Nome do Curso: Gestão de Cibersegurança e Risco

- 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 Gestão de Cibersegurança e Riscos. 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.
- Objetivos: Capacitar profissionais a fim de garantir que as iniciativas de Gestão de Cibersegurança e Riscos estejam alinhadas com as estratégias do negócio através do planejamento estratégico de TI, que os riscos sejam geridos adequadamente e que as organizações operem em conformidade com normas e regulamentações para agregar valor ao negócio. O curso permitirá aos profissionais: Entender a importância do

tema de gestão de Cibersegurança e Risco no contexto corporativo e para os resultados do negócio; Desenvolver e alinhar a estratégia de governança, gestão de risco e compliance de cibersegurança com as estratégias de negócios; Ter ampla visão sobre os conceitos, protocolos, tecnologias, melhores práticas e processos que norteiam sua gestão de cibersegurança na organização; Projetar e aplicar estruturas de governança e conformidade para proteger as empresas contra riscos e ameaças à segurança cibernética; Usar frameworks, técnicas, ferramentas e tecnologias de segurança cibernética para o garantir níveis de segurança da informação de acordo definições estratégicas da organização; Garantir a confidencialidade, integridade, disponibilidade e autenticidade, por meio da aplicação de princípios de segurança da informação; Contribuir para um plano de continuidade de negócios que priorize os processos de negócios; Promover a adesão e a conformidade às normas e legislações de cibersegurança e estruturas relacionadas visando garantir a disponibilidade segura e íntegra das soluções de TI; Gerenciar as expectativas dos stakeholders com base em uma estratégia de comunicação e de geração de valor; Assumir posições de liderança e gestão de equipes voltada à governança corporativa aplicada a riscos tecnológicos e legislação digital em organizações; Identificar, discutir e aplicar conceitos emergentes relacionados à riscos, conformidade com legislações de privacidade e proteção de dados, cibersegurança e governança de dados e verificar seus impactos no ambiente corporativo e em novos projetos.
- Público Alvo: Profissionais com diploma de nível superior em cursos de Tecnologia da Informação, Engenharias, Administração ou áreas afins, que ocupam ou que desejam ocupar posições de tomada de decisão em relação a TI com ênfase nas boas práticas gerenciais envolvendo: técnica, estratégia, liderança e negócios.

Disciplinas:

Disciplina 1: 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 2: 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 3: 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 4: 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 5: INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS

Ementa: Cyber Threat Intelligence. Análise de ameaças persistentes avançadas (APT). Reconhecimento de táticas, técnicas e procedimentos (TTPs) de atacantes. Estratégias e meios de coleta de informações. Inteligência para contra-ataque cibernético. Estratégia de Inteligência Cibernética Investigativa. Análise de ameaças em tempo real. Perfil de atores cibernéticos. Identificação de padrões de ataques. Ciclo de vida de Inteligência de Ameaças, Frameworks, Tecnologias e Ferramentas de Inteligência de Ameaças. Técnicas de Segurança Operacional - OpSec. Técnicas de Infiltração e de Contrainteligência. Tendências e Desafios em Inteligência de Ameaças Cibernéticas. Inteligência Artificial Aplicada à Segurança da Informação.

Disciplina 6: SEGURANÇA DEFENSIVA

Ementa: Programa de Segurança Defensivo. Princípios de design seguro e arquitetura de segurança. Identificação, análise, gestão e classificação de vulnerabilidades. Controles de Acesso e Autenticação. Proteção de Dados e Criptografia. Detecção e Prevenção de Intrusões. Monitoramento de sistemas para identificação de atividades suspeitas. Sistemas de detecção e prevenção de intrusões (IDS/IPS). Avaliação contínua de vulnerabilidades e correções. Patch management e atualização de sistemas. Melhores Práticas em Segurança Defensiva. Estratégias e táticas para fortalecer a segurança. Estrutura e gestão de Blue Team.Ð

Disciplina 7: SEGURANÇA OFENSIVA

Ementa: Estratégias, técnicas e ferramentas de ataques cibernéticos. Ataques OSINT (Open Source Intelligence) e Engenharia Social. Exploração de Redes e Sistemas. Engenharia Reversa. Metodologias de teste de invasão. OWASP ZAP. OWASP Top Ten. Ética e Responsabilidade. Ferramentas e técnicas de análise de vulnerabilidades. Programa de Segurança Ofensivo. Monitoramento e acompanhamento de um Programa de Segurança Ofensivo. Estrutura e gestão de Red Team.

Disciplina 8: COMPLIANCE E AUDITORIA

Ementa: Conceitos fundamentais de conformidade e auditoria em cibersegurança. Papel da conformidade regulatória e auditoria. Principais leis e regulamentações relacionadas à cibersegurança e outras normas. Planejamento, execução e documentação de auditorias e coleta de evidências de conformidade. Gestão de Incidências de Conformidade. Ações corretivas e planos de ação. Tendências e Desafios em Conformidade e Auditoria em Cibersegurança. Gestão de controles de

Segurança da Informação dentro de um programa de compliance.

Disciplina 9: GOVERNANÇA DE PRIVACIDADE E PROTEÇÃO DE DADOS

Ementa: Conceito de privacidade e proteção de dados. Visão geral sobre legislações de privacidade e proteção de dados. Fundamentos da Lei Geral de Proteção de Dados (LGPD). Direitos dos titulares dos dados. Sanções administrativas e responsabilidades. 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). Projeto de adequação e implantação de um Programa de Governança em Privacidade e Proteção de Dados.

Disciplina 10: ESTRATÉGIA E LIDERANÇA EM CIBERSEGURANÇA

Ementa: Fundamentos de Liderança. Soft Skills de Liderança. Visão estratégica da liderança e da gestão de equipes. Ferramentas e abordagens de liderança. Liderança e influência na cultura organizacional. Competências e soft-skills fundamentais no contexto da cibersegurança. Desenvolvimento de equipes e retenção de talentos. Papéis, responsabilidades e resultados em times ágeis. Estratégias para desenvolvimento individual. Construção de consciência sobre segurança cibernética e sobre estratégia de segurança cibernética. Organização e estrutura de um time dentro de um programa de cibersegurança. Avaliação e Métricas de Desempenho em Cibersegurança.

Disciplina 11: GESTÃO DE PROJETOS DE CIBERSEGURANÇA

Ementa: Conceitos fundamentais de gestão de projetos. Importância da gestão de projetos em cibersegurança. Ciclo de vida de projetos de cibersegurança. Definição de escopo de projetos de cibersegurança. Estabelecimento de objetivos e metas. Gerenciamento, monitoramento e controle de riscos e de recursos em projetos de cibersegurança. Controle de mudanças e resolução de problemas. Ferramentas e Técnicas de Gestão de Projetos. Security and Privacy by design.

Disciplina 12: GOVERNANÇA E CULTURA EM CIBERSEGURANÇA

Ementa: Princípios da Governança de Cibersegurança. Políticas, procedimentos e controles de governança de Cibersegurança. Políticas de Segurança da informação. Programa de cultura e conscientização. Avaliação de Maturidade em Cibersegurança. Estratégia de Cibersegurança e alinhamento com o Planejamento Estratégico Corporativo. GRC e sua contextualização em Cibersegurança.

Disciplina 13: 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 14: 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.

Disciplina 15: 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.