PROGRAMA DE ESTUDOS

Conhecimentos Específicos – Analista de Tecnologia da Informação (Segurança da Informação)

1. Histórico e conceitos básicos de segurança da informação: propriedades básicas da segurança da informação; níveis de segurança da informação.
2. Criptografia: histórico e conceitos básicos de criptografia e suas aplicações; sistemas criptográficos simétricos e assimétricos; modos de operação de cifras; certificação e assinatura digital; tokens e smartcards; protocolos criptográficos; características do RSA, DES e AES; funções hash; MD5 e SHA.
3. Autenticação: Protocolos e Mecanismos.
4. Controle de Acesso: Mecanismos de Controle de Acesso.
5. Softwares maliciosos (vírus, cavalo de Tróia, adware, spyware, backdoors, keylogger, worm, Rootkit, ransomware) e Antivírus.
6. Segurança em redes wireless: WEP e WPA1/2/3.
7. Segurança de software: programação segura; tratamento de dados; segurança em banco de dados; comprometimento de memória e engenharia reversa.
8. Segurança de aplicativos web: conceitos de segurança de aplicativos web; vulnerabilidades em aplicativos web; metodologia Open Web Application Security Project (OWASP); técnicas de proteção de aplicações web; ataques de dicionário e ataques de força bruta; ameaças e vulnerabilidades em aplicações: Injection [SQL, LDAP], Cross-Site Scripting (XSS), quebra de autenticação e gerenciamento de sessão, referência insegura a objetos, Cross-Site Request Forgery, armazenamento inseguro de dados criptografados; ataques de dia zero (Zero Day attacks).
9. Respostas a incidentes: phishing, SCAMS e SPAMs; engenharia social; cybercrime; ameaças em redes sociais; procedimentos de resposta a incidentes; análise de Malware; investigação forense.
10. Segurança em redes IPv4 e IPv6: segurança na comunicação com SSL, HTTPS, IPSec e VPN; Firewall, IDS e IPS; ataques a redes de computadores: spoofing, flooding, DoS, DdoS e outros; segurança de ativos de rede (switches, roteadores, access points entre outros).
11. Segurança de serviços de rede (por exemplo, HTTP, SMTP, POP, FTP, DNS, entre outros), servidores e estações de trabalho: configurações de segurança em sistemas Linux e Windows.
12. Registros de auditoria: sistemas de log e gerenciador de eventos.
13. Sistemas de backup: tipos de backup, planos de contingência e meios de armazenamento para backups.
14. Gestão de riscos e plano de continuidade do negócio: planejamento, identificação e análise e tratamento de riscos de segurança; análise de impacto nos negócios; plano de

administração de crises; plano de continuidade operacional; plano de recuperação de desastres.

15. Política de segurança da informação: processos de definição, implantação e gestão de políticas de segurança da informação.
16. Legislação em segurança da informação: GDPR (General Data Protection Regulation); Lei Geral de Proteção de Dados (LGPD); Marco Civil da Internet (Lei N° 12.965/14); Normas de segurança da informação: Gestão de segurança da informação (Normas NBR ISO/IEC 27001 e 27002); Gestão de riscos e continuidade de negócio (Normas NBR ISO/IEC 27005 e 15999).
17. Conceitos básicos sobre perícia forense computacional/digital; técnicas de investigação forense computacional; legislação de crimes cibernéticos; persistência e volatilidade da informação; técnicas e ferramentas forenses computacionais.