informação, conhecimento e inteligência; dados estruturados e não estruturados; dados abertos; coleta, tratamento, armazenamento, integração e recuperação de dados. 3.3 Modelagem dimensional; dimensões; fatos; arquiteturas OLAP, ROLAP e MOLAP; projeto e arquitetura de ETL; funções e componentes de Data Mart e Data Warehouse; ciclo de vida do DW; bancos de dados multidimensionais. 3.4 Noções de mineração de dados: conceituação e características; modelo de referência CRISP-DM; técnicas para pré-processamento de dados; técnicas e tarefas de mineração de dados; classificação; regras de associação; análise de agrupamentos (clusterização); detecção de anomalias; modelagem preditiva; aprendizado de máquina; mineração de texto. 4 Noções de Big Data: conceito, premissas e aplicação. 5 Visualização e análise exploratória de dados. 6 Microsoft SQL Server 2008 R2: arquitetura, estrutura e administração do banco de dados; administração de usuários e perfis de acesso; gerenciamento de transações; recuperação; controle de proteção, integridade, concorrência e bloqueio de transações; segurança, backup e restauração de dados; tolerância a falhas e continuidade de operação; monitoração, otimização e análise de desempenho; implementação e operação; cluster e replicação de dados. 7 Ferramentas para Banco de Dados. 7.1 Ferramentas de Front End: principais recursos e aplicações para o banco de dados SQL Server 2008 R2, Oracle 11g e MySQL Server 5.x. 7.2 Ferramentas SAP Business Objects Enterprise Infoview. 3.1; Crystal Reports; Microsoft SQL Server 2008 R2 Analysis Service; Microsoft SQL Server 2008 R2 Integration Service e Microsoft SQL Server 2008 R2 Reporting Service.
ARMAZENAMENTO DE DADOS: Rede SAN (Storage Area Network) e NAS (Network Attached Storage); Switches e Directors Fiber Channel; Fibre Channel Protocol (FCP); sistemas de fitoteca; sistemas de armazenamento em disco; soluções de armazenamento RAID (níveis 0, 1, 5, 6, 1+0 e 0+1); virtualização e cluster de servidores; balanceamento de carga; contingência e continuidade de operação; Protocolos Common Internet File System (CIFS) e Network File System (NFS); elaboração e execução de política de backup e restauração de dados.
ARQUITETURA E TECNOLOGIAS DE SISTEMAS DE INFORMAÇÃO: 1 Conceitos básicos; arquitetura cliente/servidor; arquitetura distribuída; especificação de metadados; 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. 2 Padrões XML, XSLT, UDDI, WSDL, SOAP e JSON/REST.
REDES DE COMPUTADORES: 1 Meios de transmissão. 2 Topologias de redes de computadores, Internet, Intranet, modelo de referência OSI e arquitetura TCP/IP. 3 Tecnologias e protocolos de redes locais: padrões Ethernet, endereçamento IP, máscara de rede, protocolos (IP, ARP, ICMP, UDP, TCP, FTP, SMTP e SSH), roteamento. 4 Elementos de interconexão de redes de computadores (hubs, bridges, switches, roteadores, gateways). 5 Protocolos de acesso múltiplo: CSMA-CD e CSMA-CA. 6 Padrões IEEE 802: VLAN, redes sem fio. 7 Administração do sistema operacional Windows Server 2008 R2.
ARQUITETURA DE SISTEMAS COMPUTACIONAIS: 1 Organização e arquitetura de computadores: componentes básicos de hardware e software, sistemas de entrada e saída, sistemas de numeração e codificação, aritmética computacional, características dos principais processadores do mercado. 2 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; clusters; sistemas multiprogramados; escalonamento de processo; gerência de memória; deadlock; gerência de recursos; sistema de arquivos.

CARGO 33: AUDITOR DE CONTROLE EXTERNO - ÁREA: INFORMÁTICA- ESPECIALIDADE: ANALISTA DE SEGURANÇA

SEGURANÇA DA INFORMAÇÃO: 1 Conceitos de segurança da informação: 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. 2 Política de segurança da informação: processos de definição, implantação e gestão de políticas de segurança. 3 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. 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/IEC 27001:2013 - sistemas de gestão da segurança da informação - requisitos; ABNT NBR ISO/IEC 27002:2013 - código de prática para controles de segurança da informação; ABNT NBR ISO 27003:2011 versão corrigida: 2015 - diretrizes para implantação de um sistema de gestão da segurança da informação; ABNT NBR ISO 27004:2010 - gestão da segurança da informação - medição; ABNT NBR ISO/IEC 27005:2011 - gestão de riscos de segurança da informação; ABNT NBR ISO 31000:2009 - gestão de riscos - princípios e diretrizes; ABNT NBR ISO 22301:2013 - sistemas de gestão de continuidade de negócios - requisitos; ABNT NBR ISO 22313:2015 - sistemas de gestão de continuidade de negócios - orientações. 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, engenharia social, ataque de dia zero (Zero Day Attack), ataques de dicionário e ataques de força bruta. 11 Procedimentos de resposta a incidentes: tratamento de incidentes de segurança; análise de malwares; investigação forense; seleção das técnicas apropriadas para mitigação e resposta. 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), DMZ, proxies, Virtual Private Networks (IPSEC VPN, SSL VPN, client-to-site e site-to-site), defesa de perímetros, topologias de redes seguras. 13 Softwares maliciosos: conceitos e características de vírus, worm, cavalo de tróia, backdoor, keylogger, screenlogger, exploit, spyware, adware, ransomware, rootkit e bot. 14 Segurança em redes wireless. 15 Segurança de servidores e estações de trabalho, configurações de segurança em servidores Linux e Windows, softwares de segurança. 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). 23 Padrões de Interoperabilidade do Governo Brasileiro (e-PING). 24 Boas práticas em segurança da informação no âmbito da Administração Pública Federal: Instrução Normativa GSI/PR nº 1/2008 e normas complementares do GSI/PR. 25 Lei nº 12.527/2011 (LAI - Lei de Acesso à Informação). 26 Lei nº 12.965/2014 (Marco Civil da Internet).
SISTEMAS DE COMPUTAÇÃO: 1 Sistemas operacionais. 1.1 Linux (CentOS e Debian). 1.2 Windows Server (2008 R2 e 2012 R2). 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 ModSecurity. 5.3 SELinux. 5.4 Hardening. 6 SSL/TLS. 6.1 OpenSSL. 6.2 OpenVPN. 7 Information Lifecycle Management. 8 Computação na nuvem (Cloud Computing). 8.1 Segurança em Cloud Computing. 9 Tecnologias e arquiteturas de Data Center. 9.1 Tipos de Data Centers 9.2 Disciplinas e soluções: Elétrica, Climatização, Conectividade, Segurança, Combate a incêndio e Monitoramento. 9.3 Classificações TIER.

CARGO 34: AUDITOR DE CONTROLE EXTERNO - ÁREA: INFORMÁTICA- ESPECIALIDADE: ANALISTA DE SISTEMA

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 (ALM). 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 Microsoft Team Foundation Server 2010. 3 Qualidade de software. 3.1 Conceitos básicos. 3.2 Métricas de qualidade de software. 3.2 MPSBR. 3.2.1 Conceitos básicos e objetivos. 3.2.2 Processos. 3.2.3 Níveis de capacidade e maturidade. 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 Análise e projeto orientados a objetos: Conceitos básicos. 5.1 UML 2.2: visão geral, modelos e diagramas. 6 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. 1.2 Linguagens: .NET/C#, PHP, Flex, Ruby, Javascript, Java e Delphi. 1.3 Ambientes de programação: Visual Studio 2010, Eclipse. 1.4 Conhecimentos básicos de Java: servlets, Hibernate, JSP. 2 Desenvolvimento de sistemas web: HTML5, CSS3, WebSocket, Single Page Application (SPA), Javascript Frameworks (jQuery). 3 Programação avançada em .NET: LINQ, lambda, delegate, T4, WF, WCF, programação web, arquitetura de aplicação ASP.NET, controles de servidor, acesso a dados com ADO.NET e Entity Framework, web services, instalação e configuração de uma aplicação ASP.NET, conceitos de AJAX, desenvolvimento com ASP.NET AJAX. 4 Programação avançada em PHP 5 Orientado a Objetos: fundamentos da linguagem, arrays, funções, declarações, inicialização, escopo, estruturas de controle de fluxo, Namespaces, PHP Standard Library (SPL), PHP Data Objects (PDO), Frameworks PHP: Zend, Symfony. Segurança em Aplicação Web (Formulários, Password hashing, Data Filtering, Sanatization, Sessões e Cookies). 5 Desenvolvimento para Plataformas Móveis (Android, iOS, Windows Phone). 6 Análise estática de código fonte (Clean Code e ferramenta SonarQube). 7 Desenvolvimento orientado a testes (TDD). 7.1 Automação de testes com Selenium. 8 Segurança no desenvolvimento. 8.1 Práticas de programação segura e revisão de código. 8.2 Controles e testes de segurança para aplicações web e web services. 9 Arquitetura e tecnologias de sistemas de informação. 9.1 conceitos básicos; arquitetura cliente/servidor; arquitetura distribuída; especificação de metadados; 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. 9.2 Padrões XML, XSLT, UDDI, WSDL, SOAP e JSON/REST. 10 Sistemas de gestão de conteúdo; arquitetura de informação: conceitos básicos e aplicações; portais corporativos: conceitos básicos e aplicações, portlets, RSS; workflow; 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.
BANCO DE DADOS: 1 Algoritmos e Estruturas de dados. 1.1 Tipos básicos de estruturas de dados: listas lineares, pilhas, filas, árvores binárias, e grafos. 1.2 Operações básicas sobre estruturas de dados: inserção, retirada, percurso e busca. 1.3 Ordenação em estruturas de dados. 2 Teoria e Prática de Banco de Dados. 2.1 SGBD: conceitos, conceitos de administração de dados, arquitetura, independência de dados, SGBD relacionais. 2.2 Modelagem de dados: conceitos, modelo relacional, álgebra relacional, dependência funcional, formas normais, normalização, modelo de entidades e relacionamentos, diferentes representações gráficas do modelo ER. 2.3 SQL: linguagem de definição de dados (DDL), linguagem de manipulação de dados (DML), SQL ANSI, SQL para Oracle, SQL SERVER e MYSQL. 2.4 T-SQL (Transact/Structured Query Language) e PL/SQL (Procedure Language/Structured Query Language). 3 Business Intelligence. 3.1 Noções de Data Warehouse e Data Mining. 3.2 Ferramenta SAP Business Objects Enterprise Infoview 3.1. 3.3 Crystal Reports.

CARGO 35: AUDITOR DE CONTROLE EXTERNO - ÁREA: INFORMÁTICA- ESPECIALIDADE: ANALISTA DE SUPORTE

SEGURANÇA DA INFORMAÇÃO: 1 Normas de segurança da informação: ABNT NBR ISO/IEC 27001:2013 - sistemas de gestão da segurança da informação - requisitos; ABNT NBR ISO/IEC 27002:2013 - código de prática para controles de segurança da informação; ABNT NBR ISO/IEC 27005:2011 - gestão de riscos de segurança da informação; ABNT NBR ISO 31000:2009 - gestão de riscos - princípios e diretrizes; ABNT NBR ISO 22301:2013 - sistemas de gestão de continuidade de negócios - requisitos; ABNT NBR ISO 22313:2015 - sistemas de gestão de continuidade de negócios - orientações. 2 Políticas de segurança da informação. 3 Sistema de Gestão de Segurança da Informação. 4 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. 5 Segurança em redes: segmentação de redes, sistemas de firewall, firewall de aplicação web (WAF), detectores de intrusão (IDS e IPS), analisadores de tráfegos de rede (Sniffers), DMZ, proxies, Virtual Private Networks (IPSEC VPN, SSL VPN, client-to-site e site-to-site), defesa de perímetros, topologias de redes seguras. 6 Softwares maliciosos: conceitos e características de vírus, worm, cavalo de tróia, backdoor, keylogger, screenlogger, exploit, spyware, adware, ransomware, rootkit, bot.7 Segurança em redes wireless. 8 Segurança de servidores e estações de trabalho, configurações de segurança em servidores Linux e Windows, softwares de segurança. 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, MAN e WAN. 4 Tecnologia de roteamento - switches layer 3 e roteadores. 5 Administração de ativos de rede (switches, roteadores, concentradores). 6 Protocolos de roteamento RIP v.1 e v.2, OSPF e BGP. 7 Elementos de interconexão de redes de computadores (hubs, bridges, switches, roteadores, gateways). 8 Configuração, gerenciamento e segurança de redes de computadores Windows e Linux. 9 NAT. 10 Protocolos: TCP/IP, TCP, UDP, ICMP, HTTP, SMTP, POP, IMAP, DNS, DHCP, NIS, SSH,