PÓS-GRADUAÇÃO

GESTÃO DE CIBERSEGURANÇA E RISCOS TECNOLÓGICOS

INSCRIÇÕES ABERTAS

Carga horária: 360 Horas

Coordenação: Prof. Dr. Nicolau Reinhard

Coordenação Adjunta: Prof. Edson Germano

*As informações podem sofrer alterações sem aviso prévio.

FUNDAÇÃO INSTITUTO DE ADMINISTRAÇÃO
BUSINESS SCHOOL

proinfo

A Internet quebrou barreiras entre países e cidadãos, permitindo o compartilhamento de informações em todo o mundo. Hoje as redes e os sistemas de informação sustentam os serviços, que apoiam o funcionamento da nossa sociedade e economia. A Segurança Cibernética (no termo inglês *Cyber Security*) está se tornando cada vez mais uma prioridade fundamental à luz do papel crucial desempenhado pela informação e comunicação no desenvolvimento econômico e social. O setor de energia e os serviços oferecidos por este são um excelente exemplo da necessidade da resiliência e segurança cibernética, ao lado de outros setores, como telecomunicações, finanças, transportes, saúde, varejo e setor público. Atualmente, muitas empresas no Brasil e no mundo, passaram a se preocupar com a Segurança Cibernética em seus negócios. Porém, os investimentos necessários e as práticas de governança, prevenção e respostas a incidentes são pouco disseminadas entre o *middle management* e os executivos *C-level* das organizações. Neste contexto, o objetivo deste curso de Pós-Graduação é suprir no mercado brasileiro a demanda por capacitação técnica, gerencial e estratégica, destinada a desenvolver competências relevantes aos profissionais que atuam ou desejam atuar na gestão de áreas de Segurança Cibernética, Proteção dos Ativos (físicos e digitais) e na Privacidade de Dados das empresas.

OBJETIVO

O curso tem como foco a capacitação de profissionais que atuam ou desejam preparar-se para atua à frente de operações de segurança cibernética, segurança de TI e na proteção dos dados em organizações públicas ou privadas, membros de ISACs (Centros de compartilhamento de informações e análise) ou CSIRTs (Equipes de Segurança de Computadores e de Resposta a Incidentes). Ao aluno serão apresentados conceitos, técnicas, ferramentas e práticas adotadas na prevenção e resposta a incidentes de segurança cibernética. Entre as competências a serem desenvolvidas pelo aluno estão:

- Atuar na construção de planos e estruturas de resposta a incidentes e na proteção de dados e informações;
- Conhecer e simular práticas existentes de resposta a incidentes;
- Construir uma política e cultura de confiança contínua para segurança física e cibernética nas organizações;
- Atuar em situações de ataques cibernéticos, gerenciar situações de crises e a comunicação adequada com os atores externos e internos;
- Desenvolver competências para Liderança e Gestão de Equipes.

PERFIL DO ALUNO

O curso é destinado para profissionais analistas e gestores de tecnologia, de negócios, de auditoria, consultores, empreendedores, advogados e gestores de projetos de soluções de segurança cibernética que buscam conhecer e aprofundar-se nas técnicas e ferramentas para gestão de riscos tecnológicos, proteção e privacidade de dados e na prevenção e respostas a incidentes cibernéticos. Destinado a profissionais de setores considerados críticos na segurança cibernética como: Energia, Telecomunicações, Finanças, Saúde, Varejo, Transporte e Governo, mas não limitado a esses setores.

DIFERENCIAL

O curso desenvolverá no participante competências relevantes para a função gerencial e executiva em segurança cibernética e gestão de riscos tecnológicos nas organizações, alinhando conhecimentos técnicos, gerenciais e estratégicos. Temas como gestão de equipes, liderança, gestão de riscos, gestão de projetos e processos, ferramentas, tecnologias e práticas, alinhados com a aplicação em Cibersegurança, essenciais para que o aluno desenvolva competências relevantes para o profissional da área de Segurança Cibernética, Proteção de Dados e Gestão de Riscos Tecnológicos, capacitando-o para ocupar a função de *Chief Security Information Officer*. (CISO).

METODOLOGIA

A metodologia do curso enfatiza a combinação de teoria e troca de experiências, usando aulas expositivas, métodos participativos, simulações e trabalhos em equipe, adequados aos diferentes temas do curso. Os conhecimentos e experiências dos docentes, aliados à vivência dos alunos em diferentes seguimentos empresariais, permitem maximizar as oportunidades de troca de conhecimentos e experiências e a criação de redes de relacionamento de grande valor para todos os participantes.

CORPO DOCENTE

O corpo docente é composto por professores com nível de Mestrado e Doutorado da Fundação Instituto de Administração, professores titulados de outras instituições, por profissionais e palestrantes de grande capacidade na área de Gestão de Cibersegurança, Segurança da Informação, Proteção e Privacidade de Dados e Gestão de Negócios de Tecnologia. Todos os docentes do curso mantêm atividade alinhada as áreas de sua atuação no curso, o que lhes confere ao lado do conhecimento técnico, o realismo decorrente da vivência profissional.

CONTEÚDO PROGRAMÁTICO

INTRODUÇÃO À SEGURANÇA CIBERNÉTICA E SEGURANÇA DE INFORMAÇÕES

- Gestão da Segurança da Informação
- Segurança Digital
- Introdução a Segurança Cibernética
- Riscos Corporativos
- Processo Organizacional de Segurança da Informação
- Processo Corporativo de Segurança da Informação
- Segurança de Sistemas de Informação
- Fraudes e Crimes digitais
- Técnicas de Segurança e controle de informação
- Normas NBR ISO/IEC
- Palestras e eventos direcionados ao tema

GOVERNANÇA DE SEGURANÇA CORPORATIVA

- Cybersecurity Frameworks
- Processo Corporativo de Segurança da Informação
- Arquitetura da Política de Segurança da Informação
- Acesso a Informação
- Classificação da Informação e Controles de Acesso
- Cópias de Segurança
- Conscientização e Políticas de Treinamento
- Estratégias de governança
- Gerenciamento de risco de segurança da informação
- Gerenciamento de risco cibernético
- Métricas de Segurança
- Sarbanes-Oxley
- Governança de Dados

ESTRUTURAS E OPERAÇÕES DE SEGURANÇA

- Arquiteturas de hardware para segurança
- Segurança do sistema operacional
- Segurança de rede e design de protocolo
- Linguagens de Programação Seguras
- Verificação de Sistemas
- Criptografia e Chaves públicas
- Computação multipartidária, compartilhamento de sigilo e confiança distribuída
- Criptografia Funcional e Homo mórfica
- Perspectivas para Políticas Cibernéticas

GESTÃO DE CRISES E ESTRATÉGIAS DE COMUNICAÇÃO

- Práticas de Governança de Segurança
- Comunicação efetiva e demonstração de valor
- Medidas e métricas de segurança
- Valores, Objetivos e Métricas de Sucesso
- Avaliação do Risco de Crises
- Definição de Funções e Papéis
- Desenvolvimento de respostas provisórias
- Elaboração do Plano de Resposta
- Guerra cibernética
- Métodos de identificação de ameaças e geração de alertas
- Riscos Tecnológicos Emergentes

ESTRATÉGIA E LIDERANÇA EM CIBERSEGURANÇA

- Estratégia e Inovação em Segurança de Negócios Digitais;
- Cibersegurança em uma perspectiva global;
- O papel do Chief Information Security Officer nas organizações
- Construção de um programa integrado de gestão de riscos digitais
- Princípios de Prevenção à Fraude e Integração à Segurança Cibernética;
- Planejamento e Liderança de equipes de alta performance;
- Decisões em situações complexas e em condições de incertezas
- Negociando sob pressão;

- Finanças e Contabilidade em Projetos e Investimentos de segurança;
- Os desafios do empreendedorismo em Cyber Security no Brasil
- Empreendedorismo em Cibersegurança no Brasil

INTELIGÊNCIA ARTIFICIAL APLICADA A SEGURANÇA DA INFORMAÇÃO

- Domínio das políticas de Gestão de Acesso de Identidade (IAM) e inteligência
- Gestão de acessos e prevenção contra fraudes
- Pontos fortes e limitações de tecnologias de segurança passadas, presentes e perspectivas para o futuro
- Práticas modernas de segurança para ativos empresariais
- Bigdata, segurança e monitoramento preventivo
- Soluções de segurança com inteligência artificial e machine learning
- Modelos de Modelos de Negócios e Serviços para AI
- War Games
- Smart Grid Cyber Security
- Uso de Inteligência Artificial (IA) e Machine Learning em ambientes de Tecnologia da Informação (TI) e Tecnologia Operacional (TO)
- Uso da IA na Cibersegurança para proteção de informações sensíveis e na identificação automática de vulnerabilidades
- Cyber Threat Intelligence, Cyber Security Analytics e Governança de Dados

ÉTICA E ASPECTOS JURÍDICOS EM CIBERSEGURANÇA

- Lei de Segurança da Informação
- Estruturação de programas de Segurança Organizacional
- Cibersegurança e Governança Corporativa
- Direito Digital aplicado a Cibersegurança
- Contratos e Auto-Regulamentação
- Legislação e Práticas para Privacidade e Proteção de Dados
- Regulação de Cibersegurança no mundo
- Patentes e Propriedade Intelectual
- Questões éticas no monitoramento e controle de privacidade
- Ética Profissional
- Leis e Educação Digital

GERENCIAMENTO ESTRATÉGICO DE RISCOS E AMEAÇAS

- Gestão do Risco Cibernético
- Ameaças digitais e físicas
- Avaliação de Riscos
- Efetividade e Controle
- Critérios de Impacto
- Plano de Ação para Segurança Cibernética
- Plano de continuidade da Operação/Negócio
- Arquiteturas flexíveis de segurança
- Fatores externos e Gerenciamento de Risco da Cadeia de Valor
- Ameaças para cadeias de suprimentos cyber-dependentes
- Limitações do “risco de terceirização” e SLA
- Construção e gerenciamento de cadeias de valor resilientes

- Gestão de Resposta de incidentes
- Desenvolvimento de equipe para CSIRT
- Métricas de capacidade de gerenciamento de incidentes
- Plano de ação efetivo para a educação, resposta e defesa contra ataques humanos
- BYoD

RESILIÊNCIA CIBER OPERACIONAL

- Conceitos básicos de gerenciamento de operacional
- Papel da gestão de riscos no gerenciamento de resiliência operacional
- Aproveitamento de padrões, diretrizes e práticas líderes
- Capacidades de gerenciamento de resiliência operacional
- Comunicações, governança, métricas e engajamento
- Estratégias nacionais e internacionais para gerenciar riscos operacionais e segurança cibernética
- Melhores práticas e tecnologias para monitoramento da segurança e resposta
- Gestão de acessos e prevenção contra fraudes
- Proteção contra ataques DDoS
- Proteção de dados críticos
- Gerenciamento de Ameaças Operacionais
- Situações adversas
- Estratégias para a Segurança das Infraestruturas Críticas de Energia e Telecomunicações no Brasil

TECNOLOGIAS E PRÁTICAS EM CIBERSEGURANÇA

- Segurança móvel nos negócios digitais
- IoT, redes, endpoints e desafios de segurança
- Segurança e os novos modelo de Desenvolvimento de Sistemas - Agile, DevOps
- Análise de confiança e comportamento digital
- Cloud Computing: segurança como fundamento para a adoção de serviços de nuvem em alta escala
- Identidade e Privacidade Digital
- OpenBanking e Gateways de API
- Tecnologias em Cibersegurança
- Computação social e colaborativa - Redes sociais, aplicativos móveis e tecnologias da nuvem estão invadindo a força de trabalho
- Threat Intelligence como ferramenta de Gestão
- Próxima Geração de Trabalhadores Digitais - Geração Z
- Aplicações do Blockchain em Cibersegurança
- Guerra Cibernética
- Cyber-armas
- Desafios e tendências para segurança e defesa cibernética nas Utilities Energéticas

MÓDULO – TRABALHO DE CONCLUSÃO DO CURSO

- Metodologia para o Desenvolvimento de Projeto de Aplicação

FUNDAÇÃO INSTITUTO DE ADMINISTRAÇÃO
BUSINESS SCHOOL


@businessschool.fia


faculdadeFIA


/company/FIA


FIABusinessSchool

fia.com.br/blog

Fale conosco:
e-mail: proinfociber@fia.com.br
telefone: (11) 3732-3505
whatsapp: (11) 94307-3353

FUNDAÇÃO INSTITUTO DE ADMINISTRAÇÃO
Avenida Doutora Ruth Cardoso, 7.221 – CEP 05425-070 – Pinheiros – São Paulo/SP
Informações: Tel: (11) 3732-3535 | www.fia.com.br