3. 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 2008 R2; 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.

4. Sistemas operacionais de rede: Microsoft Windows Server 2008 R2: instalação, customização, administração, operação e suporte em ambiente; serviço de diretório active directory; conhecer arquitetura e funcionamento de ambiente de virtualização (Hyper-v) com Failover Cluster; integração com ambiente Unix; gerenciamento de políticas de grupo (GPO); serviços de arquivos, impressão, web (IIS), terminal (TS), DNS, DHCP; gerenciamento e planejamento de cópias de segurança (backup); configuração dos protocolos IPv4 e IPv6; linguagem de script powershell; Microsoft clustered shared volumes; Servidor de correio Exchange Server 2010; WSUS; VPN; instalação, customização, administração, operação e suporte em ambiente Linux (distribuições Debian e CentOS); instalação e suporte a TCP/IP, DHCP, DNS, NIS, CIFS, CUPS, SAMBA, CIFS, NFS; instalação e configuração do servidor Apache; linguagens de script; integração com ambiente Windows; serviços de diretório: LDAP e Open LDAP; virtualização; Squid; ModSecurity; Bind; IPTables; Nagios; DHCP; SSH; FTP; estações de trabalho: Windows XP, Windows Vista e Windows 7 (instalação e configuração de ambiente e dispositivo).

5. Redes de computadores: princípios e fundamentos de comunicação de dados; meios de transmissão; técnicas básicas de comunicação; técnicas de comutação de circuitos, pacotes e células; topologias de redes de computadores; arquitetura e protocolos de redes de comunicação; modelo de referencia OSI e principais padrões internacionais; arquitetura cliente/servidor; padrão X. 500; métodos de autenticação; internet e intranet; Protocolo TCP/IP v4 e v6; conceitos e configuração de serviços DNS, HTTP,HTTPS, SSL, NTP, SSH, TELNET, FTP, DHCP, SMTP, POP, IMAP; proxy cache, proxy reverso e NAT; conceito de VPN, IPSec e VLAN; LDAP, NFS, NTP; tecnologias de WAN: Comutação por circuitos, pacotes e células, circuitos virtuais, topologias; Protocolos: ATM; Frame Relay, HDLC e tecnologia MPLS; Roteamento estático e dinâmico; determinação de rotas: métricas e distância administrativa; tipos de protocolos: distance vector e link state (OSPF, RIPv2); BGP: vizinhança e métricas; sistemas autônomos (AS); estratégias de roteamento; tecnologias de LAN e MAN: tipos de transmissão; Protocolos de acesso múltiplo: CSMA-CD e CSMA-CA; topologias; elementos de interconexão de redes de computadores (gateways, hubs, repetidores, bridges, switches, roteadores); ethermet, fast ethernet, gigabit ethernet e metro ethernet; Endereçamento MAC, STP, PVSTP, RSTP, ARP, IEEE 802.1q, IEEE 802.1x e IEEE 802.11a/b/g/n; fibras ópticas: fundamentos, padrões 1000BaseSX e 1000BaseLX; redes sem fio (wireless); gerência de redes: protocolo SNMP (versão 2 e 3) RMON; conceitos de MIB, MIB II e MIBs proprietárias; serviços de gerenciamento de rede (NMS); Gerencia de falha, de capacidade e de mudança; conhecimento de ferramentas para administração, análise de desempenho, inventário e tunning de sistemas aplicativos; monitoramento e logging; performance e detecção de problemas; virtualização; instalação e configuração de roteadores e switches; sincronização de tempo.

6. Tópicos avançados: consolidação de servidores; integração de plataformas; cluster (alta disponibilidade, balanceamento de carga e performance); conceitos de mensageria (MTA e MUA); computação em grid e em nuvem; servidores de aplicação: Apache, Tomcat, Jboss e IIS; arquitetura e funcionamento de datacenters; convergência de rede: voz sobre IP (Codecs, RTP, Projeto em VoIP); telefonia IP; videoconferência (SIP, H323, Multicast, IGMP) e qualidade de serviços (QoS): DiffServ, Filas, DCSP e CoS (IEEE 802.1p).

7. Arquitetura de sistemas computacionais: organização e arquitetura de computadores: componentes básicos de hardware e software, sistemas de entrada e saída, periféricos, sistemas de numeração e codificação, aritmética computacional, arquitetura de computadores RISC e CISC, características dos principais processadores do mercado; sistemas operacionais: arquiteturas, gerenciamento de sistemas de arquivos, características dos sistemas operacionais corporativos da família Windows e Linux; sistemas operacionais de redes; interoperação de sistemas operacionais; processos concorrentes; sistemas distribuídos; sistemas multiprogramados; escalonamento de processo; gerência de memória; deadlock; gerência de recursos; virtualização.

CARGO 406: ASSESSOR TÉCNICO DE INFORMÁTICA – ANALISTA DE SISTEMAS

Conhecimentos Específicos: 1. Gerência de projetos: conceitos básicos; processos do PMBOK; gerenciamento da integração, do escopo, do tempo, de custos, de recursos humanos, de riscos, das comunicações, da qualidade e de aquisições; gestão de projetos com SCRUM.

2. Governança de TI: gestão estratégica: noções e metodologias de planejamento estratégico; noções de Balanced Scorecard (BSC); matriz SWOT; análise de cenários; indicadores de desempenho: conceito, formulação e análise; conceitos de Planejamento Estratégico de TI e Plano Diretor de TI; modelos de governança; fundamentos de Cobit 4.1: objetivos do modelo, estrutura do modelo, aplicabilidade do modelo e benefícios do modelo; noções de gerenciamento de serviços de TI - ITIL V3: conceitos, objetivos, estrutura do modelo, aplicabilidade e benefícios do modelo.

3. Modelagem de processos de negócio: modelagem de processos; técnicas de análise de processo; melhoria de processos; integração de processos; gerenciamento de processos de negócio (BPM).

4. Segurança da informação: conceitos; políticas de segurança; classificação de informações; procedimentos de segurança; auditoria e conformidade; Confiabilidade. Integridade. Disponibilidade. Mecanismos de segurança: criptografia, assinatura digital, garantia de integridade, controle de acesso e certificação digital; desenvolvimento de sistemas seguros.

5. Arquitetura e tecnologias de sistemas de informação: conceitos básicos; arquitetura cliente/servidor; arquitetura orientada a serviço (SOA); arquitetura distribuída; portais corporativos; sistemas colaborativos; gestão de conteúdo; especificação de metadados; arquitetura de aplicações para ambiente web: servidor de aplicações, servidor Web; arquitetura de software: arquitetura 3 camadas, modelo MVC; web services.

CONTINUA NO CADERNO 9