atribuição, entrada e saída; avaliação de expressões; funções pré-definidas; conceito de bloco de comandos; estruturas de controle, seleção, repetição e desvio; operadores e expressões; passagem de parâmetros; recursividade; conceitos básicos de programação estruturada e orientada a objetos; métodos de ordenação, pesquisa e "hashing". Engenharia de Requisitos: Conceitos básicos; técnicas de elicitação de requisitos; gerenciamento de requisitos; especificação de requisitos; técnicas de validação de requisitos; prototipação. Qualidade de Software: Metodologias de desenvolvimento de software; processo unificado: conceitos, diretrizes, disciplinas; metodologias ágeis; métricas e estimativas de software; análise por pontos de função. Análise e Projeto Orientados a Objetos: Conceitos básicos, padrões de projetos. UML: Visão geral, modelos e diagramas. Programação Orientada a Objetos: classes, objetos, métodos, mensagens, sobrecarga, herança, polimorfismo, interfaces e pacotes; tratamento de exceção. Linguagens e Tecnologias de Programação: Linguagens de programação Java e PHP; Javascript; AJAX; JQUERY; XML; CSS; Frameworks Java EE: Jboss seam framework; Java Server Faces (jsf); Richfaces; Hibernate. Ferramentas de desenvolvimento e teste: Eclipse Galileo; TestNG / Junit; Jakarta Jmeter; Apache; Tomcat; Especificação de metadados e web services; Servidores de aplicação Java; ferramentas de gerência de configuração; práticas ágeis: Integração contínua, Test-driven Development (TDD), Refactoring; Design Patterns; Testes: Teste funcional e de unidade; Arquitetura cliente-servidor; arquitetura distribuída; portais corporativos; sistemas colaborativos; gestão de conteúdo. Segurança da Informação: auditoria; sistemas de criptografia e suas aplicações; assinatura e certificação digital; ABNT NBR ISO/IEC 27002-2005: Análise/avaliação e tratamento dos riscos; política de segurança da informação; gestão de ativos; controle de acessos; desenvolvimento e manutenção de sistemas de informação; gestão da continuidade do negócio. Segurança de aplicativos web: conceitos de segurança de aplicativos web; vulnerabilidades em aplicativos web; análise de vulnerabilidades em aplicações 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; 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. Banco de Dados: Modelo de entidade-relacionamento (MER); modelo conceitual, lógico e físico; conceitos básicos de banco de dados: esquema, tabelas, campos, registros, índices, relacionamentos, transação, triggers, tipos de bancos de dados; normalização de dados: conceitos, primeira, segunda e terceira formas normais. DML: Linguagem de manipulação de dados e DDL: Linguagem de definição de dados.

TÉCNICO – ANALISTA DE SISTEMA – SUPORTE A REDE DE COMPUTADORES

Governança de Tecnologia da Informação: Conceitos básicos; planejamento estratégico; gerência de portfólio; escritório de projetos: implantação, estrutura e funcionamento. COBIT 4.1: conceitos básicos, estrutura e objetivos, requisitos da informação, recursos de tecnologia da informação, domínios, processos e objetivos de controle. ITIL v.3: conceitos básicos, estrutura e objetivos; processos e funções de estratégia, desenho, transição e operação de serviços. PMBOK 4ª edição: conceitos básicos, estrutura e objetivos; projetos e a organização; ciclo de vida de projeto e de produto; processos, grupos de processo e áreas de conhecimento. Gestão de segurança da informação. Normas NBR ISO/IEC 27001 e 27002; Gestão de riscos e continuidade de negócio. Normas NBR ISO/IEC 15999 e 27005; Noções Gerais sobre computadores e sistemas computacionais: Computadores: arquitetura de computadores, componentes de um computador (hardware e software), linguagens de programação, compiladores e interpretadores, sistemas de numeração e representação de dados, aritmética computacional; Sistemas operacionais: Funções básicas, sistemas de arquivos e gerenciamento de memória; Redes de computadores: fundamentos de comunicação de dados, meios físicos, serviços de comunicação, redes LANs e WANs, arquitetura TCP/IP, protocolos e serviços; Organização, arquiteturas CISC e RISC, Processamento distribuído e processamento paralelo; Entradas e saídas de dados; Hardware: Diagnóstico de Falhas; Instalação de periféricos. Infraestrutura de TI: Sistemas Operacionais Windows e Linux: administração de servidores; Interoperabilidade; Virtualização; Sistema de Arquivos (FAT, FAT32, NTFS e EXFAT) envolvendo direitos de acesso, segurança e integridade; Compartilhamento de recursos; Ferramentas de Backup nativas; Detecção de falhas em dispositivos, serviços e aplicativos (Log de Eventos, ferramentas de desempenho, etc.); Configuração, instalação e manutenção de software; Gerenciamento de discos e volumes (HD, Pendrive, CDROM, etc); Configuração de rede local; Configurações avançadas de firewall; Configurações de segurança de navegador (Internet Explorer, Firefox, Chrome); Conceitos de serviços de armazenamento; ferramentas de backup; Conceitos de Virtualização; Interoperabilidade; Cloud Computing; Conceitos de alta disponibilidade e escalabilidade; redundância e tolerância a falhas: Tipos de RAID. RAID 1 e RAID 0 + 1; Balanceamento de carga; cluster fail-over e replicação; Técnicas para detecção de problemas e otimização de desempenho; Tecnologias de armazenamento DAS, NAS e SAN. Tecnologias de backup, Deduplicação e ILM – Information Lifecycle Management; Plataforma de virtualização Vmware; Protocolo de Armazenamento Fibre Channel; Solução de Colaboração Zimbra; Proxy Web Cache Squid. Redes de computadores: Redes LAN e WAN; Endereçamento e protocolos da família TCP/IP; Gerenciamento de redes TCP/IP; Protocolos: SNMP, SMI, MIB, RMONRedes de longa distância: MPLS; Tecnologia de acesso para última milha: ADSL, DOCSIS, FTTH, PON; Cabeamento estruturado: Cabo da categoria 7 (CAT5), CAT6 e CAT7, fibra ótica Monomodo, Multimodo, padrão Ethernet, Fast Ethernet e Gigabit Ethernet, Cabo da categoria 7 (CAT7), padrão TIA/EIA-568-A e TIA/EIA-568-B; Administração de Serviços de diretório: Active Directory e LDAP; Conceitos de Serviços de correio eletrônico, SMTP, gateway; serviços de rede: DNS, DHCP, WINS; Redes de computadores; Topologia de Redes; Alta disponibilidade e escalabilidade e Protocolo: VRRP, HSRP; Modelo de referência OSI; Elementos de interconexão de redes de computadores (gateways, switches, roteadores); Redes de longa distância: MPLS; Redes sem fio: padrões 802.11, protocolos 802.1x, EAP, WEP, WPA e WPA2; Conceitos de Internet e Intranet SMTP, HTTP, HTTPS, FTP; Protocolos DNS, WINS, DHCP, SMTP, HTTP, HTTPS, FTP. Ferramentas de Gerenciamento de Rede; dispositivos de comutação; Modelo de referência OSI; Elementos de interconexão de redes de computadores (gateways, switches, roteadores); protocolos: RIP, IGRP, OSPF e BGP; Equipamentos de PABX; Voz sobre IP; QOS; Modelo OSI da ISO; Arquitetura e protocolos TCP/
P; Nível de aplicação TCP/ DNS, FTP, NFS, TELNET, SMTP, HTTP, LDAP, DHCP, IPSEC, SSH, SNMP e NAT; Noções básicas de IPv6; Conceitos de Storage (NAS e SAN). Segurança da informação: conceitos básicos; classificação de informações; procedimentos de segurança; auditoria e conformidade; confiabilidade, integridade e disponibilidade; controle de acesso; autenticação; segurança física e lógica; identificação, autorização e autenticação; gestão de identidades; métricas e indicadores em segurança da informação; política de segurança da informação: processos de definição, detecção de vulnerabilidade, implantação e gestão de políticas de segurança e auditoria; criptografia: conceitos de criptografia, aplicações, sistemas criptográficos simétricos e de chave pública; 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-1; esteganografia; análise de vulnerabilidade; gerência de riscos: ameaça, vulnerabilidade e impacto; planejamento, identificação e análise e tratamento de riscos de segurança; 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; 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; normas de segurança da informação: NBR 20000-1:2011 - gestão de serviços; NBR 20000-2:2008 - gerenciamento de serviços; NBR 27001:2006 - sistemas de gestão de segurança da informação; NBR 27002:2005 - código de prática para a gestão da segurança da informação; NBR 27005:2005 - gestão de riscos de segurança; NBR 15999-1 - gestão de continuidade de negócios; segurança de aplicações: segurança em banco de dados SQL SERVER; segurança de sistema de colaboração Zimbra;segurança de plataforma de virtualização Vmware desenvolvimento seguro de software; segurança de aplicativos web: conceitos de segurança de aplicativos web; vulnerabilidades em aplicativos web; análise de vulnerabilidades em aplicações 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; 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; Respostas a incidentes: phishings, SCAMS e SPAMs; engenharia social; cybercrime; ameaças em redes sociais; procedimentos de resposta a incidentes; análise de Malwares; investigação forense; segurança em redes: segmentação de redes, sistemas de firewall, firewall de aplicação web (WAF), detectores de intrusão (IDS e IPS), NAT IP,NAT H323, analisadores de tráfegos de rede (Sniffers), DMZ, proxies, Virtual Private Networks (IPSEC VPN e SSL VPN); defesa de perímetros; ataques a redes de computadores: prevenção e tratamento de incidentes, tipos de ataques (spoofing, flood, DoS, DDoS, phishing); teste de invasão; topologias seguras; mecanismos de autenticação (TACACS,TACACS+, RADIUS, Kerberos, CHAP, MSCHAP); softwares maliciosos (vírus, cavalo de tróia, adware, spyware, backdoors, keylogger, worm, Rootkit); antivírus; segurança de switch e roteadores; segurança em redes wireless; segurança de servidores e estações de trabalho: configurações de segurança em servidores Linux e Windows (Hardening); configurações de segurança para estações Windows XP, Vista e 7; registros de auditoria: protocolo Syslog e Microsoft Event View; segurança de infraestrutura de TI: sistemas de anti-Spam; segurança em servidores WWW, SMTP, POP, FTP e DNS; sistemas de backup: tipos de backups, planos de contingência e meios de armazenamento para backups; segurança em operações: identificação e gestão de ativos; gestão de configuração; gestão de. mudanças; ataques do dia zero (Zero Day attacks); testes de Invasão (pentest) em aplicações Web, banco de dados, sistemas operacionais e dispositivos de redes; Network Access Control (NAC) e Network Access Protection (NAP); Security Information and Event Management (SIEM) – sistema de correlação de eventos relacionados a segurança da informação; segurança em dispositivos móveis.

TÉCNICO – ANALISTA DE SISTEMA – MODELAGEM DE SISTEMAS

Governança de Tecnologia da Informação: Conceitos básicos; planejamento estratégico; gerência de portfólio; escritório de projetos: implantação, estrutura e funcionamento. COBIT 4.1: conceitos básicos, estrutura e objetivos, requisitos da informação, recursos de tecnologia da informação, domínios, processos e objetivos de controle. ITIL v.3: conceitos básicos, estrutura e objetivos; processos e funções de estratégia, desenho, transição e operação de serviços. PMBOK 4ª edição: conceitos básicos, estrutura e objetivos; projetos e a organização; ciclo de vida de projeto e de produto; processos, grupos de processo e áreas de conhecimento. MPS.BR Conceitos básicos e objetivos. Disciplinas e formas de representação. Níveis de capacidade e maturidade. Processos e categorias de processos. Gestão de Negócios: noções e metodologias de planejamento estratégico; Balanced Scorecard (BSC); Matriz SWOT; análise de cenários; medição de desempenho. Arquitetura e modelagem organizacional, estruturas funcionais, matriciais, por processos e por projetos. Conceitos básicos de programação estruturada e orientada a objetos; Engenharia de requisitos: Conceitos. Técnicas de elicitação de requisitos. Gerenciamento de requisitos. Especificação de requisitos. Técnicas de validação de requisitos. Prototipação. Notações UML e ER. Engenharia de software: processos de desenvolvimento de software (processo cascata, processo iterativo), RUP, Scrum e Programação Extrema(XP); projeto de software orientado a objetos (OOP) e aspectos (AOP), Padrões de Projeto (Design Patterns) e Anti-Patterns. Ciclo de vida do software. Conceitos de qualidade de software. Garantia da Qualidade de software (SQA). ISO 12207. ISO 15504. ISO 9126. NBR ISO 25000. IEEE 829. Processos de desenvolvimento de software CMMI-DEV v.1.2, MPS.BR. Engenharia de usabilidade. Conceitos básicos e aplicações. Critérios, recomendações e guias de estilo. Análise de requisitos de usabilidade. Métodos para avaliação de usabilidade. Acessibilidade na web: conceitos básicos, recomendações W3C, e-Mag. Segurança da informação: conceitos básicos; políticas de segurança; classificação de informações. Testes de Software. Conceitos de teste: tipos, padrões, métodos e processos. Test Driven Development (TDD). Planejamento, Elaboração Execução e Automatização de testes. Métricas e Estimativas aplicadas a Teste de Software. Aplicações: Arquitetura e tecnologias de sistemas de informação: conceitos básicos; Workflow e gerenciamento eletrônico de documentos; Conceitos de Sistemas Integrados de Gestão (ERP); Conceitos de Arquitetura Orientada a Serviços (SOA); arquitetura cliente-servidor; arquitetura distribuída; portais corporativos; sistemas colaborativos; gestão de conteúdo; especificação de metadados e web services. Noções de SQL. Software livre e software público: conceito, tipos de licença, estágio atual das principais aplicações. Análise por pontos de função. Conceitos básicos e aplicações. Contagem em projetos de desenvolvimento: IFPUG e Nesma. Contagem em projetos de manutenção: IFPUG, Nesma e uso de deflatores.

TÉCNICO - BIBLIOTECONOMISTA

Documentação: conceito, teoria, ciclo, tipologia, objetivos, caracterização e estrutura da documentação geral e jurídica. Centros de documentação. Biblioteconomia e Ciência da Informação: origens, teorias, conceitos básicos, definições, terminologia, objetivos, histórico e tendências. Gestão de unidades de informação: Estrutura organizacional. Planejamento, organização e administração de serviços de informação. Gestão da informação e do conhecimento. Formação e desenvolvimento de coleções: políticas e princípios de aquisição, seleção e descarte. Fatores de uso. Avaliação, preservação e conservação de coleções. Representação descritiva de documentos: processos, instrumentos e produtos. Código de Catalogação Anglo-Americano - 2ª edição revista: normas vigentes. Catalogação descritiva. Catálogos: funções e tipos. Requisitos Funcionais para Registros Bibliográficos: FRBR. Código RDA. Metadados. Dublin Core. Representação temática de documentos: processos, instrumentos e produtos. Sistemas de classificação bibliográfica: CDU e CDD. Indexação: coerência, qualidade, linguagens, processos e tipos. Tesauros, ontologias, cabeçalhos de assuntos e vocabulários controlados. Normalização de documentos: normas técnicas vigentes da Associação Brasileira de Normas Técnicas (ABNT). Fontes de informação gerais e especializadas: tipologia e função. Fontes oficiais nacionais e internacionais, bases de dados especializadas, repertórios, portais e vortais de organizações governamentais e não-governamentais. Redes de informação. Disseminação da informação: princípios e serviços. Serviço de referência. Comutação bibliográfica. Fluxo da informação. Estudos de uso e de usuários. Tecnologias de