ESPECIALIDADE: ANALISTA DE SISTEMAS

Engenharia de software: 1 Engenharia de requisitos: conceitos básicos, técnicas de elicitação e especificação. 1.1 Gerenciamento de requisitos. 1.2 Especificação de requisitos. 1.3 Técnicas de validação de requisitos. 1.4 Prototipação. 2 Ciclo de vida do software (Application Lifecycle Management). 2.1 Metodologias de desenvolvimento de software. 2.2 Metodologias ágeis: Scrum, XP, Kanban e TDD. 2.3 Ferramenta de gerenciamento de ciclo de vida de aplicações Azure Devops. 3 Qualidade de software. 3.1 Objetivos da qualidade, restrições e atributos de qualidade, métricas de processo e de código-fonte, análise estática e dinâmica de software. 4 Métricas e estimativas de software. 4.1 Análise por pontos de função. 4.2 Conceitos básicos e aplicações. 4.3 Contagem em projetos de desenvolvimento: IFPUG e Nesma. 4.4 Contagem em projetos de manutenção: IFPUG, Nesma e uso de deflatores. 5 Testes de software: Unidade, Integração, Sistema, Aceitação, Regressão, Desempenho e Carga. **Desenvolvimento de sistemas**: 1 Linguagens e ferramentas de programação. 1.1 Paradigmas de linguagens de programação; conceitos e características estruturais das linguagens de programação; construção de algoritmos, procedimentos, funções, bibliotecas e estruturas de dados; programação estruturada; programação orientada a objetos. 2 Programação avançada em .NET: lambda, delegate, programação web C#, arquitetura de aplicação ASP.NET Core, acesso a dados com ADO.NET e Entity Framework, web services, instalação e configuração de uma aplicação ASP.NET, Razor Pages e Blazor. 3 Boas práticas de análise estática de código fonte (Clean Code). 4 Desenvolvimento orientado a testes (TDD). 5 Segurança da informação: 5.1 Segurança de aplicativos web; vulnerabilidades em aplicativos web; metodologia Open Web Application Security Project (OWASP); técnicas de proteção de aplicações web; gestão de patches e atualizações. 5.2 Certificados digitais e infraestrutura de chaves públicas (PKI). 5.3 Práticas de programação segura e revisão de código. 5.4 Controles e testes de segurança para aplicações web e web services. 6 Arquitetura e tecnologias de sistemas de informação. 6.1 Arquitetura cliente/servidor; arquitetura distribuída; arquitetura de aplicações para ambiente web: servidor de aplicações, servidor Web; arquitetura de software: arquitetura 3 camadas, modelo MVC. Desenvolvimento de integrações: tecnologia Middleware. APS (Application Platform Suite); Interoperabilidade de sistemas: arquitetura orientada a serviço (SOA) e Web Services. Arquitetura Hexagonal e Domain Driven Design. 6.2 Padrões XML, XSLT, SOAP, GRAPHQL e JSON/REST. 6.3 Swagger; Service Discovery; API Gateway; Serviços de autenticação; SSO Single Sign On; Keycloak; Protocolo OAuth2 (RFC 6749); Mensageria e Webhooks; Message Broker; RabbitMQ; Prefect workflow orchestration; 6.4 Low-code e no-code software development 7 Sistemas de gestão de conteúdo; arquitetura de informação: conceitos básicos e aplicações; portais corporativos: conceitos básicos e aplicações; gerenciamento eletrônico de documentos (GED); conceitos de acessibilidade e usabilidade; recomendações W3C para desenvolvimento web (Web Standards); e-Mag; desenho e planejamento de interação em aplicações web. 8 Devops e DevSecOps: 8.1 Desenvolvimento com containers: Docker; Kubernetes. Boas práticas para desenvolvimento de containers. Orquestração containers. Arquitetura de microserviços. 8.2 Controle de versão de código-fonte com GIT, branches, tags, trunk, geração de builds. 8.3 AzureDevops; Rancher; Deploy de aplicações, Continuous Delivery e Continuous Integration (CI/CD). **Banco de dados**: 1 Business Intelligence. 1.1 Data Warehouse e Data Mining. 1.2 Power BI e Crystal Reports 2 Bancos de dados NoSQL: definição de NoSQL, orientação à agregados, tipos de SGBD NoSQL: chave valor, chave valor orientado à documentos, família de colunas, grafos. **Inteligência artificial**: 1 Conceitos e principais tecnologias. 2 Modelos de aprendizado de máquina supervisionados e não supervisionados, deep learning, processamento de linguagem natural. 3 Desenvolvimento de serviços de Chatbots. 4 Ferramentas de desenvolvimento de aplicações de aprendizado de máquina: Python 3; Bibliotecas: TensorFlow, Pandas, Scikit-learn, Keras, Pytorch. 5 Inteligência Artificial Generativa e LLM (Large Language Models).

ESPECIALIDADE: ANALISTA DE SEGURANÇA

Segurança da informação: 1 Segurança em serviços de e-mail: Conceitos e métodos de autenticação de e-mails utilizando DMARC, DKIM e SPF. 2 Política de segurança da informação: processos de definição, implantação e gestão de políticas de segurança. 3 Conceitos avançados de criptografia e sistemas criptográficos: simétricos, assimétricos, infraestrutura de chaves públicas, certificação e assinatura digital, ataques a sistemas criptográficos. 4 Gerência de riscos: ameaça, vulnerabilidade e impacto; planejamento, identificação, análise e tratamento de riscos de segurança; melhores práticas de gerenciamento de risco. 5 Gestão de continuidade do negócio: análise de impacto nos negócios (BIA), análise de riscos, estratégia de continuidade, plano de administração de crises, plano de continuidade operacional, plano de recuperação de desastres, plano de testes. 6 Gestão de segurança da informação: classificação e controle de ativos de informação, segurança de ambientes físicos e lógicos, controles de acesso, segurança de serviços terceirizados. 7 Normas de segurança da informação: ABNT NBR ISO 27003:2020 - Sistemas de gestão da segurança da informação — Orientações; ABNT NBR ISO 27004:2017 - Sistemas de gestão da segurança da informação — Monitoramento, medição, análise e avaliação; ABNT NBR ISO/IEC 27005:2023 - Orientações para gestão de riscos de segurança da informação; ABNT NBR ISO 31000:2018 - gestão de riscos - diretrizes; ABNT NBR ISO 22301:2020 - sistemas de gestão de continuidade de negócios - requisitos; ABNT NBR ISO 22313:2020 - sistemas de gestão de continuidade de negócios - orientações para o uso da ABNT NBR ISO 22301. 8 Segurança de aplicações: segurança em banco de dados; desenvolvimento seguro de software. 9 Segurança de aplicativos web: conceitos de segurança de aplicativos web; vulnerabilidades em aplicativos web; análise de vulnerabilidades em aplicativos web; ferramentas e técnicas de exploração de vulnerabilidades em aplicativos web; testes de invasão em aplicativos web; metodologia Open Web Application Security Project (OWASP); técnicas de proteção de aplicações web; gestão de patches e atualizações. 10 Ataques a redes e serviços: Injection [SQL, LDAP], DDoS, DoS, IP spoofing, buffer overflow, Cross-Site Scripting (XSS), spear phishing, port scan, quebra de autenticação e sequestro de sessão, referência insegura a objetos, Cross-Site Request Forgery, APT - Advanced Persistent Threat, armazenamento inseguro de dados criptografados, ataque de dia zero (Zero Day Attack), ataques de dicionário, ataques de força bruta e sequestro de dados. 11 Procedimentos de resposta a incidentes: tratamento de incidentes de segurança; análise de malwares; investigação forense; seleção das técnicas apropriadas para mitigação e resposta; Frameworks de segurança da informação e segurança cibernética: MITRE ATT&CK; Guia de aperfeiçoamento da segurança cibernética para infraestrutura crítica V1.1 (NIST). 12 Segurança em redes: segmentação de redes, sistemas de firewall, firewall de aplicação web (WAF), detectores de intrusão (IDS e IPS), NAT, analisadores de tráfegos de rede (Sniffers), NDR (Network Detection and Response), XDR (Extended Detection and Response), Privileged Access Management – PAM, DMZ, Virtual Private Networks (IPSEC VPN, SSL VPN, client-to-site e site-to-site), defesa de perímetros, topologias de redes seguras, técnicas de microsegmentação de firewall e Zero Trust. 13 Ameaças cibernéticas: conceitos e características de vírus, worm, cavalo de tróia, backdoor, keylogger, screenlogger, exploit, spyware, ransomware, rootkit e bot; Phishing; Engenharia social. 14 Segurança em redes wireless. 15 Segurança de servidores e estações de trabalho, configurações de segurança em servidores Linux e Windows, EDR (Endpoint Detection and Response). 16 Sistemas de backup: boas práticas, tipos de backups, planos de contingência e meios de armazenamento para backups. 17 Testes de invasão (pentest) em aplicações web, banco de dados, sistemas operacionais e dispositivos de redes. 18 Network Access Control (NAC) e Network Access Protection (NAP). 19 Registros de auditoria: conceitos, servidor de log centralizado, protocolos Syslog e Microsoft Event Viewer. 20 Security Information and Event Management (SIEM) - Sistema de gerenciamento e correlação de eventos relacionados à segurança da informação. 21 Segurança de dados em dispositivos móveis. 22 Controle de acesso baseado em papéis (Role Based Access Control – RBAC). **Sistemas de computação**: 1 Sistemas operacionais. 1.1 Linux (Ubuntu Server). 1.2 Windows Server 2022. 2 Tipologias de ambientes com alta disponibilidade e escalabilidade. 2.1 Clusterização. 2.2 Balanceamento de carga. 2.3 Fail Over. 2.4 Replicação de estados. 3 Microsoft Active Directory e LDAP. 4 Shellscript. 4.1 Script Bash. 4.2 Powershell. 5 Segurança linux. 5.1 IPTables. 5.2 SELinux. 5.3 Hardening. 6 SSL/TLS. 7 Information Lifecycle Management. 8 Computação na nuvem (Cloud Computing). 8.1 Segurança em Cloud Computing. 9 Virtualização de servidores: VMware vSphere, vCenter, vSAN, vNetwork Distributed Switch. 10. Soluções de Hiperconvergência. 11. Virtualização de Aplicações: Docker e orquestração de containers com Kubernetes.

ESPECIALIDADE: ANALISTA DE SUPORTE

Segurança da Informação: 1 Normas de segurança da informação: ABNT NBR ISO 27003:2020 - Sistemas de gestão da segurança da informação — Orientações; ABNT NBR ISO 27004:2017 - Sistemas de gestão da segurança da informação — Monitoramento, medição, análise e avaliação; ABNT NBR ISO/IEC 27005:2023 - Orientações para gestão de riscos de segurança da informação; ABNT NBR ISO 31000:2018 - gestão de riscos - diretrizes; ABNT NBR ISO 22301:2020 - sistemas de gestão de continuidade de negócios - requisitos; ABNT NBR ISO 22313:2020 - sistemas de gestão de continuidade de negócios - orientações para o uso da ABNT NBR ISO 22301. 2 Políticas de segurança da informação. 3 Sistema de Gestão de Segurança da Informação. 4 Conceitos avançados de criptografia e sistemas criptográficos: simétricos, assimétricos, infraestrutura de chaves públicas, certificação e assinatura digital, ataques a sistemas criptográficos. 5 Segurança em redes: segmentação de redes, sistemas de firewall, firewall de aplicação web (WAF), detectores de intrusão (IDS e IPS), NAT, analisadores de tráfegos de rede (Sniffers), NDR(Network Detection and Response), XDR (Extended Detection and Response), Privileged Access Management – PAM, DMZ, Virtual Private Networks (IPSEC VPN, SSL VPN, client-to-site e site-to-site), defesa de perímetros, topologias de redes seguras, técnicas de microsegmentação de firewall e Zero Trust. 6 Ameaças cibernéticas: conceitos e características de vírus, worm, cavalo de tróia, backdoor, keylogger, screenlogger, exploit, spyware, ransomware, rootkit e bot; Phishing; Engenharia social. 7 Segurança em redes wireless. 8 Segurança de servidores e estações de trabalho, configurações de segurança em servidores Linux e Windows, EDR (Endpoint Detection and Response). 9 Registros de auditoria: conceitos, servidor de log centralizado, protocolos Syslog e Microsoft Event Viewer. 10 Sistemas de backup: boas práticas, tipos de backups, planos de contingência e meios de armazenamento para backups. **Redes de computadores**: 1 Comunicação de dados. 2 Internet: governança, estrutura, protocolos e serviços. 3 Tecnologias, protocolos, topologias e elementos de redes LAN e WAN; SDWAN. 4 Tecnologia de roteamento - switches layer 3 e roteadores. 5 Administração de ativos de rede (switches e roteadores). 6 Protocolos de roteamento RIP, OSPF e BGP. 7 Qualidade de serviços (QoS): DiffServ, Filas, DCSP e CoS (IEEE 802.1p). 8 Configuração, gerenciamento e segurança de redes de computadores Windows e Linux. 9 NAT. 10 Protocolos: IP, TCP, UDP, ICMP, HTTP, SMTP, POP, IMAP, DNS, DHCP, NIS, SSH, FTP, LDAP v.3, ICAP, NTP v4, EAP, ONVIF, RTSP. 11 SNMP. 11.1 conceitos de MIB, MIB II e MIBs proprietárias. 11.2 Zabbix. 12 Protocolo IPv4 e IPv6; Transição do IPv4 para o IPv6: Técnicas de transição e coexistência. 13 Endereçamento MAC, STP, PVSTP, ARP, IEEE 802.1q, IEEE 802.1x e IEEE 802.11 g/n/ac/ax. 14 Fibras ópticas: fundamentos e padrões. 15 Fibre Channel Protocol (FCP), Fibre Channel over Ethernet (FCoE) e iSCSI. 16 Projeto, implementação e administração de redes de comunicação de dados, voz e vídeo em LAN e WAN. 16.1 voz sobre IP (Codecs, RTP, Projeto em VoIP). 16.2 telefonia IP. 16.3 videoconferência (SIP, H323, Multicast, IGMP).