria na organização. Entender os princípios, o conceito, o escopo, os termos e as definições na Governança de TIC. Aprender sobre os riscos na Governança de TIC. Entender os mecanismos de decisão e as melhores práticas para Governança de TI. Elaborar o Planejamento Estratégico de TI (PETI). Entender a importância de Segurança da Informação na Governança de TI (política, risco, planejamento, operação e auditoria). Entender o papel da conformidade e das regulações dentro das organizações e os seus impactos.

**Bibliografia básica**

PRADO, Roberta N. **Governança Corporativa**. v. III. Editora Saraiva, 2023. E-book. ISBN 9786553625129. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9786553625129/>.

BLOK, Marcella. **Compliance e Governança Corporativa**. 3º edição. Freitas Bastos Editora. São Paulo, 2020. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/184827/pdf/0>.

FERNANDES, Aguinaldo; ABREU, Vladimir. **Implantando a Governança de TI: da Estratégia à Gestão de Processos e Serviços**. 4º ed. Brasport Livros e Multimídia, 2014. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/160678 epub/0>.

**Bibliografia Complementar**

NEVES, Edmo C. **Fundamentos de governança corporativa: riscos, direito e compliance**. Editora Intersaberes, 2021. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/194862/pdf/0>

TORRECILHAS, Arthur R. **Administração aplicada à engenharia de segurança**. Editora Saraiva, 2021. E-book. ISBN 9786559031047. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9786559031047/>.

MARINHO, Fernando. **Os 10 Mandamentos da LGPD - Como Implementar a Lei Geral de Proteção de Dados em 14 Passos**. Grupo GEN, 2020. E-book. ISBN 9788597026009. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788597026009/>.

MANOEL, Sérgio S. **Governança de Segurança da Informação**. Brasport Livros e Multimídia, 2014. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/160684 epub/0>

BGC. **Governança Corporativa Internacionalização E Convergência - 1º edição 2010**. Saint Paul Publishing (Brazil), 2010. E-book. ISBN 9788580040104. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788580040104/>.

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		Etapas	5	
Comp. Curricular	Inteligência de Ameaça Cibernética						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					Creditação da Extensão	Sim	
	Assíncrono	Prática como CC							
EaD	4	Outras Modalidades					Percentual	%	

**Ementa**

Fundamentos de inteligência de ameaça (tipos, ciclo de vida, estratégias, metodologias). Ameaças cibernéticas, atores e seus objetivos para os ataques cibernéticos. Passos para programa de inteligência de ameaça. Planejamento e direção. Aquisição e coleção de dados. Processamento de dados. Análise de dados. Relatório.

**Bibliografia básica**

PALACIN, V. **Practical Threat Intelligence and Data-Driven Threat Hunting: A Hands-on Guide to Threat Hunting with the ATT&CK™ Framework and OpenSource Tools**. Packt Publishing Limited, 2021.

ROBERTS, S. J.; BROWN, R. **Intelligence-driven incident response: Outwitting the adversary**. O'Reilly Media, Inc., 2017.

ROBERTS, Aaron. **Cyber threat intelligence: The no-nonsense guide for cisos and security managers**. Berkeley, CA, USA: Apress, 2021.

**Bibliografia Complementar**

DAHJ, J.N.M. **Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense**. Packt Publishing; 1ª edição, 2022.

MARTINEZ, R. **Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence-based threat hunting**. Packt Publishing, 2022.

MURDOCH, D. W. **Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases Notes from the Field: a Condensed Field Guide for the Security Operations Team**. Don Murdoch, 2018.

SHOSTACK, A. **Threat modeling: Designing for security**. John Wiley & Sons, 2014.

WILHOIT, K.; OPACKI, J.. **Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs**. Packt Publishing, 2022.

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	5
Comp. Curricular	Engenharia Social					Código		
Componente Curricular (CC)	Carga horária (horas)			31,67	EIXO	Projetual	Não	X
	Créditos			Universal			Sim	
	Teórica	Prática	Ateliê	Comum			Não	
Presencial				Específico	X	Creditação da Extensão		
				Optativo			Sim	
				Prática como CC			X	
EaD	2			Outras Modalidades		Percentual	50	%

**Ementa**

Compreender o conceito de engenharia social. Entender o comportamento humano e os impactos na engenharia social. Abordar a cultura de segurança cibernética e a prática de BYOD (*bring your own device*). Aprender a usar a ferramenta *Social-Enginner Toolkit*. Entender os meios de ataques *spear-phishing*, ataques *web*, ataques de *e-mail* em massa e outras direções no ambiente organizacional e na sociedade como um todo.

**Bibliografia básica**

GRANGER, Sarah. **Social Engineering Fundamentals, Part I: Hacker Tactics. Edpoint Protection.** 2001. Disponível em: <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=891b1f29-e2e7-4484-89c0-a2137ee82f8b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>

MANN, Ian. **Engenharia Social.** Editora Blucher, 2011. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/177672/pdf/0>

WEIDMAN, G.. **Testes de Invasão. Uma introdução prática ao hacking.** Editora Novatec, 2014.

**Bibliografia Complementar**

ALENCAR, G. LIMA, M. **O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e Phishing.** SBC, 2013. Disponível em: <https://sol.sbc.org.br/index.php/sbsi/article/view/5694/5591>.

ALVES, C. B. **Segurança da Informação vs. Engenharia Social: Como se proteger para não ser mais uma vítima.** Brasília, 2010. Disponível em: [https://cdn.administradores.com.br/app/uploads/2022/01/29175135/academico\\_3641\\_190226\\_185626.pdf](https://cdn.administradores.com.br/app/uploads/2022/01/29175135/academico_3641_190226_185626.pdf).

AZZOLIN, M. M. **Ataques de Engenharia Social.** Revista O Comunicante, 2018. Disponível em: <http://www.ebrevistas.eb.mil.br/OC/article/view/1674/1389>.

COELHO, C. F.; RASMA, E. T.; MORALES, G. Engenharia Social: Uma Ameaça À Sociedade Da Informação. **Exatas & Engenharias**, v. 3, n. 05, 23 mar. 2013. Disponível em: <https://doi.org/10.25242/885X305201387>.

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	5
Comp. Curricular	Inteligência Artificial para Segurança Cibernética					Código			
Componente Curricular (CC)	Carga horária (horas) 63,33			EIXO		Projetual	Não	X	
	Créditos			Universal			Sim		
	Teórica	Prática	Ateliê	Comum					
Presencial				Específico	X		Não		
Online	Síncrono			Optativo			X		
	Assíncrono			Prática como CC				Sim	
EaD	4			Outras Modalidades			Percentual	50	%
Ementa									
Conceitos e visão geral da IA em operações de segurança, geração de insights para alertas de ameaças, padrões e conexões entre ameaças, uso de modelos de aprendizado de máquina em segurança para análise de risco, investigação de incidentes e identificação de vulnerabilidades. Abordagem da IA na gestão de assets em organizações: conformidade, restrições e gestão de identidades. Exemplos de aplicações.									
<i>Bibliografia básica</i>									
LIMA, I. <b>Inteligência Artificial</b> . Ed. Grupo Gen, 2014.									
LUGER, G.F. <b>Inteligência Artificial</b> . 6ª.Ed. Pearson, 2013.									
RUSSELL, S.; NORVIG, P. <b>Inteligência Artificial</b> . Rio de Janeiro: LTC, 2013.									
<i>Bibliografia Complementar</i>									
BURKOV, A. <b>The Hundred-page Machine Learning Book</b> . 2019. Disponível em < <a href="https://github.com/dwelcaslu/machine-learning-books/blob/master/Andriy%20Burkov%20-%20The%20Hundred-Page%20Machine%20Learning%20Book-Andriy%20Burkov%20(2019).pdf">https://github.com/dwelcaslu/machine-learning-books/blob/master/Andriy%20Burkov%20-%20The%20Hundred-Page%20Machine%20Learning%20Book-Andriy%20Burkov%20(2019).pdf</a> >									
FACELI, K.; et al. <b>Inteligência Artificial – Uma abordagem de Aprendizado de Máquina</b> . Rio de Janeiro: LTC, 2011.									
LEINZ, M.L. <b>Fundamentos de Aprendizagem de Máquina</b> . Grupo A, 2020.									
MEDEIROS, L.F. <b>Inteligência Artificial Aplicada: Uma abordagem introdutória</b> . Ed. Intersaberes, 2018.									
SILVA, F.M., et al. <b>Inteligência Artificial</b> . Porto Alegre: SAGAH, 2019									
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		Etapas	5							
Comp. Curricular	Projeto Aplicado em Segurança Cibernética II					Código									
Componente Curricular (CC)	Carga horária (horas)			63,33	EIXO		Projetual	Não							
	Créditos			Universal				Sim							
	Teórica	Prática	Ateliê	Comum				X							
Presencial				Específico	X										
				Optativo			Creditação da Extensão	Não							
				Prática como CC				Sim							
Online				Outras Modalidades				X							
							Percentual	100							
								%							
Ementa															
Continuidade do projeto iniciado no componente de projeto Aplicada em Segurança Cibernética II. Elaboração do relatório técnico, envolvendo ações de resposta incidentes, Aspectos de Governança de TIC e Inteligência de Ameaça Cibernética.															

**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**

MANN, Ian. **Engenharia Social**. Editora Blucher, 2011. Disponível em:  
<https://plataforma.bvirtual.com.br/Leitor/Publicacao/177672/pdf/0>

ROBERTS, S. J.; BROWN, R. **Intelligence-driven incident response: Outwitting the adversary**. O'Reilly Media, Inc., 2017.

SHOSTACK, A. **Threat modeling: Designing for security**. John Wiley & Sons, 2014.

WEIDMAN, G. **Testes de Invasão. Uma introdução prática ao hacking**. Editora Novatec, 2014.

WILHOIT, K.; OPACKI, J.. **Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs**. Packt Publishing, 2022.

Coordenador do Curso	Fabio Silva Lopes	Diretor da Unidade	Daniela Vieira Cunha
Coordenador Adjunto	Leandro Carlos Fernandes		