

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)								
MÓDULO I - CONHECIMENTOS GERAIS								
LÍNGUA PORTUGUESA								
1. Compreensão e interpretação de textos de gêneros variados.								
2 Reconhecimento de tipos e gêneros textuais.								
3 Domínio da ortografia oficial.								
4 Domínio dos mecanismos de coesão textual.								
4.1 Emprego de elementos de referência, substituição e repetição, de conectores e de outros elementos de sequenciação textual.								
4.2 Emprego de tempos e modos verbais.								
5 Domínio da estrutura morfosintática do período.								
5.1 Emprego das classes de palavras.								
5.2 Relações de coordenação entre orações e entre termos da oração.								
5.3 Relações de subordinação entre orações e entre termos da oração.								
5.4 Emprego dos sinais de pontuação.								
5.5 Concordância verbal e nominal.								
5.6 Regência verbal e nominal.								
5.7 Emprego do sinal indicativo de crase.								
5.8 Colocação dos pronomes átonos.								
6 Reescrita de frases e parágrafos do texto.								
6.1 Significação das palavras.								
6.2 Substituição de palavras ou de trechos de texto.								
6.3 Reorganização da estrutura de orações e de períodos do texto.								
6.4 Reescrita de textos de diferentes gêneros e níveis de formalidade.								
6.5. Redação Oficial.								
RACIOCÍNIO LÓGICO E MATEMÁTICO								
1. Conjuntos numéricos;								

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
<u>PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)</u>								
2. Razões e proporções;								
3. Regra de três simples e composta;								
4. Porcentagem;								
5. Juros simples e compostos;								
6. Equações, inequações e sistemas de equações;								
7. Funções;								
8. Sequências;								
9. Matrizes e determinantes;								
10. Probabilidade;								
11. Análise combinatória;								
12. Estatística descritiva;								
13. Proposições lógicas;								
14. Conectivos;								
15. Tabelas verdade;								
16. Equivalências e negações;								
17. Argumentação lógica;								
18. Diagramas lógicos;								
19. Resolução de problemas envolvendo raciocínio lógico-matemático.								
MÓDULO II - CONHECIMENTOS ESPECÍFICOS								
FUNDAMENTOS DE TECNOLOGIA DA INFORMAÇÃO								
Arquitetura de computadores.								
Sistemas operacionais.								
Redes de computadores e protocolos TCP/IP.								
Bancos de dados.								
Computação em nuvem.								
Engenharia De Software: Ciclo de vida de sistemas.								

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
<u>PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)</u>								
Engenharia de requisitos.								
Arquitetura e integração de sistemas.								
Metodologias ágeis (Scrum e Kanban).								
Qualidade e testes de software.								
Segurança Da Informação: Confidencialidade, integridade e disponibilidade.								
Controle de acesso.								
Gestão de riscos e incidentes.								
Continuidade de negócios.								
Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).								
Normas ISO/IEC 27001, 27002 e 27005.								
Governança e Gestão de TI: COBIT 2019 e ITIL 4.								
Planejamento estratégico.								
Gestão de projetos, processos e serviços de TI.								
Indicadores de desempenho.								
Contratações de soluções de TIC.								
Gestão de Dados e Inteligência Artificial: Modelagem e governança de dados.								
SQL.								
Business Intelligence (BI).								
Fundamentos de inteligência artificial, aprendizado de máquina e IA generativa.								
Transformação Digital no Poder Judiciário: Governo digital.								
Automação de processos.								
Interoperabilidade.								
Processo Judicial Eletrônico (PJe).								
Plataforma Digital do Poder Judiciário (PDPJ-Br).								
Acessibilidade digital.								

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)								
Normas de TIC no Poder Judiciário: Resoluções CNJ nº 370/2021, nº 396/2021, nº 468/2022, nº 615/2025, com suas alterações.								
Gestão de Processos e Documentos do Poder Judiciário (MoReq-Jus).								
Gestão documental arquivística digital: metadados, ciclo de vida, preservação e RDC-Arq.								
Resolução CNJ n. 522/2023, com suas alterações.								
Plano Diretor de Tecnologia da Informação do TJPB (PDTI 2024–2026).								
GOVERNANÇA, NORMAS E CONFORMIDADE								
Princípios de segurança da informação: confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade (não repúdio) e privacidade.								
Políticas, normas, procedimentos e controles de segurança da informação: hierarquia normativa, elaboração e revisão.								
Classificação e tratamento da informação: níveis de classificação, rotulagem e classificação de ativos.								
Gestão de riscos de segurança da informação (ISO/IEC 27005): identificação, análise, avaliação e tratamento de riscos.								
Normas ISO/IEC 27001 e ISO/IEC 27002: sistema de gestão de segurança da informação (SGSI) e controles de segurança.								
Norma ISO/IEC 27701 (gestão da privacidade da informação).								
Conformidade, auditoria e indicadores de segurança da informação.								
Frameworks de referência em segurança: NIST Cybersecurity Framework (funções e perfis) e CIS Controls.								
Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ, Resolução CNJ nº 396/2021) e Portaria CNJ nº 162/2021 (protocolos e manuais de segurança cibernética).								
Plataforma Digital do Poder Judiciário (PDPJ-Br, Resolução CNJ nº 335/2020): arquitetura de microserviços, marketplace do CNJ e proteção dos serviços digitais.								

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)								
PRIVACIDADE E LEGISLAÇÃO								
Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018): princípios, dados pessoais e sensíveis, bases legais, direitos do titular e controles técnicos.								
Anonimização, pseudonimização, minimização, retenção e descarte seguro de dados pessoais.								
Marco Civil da Internet (Lei nº 12.965/2014): princípios, guarda de registros de conexão e de acesso a aplicações e responsabilidade dos provedores.								
Lei de Acesso à Informação (LAI, Lei nº 12.527/2011).								
GESTÃO DE IDENTIDADES E CONTROLE DE ACESSO								
Ciclo de vida de usuários: contas administrativas, contas de serviço e contas inativas.								
Revisão periódica de acessos e recuperação segura de credenciais.								
Controle de acesso lógico: menor privilégio, segregação de funções e controle de acesso baseado em papéis (RBAC).								
Soluções de gestão de identidades e acessos (IAM) e de gestão de acessos privilegiados (PAM).								
Autenticação multifator (MFA), Single Sign-On (SSO) e federação de identidades.								
Protocolos de autenticação e autorização: SAML 2.0, OAuth 2.0, OpenID Connect e JWT.								
SEGURANÇA DE REDES E INFRAESTRUTURA								
Arquitetura TCP/IP: camadas, protocolos e endereçamento IPv4 e IPv6.								
Arquitetura de segurança de redes: segmentação, zona desmilitarizada (DMZ), defesa em profundidade e padrões de design de rede.								
Controle de acesso à rede (NAC): autenticação de dispositivos (IEEE 802.1X) e verificação de conformidade.								

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)								
Modelo Zero Trust (Confiança Zero): verificação contínua, Zero Trust Network Access (ZTNA) e microssegmentação.								
Firewalls de Próxima Geração (NGFW): configuração e gerenciamento.								
Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS).								
Web Application Firewall (WAF).								
Redes privadas virtuais (VPN IPSec e SSL): tunelamento, VPN site-to-site e de acesso remoto;								
DNS e DNS seguro (DNSSEC): resolução de nomes, tipos de registro e ataques ao DNS.								
Proteção contra ataques de negação de serviço (DoS/DDoS).								
Hardening: menor privilégio, redução da superfície de ataque, configuração segura e linha de base de segurança.								
Gestão de configuração e inventário de ativos de TI: identificação, registro e base de dados de gerenciamento de configuração (CMDB);								
gestão de patches.								
Segurança de servidores, bancos de dados, estações de trabalho e endpoints;								
segurança de sistemas operacionais Linux e Windows: controle de serviços, permissões, SELinux/AppArmor, GPO, logs, auditoria e atualizações.								
Malware, ransomware e ameaças persistentes avançadas.								
SEGURANÇA DE APLICAÇÕES E DESENVOLVIMENTO SEGURO								
OWASP Top 10: principais riscos de segurança em aplicações web.								
Segurança de aplicações web e APIs: autenticação, autorização, controle de acesso e limitação de taxa (rate limiting).								
Ataques a aplicações: injeção, XSS, CSRF e falhas de controle de acesso.								
Desenvolvimento seguro: práticas de codificação segura e modelagem de ameaças.								
Testes de segurança de aplicações: análise estática (SAST), dinâmica (DAST) e interativa (IAST).								

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
<u>PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)</u>								
DevSecOps: automação de segurança em pipelines.								
Controle de versão com Git: branches, merge, fluxos Gitflow e Trunk-Based;								
GitOps;								
integração e entrega contínua (CI/CD): pipelines de automação (Jenkins, GitLab CI/CD e GitHub Actions).								
Segurança em contêineres e arquiteturas modernas (microserviços, serverless e service mesh): imagens seguras, RBAC, network policies, admission controllers, namespaces, service accounts e segurança de registry.								
GESTÃO DE VULNERABILIDADES E TESTES DE SEGURANÇA								
Gestão de vulnerabilidades: identificação, classificação, priorização, correção e monitoramento.								
Padrões CVE e CVSS.								
Varreduras de vulnerabilidades autenticadas e não autenticadas.								
Testes de invasão (pentest).								
Planos de remediação, reteste e aceitação de riscos.								
Testes de resiliência e programas de bug bounty.								
MONITORAMENTO, OBSERVABILIDADE E OPERAÇÕES DE SEGURANÇA (SECOPS)								
Observabilidade: monitoramento de ativos, disponibilidade e desempenho, métricas e alertas (Zabbix, Prometheus e Grafana);								
Site Reliability Engineering (SRE): princípios, SLIs, SLOs e orçamento de erros.								
Gerenciamento de logs: coleta, retenção, centralização, indexação, correlação e análise (ELK Stack/OpenSearch).								
Trilhas de auditoria e rastreabilidade de acessos e operações.								
SIEM e Centro de Operações de Segurança (SOC): coleta, correlação de eventos e geração de alertas.								

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
<u>PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)</u>								
Detecção e resposta em endpoints, rede e ambiente estendido: EDR, NDR e XDR.								
Inteligência de ameaças: indicadores de comprometimento (IoCs) e framework MITRE ATT&CK.								
Detecção proativa de anomalias e eventos suspeitos.								
Automação e orquestração de resposta em segurança (SOAR): playbooks e integração de ferramentas.								
Métricas de segurança e melhoria contínua: MTTD e MTTR.								
RESPOSTA A INCIDENTES E EVIDÊNCIAS DIGITAIS								
Ciclo de resposta a incidentes de segurança: preparação, identificação, contenção, erradicação, recuperação e lições aprendidas.								
Classificação, triagem e comunicação de incidentes.								
Resposta a incidentes críticos.								
Ransomware: prevenção, resposta e recuperação (backup imutável, air gap e testes periódicos de restauração);								
malware, phishing e engenharia social, injeção de código e negação de serviço (DoS/DDoS).								
Resposta a incidentes de vazamento de dados e de credenciais, acessos indevidos, exploração de vulnerabilidades e indisponibilidade de serviços.								
Preservação de evidências, cadeia de custódia e análise forense.								
CRIOGRAFIA E CERTIFICAÇÃO DIGITAL								
Criptografia simétrica e assimétrica: conceitos, principais algoritmos (AES, RSA e curvas elípticas) e aplicações.								
Funções de hash (SHA-2 e SHA-3) e HMAC: integridade e autenticação de mensagens.								
Certificados digitais, infraestrutura de chaves públicas (PKI) e ICP-Brasil.								
Assinatura digital: integridade, autenticidade e validade de documentos eletrônicos.								

Conteúdo	PDFs	Lei Seca	Videoaulas	Questões	Revisão			
					24 h	7 dias	30 dias	90 dias
PROVA DISCURSIVA (MATERIAL - CLIQUE AQUI)								
Gerenciamento de chaves criptográficas e de segredos (secrets): geração, armazenamento, rotação e revogação.								
Protocolos TLS/SSL e proteção de dados em repouso e em trânsito.								
Prevenção contra vazamento de informações (DLP).								
SEGURANÇA EM NUVEM, BACKUP E CONTINUIDADE								
Computação em nuvem: modelos de serviço (IaaS, PaaS e SaaS) e modelos de implantação (pública, privada e híbrida);								
modelo de responsabilidade compartilhada.								
Segurança em nuvem pública e híbrida: configuração segura, proteção de workloads, security groups, redes virtuais (VPC/VNet), logs, auditoria e gestão de postura de segurança (CSPM).								
Backup e Plano de Recuperação de Desastres (DRP): elaboração, estratégias de recuperação e testes periódicos.								
Continuidade de negócios: análise de impacto nos negócios (BIA) e planos de continuidade de serviços judiciais e de serviços digitais essenciais.								
Indicadores RTO e RPO e resiliência operacional.								
CONSCIENTIZAÇÃO E SEGURANÇA NO USO DE TECNOLOGIAS								
Boas práticas de segurança para usuários: e-mail, navegação, senhas, MFA e ferramentas colaborativas.								
Uso seguro de ferramentas externas e prevenção de vazamento de informações.								
Engenharia social: técnicas e prevenção.								
Segurança de aplicações de inteligência artificial: prompt injection, jailbreak e ataques adversariais;								
exposição indevida de dados.								
Governança algorítmica: avaliação de impacto algorítmico, transparência, explicabilidade, auditabilidade e supervisão humana;								
estratégias de mitigação e auditoria de riscos de IA.								