Especialização em Gestão de Cibersegurança e Riscos

OFERTA 1, TURMA 1, MODALIDADE Assíncrono

EMENTÁRIO DAS DISCIPLINAS

Compliance e Auditoria
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.

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.

Estratégia e Liderança em Cibersegurança
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.

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.

Gestão de Projetos de Cibersegurança
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.

Gestão de Riscos de Segurança da Informação e infraestrutura
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.

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.

Governança de Privacidade e Proteção de Dados
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.

Governança e Cultura em Cibersegurança
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.

Inteligência de Ameaças Cibernéticas
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.

Monitoramento e Observabilidade
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.

Resiliência em Cibersegurança
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.

Segurança Defensiva
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.

Segurança em Cloud-Computing

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.

Segurança Ofensiva

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.