

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)								
CONHECIMENTOS BÁSICOS								
LÍNGUA PORTUGUESA								
1. Compreensão de textos.								
2. Ortografia oficial.								
3. Mecanismos de coesão textual.								
4. Significação das palavras.								
5. Emprego de tempos e modos verbais.								
6. Emprego das classes de palavras.								
7. Coordenação e de subordinação.								
8. Emprego dos sinais de pontuação.								
9. Concordância verbal e nominal.								
10. Regência verbal e nominal.								
11. Emprego do sinal indicativo de crase.								
12. Colocação dos pronomes átonos.								
LÍNGUA INGLESA								
1. Compreensão de texto escrito em língua inglesa.								
2. Itens gramaticais relevantes para a compreensão dos conteúdos semânticos.								
CONHECIMENTOS ESPECÍFICOS								
1. Segurança Ofensiva								
1.1 Conceitos básicos: vulnerabilidades, ameaças e ataques.								
1.2 Ataques Passivos: Escuta Passiva e Inferência.								
1.3 Ataques Ativos: Escuta Ativa, Disfarce, Repetição e Negação de Serviço.								
1.4 Etapas do Ataque: Footprinting, Varredura, Enumeração, Ganho de acesso, Escalação de privilégios, Criação de Porta dos Fundos, Encobrimento de rastros e Recusas de serviço.								

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)								
1.5 Ataques aos protocolos de comunicação: ARP, IP, ICMP, UDP, TCP, DHCP, SMTP, IMAP, POP3, HTTP, FTP, SMB.								
1.6 Ataques à Rede Wi-Fi: Rogue Access Point, Evil Twin, SSID Tracking, Jamming e Disassociation.								
1.7 Ataques do Man-in-the-Middle: Sniffing e Spoofing.								
1.8 Ataques de Engenharia Social: Ciclo de Ataque e Técnicas.								
1.9 Código Malicioso: Vírus, Worm, Trojan Horse, Backdoor, Screenlogger, Keylogger, Injector, Downloader, Flooder, Rootkit, Bot, Botnet, Exploit, Spyware, Ransomware, Cryptojacking e Formjacking.								
1.10 MITRE ATT&CK: matrizes, táticas, técnicas, procedimentos e mitigações.								
1.11 – MITRE CAPEC: Padrões de Ataques Cibernéticos, Mecanismos de Ataque, Domínios de Ataque.								
1.12 Ferramentas de Hacking: amass, aircrack-ng, aircgeddon, arpswatch, beef-xss, burpsuite, ettercap, ghidra, hashcat, hydra, john the ripper, nmap, netcat, metasploit, metasploit-framework, set, smbmap, sqlmap, theharvester, veil, wireshark.								
2. Segurança Defensiva								
2.1 Defesa em profundidade: Perímetro de segurança (Filtro de Pacotes, Firewall de Estado, Firewall Proxy, IDS, IPS, VPN).								
2.2 Controle de Acesso à Rede: IEEE 802.1X, EAP e RADIUS. Segurança em Aplicações: OWASP Top 10, OWASP SAMM, CVE, CWE.								
2.3 Segurança da Informação: Integridade, Autenticidade, Confidencialidade, Autorização de Acesso, Disponibilidade e Irretratibilidade.								
2.4 Mecanismos de Segurança: Resumo de Mensagem, Cifragem de Dados, Assinatura Digital, Envelope Digital, Certificado Digital, Autenticação Multifator, Carimbo do Tempo e Técnicas de Redundância e Tolerância a Falhas.								
2.5 ICP-Brasil: Autoridade Certificadora, Autoridade de Carimbo do Tempo, Organização, Normas e Padrões.								

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)								
2.6 Comunicação Segura: TLS, SSL, IPsec.								
2.7 Segurança no Endpoint: Antimalware e Firewall Pessoal.								
2.8 Segurança em Sistemas Operacionais: CIS Benchmarks, Linux e Windows.								
2.9 Segurança em Sistemas de Controle e Automação Industrial: ameaças e vulnerabilidades, ICS Advisory Project, Série ISA/IEC 62443 e NIST SP 800-82.								
2.10 Forense Digital: Evidência Digital, Processo de Análise Forense, Análise Forense de Dispositivos de Armazenamento, Sites e E-mails e Open Source Intelligence (OSINT).								
3. Compliance de Segurança e Privacidade								
3.1 Normas: ABNT NBR ISO/IEC 27001:2022 (Versão Corrigida: 2023), ABNT NBR ISO/IEC 27002:2022, ABNT NBR ISO/IEC 27005:2023, ABNT ISO/IEC 27035-1:2023, ABNT NBR ISO 22301:2020, ABNT NBR ISO 22313:2020, ABNT NBR ISO/IEC 29100:2024, ABNT NBR ISO/IEC 29134:2024, ABNT NBR ISO/IEC 27701:2019 (Versão corrigida: 2020)								
3.2 Frameworks e Controles: The NIST Cybersecurity Framework (CSF) 2.0, CIS Critical Security Controls Version 8.1.								
3.3 Leis e Regulamentações: Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014, e suas alterações); LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018, e suas alterações); Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações – ANATEL (Resolução nº 740, de 21 de dezembro de 2020, e suas alterações).								