PUC Minas Virtual
educação sem distância

Pós-Graduação a distância

Cibersegurança e governança de dados

DISCIPLINAS:

1) ESTRATÉGIA E GOVERNANÇA EM CIBERSEGURANÇA
2) PRIVACIDADE E PROTEÇÃO DE DADOS
3) LEI GERAL DE PROTEÇÃO DE DADOS
4) SEGURANÇA E GESTÃO DA IDENTIDADE DIGITAL
5) CRIPTOGRAFIA E SEGURANÇA DE APLICAÇÕES
6) CULTURA E PRÁTICAS DEVSECOPS
7) ETHICAL HACKING E GESTÃO DE VULNERABILIDADES
8) COMPUTAÇÃO FORENSE E PERÍCIA DIGITAL
9) GOVERNANÇA DE DADOS
10) GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO
11) SEGURANÇA DE INFRAESTRUTURA
12) SEGURANÇA EM CLOUD-COMPUTING
13) ANÁLISE E GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO
14) RESILIÊNCIA EM CIBERSEGURANÇA
15) ANALYTICS EM SEGURANÇA DA INFORMAÇÃO
16) HUMANIDADES

EMENTAS:

DISCIPLINA 1: ESTRATÉGIA E GOVERNANÇA EM CIBERSEGURANÇA

Princípios da Governança de Segurança da Informação. Governança Corporativa e a Governança de Segurança da Informação. Modelos de governança de segurança da informação. Políticas, procedimentos e controles de governança de Segurança da Informação. Políticas de Segurança da informação. Visão geral da família NBR ISSO/IEC 27000. Processos de auditoria. Tecnologias e

soluções para a proteção cibernética dos negócios. Estrutura e papéis em Cibersegurança. Programa de cultura e conscientização. Avaliação de Maturidade em Segurança da Informação. Security Awareness Maturity Model – SANS. NIST 800.50. Plano estratégico de Segurança da Informação.

DISCIPLINA 2: PRIVACIDADE E PROTEÇÃO DE DADOS

Conceito de dados e informação. Conceito de privacidade e proteção de dados. Direito à proteção de dados pessoais como direito fundamental. Visão geral sobre legislações de privacidade e proteção de dados. Marco civil da internet. Código de Defesa do Consumidor (CDC) e a relação com privacidade e proteção de dados. Direito penal no cenário digital. Convenção de Budapeste (convenção contra cibercrimes).

DISCIPLINA 3: LEI GERAL DE PROTEÇÃO DE DADOS

Fundamentos da Lei Geral de Proteção de Dados (LGPD). Tipos de dados. Princípios. Bases legais. Direitos dos titulares dos dados. Sanções administrativas e responsabilidades. Prestação de contas. Transferência internacional de dados. Agentes de tratamento. Incidentes de vazamento de dados e processo de comunicação com ANPD. Risco e Relatório de Impacto à Proteção de Dados Pessoais (RIPDP). Gestão dos consentimentos. Projeto de adequação e implantação de um Programa de Governança em Privacidade e Proteção de Dados.

DISCIPLINA 4: SEGURANÇA E GESTÃO DA IDENTIDADE DIGITAL

Conceitos fundamentais na gestão de identidade. Identificação e autenticação. Ciclo de vida de uma identidade. Tipos de controle de acesso. Tipos de biometria. Digital Adaptive Authentication. Segurança da identidade. Segurança Zero Trust. Principais metodologias (RBAC) e tecnologias para implementação de gestão de identidades e controle de acesso. Processos de gerência de identidades e de controle de acesso. Políticas de Gestão de Acesso de Identidade (IAM).

DISCIPLINA 5: CRIPTOGRAFIA E SEGURANÇA DE APLICAÇÕES

Conceito de Desenvolvimento Seguro. Fundamentos de criptografia. Breve histórico da criptografia clássica e moderna. Conceituação de sistemas simétricos e assimétricos. Principais algoritmos simétricos e assimétricos de ciframento (chave pública e privada) e Criptoanálise. Principais algoritmos para “hashing” e hashing criptográfico. Principais algoritmos para assinaturas digitais. Protocolos para autenticação em sistemas distribuídos. Protocolos SSL e TLS. Prática com o GnuPG (OpenPGP). Considerações de segurança para o Blockchain. Segurança em carteiras. Segurança em

aplicação: vulnerabilidades. Melhores práticas. Ferramentas de segurança e auditoria. Gerência de permissões de aplicações.

DISCIPLINA 6: CULTURA E PRÁTICAS DEVSECOPS

Segurança e desenvolvimento ágil. Principais conceitos DevOps e DevSecOps. SDLC (Secure Development Lifecycle). Implementação de end-to-end security. Pipeline DevSecOps. Melhores práticas DevSecOps. Verificação de segurança: (IAST – Interactive Application Security Testing), SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), RASP (Run-time Application Security Protection). Monitoração de recursos e ambientes. Security Observability.

DISCIPLINA 7: ETHICAL HACKING E GESTÃO DE VULNERABILIDADES

Cenário da cibercriminalidade. Diferença entre ameaça, ataque e fraude. Fraude pela perspectiva do crime cibernético. Principais ameaças e tipos de ataques. Offensive Security. Abordagens Pentest e Red Team. Metodologias, frameworks e tecnologias para processos de análise de vulnerabilidade, testes de segurança e de proteção. Processo de identificação e gestão de vulnerabilidades. Estratégia antifraude em cibersegurança.

DISCIPLINA 8: COMPUTAÇÃO FORENSE E PERÍCIA DIGITAL

Conceitos de computação forense. Cenários de perícia em informática. Evidências digitais. Tipos de exames periciais em Informática. Ferramentas para análise forense. Recuperação de dados e arquivos. Processo de perícia digital. Ata notarial, laudo pericial e parecer técnico. Padrões periciais. Antiforense digital.

DISCIPLINA 9: GOVERNANÇA DE DADOS

Contexto organizacional de dados. Conceitos de Governança de Dados – GD. Framework DMBoK. Políticas, padrões e procedimentos aplicados aos dados. Processo de implantação de GD. Modelos de maturidade de dados. GD aplicada em leis de proteção (LGPD-GDPR). GD 2.0: Ética nos dados, Agilidade em GD, Gerência de Mudanças. Aplicações dos conceitos de GD.

DISCIPLINA 10: GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Fundamentos da Lei Geral de Proteção de Dados (LGPD). Tipos de dados. Princípios. Bases legais. Direitos dos titulares dos dados. Sanções administrativas e responsabilidades. Prestação de contas. Transferência internacional de dados. Agentes de tratamento. Incidentes de vazamento de dados e processo de comunicação com ANPD. Risco e Relatório de Impacto à Proteção de Dados Pessoais

(RIPDP). Gestão dos consentimentos. Projeto de adequação e implantação de um Programa de Governança em Privacidade e Proteção de Dados.

DISCIPLINA 11: SEGURANÇA DE INFRAESTRUTURA

Soluções de segurança em infraestrutura e sistemas operacionais. Segurança em ambientes Unix/Linux e Windows. Soluções de segurança, alguns tipos de ataque e mecanismos de defesa (Firewalls, UTM, IDS, IPS). Práticas com PFSense ou UTM. Gestão de Log. Segurança de EndPoint. Projeto de arquitetura de infraestrutura segura. Tipos de Arquitetura e Tecnologias de Segurança. Funcionamento de centros de operação de cibersegurança (Security Operations Center – SOC). Aspectos relacionados às tecnologias e práticas utilizadas em processos de proteção de infraestruturas críticas.

DISCIPLINA 12: SEGURANÇA EM CLOUD-COMPUTING

Aspectos da Computação em Nuvem: conceitos, tipos, utilização e principais provedores de serviço.Security as a service (SECaaS) e os principais provedores SECaaS. Gerenciamento de mudanças na nuvem. Identity and Access Management (IAM). Aspectos de segurança em arquiteturas Cloud-computing: Segurança de aplicações, automação de segurança, detecção de Intrusão e análises de comportamento fora do padrão, ferramentas de monitoramento de segurança e auditoria. Governança e compliance dos provedores de nuvem. Resposta a Incidentes no contexto de produtos com arquitetura Cloud-computing. Plano de continuidade de negócio e estratégia de resiliência em Cloud-computing. Tendências, regulamentações e ferramentas de apoio em compliance para a nuvem.

DISCIPLINA 13: ANÁLISE E GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Conceito de risco. Tipos de riscos no contexto de segurança da informação. Processo de identificação, análise e identificação de ações de mitigação. Aspectos de análise de risco e segurança aos componentes críticos. Boas práticas na gestão de risco. Gestão de Riscos de Segurança da Informação: NBR ISSO/IEC 27005:2019. Metodologias para mensurar riscos. Avaliação de risco em privacidade e proteção de dados.

DISCIPLINA 14: RESILIÊNCIA EM CIBERSEGURANÇA

Conceito de resiliência e resiliência em Cibersegurança. Estratégia de resiliência em cibersegurança. Técnicas e frameworks para resiliência de cibersegurança. Práticas e padrões em Contingenciamento e Continuidade de Negócios: NIST 800-34, ISSO 22301. Protocolos e tecnologias para resiliência de cibersegurança. Governança, comunicação e gestão de equipes em resiliência de cibersegurança.

DISCIPLINA 15: ANALYTICS EM SEGURANÇA DA INFORMAÇÃO

Data driven e processos de analytics em Segurança da Informação. Análise, visualização e comunicação de dados. Ferramentas de Data Discovery e Self-Service Analytics. Indicadores de comprometimento (IoC). Definição e implementação de KPIs de segurança. Perspectivas do uso de IA e Machine Learning em Cibersegurança.

DISCIPLINA 16: HUMANIDADES

O ser humano, o processo de humanização e o conceito de pessoa. Desafios contemporâneos e o lugar da religião e da espiritualidade. Autonomia e heteronomia na sociedade atual. Princípios éticos e ética profissional.