CIBERSEGURANÇA
E PROTEÇÃO DIGITAL
DE NEGÓCIOS

PÓS-GRADUAÇÃO

CIBER-SEGURANÇA

Sumário

Ciber-Segurança

Por que

A FIA?

FIA: desde 1980 formando executivos de sucesso no Brasil e exterior.

A FIA -Fundação Instituto de Administração foi fundada há 40 anos por professores do Departamento de Administração da USP.

É formada por profissionais conceituados do mercado: professores, gestores, consultores e líderes de grandes empresas. Isso permite que nossos alunos **ampliem** seus olhares, com a melhor convergência entre a teoria e aprática.

+ de

40.000

alunos formados na Pós-Graduação e MBA

A FIA é credenciada pela Portaria MEC nº 750, de 26/05/2000 e publicada noDiário Oficial da União, Seção I, de30/05/2000.

Educação
Ministério da Educação

O EAD da FIA é credenciado em conformidade com o art. 16, do Decreto nº 9,57. de 25 de maio de 2017 e art. 12, da Portaria Normativa MEC nº 11 de 21 de junho de 2017.

Uma das instituições mais bem avaliadas em rankings nacionais e internacionais de educação.

FT FINANCIAL TIMES

25º melhor EMBA das Américas
6º quadro de alunos mais experiente do mundo

EUROPEANCEO

Escola **mais inovadora** da América do Sul

Diversos MBA apontados entre os **melhores do país**

Excelência para oferecer as melhores oportunidades de formação aos alunos

Os cursos da FIA seguem rigorosos padrões de excelência didática e programáticae são credenciados por importantes instituições nacionais e internacionais, garantindo aos alunos valor à certificação obtida e, aos empregadores, a certeza de que seus colaboradores possuem formação de padrão internacional.

Acreditações, filiações e Convênios da FIA

Executive MBA Council

Project Management Institute

Association AMBA Accredited

ANAMBA Instituição Associada

AACSB Business Education Alliance Member

ipmabr IPMA

PRME Principles for Responsible Management Education

Harvard Business Publishing

EFMD Global Network

eduniversal 3 Palmes

Educação, Consultoria

E PESQUISA

Você sabia que a FIA é responsável por desenvolver os principais conhecimentos na área de Administração? Com os melhores parceiros e aliando consultoria e pesquisa, mantemos um corpo docente extremamente atualizado, realizando projetos e estudos relevantes para as organizações em todo o Brasil.

São alguns dos projetos e pesquisas desenvolvidas pela FIA:

Nos dedicamos ao estudo e geração de novos conhecimentos para compreensão do ambiente de negócios e oferecer suporte às organizações.

Já realizamos mais de 8.000 projetos de consultoria nas iniciativas pública e privada, desenvolvendo metodologia própria, de forma lógica e transparente, para promover aprimoramento da gestão e planejamento e ações estratégicas e operacionais.

Algumas das áreas de atuação da FIA:

- Análise de Dados e Big Data
- Indústria 4.0
- Desenvolvimento e Modernização Organizacional
- Gestão de Projetos
- Gestão Socioambiental
- Gestão Estratégica de Pessoas
- Marketing
- Gestão Pública e PPP
- Pequenas e Médias Empresas
- Agronegócio
- Inovação e Empreendedorismo
- Redesenho de Processos
- Comércio Internacional
- Tecnologia da Informação
- Estudos do Futuro

5 razões para investir na sua carreira

01 Preparação para o mercado de trabalho em transformação

02 Aumento de possibilidades por meio da educação

03 Crescimento da rede de contatos.

04 Aumento de possibilidades perante o mercado

05 Assumir o protagonismo em sua carreira.

Você entre os líderes do seu mercado

A FIA tem colaborado na formação de pessoas e profissionais se empenhando na excelência de um corpo docente dedicado e atualizado, com técnicas modernas e criadores de novos paradigmas de uma sociedade moderna e conectada.Os programas unem pessoas, estratégias, métodos, práticas e inovação, oferecendo condições de desenvolvimento tanto aos jovens executivos como também aos profissionais que buscam, em nossos cursos, os conhecimentos que o mundo globalizado e conectado demanda para um crescimento em empresas ou no desenvolvimento de seu próprio negócio.

Por que fazer uma **PÓS-GRADUAÇÃO AGORA?**

A opção de se formar em uma faculdade e parar de estudar já não existe. Você fica obsoleto no mercado de trabalho em muito pouco tempo. Segundo o Fórum Econômico Mundial, cerca de

1/3 das competências ficam obsoletas em menos de 5 anos.

Em mercados mais digitalizados, como o mercado financeiro, comércio eletrônico ou tecnologia, este percentual pode ser até maior.

Aprender continuamente é essencial para se adaptar às constantes mudanças no trabalho nesta nova década.

Continuar sua formação com um curso de pós-graduação ou MBA é uma forma segura de manter-se atualizado no mercado de trabalho. Garante que você está se preparando para evoluir numa carreira. Certifica que você está investindo na sua vida profissional.

Financeiramente também é um investimento que traz retorno. Segundo a OECD, se no Brasil uma pessoa formada com

nível superior ganha cerca de 2,3x mais que uma apenas com ensino médio, se você tem uma pós-graduação ou MBA esta diferença sobe para 4,49x.

Ou seja, fazer uma pós ou MBA é um investimento que retorna para o indivíduo na forma de maiores salários.

Uma pós-graduação *latu senso* é um curso direcionado ao desenvolvimento e especialização de competências profissionais. Já um MBA – Master in Business Administration - foca nas competências para gestão de negócios, muito valorizadas em cargos mais altos nas empresas.

Por que estudar na

FIA ONLINE?

DEPOIMENTOS

“A FIA te dá uma gama de desafios que você conseguirá aplicar no dia a dia, na prática.”

“É uma escola de muita credibilidade no Brasil inteiro e isso me fez ter segurança para buscar o conhecimento na FIA”

“O que me fez optar pela FIA foi unir uma instituição com bastante tradição no mercado e eu sabia que isso seria bastante considerado pelas empresas.”

Algumas das conveniências de fazer nossos cursos de pós-graduação e MBA 100% online.

01

Discussão e troca de experiências com profissionais que lideram o mercado;

02

Inovação com a nossa metodologia 100% online que respeita sua disponibilidade;

03

Certificado respeitado pelos maiores gestores e especialistas do mercado

A presença da FIA no dia a dia das grandes organizações, por meio de nossos professores e especialistas convidados, fornece a nosso corpo docente expertise para levar aos nossos cursos casos reais sobre o mundo dos negócios.

Como funciona na prática
ESTUDAR NA FIA ONLINE?

A metodologia de estudo utilizada nos cursos da FIA Online é fundamentada no protagonismo do aluno, e na conveniência do estudo às necessidades de cada indivíduo. O formato das videoaulas, dos materiais de estudo, dos podcasts, das avaliações, das aulas ao vivo, dos grupos de discussão, tudo é pensado para oferecer praticidade ao aluno, e para transmitir a experiência da sala de aula da FIA no ambiente digital, com alta qualidade.

A cada mês (ou quinzena, dependendo do curso), você recebe uma mensagem informando que sua disciplina já está disponível na plataforma da FIA ONLINE.
Ao acessar, o aluno pode assistir as **Videoaulas** daquela disciplina, gravadas dentro das aulas reais da FIA com grandes professores, e editadas para que sejam objetivas e que todo o conteúdo fique bem explicado.
Além das videoaulas, toda disciplina possui um **Guia da Disciplina**, para ajudar a estudar aqueles conteúdos, um **Livro Digital**, que além de condensar os conteúdos também amplia o acesso a bibliografias recomendadas, a **Apresentação do Professor**, quando ele utilizar algum material audiovisual durante a aula, o conteúdo da videoaula em formato de **Podcast**, **Cases de mercado**, para conectar conteúdo acadêmico com aplicação prática no mercado. Além disso, toda disciplina possui uma **Aula ao Vivo** com o professor, onde os alunos podem interagir e onde o professor conecta o conteúdo com o contexto atual. Também, durante toda a experiência o aluno tem acesso a um **Grupo no Whatsapp** exclusivo de sua turma, e pode se conectar com pessoas em todo o país, tirar dúvidas, e compartilhar conhecimentos. E, ao final de cada disciplina, o aluno faz uma avaliação de conhecimento.

Composição **DA DISCIPLINA**

VIDEOAULAS

APRESENTAÇÃO DO PROFESSOR

CONEXÃO COM O MERCADO

LIVRO DIGITAL

PODCAST

WEBINAR MENSAL

GUIA DO CURSO EM PDF

CASES

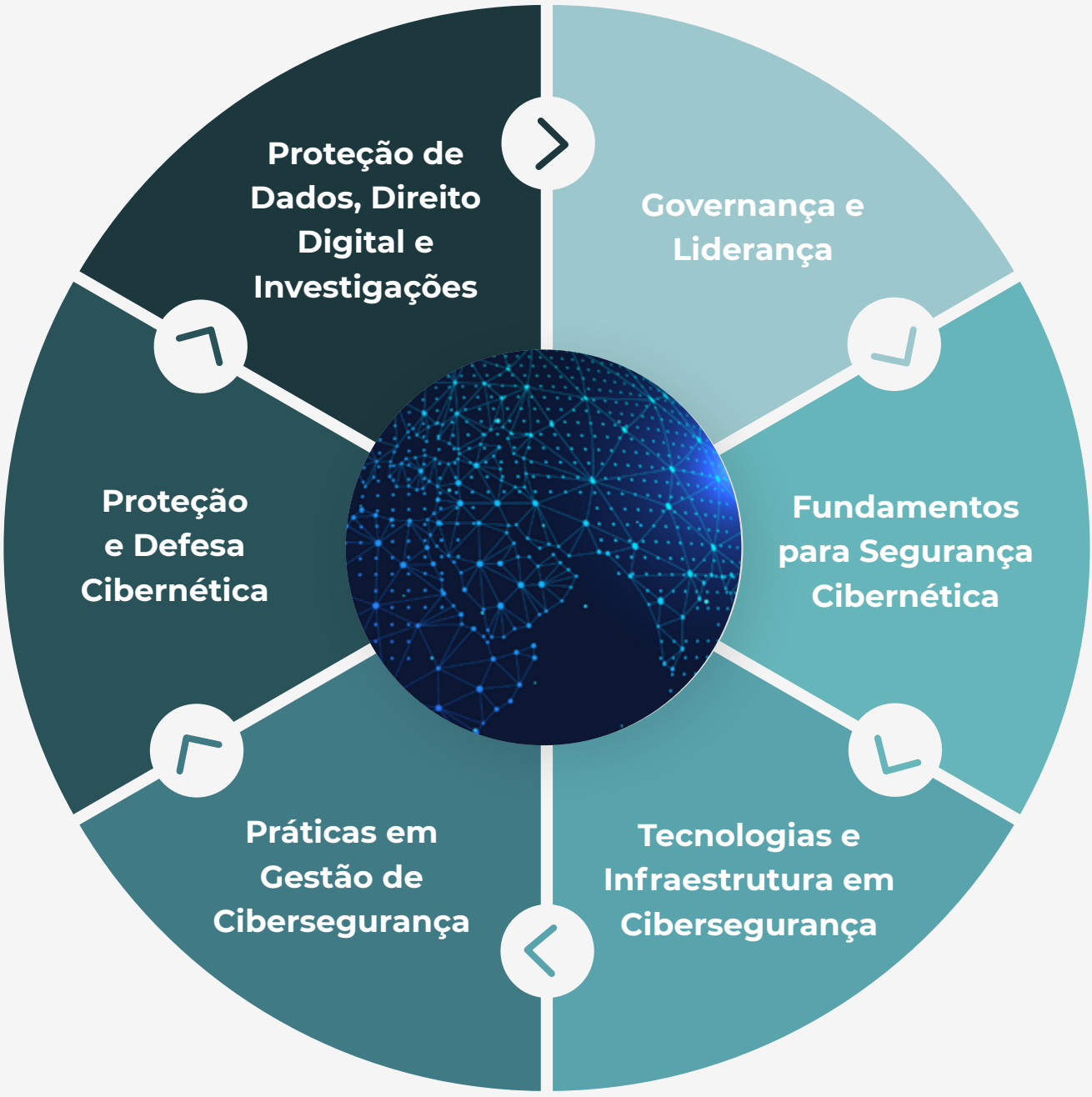
WHATSAPP DO PROFESSOR

Portanto, cada aluno pode se organizar para estudar da melhor forma para suas necessidades. Alguns alunos estudam um pouco a cada dia, outros estudam no final de semana, ou estudam após o trabalho, ou aproveitam o tempo no trânsito ou nos horários de almoço. É você quem organiza seu tempo.

A cada período (mensal ou quinzenal) uma nova disciplina é disponibilizada. As pós-graduações são disponibilizadas num período de 12 meses, e os MBAs em 15 meses. Ou seja, em um ano e meio você se forma numa pós-graduação ou MBA de ponta, estudando de qualquer lugar do país, de acordo com sua própria agenda.

COMO SERÁ O MEU CURSO?

Matriz curricular por eixo temático



Carga Horária Total do curso. **PÓS: 360h**

Carta da PRESIDÊNCIA

É um prazer receber você aqui na FIA Online. Quando criamos a FIA, em 1980, nosso objetivo era desenvolver o conhecimento em Administração e disseminar as melhores práticas do setor. Hoje, com a internet fixa e móvel, a evolução da tecnologia e da educação digital, nada mais natural que trazer esse conhecimento também ao mundo online. Um formato adequado à vida moderna, mais prático, porém mantendo a qualidade e o rigor que nos levaram a atingir a pontuação máxima nos mais importantes rankings de ensino. Será um prazer contar com você entre os nossos alunos.

Isak Kruglianskas
Presidente da FIA

É com imensa satisfação que lançamos o FIA Online. A FIA carrega consigo, nesses 40 anos, a referência como escola de negócios que forma profissionais e gestores que lideram as empresas brasileiras. Vivemos um período extraordinário, de transformação digital, intensa competição e novas tecnologias. É fundamental preparar-se para essa realidade, adquirir novas competências e liderar negócios inovadores. Os participantes terão uma nova experiência de ensino, ao acessar os cursos em qualquer lugar, a qualquer hora, no seu espaço, de acordo com suas necessidades: um ensino de alto nível, propiciado por docentes altamente reconhecidos pela academia e pelo mercado.
Seja bem-vindo a esse novo mundo! Juntos construiremos a nova educação do século XXI!

Maurício Jucá de Queiroz
Diretor da Faculdade FIA

Linha de frente:
COORDENAÇÃO

Prof. Dr. Nicolau Reinhard
COORDENADOR

Para Pós

12 MESES + 3 meses para o Projeto Final*

* O Projeto Final, a depender do curso, poderá ser desenvolvido ao longo do curso, sem os 3 meses adicionais.

Disciplinas
DO CURSO

01 GOVERNANÇA E LIDERANÇA

Eixo temático

Carga Horária Total do Eixo - **60h**

Disciplina
Liderança, Gestão de Pessoas e Soft-skills
Práticas de Gestão de Projetos para Cibersegurança
Governança Corporativa Aplicada a Segurança
Estratégias de Comunicação e Gestão de Crises
Estratégias de Comunicação e Gestão de Crises
Liderança, Gestão de Pessoas e Soft-skills

02

FUNDAMENTOS PARA SEGURANÇA CIBERNÉTICA

Eixo temático

Carga Horária Total do Eixo - **90h**

Disciplina
Fundamentos da Internet e Princípios de Cibersegurança (Disciplina Optativa)
Princípios de Prevenção à Fraudes e Crimes Cibernéticos
Gerenciamento e Avaliação de Riscos em Negócios
Treinamento, educação e conscientização para Cibersegurança
Fundamentos da Internet e Princípios de Cibersegurança

DISCIPLINAS DO CURSO

03

Eixo temático

TECNOLOGIAS E INFRAESTRUTURA EM CIBERSEGURANÇA

Carga Horária Total do Eixo - **75h**

Disciplina
Tecnologias de Cibersegurança
Segurança em Cloud-computing
Aplicação de Biometria em Segurança
Segurança e Gestão da Identidade Digital
Aplicações de Inteligência Artificial em Cibersegurança
Tecnologias de Cibersegurança

04

Eixo temático

PRÁTICAS EM GESTÃO DE CIBERSEGURANÇA

Carga Horária Total do Eixo - **60h**

Disciplina
Monitoramento da Internet e Inteligência em Cibersegurança
Testes de Segurança e Conceitos
Cultura Ágil, Desenvolvimento e Automação da Segurança
Políticas e Planejamento Estratégico de Cibersegurança
Monitoramento da Internet e Inteligência em Cibersegurança

DISCIPLINAS DO CURSO

05

Eixo temático

PROTEÇÃO E DEFESA CIBERNÉTICA

Carga Horária Total do Eixo - **60h**

Disciplina
Ameaças, Ataques e Gerenciamento de Vulnerabilidades
Infraestrutura para Defesa Cibernética
Centros de Resposta à Incidentes
Resiliência em Cibersegurança
Ameaças, Ataques e Gerenciamento de Vulnerabilidades
Infraestrutura para Defesa Cibernética

06

Eixo temático

PROTEÇÃO DE DADOS, DIREITO DIGITAL E INVESTIGAÇÕES

Carga Horária Total do Eixo - **60h**

Disciplina
Proteção de Dados, Privacidade e Regulamentações
Práticas de Proteção de Dados e Atribuições do DPO
Direito Digital e Crimes Eletrônicos
Princípios de Investigação Cibernética e Forense Digital
Proteção de Dados, Privacidade e Regulamentações

Liderança, Gestão de Pessoas e Soft-skills

Carga Horária: **15h**

Ementa

A disciplina apresentada uma visão estratégica da liderança e da gestão de pessoas no contexto dos negócios digitais e da sociedade hiperconectada. O sucesso para equipes de alto desempenho na empresa exponencial e nos negócios digitais é resultado de uma liderança e gestão de pessoas alinhadas com a estratégia organizacional e com os diferentes perfis e expectativas pessoais dos profissionais. A disciplina desenvolve também competências soft-skills fundamentais para o mercado de trabalho da nova década.

Conteúdo Programático

- Importância da Liderança
- Características e Competências do Líder
- Estilos de Liderança
- Liderança Positiva – Criando um ambiente positivo
- Autoconhecimento e estilos de personalidade
- Estilos de atuação, estilos de personalidade e liderança para empresas digitais
- Produtividade – Equipes de Alta Performance
- Competências Pessoais e Coletivas

Práticas de Gestão de Projetos para Cibersegurança

Carga Horária: **15h**

Ementa

O gerenciamento tradicional de projetos há tempos já demonstrou sua relevância e eficácia para os processos de gestão, em projetos e organizações de qualquer porte. Mas, em um cenário onde a pressão de ameaças digitais e a necessidade de manter a continuidade e ininterrupção dos negócios é vital, a adoção de práticas de gestão de projetos é essencial para garantir que mudanças programadas e a implementação de novas tecnologias e serviços ocorra de acordo com o seu planejamento.

Conteúdo Programático

- Noções básicas sobre estruturas de gerenciamento de projetos
- Princípios básicos e diferenças entre os métodos ágil e tradicional
- Como melhorar a agilidade organizacional em resposta à mudanças
- Definição de papéis e responsabilidades no modelo híbrido
- Adoção de uma abordagem híbrida para enfrentar os desafios de integração
- Uso de estratégias híbridas para gerenciar os riscos do projeto
- Comunicação estratégica entre projetos híbridos
- Uso de abordagens híbridas para obter rapidez operacional
- Como implementar um modelo de gerenciamento de projeto híbrido

Governança Corporativa Aplicada a Segurança

Carga Horária: **15h**

Ementa

A disciplina apresenta os princípios de Governança Corporativa devem nortear as definições estratégicas da Governança de Segurança da Informação. O sucesso da Governança de Segurança é alcançado através do desenvolvimento e execução do Planejamento Estratégico de Segurança da Informação, o qual oferece à Governança Corporativa valores como transparência, confiabilidade, previsão de investimentos, e a percepção de total alinhamento com os objetivos de negócios. Essa conexão da Estratégia do Negócio com a Governança de Segurança da Informação é essencial para o sucesso da segurança cibernética da organização. Líderes e gestores de Segurança da Informação devem se dedicar à educação continuada, mantendo os conhecimentos técnicos atualizados e ainda desenvolver a capacidade de "falar a mesma língua" que os gestores do negócio.

Conteúdo Programático

- Governança Corporativa
  – Relações de influência entre a Governança Corporativa e a Governança de Segurança da Informação
  – Prós e Contras dos Modelos de Gestão
  – Boas Práticas de Governança Corporativa que influenciam a Governança de Segurança
  – Gestão de Riscos Corporativos–as contribuições da Governança de Segurança
  – Radar da Governança–Aspectos que devem estar na agenda do Gestor de Segurança

- Governança de Segurança da Informação
  – Modelos de Governança para Segurança da Informação
  – ISO 27014
  – Princípios da Governança de Segurança da Informação
  – Radar da Governança de Segurança

- Planejamento Estratégico de Segurança
  – Avaliação das Necessidades do Negócio e de Segurança da Informação
  – Estruturação da Segurança
  – Organização das Estratégias, Projetos, Processos e Serviços.
  – Métricas de Segurança

Estratégias de Comunicação e Gestão de Crises

Carga Horária: **15h**

Ementa

A disciplina apresenta ao aluno as etapas de planejamento, desenvolvimento e implementação de estratégias de comunicação e gestão em cenários de crises. A gestão de crise exige transparência, preparação prévia e comunicação alinhada entre os envolvidos no gerenciamento e na atuação para resolver a situação de crise. Documentação, simulações e exercícios de preparo são obrigatórios para êxito durante tratamento de crise. Os alunos aprenderão a usar o pensamento crítico para criar e comunicar "mensagens-chave" de maneira correta em momentos de crise.

Conteúdo Programático

- Práticas de Governança de Segurança em Gestão de Crises
- 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 e Plano de Comunicação
- Métodos de identificação de ameaças e geração de alertas
- Relação entre as novas legislações de privacidade e a gestão de crise

Fundamentos da Internet e Princípios de Cibersegurança

Carga Horária: **15h**

Ementa

Esta disciplina introduz os conceitos básicos de redes de computadores, do funcionamento da internet e os conceitos fundamentais de segurança da informação. Tem como objetivo fornecer os conhecimentos básicos necessários para a participação e acompanhamento das demais disciplinas do curso. A frequência nesta disciplina é optativa. Alunos que já possuem um conhecimento prévio não necessitam realizar esta disciplina.

Conteúdo Programático

- Fundamentos e Arquitetura da Internet
- Princípios de telecomunicações
- Serviços e Protocolos da Internet
- Controles de Domínios no Brasil e no Mundo
- IPV4 vs IPV6
- Princípios de Segurança da Informação
- Evolução da Cibersegurança
- Disciplinas da Cibersegurança
- Guerras Cibernéticas

Princípios de Prevenção à Fraudes e Crimes Cibernéticos

Carga Horária: **15h**

Ementa

A disciplina apresenta como ocorrem as fraudes envolvendo o ambiente cibernético. Característica muito presente nestes formatos de fraude, a engenharia social, é abordada sob a perspectiva das situações que envolvem tecnologias informáticas. Discute-se ainda como é a conduta do fraudador, quais as estratégias para combater a fraude e as perspectivas futuras para prevenção e atuação antifraude envolvendo as tecnologias cibernéticas.

Conteúdo Programático

- Fraude pela perspectiva do crime cibernético
- Diferença entre Ataque e Fraude
- Setores mais afetados por Fraudes Cibernéticas
- Engenharia Social – Conceito e usos pelos fraudadores
- Modalidades de Fraudes Informáticas
- Estratégia antifraude em cibersegurança
- Perspectivas para proteção e prevenção à fraudes cibernéticas

Gerenciamento e Avaliação de Riscos em Negócios

Carga Horária: **15h**

Ementa

O objetivo é compreender os conceitos e definições de risco, conhecer as metodologias para identificar, mensurar e gerenciar os riscos no negócio e na organização. Explorar fontes de risco dentro da organização e fora, com serviços terceirizados ou parceiros de negócio. Discute ainda o gerenciamento integrado de riscos, a construção de programas de risco e conformidade e o debate sobre a mensuração e demonstração de risco cibernético.

Conteúdo Programático

- Introdução, Definição de Riscos e Tipos de Riscos
- Representação de Riscos em Demonstrações Financeiras
- Como calcular e demonstrar o Risco Cibernético?
- Metodologias para Mensurar Riscos
- Risco Sistêmico
- Ferramentas para Controles dos Riscos (Norma ISSO 31000, COSO ERM, PMBOOK, CMMI, COBIT, RMF for DoD
- Divulgação de Informações
- Riscos em Terceirização, Outsourcing
- Gestão dos Riscos Corporativos
- Gestão dos Riscos Operacionais
- Gerenciamento Integrado de Riscos
- Programas de risco e conformidade.
- Políticas, Procedimentos, Normas, Linhas de Base, Diretrizes, Ética

Treinamento, educação e conscientização para Cibersegurança

Carga Horária: **15h**

Ementa

Educar sua equipe de colaboradores sobre segurança cibernética por meio de um programa de conscientização é um requisito fundamental que todos os padrões de segurança cibernética compartilham. Então, por que não temos uma equipe de colaboradores minimamente capacitada quando se trata de segurança cibernética? Educação e conscientização estão relacionados a pessoas e, mais especificamente, ao papel que cada indivíduo desempenha. É importante acompanhar e medir o que cada indivíduo faz, além de criar mecanismos para que os treinamentos e programas de conscientização seja alterado a medida que cada vulnerabilidade e incidente é identificado.

Conteúdo Programático

- Atributos e características de uma cultura de Cibersegurança
- Impactos de uma cultura de Cibersegurança no desempenho e na receita da empresa
- Uso de KPIs de monitoramento de Cibersegurança
- Plano e política de gerenciamento da cultura de segurança cibernética
- Práticas para comunicação e disseminação da política organizacional de cibersegurança
- Modificando o mindset dos colaboradores para à prevenção de riscos cibernéticos
- Práticas de sucesso adotadas pelas organizações
- Gamificação para treinamento e conscientização em cibersegurança

PROGRAMA POR DISCIPLINA

Tecnologias de Cibersegurança I

Carga Horária: **15h**

Ementa

A disciplina apresenta as tecnologias e soluções disponíveis para a proteção cibernética dos negócios. Ferramentas que analisam e monitoram padrões de comportamento, detecção de sinais, execução e uma série de outras tarefas precisam ser examinadas e reexaminadas para garantir a segurança do negócio à medida que a organização se adapta às mudanças de funcionários, parceiros e clientes cada vez mais digitais.

Conteúdo Programático

- Tecnologias para mitigar o risco proveniente de ameaças
- Arquitetura e conceitos essenciais (Ameaça, agende de ameaça, vulnerabilidade, incidente, controles, impacto, riscos e ativos)
- O ciclo Prevenção – Detecção – Resposta - Predição
- Tendências e tecnologias emergentes em cibersegurança
- Openness e OpenAPI
- Shadow IT
- BYOID
- Breach and Attack Simulation (BAS)
- User and Entity Behavior Analytics (UEBA)
- Security Orchestration Automation and Response (SOAR)
- Security Rating Services (SRS)
- Threat and Vulnerability Management (TVM)
- Cloud Access Security Broker (CASB)
- Cloud Workload Protection Platform (CWPP)
- Cloud Security Posture Management (CSPM)
- Deception Platforms
- Security Information and Event Management (SIEM)
- Network Traffic Analysis (NTA)

Segurança em Cloud-computing

Carga Horária: **15h**

Ementa

O objetivo desta disciplina é o estudo dos sistemas de computação em nuvem de uma maneira ampla e sistêmica, permitindo a contextualização da tecnologia sob a perspectiva da segurança digital nos negócios. A disciplina discute ainda a adoção de nuvem do ponto de vista estratégico para a organização e os negócios, de modo a capacitar os gestores a conduzir projetos de migração para computação em nuvem, assim como gerir e implementar os ambientes da empresa nos provedores de computação em nuvem de forma segura e ordenada.

Conteúdo Programático

- Introdução e Conceitos de Cloud-Computing
- Vantagens de uso de nuvem para a Segurança
- Segurança DA Nuvem vs Segurança NA Nuvem
- Segurança by Design / Segurança como código
- Responsabilidade Compartilhada
- Criando a sua jornada segura
- Regulamentações relevantes para nuvem
- Programas de Compliance
- Princípios de Segurança NA Nuvem
- Mitos, fatos e assuntos quentes

Aplicação de Biometria em Segurança

Carga Horária: **15h**

Ementa

"Você é sua senha!" A biometria faz uso de medidas e características dos seres humanos para o reconhecimento de usuários e vem sendo cada vez mais utilizada para questões de segurança no mundo digital e na integração entre o físico e o digital. Esta disciplina discutirá as formas de uso da biometria em segurança e as oportunidades e desafios de cada forma.

Conteúdo Programático

- Características biométricas – Fisiológicas e comportamentais
- Principais biometrias utilizadas (impressão digital, face, íris, palma, vascular, voz, escrita e digitação)
- Biometrias emergentes (cognitiva, cardíaca, muscular, caminhar, comportamental)
- Aplicabilidades e desafios no mercado de segurança

Segurança e Gestão da Identidade Digital

Carga Horária: **15h**

Ementa

A gestão de identidade é o processo de automatizar e auditar as concessões de acesso dos sistemas e dados da organização. Fluxos integrados entre os sistemas e plataformas, com apoio de processos automatizados permitem o mapeamento e monitoramento de acessos de usuário.

Conteúdo Programático

- Conceitos Fundamentais na Gestão de Identidade
- Domínio das políticas de Gestão de Acesso de Identidade (IAM) e inteligência
- Gestão de acessos e prevenção contra fraudes
- Ciclo de vida de uma identidade
- Tipos de controle de acesso
- Segurança da Identidade Digital
- Adaptive Authentication
- Cofre de senhas
- Perspectivas para gestão da identidade em cibersegurança

Aplicações de Inteligência Artificial em Cibersegurança

Carga Horária: **15h**

Ementa

A disciplina tem como objetivo apresentar aos alunos os conceitos e técnicas de inteligência artificial utilizadas na Segurança Cibernética nas empresas. Destaca-se também como as técnicas de análise preditiva e as ferramentas de big-data podem servir para melhorar o alcance e a efetividade da segurança cibernética nas organizações.

Conteúdo Programático

- Conceitos de Inteligência Artificial, Machine Learning e Deep Learning
- O papel da IA e da ML na segurança cibernética
- Uso da IA na cibersegurança para proteção de informações sensíveis e na identificação automática de vulnerabilidades
- Aplicações na Detecção e Resposta de ameaças
- Aplicações na Proteção de Dados
- Aplicações na Segurança da Identidade
- Aplicações no monitoramento dos usuários e melhora na experiência do usuário
- Smart Grid Cyber Security
- Cyber Threat Intelligence, Cyber Security Analytics e Governança de Dados
- Prós e Contras do uso de I.A. em cibersegurança
- Perspectivas do uso de IA e Machine Learning em Cibersegurança

Monitoramento da Internet e Inteligência em Cibersegurança

Carga Horária: **15h**

Ementa

A disciplina apresenta os cenários de ameaças e apresenta porquê é necessário conhecer e monitorar o ambiente cibernético para uma proteção eficaz dos negócios e da organização. As técnicas de inteligência utilizadas para monitoramento do ambiente se tornam necessárias em meio a uma avalanche de informações, nem sempre precisas, e como ocorre o uso dessas informações com objetivo de priorizar ações de resposta e de prevenção. A disciplina discute ainda o ciclo de vida e o custo dos ataques.

Conteúdo Programático

- Cyber Threat Intelligence - Conceitos
- Ciclo de Inteligência
- Siglas e terminologias utilizadas em inteligência e contra inteligência em cibersegurança
- Coleta, qualificação, análise e compartilhamento
- Information sharing
- Hacktivismo
- Ciber crime
- Ciber espionagem

Testes de Segurança e Conceitos

Carga Horária: **15h**

Ementa

A proposta da disciplina é apresentar aos participantes conceitos que lhes permitam aprender e discutir de forma organizada como realizar testes de invasão em sistemas e soluções de tecnologia. Também conhecido como Ethical Hacking, os procedimentos e ferramentas utilizadas para realização de testes de segurança são fundamentais para a identificação de vulnerabilidades, falhas na cibersegurança e múltiplos vetores de ataque à organização e ao ambiente digital do negócio..

Conteúdo Programático

- Análise de Vulnerabilidades
- Teste de Invasão Compliance PCI-DSS
- Teste de Invasão Standard e Advanced
- Red Team – in loco e remote
- Metodologias de testes de invasão

Cultura Ágil, Desenvolvimento e Automação da Segurança

Carga Horária: **15h**

Ementa

Vários conceitos e técnicas de gestão e tecnologia permitiram o surgimento e disseminação prepararam o terreno para o movimento DevOps, que resulta da aplicação dos princípios mais confiáveis para o desenvolvimento contínuo e a liderança no fluxo de valor de TI. Nesta disciplina o aluno conhecerá como as organizações que adotam os princípios e práticas Lean podem melhorar significativamente a produtividade no desenvolvimento de softwares, o tempo de disponibilização de atualizações e novas funcionalidades, a qualidade do produto e a satisfação do cliente, gerando um diferencial competitivo ao negócio.

Conteúdo Programático

- Gestão de Infraestrutura, serviços e operações
- Impactos da cultura ágil nas organizações
- Frameworks ágeis (Scrum, Kanban, DevOps)
- Microserviços e Gestão de Mudanças
- Desenvolvimento e Operações (DevOps)
- Modelo de maturidade para desenvolvimento
- IAM – Identidade e gestão de acessos
- Desenvolvimento e Automação da Segurança (DevSecOps)

Políticas e Planejamento Estratégico de Cibersegurança

Carga Horária: **15h**

Ementa

A disciplina capacitará aos alunos articular os desafios e as diferenças entre várias abordagens de governança da segurança cibernética, ser capaz de aplicar sua aprendizagem ao seu ambiente atual e compreender os efeitos além das implicações da segurança cibernética para eventos futuros ou previstos.

Conteúdo Programático

- Ciclo de vida da informação
- Organização da segurança da informação
- Classificação e gestão de ativos de informação
- Aspectos humanos da cibersegurança
- Controles de cibersegurança
- Política de Segurança da Informação
- Plano de Continuidade de negócios
- Plano de contingência
- Gestão de segurança segundo o COBIT

Ameaças, Ataques e Gerenciamento de Vulnerabilidades

Carga Horária: **15h**

Ementa

A evolução das ameaças, tanto nas tecnologias, quanto nas estratégias, ocorre em uma velocidade que nem sempre a as estruturas de defesa e prevenção conseguem acompanhar. A disciplina discute as principais ameaças e tipos de ataques que ocorrem no mundo cibernético. Discute ainda estratégias de segurança utilizadas para evitar ataques e minimizar os riscos de incidentes.

Conteúdo Programático

- Ameaças digitais e físicas
- Tipos de ataques: força bruta, engenharia social, scan, etc
- Ameaças Digitais — a evolução das preocupações e riscos atuais (Vazamento de Informações, Ransomware)
- Vazamento de Informações e Roubo de Dados - dos primeiros anos da Internet aos dias atuais, quais são os cenários de risco
- Hacktivismo, Grupos Organizados e os “state-sponsored”
- Fatores externos e Gerenciamento de Risco da Cadeia de Valor
- Ameaças para cadeias de suprimentos cyber-dependentes
- Limitações do “risco de terceirização” e SLA
- BYoD

Infraestrutura para Defesa Cibernética

Carga Horária: **15h**

Ementa

Nesta disciplina serão discutidos tipos de Arquitetura e Tecnologias de Segurança, o desenvolvimento e implantação de projetos com essa finalidade e o funcionamento de centros de operação de cibersegurança (Security Operations Center - SOC)

Conteúdo Programático

- Regras e responsabilidades do SOC
- Diferença entre o SOC e o CSIRT
- Composição e papeis de uma equipe de operação de SOC
- Processos e procedimentos
- Tecnologias e soluções adotadas em um SOC
- Gestão do conhecimento no SOC
- Workflow e fluxo de informação
- Métricas e monitoramento
- Ciclo de vida e maturidade do SOC

Centros de Resposta à Incidentes

Carga Horária: **15h**

Ementa

O que são os CSIRTs (Equipes de resposta a incidentes de segurança de computadores) e qual seu papel na organização e na proteção digital do negócio? A disciplina discute o relacionamento entre CSIRTs, gestão de cibersegurança e gestão de incidentes na organização. Debaterá ainda quais os fatores para o sucesso no gerenciamento de incidentes.

Conteúdo Programático

- Fundamentos e frameworks adotados
- Relacionamento entre os processos de Gerenciamento de Incidentes e os CSIRTs
- Atribuições e ações de um CSIRT
- Composição e estrutura de um CSIRT
- Gerenciamento Operacional
- Processo de Gestão de Incidentes

Resiliência em Cibersegurança

Carga Horária: **15h**

Ementa

Analisar os casos de incidentes cibernéticos e apresentar aos alunos os conceitos de resiliência em cibersegurança. Quais são os frameworks adotados na estruturação e operação de equipes de resiliência cibernética e as estratégias para implantação dessas operações.

Conteúdo Programático

- Definição de Resiliência e Resiliência em Cibersegurança
- Cyber Security versus Cyber Resilience
- Framework para resiliência cibernética
- Técnicas adotadas em resiliência de cibersegurança
- Estratégia de resiliência em cibersegurança
  - Ameaças, regulamentações, perspectivas
  - Proteção, Detecção e Resposta
  - Governança e gestão de equipes

Proteção de Dados, Privacidade e Regulamentações

Carga Horária: **15h**

Ementa

A disciplina discute a importância da proteção de dados pessoais e da privacidade em uma nova era da sociedade. Legislações demandam agora o uso ético e seguro de dados. Para isso é necessário compreender os benefícios e impactos que a LGPD (Lei Geral de Proteção de Dados) no Brasil, a GDPR (General Data Protection Regulation) na Europa e demais regulações e legislações causam para os negócios e as empresas no cenário brasileiro e mundial. Avaliar os fundamentos, princípios gerais e conceitos legais da legislação, construindo bases conceituais para a implementação de um plano de adequação jurídica da empresa à legislação.

Conteúdo Programático

- Introdução e fundamentos ao Estudo da LGPD
- Conceitos relevantes da privacidade e da proteção de dados pessoais
- Princípios legais para o tratamento de dados pessoais
- Bases legais para o tratamento de dados pessoais e dados sensíveis
- Direitos dos titulares e Consentimento
- LGPD
- GDPR
- GDPR x LGPD
- Autoridade Nacional de Proteção de Dados
- Jurisprudência (Casos)

Práticas de Proteção de Dados e Atribuições do DPO

Carga Horária: **15h**

Ementa

Conhecer a arquitetura de geração, armazenamento e distribuição dos dados, garantindo que a organização adote políticas e processos alinhados com as legislações de proteção de dados e da garantia de privacidade do titular dos dados. Atuar como responsável pela comunicação com os titulares de dados e com a autoridade governamental de proteção de dados, além de orientar funcionários e empresas terceirizadas a respeito das práticas exigidas para a proteção de dados pessoais.

Conteúdo Programático

- Práticas de Proteção de Dados
  - Marketing
  - Políticas Internas
  - Sistema de Gestão de Proteção de Dados
  - Papéis do Controlador, Processador/ Operador e DPO
  - Avaliação/Relatório de Impacto sobre a Proteção de Dados
  - Violação de dados, notificação e resposta a incidentes
- Programa de Compliance de LGPD
- Controles e Testes de Compliance
- Segurança e Práticas:
  - Medidas de segurança técnicas e administrativas
  - Privacy by design
  - Governança da privacidade
  - Comunicação em casos de incidentes
- Agentes de Tratamento
- Ferramentas do Data Protection Officer

Direito Digital e Crimes Eletrônicos

Carga Horária: **15h**

Ementa

Os crimes praticados PELA e NA Internet fazem parte dos problemas enfrentados pelas empresas em todo o mundo. O Brasil já é o segundo país com maior número de crimes cibernéticos, o que gera um prejuízo estimado da ordem de US$22 bilhões. A grande maioria dos crimes digitais são crimes que podem ser enquadrados em alguma lei já vigente, mas que muitas vezes apenas o meio de realização desses crimes é diferente, ou seja, são crimes cometidos através do uso de um dispositivo informático (smartphone, laptop, computador de mesa ou tablet). Esta disciplina irá desmistificar estes crimes e comentar sobre os procedimentos legais a serem adotados em diversas situações, qual a legislação aplicável e formas de prevenção e atuação quando uma pessoa ou organização se torna vítima.

Conteúdo Programático

- Legislação de Direito Digital
- Marco Civil da Internet
- Definições, Nomenclatura e Classificação de crimes
- Premissas dogmáticas
- Artefatos, técnicas e métodos
- Medidas jurídicas, Investigações, Validade de Provas e Meios Lícitos
- Crimes em espécie e Crimes Cibernéticos
- Bloqueio de aplicações e Responsabilidade civil dos provedores
- Assinaturas Eletrônicas
- Compliance Digital
- Modelos de Negócios Digitais e sua Validade Jurídica
- Direitos Autorias e Tecnologia

Princípios de Investigação Cibernética e Forense Digital

Carga Horária: **15h**

Ementa

Apresentar aos alunos técnicas de computação forense. Metodologia e técnicas de análise forense computacional. Abordar a questão da Criminalística

Conteúdo Programático

- Conceitos de computação forense.
- Técnicas de Investigação Tecnológica
- Investigação em Sistemas Informatizados.
- Recuperação de dados e arquivos
- Ferramentas para análise forense
- Criminalística computacional.
- Metodologia e Processo Pericial
- Ata notarial, laudo pericial e parecer técnico.

Como me

MATRICULAR?

Documentação:

São requisitos indispensáveis à matrícula a apresentação dos **documentos pessoais** e a apresentação do **Diploma de Graduação** (frente e verso) emitido por Instituição de Ensino Superior (IES) devidamente credenciada pelo Ministério da Educação (MEC), no decorrer do Curso.

Os documentos pessoais e o Diploma de Conclusão da Graduação deverão ser encaminhados em cópia autenticada e o presente instrumento devidamente assinado , por correio no seguinte endereço:

Avenida Dra. Ruth Cardoso, nº 7.221, térreo, Pinheiros, CEP: 05425-902, São Paulo – SP

aos cuidados da Coordenação do Curso.

E-mail: **atendimento.fiaonline@fia.com.br**
Telefone de contato: **(11) 93471-2100**

PRONTO!

1. Você já sabe que a atualização é indispensável!
2. Você já sabe que o mercado valoriza e recompensa agora aqueles que evoluem e são protagonistas.
3. Você já sabe que a FIA é autoridade em educação, pesquisa e consultoria e que você pode pertencer a esse grupo.
4. Você precisa de uma Metodologia com a qualidade FIA, pensada para você.

Você não pode esperar mais.

Amplie seu mundo agora e

SEJA BEM-VINDO!


FIA ONLINE