NOÇÕES DE SEGURANÇA DA INFORMAÇÃO
LEGISLAÇÃO ESTADUAL
CAPACIDADE TÉCNICA - CONHECIMENTO ESPECÍFICO:
SEGURANÇA DA INFORMAÇÃO:
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.
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: PROCESSOS DE DEFINIÇÃO, IMPLANTAÇÃO E GESTÃO DE POLÍTICAS DE SEGURANÇA.
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.
GERÊNCIA DE RISCOS: AMEAÇA, VULNERABILIDADE E IMPACTO; PLANEJAMENTO, IDENTIFICAÇÃO, ANÁLISE E TRATAMENTO DE RISCOS DE SEGURANÇA; MELHORES PRÁTICAS DE GERENCIAMENTO DE RISCO.
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: 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.
SEGURANÇA DE APLICAÇÕES: SEGURANÇA EM BANCO DE DADOS; DESENVOLVIMENTO SEGURO DE SOFTWARE.
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.
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.
PROCEDIMENTOS DE RESPOSTA A INCIDENTES: TRATAMENTO DE INCIDENTES DE SEGURANÇA; ANÁLISE DE MALWARES; INVESTIGAÇÃO FORENSE; SELEÇÃO DAS TÉCNICAS APROPRIADAS PARA MITIGAÇÃO E RESPOSTA.
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.
SOFTWARES MALICIOSOS: CONCEITOS E CARACTERÍSTICAS DE VÍRUS, WORM, CAVALO DE TRÓIA, BACKDOOR, KEYLOGGER, SCREENLOGGER, EXPLOIT, SPYWARE, ADWARE, RANSOMWARE, ROOTKIT E BOT.
SEGURANÇA EM REDES WIRELESS.
SEGURANÇA DE SERVIDORES E ESTAÇÕES DE TRABALHO, CONFIGURAÇÕES DE SEGURANÇA EM SERVIDORES LINUX E WINDOWS, SOFTWARES DE SEGURANÇA.
SISTEMAS DE BACKUP: BOAS PRÁTICAS, TIPOS DE BACKUPS, PLANOS DE CONTINGÊNCIA E MEIOS DE ARMAZENAMENTO PARA BACKUPS.
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).
REGISTROS DE AUDITORIA: CONCEITOS, SERVIDOR DE LOG CENTRALIZADO, PROTOCOLOS SYSLOG E MICROSOFT EVENT VIEWER.
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - SISTEMA DE GERENCIAMENTO E CORRELAÇÃO DE EVENTOS RELACIONADOS À SEGURANÇA DA INFORMAÇÃO.
SEGURANÇA DE DADOS EM DISPOSITIVOS MÓVEIS.
CONTROLE DE ACESSO BASEADO EM PAPÉIS (ROLE BASED ACCESS CONTROL – RBAC).
PADRÕES DE INTEROPERABILIDADE DO GOVERNO BRASILEIRO (E-PING).
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.
LEI Nº 12.527/2011 (LAI – LEI DE ACESSO À INFORMAÇÃO).
LEI Nº 12.965/2014 (MARCO CIVIL DA INTERNET).
SISTEMAS DE COMPUTAÇÃO:
SISTEMAS OPERACIONAIS.
TIPOLOGIAS DE AMBIENTES COM ALTA DISPONIBILIDADE E ESCALABILIDADE.
MICROSOFT ACTIVE DIRECTORY E LDAP.
SHELLSCRIPT.
SEGURANÇA LINUX.
SSL/TLS.
INFORMATION LIFECYCLE MANAGEMENT.
COMPUTAÇÃO NA NUVEM (CLOUD COMPUTING).
TECNOLOGIAS E ARQUITETURAS DE DATA CENTER.
34.
CARREIRA: TÉCNICA ÁREA: INFORMÁTICA
CARGO EFETIVO: AUDITOR DE CONTROLE EXTERNO
ESPECIALIDADE: ANALISTA DE SISTEMA
CAPACIDADE TÉCNICA - CONHECIMENTO BÁSICO:
LÍNGUA PORTUGUESA
CONTROLE EXTERNO DA ADMINISTRAÇÃO PÚBLICA
LÍNGUA INGLESA
GOVERNANÇA E GESTÃO DE TI
AQUISIÇÕES DE BENS E SERVIÇOS DE TI
NOÇÕES DE SEGURANÇA DA INFORMAÇÃO
LEGISLAÇÃO ESTADUAL.
CAPACIDADE TÉCNICA - CONHECIMENTO ESPECÍFICO:
ENGENHARIA DE SOFTWARE:
ENGENHARIA DE REQUISITOS: CONCEITOS BÁSICOS, TÉCNICAS DE ELICITAÇÃO E ESPECIFICAÇÃO.
CICLO DE VIDA DO SOFTWARE (ALM).
QUALIDADE DE SOFTWARE.
MÉTRICAS E ESTIMATIVAS DE SOFTWARE.
ANÁLISE E PROJETO ORIENTADOS A OBJETOS: CONCEITOS BÁSICOS.
TESTES DE SOFTWARE: UNIDADE, INTEGRAÇÃO, SISTEMA, ACEITAÇÃO, REGRESSÃO, DESEMPENHO E CARGA.
DESENVOLVIMENTO DE SISTEMAS:
LINGUAGENS E FERRAMENTAS DE PROGRAMAÇÃO.
DESENVOLVIMENTO DE SISTEMAS WEB: HTML5, CSS3, WEBSOCKET, SINGLE PAGE APPLICATION (SPA), JAVASCRIPT FRAMEWORKS (JQUERY).
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.
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).
DESENVOLVIMENTO PARA PLATAFORMAS MÓVEIS (ANDROID, IOS, WINDOWS PHONE).
ANÁLISE ESTÁTICA DE CÓDIGO FONTE (CLEAN CODE E FERRAMENTA SONARQUBE).
DESENVOLVIMENTO ORIENTADO A TESTES (TDD).
SEGURANÇA NO DESENVOLVIMENTO.
ARQUITETURA E TECNOLOGIAS DE SISTEMAS DE INFORMAÇÃO.
BANCO DE DADOS:
ALGORITMOS E ESTRUTURAS DE DADOS.
TEORIA E PRÁTICA DE BANCO DE DADOS.
BUSINESS INTELLIGENCE.
35.
CARREIRA: TÉCNICA ÁREA: INFORMÁTICA
CARGO EFETIVO: AUDITOR DE CONTROLE EXTERNO
ESPECIALIDADE: ANALISTA DE SUPORTE
CAPACIDADE TÉCNICA - CONHECIMENTO BÁSICO:
LÍNGUA PORTUGUESA,
CONTROLE EXTERNO DA ADMINISTRAÇÃO PÚBLICA,
LÍNGUA INGLESA
GOVERNANÇA E GESTÃO DE TI
AQUISIÇÕES DE BENS E SERVIÇOS DE TI
NOÇÕES DE SEGURANÇA DA INFORMAÇÃO
LEGISLAÇÃO ESTADUAL
CAPACIDADE TÉCNICA - CONHECIMENTO ESPECÍFICO:
SEGURANÇA DA INFORMAÇÃO:
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;