Nome do Curso: CiberSegurança e Governança de Dados

- Justificativa: A Cyber Security (cibersegurança) é uma medida cada vez mais importante no mundo digital. Praticamente tudo o que movimenta a economia: desde o acesso individual à internet, até a nossa interação com todos os componentes de uma rede, tudo está fortemente integrado à necessidade da proteção de dados, prevenção de fraudes e outros riscos emergentes da inovação. Então, empresas de qualquer tipo de negócio requerem a aplicação prática em segurança da informação, pois as ameaças digitais em relação a ataques cibernéticos e à segurança de informação podem conferir, entre outros aspectos, a perda de confiança de seus clientes. Por isso, projetos de cibersegurança e de governança de dados e bem estruturados são importantes para todos os tipos de empresas e para os mais variados negócios. Diversos estudos e pesquisas evidenciam isso. Estudo da Anatel mostra que o Brasil sofreu cerca de 2,6 bilhões de ataques no primeiro semestre de 2019. A Comissão de Valores Mobiliários (CVM) diz que notificações referentes a ataques cibernéticos contra empresas brasileiras cresceram 220% no primeiro semestre de 2021 em comparação com o mesmo período de 2020. A Federação Nacional de Seguros Gerais (Fenseg) afirma que entre janeiro e agosto de 2020 houve um aumento de 63% na contratação de apólices de seguros relacionados à cibersegurança em relação ao mesmo período de 2019. Especificamente no Brasil, a Lei Geral de Proteção de Dados (LEI Nº 13.709), além da clareza sobre o tratamento de dados, traz desafios para diversas áreas como jurídica, tecnologia da informação, recursos humanos, marketing, saúde e outros. Sendo relevante ainda as discussões multidisciplinares. Por outro lado, o Gartner Group afirma que Governança de Dados e Cybersecurity Mesh estão entre as principais estratégias das organizações para os próximos cinco anos. Segundo relatório da MarketsandMarkets, o tamanho do mercado global de cibersegurança está projetado para crescer de US $ 217,9 bilhões em 2021 para US $ 345,4 bilhões em 2026. Esse crescimento pode ser atribuído à crescente conscientização e aos crescentes investimentos em infraestrutura de segurança cibernética em organizações dos mais variados tipos. Relatório do Consórcio Internacional de Certificação de Segurança de Sistema de Informação (ISC - Intelligence Service Center) mostra que existe um déficit de 4 milhões de profissionais no setor a nível mundial. Somente na América Latina, a demanda é de 600 mil especialistas. Esse cenário reforça a necessidade de profissionais capacitados em segurança cibernética e em gestão e segurança de dados, justificando, assim, o curso de Cibersegurança e Governança de Dados. O curso tem como objetivo capacitar profissionais com habilidades necessárias para assumir funções voltadas à governança corporativa aplicada a Cibersegurança, bem como proporcionar conhecimentos necessários para analisar riscos à privacidade e proteção de dados no tratamento de dados pessoais, bem como identificar o que é necessário para adequar tratamento de dados e processos à LGPD. Para isso, será discutido além do texto da lei e suas aplicações, riscos cibernéticos, governança de dados, estratégia e governança de segurança da informação. Matriz curricular atualizada para atender as necessidades do mercado, oferecendo uma formação focada na definição Cibersegurança e Governança de dados em tecnologias atuais; Conteúdos

apresentados por meio de casos reais, que colocam o aluno próximo de situações comuns no dia a dia de um usuário de dispositivo móvel; Tradição de ensino PUC Minas; Professores com muita experiência de mercado e com uma sólida formação acadêmica; Mentores experientes focados em orientar e motivar para otimizar o aprendizado; Abordagens inovadoras de ensino-aprendizagem em que as aulas e atividades pedagógicas são centradas nas necessidades dos alunos. Elas seguem dinâmicas orientadas por princípios de metodologias ativas; Experiência de aprendizado é suportada por ferramentas interativas - acessível via Web ou dispositivos móveis - incluindo salas virtuais, bate-papos e fóruns de discussão para estimular o aluno a um maior engajamento com o seu curso; Aprendizagem flexível em que o aluno planeja o próprio ritmo para alcançar seus objetivos pessoais;
- Objetivos: O curso tem como objetivos principal proporcionar conhecimentos e competências que permitam aos participantes ter uma visão multidisciplinar de segurança digital e a desenvolver, operar, manter e gerir soluções de Cibersegurança de modo a agregar valor aos negócios. Entender a importância da Cibersegurança e da Governança de dados no contexto corporativo e para os resultados do negócio; Ter ampla visão sobre os conceitos, protocolos, tecnologias e melhores práticas relacionadas à segurança de informação e dos processos que norteiam sua gestão na organização; Propor propostas de políticas para gestão de Cibersegurança e Governança de Dados alinhadas aos objetivos da organização; Usar técnicas, ferramentas e tecnologias para o garantir níveis de segurança da informação de acordo definições estratégicas da organização; Assumir posições de liderança voltada à governança corporativa aplicada a Segurança Cibernética, Riscos Tecnológicos e Legislação Digital em organizações; Gerenciar as expectativas dos stakeholders com base em uma estratégia de comunicação e de geração de valor; Identificar e discutir conceitos emergentes relacionados à Cibersegurança e Governança de Dados e verificar seus impactos no ambiente corporativo e em novos projetos. O especialista em Cibersegurança e Governança de dados poderá atuar como Analista de Cibersegurança nas mais diversas áreas que demandam segurança digital e em diversos papéis como: Analista de Segurança de Aplicações, Consultor de Segurança, Analista de Segurança de Informação, DevSecOps, Analista ou Coordenador de Governança de Dados, entre outros Além disso, ele poderá atuar nos mais diversos tipos de projetos inovadores em TI.
- Público Alvo: Profissionais com formação superior: Em Ciência da Computação, Engenharia de Computação, Engenharia de Software, Sistemas de Informação e tecnólogos da área de Tecnologia da Informação e outros cursos correlatos; Nas mais diversas áreas e que necessitam de competências emergentes para o desenvolvimento e gestão de projetos em Cibersegurança Governança de Dados; Com experiência Cibersegurança e Governança de Dados que queiram ampliar e aperfeiçoar seus conhecimentos; Que pretendam investir ou mudar de carreira ou que estejam em busca de novas habilidades, competências, soft skills e networking na área de Cibersegurança e Governança de Dados.

Disciplinas:

Disciplina 1: SEGURANÇA DE INFRAESTRUTURA

Ementa: 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 2: ETHICAL HACKING E GESTÃO DE VULNERABILIDADES

Ementa: 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 3: COMPUTAÇÃO FORENSE E PERÍCIA DIGITAL

Ementa: 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 4: SEGURANÇA E GESTÃO DA IDENTIDADE DIGITAL

Ementa: 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

Ementa: 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: PRIVACIDADE E PROTEÇÃO DE DADOS

Ementa: 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 7: LEI GERAL DE PROTEÇÃO DE DADOS

Ementa: 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 8: ESTRATÉGIA E GOVERNANÇA EM CIBERSEGURANÇA

Ementa: 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 9: GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E INFRAESTRUTURA

Ementa: Stakeholders. Tipos de riscos no contexto de segurança da informação e Infraestrutura. 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. Metodologias para mensurar riscos. Avaliação de risco em privacidade e proteção de dados. Abordagens regulatórias e políticas.

Disciplina 10: RESILIÊNCIA EM CIBERSEGURANÇA

Ementa: 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 11: SEGURANÇA EM CLOUD-COMPUTING

Ementa: 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 12: MONITORAMENTO E OBSERVABILIDADE

Ementa: Processo de tomada de decisão. Monitoramento x Observabilidade. Elementos, pilares e benefícios da observabilidade. Estratégias para medições e

monitoramento contínuo. Conexão do monitoramento e observabilidade com as estratégias de SLO e Error Budgeting. Principais ferramentas de monitoramento. Abordagem de instrumentação e monitoramento SRE. Application Performance Management (APM). Definição de Dashboard. Monitoramento de aplicações: definição e geração de alertas e relatórios de performance. Utilização de logs, métricas e tracing. Métricas e medição de maturidade para DevOps. OpenTelemetry.

Disciplina 13: GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Ementa: Incidentes em cibersegurança. Medidas técnicas e administrativas de prevenção e resposta a incidentes. Threat Intelligence como ferramenta de gestão. Ransomware: prevenção e resposta a incidentes. Processo de gestão de incidentes. Plano de gestão de incidentes. CSIRTs: estabelecimento e manutenção.

Disciplina 14: HUMANIDADES

Ementa: 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.

Disciplina 15: GOVERNANÇA DE DADOS

Ementa: Contexto organizacional de dados. Conceitos de Governança de Dados (GD). Framework DMBoK. Políticas, padrões e procedimentos aplicados aos dados: Data Stewardship, Data Owners, Dados Mestres, Dados Referência, Metadados, Data Catalog. Processo de implantação de GD. Modelos de maturidade de dados. GD aplicada em leis de Proteção (LGPD-GDPR). Compliance e Risk Assessment. GD 2.0: Ética nos dados, Agilidade em GD, Gerência de Mudanças.

Disciplina 16: CULTURA E PRÁTICAS DEVSECOPS

Ementa: 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.