FIAP

PROJETO PEDAGÓGICO DO CURSO

MBA ON-LINE EM CYBER SECURITY – FORENSICS, ETHICAL HACKING & DEVSECOPS

ORGANIZAÇÃO DIDÁTICO-PEDAGÓGICA 4

Projeto Pedagógico do Curso: Aspectos Gerais 4

Objetivos do Curso 11

Tese de Transformação do Curso 13

Perfil do Egresso 14

Mercado de Trabalho 15

Metodologias Inovadoras 16

Conexão entre as fases e disciplinas 22

Competências e Ferramentas 25

Matriz Curricular 27

Ementas e Bibliografias 29

Design Experience FIAP 45

Processo de Avaliação 47

Projeto Integrador – Startup One MBA FIAP ON 48

ORGANIZAÇÃO DIDÁTICO-PEDAGÓGICA

Projeto Pedagógico do Curso: Aspectos Gerais

Contexto educacional

O **Centro Universitário FIAP** é uma Instituição de Ensino Superior com atuação principal nos eixos de tecnologia, gestão e inovação. Inserido fisicamente na região com maior densidade tecno-econômica do país, a Região Metropolitana de São Paulo tem mais de 22 milhões de habitantes[1], e possui relevância e liderança nacional no desenvolvimento da economia nacional.

A Região concentra a maioria das sedes de empresas brasileiras dos mais importantes complexos industriais, comerciais e financeiros, o que cria também grande demanda por profissionais qualificados nas principais áreas de competências e habilidades da Nova Economia, exibindo um Produto Interno Bruto (PIB) de R$ 2,3 trilhões. São Paulo seria a 21ª economia mundial[2], se fosse um país. Sua economia é maior que a de países como Polônia, Suécia, Bélgica, Argentina, Áustria, Noruega, Irlanda, Singapura e Dinamarca.

A segurança da informação envolve a proteção da informação disponível em diversas mídias, contra riscos de perda de integridade, confidencialidade ou disponibilidade. Os riscos de perda estão relacionados às fragilidades exploradas nos domínios de pessoas, processos e tecnologias.

Hoje, empresas de qualquer segmento requerem a aplicação prática em segurança da informação, pois, por conta dos riscos mencionados, a perda de integridade de dados pode conferir, entre outros aspectos, na perda de confiança em uma marca ou produto. Na questão da perda de confidencialidade, uma empresa pode perder mercado para a concorrência, em razão dos dados competitivos terem se tornado públicos, podendo ser

[1] IBGE – INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Produto Interno Bruto 2019**. Rio de Janeiro: IBGE, 2019.

[2] CASA CIVIL – GOVERNO DO ESTADO DE SÃO PAULO. **São Paulo é a 21ª maior economia do mundo**. São Paulo: GOVERNO DO ESTADO DE SÃO PAULO, 2020.

utilizados em benefício de outrem. E, em função da perda de disponibilidade, serviços críticos podem deixar de ser acessados, comprometendo o processamento e a concretização de transações sistêmicas, incluindo, entre outros, serviços bancários, processamento de folha de pagamento e outras necessidades que hoje dependem da tecnologia para a efetivação dos processos de negócio.

Portanto, percebe-se que a segurança não é mais a simples aplicação de boas práticas no âmbito da tecnologia, pois a má gestão desse segmento afeta diretamente os resultados do negócio e, consequentemente, a lucratividade de empresas, já que a segurança é um aspecto fundamental de redução de despesas.

Assim, os alunos preparados pela formação em Cyber Security atenderão à demandas já existentes e reprimidas desse mercado. As oportunidades geradas por este curso aumentarão a qualidade dos serviços oferecidos pelo mercado de segurança.

O curso também se justifica na função da preparação de profissionais que estarão aptos não só aos desafios da segurança da informação no País, mas também aptos a enfrentar os desafios desse mercado em empresas no exterior, já que o Brasil é reconhecido pela sua excelência na formação de profissionais em função da atuação exemplar no mercado de trabalho interno.

No âmbito acadêmico, o aluno ainda poderá desenvolver diversos trabalhos de alta relevância, pois há diversos comportamentos registrados no Brasil que antecedem tendências em segurança da informação, tanto no âmbito de incidentes de segurança, quanto em soluções que podem ser aplicadas como estudos de caso em meios acadêmicos e em produtos, que podem surgir em oportunidades geradas pelo mercado de trabalho local (Brasil), aplicáveis a diversas partes do mundo.

Este curso diferencia-se das demais formações em meios acadêmicos por estar alinhado à normas do mercado de segurança, aplicadas, hoje, em empresas privadas e órgãos governamentais, atendendo às necessidades

atuais em segurança da informação do mercado de trabalho brasileiro e internacional.

A demanda identificada no mercado brasileiro e estrangeiro é grande para o curso, pois o mercado ainda requer mais profissionais com conhecimentos e vivências em segurança da informação. Em um ambiente cada vez mais vulnerável a ataques, em razão da descoberta de novas fragilidades em processos, pessoas e tecnologias que influenciam diretamente os negócios de uma empresa, esses profissionais são cada vez mais necessários. O Fórum Econômico Mundial[3] aponta um hiato de 2,72 milhões (sendo destes mais de 500 mil na américa latina) em termos de ausência profissionais em cibersegurança, onde a disponibilidade de profissionais precisa crescer em 65% para defender efetivamente os ativos críticos das organizações.

O resultado do PIB (Produto Interno Bruto) brasileiro no primeiro trimestre de 2022, possibilitou ao país ocupar o 9° lugar no ranking de crescimento das economias, segundo a agência de classificação de risco Austin Rating, sendo o setor de serviços o principal responsável pelo crescimento da economia brasileira neste primeiro trimestre[4]. Setor no qual estão presentes a maior parte dos profissionais que atuam em cibersegurança.

O curso prepara os profissionais que atuam na área de Segurança da Informação e preenche uma carência de responsáveis pelo setor de segurança, também conhecido como Security Office, que está em forte crescimento em empresas de médio e grande porte. O curso ainda possibilita que demais profissionais sejam preparados para atuação em Segurança da Informação,

[3] WEF – THE WORLD ECONOMIC FORUM. **Can closing the cybersecurity skills gap change the world?**. Cologny, Switzerland: 2022.

[4] CNN BRASIL. **Com dado do 1º tri, Brasil fica em 9º lugar em crescimento do PIB em ranking com 32 países**. Disponível em: https://www.cnnbrasil.com.br/business/com-dado-do-1o-tri-brasil-fica-em-9o-lugar-em-crescimento-do-pib-em-ranking-com-32-paises/#:~:text=Greve%20dos%20caminhoneiros-,Com%20dado%20do%201%C2%BA%20tri%2C%20Brasil%20fica%20em%209%C2%BA%20lugar,em%20ranking%20com%2032%20pa%C3%ADses&text=Com%20o%20resultado%20do%20PIB,classifica%C3%A7%C3%A3o%20de%20risco%20Austin%20Rating. Acessado em: 29 de junho de 2022.

como áreas de Tecnologia de empresas, assim como áreas de apoio, como Auditoria, Compliance e Risco, bem como preparar profissionais para atuar como especialistas de cibersegurança, e que tenham as capacidades técnico-práticas de criar e desenvolver a linha de defesa das empresas públicas ou privadas, explorando as práticas adotadas nas empresas da área de Segurança da Informação

De acordo com o Relatório de Ameaças à Segurança na Internet[5], (ISTR, na sigla em inglês), que analisa 157 países, divulgado em fevereiro de 2019 pela empresa de segurança digital Symantec, sabe-se ainda que o Brasil é o quarto país no Ranking de Ameaças Detectadas por País. O Brasil, que fica atrás de Estados Unidos, China e Índia, é o quarto país mais afetado por *ransomware*, que consiste em ataques atrelados ao sequestro de dados e vazamento de informações, além de ser o terceiro país responsável pelo percentual de ataques sobre tecnologias IoT (Internet das Coisas), sendo que o Brasil está dentre os 10 países que mais disseminam spam (mensagem de cunho comercial não autorizada) no mundo, e contata-se que os ataques cibernéticos aumentaram com pandemia e já atingem companhias elétricas no Brasil e no mundo[6].

Sabe-se ainda que as leis de proteção de dados e os escândalos aparentemente intermináveis da empresa Meta (Facebook), relacionados à privacidade dos usuários, também aumentaram a conscientização regulatória e pública sobre a privacidade de dados como uma questão e preocupação importantes.

A inserção das tecnologias no mundo do trabalho e o aumento das demandas por soluções envolvendo segurança e alta disponibilidade tem levado a um considerável aumento na procura por formação específica da área de cibersegurança. Esse profissional encontra um campo de trabalho que tem

[5] ISTR – SYMANTEC. **Ranking de Ameaças Detectadas por País**. EUA: 2019.

[6] FORBES. **Brasil entre os 10 países que mais espalham spam.** Acessível em: https://forbes.com.br/listas/2019/04/10-paises-que-mais-espalham-spam/. Acesso em: 28 de jul. 2022.

aumentado consideravelmente nos últimos anos, devido a fatores como a globalização da economia e a expansão das grandes corporações, o surgimento de serviços e processos cada vez mais específicos e especializados e a informatização de micro e pequenas empresas.

O curso de Cyber Security está, portanto, adequado ao mercado de trabalho regional e global alinhado ao perfil das organizações empregadoras. As condições econômicas e sociais de São Paulo são indicadores positivos para a existência de uma instituição de ensino como a FIAP e, especificamente, para a proposição do curso.

Ainda, os objetivos do curso justificam-se, principalmente, ao empreender seus esforços construtivos na articulação entre a formação tecnológica e humanística do indivíduo, como base para a formação integral de um profissional responsável e alinhado com as necessidades do mundo do trabalho. Para isso, faz-se necessário construir uma pedagogia que aceite os desafios da Educação Profissional contemporânea, compreendendo uma abordagem reflexiva e problematizadora das diferentes realidades vivenciadas por alunos e professores.

O curso propõe-se a contribuir com a qualificação dos profissionais da área de cibersegurança, ampliando sua parcela de participação como agente transformador e reforçando seu comprometimento, principalmente, com a cidade de São Paulo e região metropolitana.

O Brasil é um ambiente propício para a oferta de prestação de serviços em cibersegurança, desta forma, torna-se necessário disponibilizar mão de obra qualificada para o desempenho de funções desta área.

Nesse contexto, as empresas de desenvolvimento de tecnologia, empresas de telecomunicações, grandes corporações multinacionais da indústria eletroeletrônica, órgãos públicos, institutos, outras indústrias, centros de pesquisa e instituições financeiras são consumidoras em potencial para esse profissional, ainda mais quando olhamos para a capital paulista.

Essas discussões continuarão no ano de 2022 e demais anos vindouros, exigindo que o mercado de trabalho possa contar com profissionais cada vez mais capacitados.

Cenário Futuro

O profissional em cibersegurança é uma necessidade tanto para o momento atual quanto em um futuro próximo, lembrando que, nos próximos anos, os desafios quanto à sua atuação recairão sobre algumas transformações socioculturais e tecnológicas que exigirão adaptações quanto à capacidade em atender a diversos desafios, dentre eles, a realidade em garantir a segurança ao trabalho na modalidade home office, pois diversos trabalhadores terão que conviver com o uso da tecnologia em ambiente externo ao anteriormente adotado (trabalho em escritórios), visando tanto a proteção de informações tratadas em ambiente residencial, quanto a proteção desses dispositivos no trabalho exercido em qualquer lugar que possa contar com infraestrutura para que exerça suas atividades laborais.

Tecnologias como 5G aumentarão os desafios quanto à proteção de informações, pois se identifica a ampliação, nos próximos anos, quanto ao uso de dispositivos interconectados por meio de IoT (Internet das Coisas), possibilitando amplificar ainda mais a troca de dados, informações e o gerenciamento em tempo real de dispositivos, ambientes e seus respectivos usuários, sendo estes dispostos em ambientes corporativos e em seus domicílios por meio de tecnologias que permitem domicílios e cidades conectadas. A necessidade do profissional que atua em cibersegurança já estar adaptado a essas mudanças tecnológicas é essencial para que empresas e usuários possam se manter seguros em face a esses novos desafios. Dessa forma, este projeto pedagógico já conta com essa visão de futuro, permitindo formar hoje o profissional que atuará com esses desafios amanhã.

A inteligência artificial deve ser ainda mais desafiadora, em relação aos aspectos de cibersegurança, pois já se tem conhecimento sobre a existência de tecnologias adaptativas que apresentam a capacidade de ataques

automatizados com base em IA (Inteligência Artificial). Dessa forma, sistemas também concebidos por meio de Inteligência Artificial serão usados amplamente como forma de proteção aos nossos dados e informações, sendo importante que esses profissionais que atuam no mercado de cibersegurança estejam atentos à essas tendências, estando esse tema já presente em ementa proposta.

Apesar de considerar que ataques tradicionais ainda deverão estar presentes nos próximos anos, como o ransomware (sequestro de dados), sabe-se que o profissional deverá se manter atentos às novas modalidades de ataque aos diversos segmentos críticos de negócio, nos quais a proteção de infraestruturas críticas e negócios considerados essenciais é uma tendência. A visão hoje oferecida ao aluno permite que já se tenha a preocupação quanto a proteção desses ambientes, permitindo ações de forma antecipada, minimizando impactos junto aos negócios e à sociedade, podendo até vir a proteger interesses e necessidades atrelados à soberania nacional.

Dado que haja todo um desenvolvimento da sociedade em direção à Indústria 4.0, desenvolvimentos de ambientes como o Metaverso, que consiste em uma rede de mundos virtuais, que buscam replicar a realidade com objetivos relacionados à conexão social, além da massiva oferta de criptoativos como criptomoedas e NFTs, devemos também estar atentos ao fato de que a tecnologia estará cada vez mais próxima do usuário final, devendo o profissional em cibersegurança estar presente tanto para trazer as melhores práticas, quanto para alertar sobre os riscos em relação ao uso de novas tecnologias, que incluem a capacidade de constante monitoramento de pessoas por meio de dispositivos que estarão cada vez mais integrados ao corpo. Cientes de que ataques ocorrerão sobre tais tecnologias, deveremos estar também cientes de que a blindagem pessoal será um dos pontos essenciais para a adoção de uma segurança orgânica junto à sociedade.

Objetivos do Curso

Objetivo geral:

O curso tem como objetivo especializar os profissionais para atuar como especialistas em cibersegurança que tenham as capacidades técnico-práticas de criar e desenvolver a linha de defesa das empresas públicas ou privadas, explorando as práticas adotadas nas empresas na área de Segurança da Informação.

Objetivos específicos:

- Formar profissionais com uma visão global dos problemas envolvidos na área de segurança da informação, nos aspectos corporativos e acadêmicos, envolvendo a compreensão dos riscos nas dimensões tecnológicas, processuais e pessoais;
- Subsidiar o aluno com elementos que o levem à realização de análise crítica sobre soluções de segurança, oferecendo um amplo conhecimento dos cenários e das ferramentas necessárias para atender aos desafios diários em segurança da informação;
- Prover capacitação ao profissional, visando à proposição, avaliação e implementação de processos, políticas e procedimentos de segurança corporativas no âmbito do Sistema de Gestão em Segurança da Informação alinhados às normativas, legais e regulatórias do mercado;
- Possibilitar que o profissional conheça os requisitos e realize a gestão de recursos necessários para a implementação e manutenção da segurança da informação, incluindo aspectos como custos, prazos, processos, tecnologias disponíveis e recursos humanos;
- Capacitar o aluno a executar possíveis ações de resposta a incidentes, ações de inteligência, ações investigativas forenses e ações de identificação e remediação de fragilidades técnicas;
- Qualificar o profissional para coordenar times de segurança Cibernética em grandes corporações, fazendo não só a gestão de processos e

pessoas, mas, principalmente, definindo escopos técnicos de testes, auditorias, implementações e produtos a nível de Cybersecurity;

- Desenvolver no aluno uma visão macro do negócio e de como a Cybersecurity poderia impactá-lo, bem como implementar conhecimentos técnicos-práticos para acessorar e/ou tomar decisões aderentes ao negócio sob o aspecto da segurança da informação; e
- Habilitar o aluno para trabalhar com as principais técnicas e táticas de segurança cibernética aplicadas às tecnologias existentes no mercado, bem como desenvolver novas técnicas e táticas para avaliação e proteção cibernética às tecnologias emergentes.

Tese de Transformação do Curso

O aluno terá a oportunidade de ser moldado às necessidades presentes e atuais em cibersegurança, assim como às necessidades de um cenário futuro e desafiador, no qual as disciplinas constroem gradativamente a percepção do conjunto de necessidades relacionadas aos conhecimentos e experiências exigidos para que esse profissional possa atuar de forma exemplar no mercado de trabalho.

Essa experiência leva em consideração a base formal do conhecimento por meio do uso de metodologias e do conhecimento estabelecido por meio de normas, padrões e boas práticas, alinhados às experiências de sucesso indicadas ao longo das disciplinas. Isso não restringe aos alunos a possibilidade de apresentar casos de insucesso, que também consistem em lições aprendidas, atrelados aos aspectos do que se deve evitar em cibersegurança.

Em cada aula, o aluno terá uma experiência única por meio do conhecimento e da experiência apresentados e discutidos. Novos conteúdos serão concluídos em cada uma das disciplinas e fases, sendo importantes para a compreensão da devida importância de cada tema abordado e sua contribuição às distintas etapas da vida do profissional em cibersegurança. Cada novo tema trabalhado permite a construção de todo um conjunto de conhecimentos e experiências aplicáveis em áreas específicas atreladas ao mercado em cibersegurança. Essas áreas e conhecimentos podem estar relacionadas às tecnologias, processos ou negócios, sendo o conjunto de fases a coroação e a compreensão de como esses temas complementares são essenciais para formação completa exigida do profissional em cibersegurança.

Devemos, ainda, ressaltar que cada turma oferece uma experiência única aos alunos, visto que as experiências individuais são consideradas em cada aula ministrada, pois seus problemas e desafios se tornam questões colocadas e devidamente discutidas, não só oferecendo aos alunos o conhecimento, mas

possibilitando um tratamento consultivo sob a ótica pedagógica das questões apresentadas pelos alunos.

Perfil do Egresso

O egresso do curso Cyber Security será um profissional que participa de decisões, planeja soluções, concebe, desenvolve e implanta projetos diretamente relacionados à área de segurança de redes e de sistemas de informação. O egresso mostrará capacidade de adaptação às novas situações que constituem um desafio contínuo da área de segurança de informação. Para tanto, ele deverá:

- Atualizar-se continuamente, incorporando, com crítica, novas tecnologias às suas ações, para acompanhar as inovações da área;
- Administrar e responder às situações novas com flexibilidade, criatividade, eficácia e eficiência, enfrentando os desafios impostos pelo trabalho no segmento de segurança computacional;
- Propor e avaliar as políticas de segurança da informação, com base na participação e análise crítica de debate junto às equipes de gestão e de auditoria de segurança, para mantê-las aderentes às novas tecnologias e tendências em segurança da informação;
- Configurar e administrar sistemas de proteção de redes com base nos requisitos dos negócios e políticas das corporações, com a aplicação da tecnologia que está articulada com os processos de gestão, com o objetivo de garantir a disponibilidade, integridade e confidencialidade dos dados armazenados e transacionados por essa infraestrutura;
- Analisar as vulnerabilidades e propor recomendações em sistemas e infraestrutura de comunicação, utilizando metodologias e ferramentas adequadas, visando mitigar riscos e seus impactos;
- Formular, desenvolver e acompanhar projetos com base nos impactos, riscos, metodologias (procedimentos) e fatores humanos, a fim de

influenciar na implementação de políticas e normas de segurança corporativas.

Mercado de Trabalho

O aluno, ao concluir o curso, estará apto a trabalhar em diversos projetos que incluam a Segurança da Informação como componente necessário para a garantia da manutenção da integridade, disponibilidade e confidencialidade, possibilitando que sejam oferecidas soluções alinhadas às necessidades dos negócios e adequadas à infraestrutura disponível para a realização do projeto. Estará capacitado para desenvolver especificações e projetos de segurança, assim como determinar os requisitos mínimos na aquisição de produtos e serviços necessários para a implementação destes projetos.

O aluno poderá atuar em organizações de diferentes tipos, em projetos na área de segurança da informação; no desenvolvimento de sistemas de softwares corporativos; na coordenação de projetos na área de desenvolvimento de sistemas de software específicos para a segurança; na área de infraestrutura, topologia e componentes de proteção de perímetro em redes corporativas; na administração de redes e sistemas computacionais voltada à aplicação de um nível apropriado de segurança, de acordo com o negócio envolvido; na auditoria de segurança e na consultoria em gestão de segurança para ambientes corporativos.

O crescimento das necessidades de segurança nas empresas faz prever um amplo espectro de especialidades a que os egressos do curso de Cyber Security poderão atender: desde administradores de rede com ênfase na segurança até administradores de políticas de segurança.

Não se espera dos alunos o conhecimento da instalação e operação de uma determinada linha de produtos, nem a capacidade de desenvolverem produtos voltados a funções específicas de segurança. Entretanto, o aluno

poderá recomendar soluções existentes no mercado, sendo capaz de indicar as implementações de menor custo em função das necessidades do mercado.

Metodologias Inovadoras

Todos os cursos do MBA On são entregues por meio de uma jornada composta por 5 fases.

A concepção da jornada é inspirada em PBL (Project Based Learning) que é uma metodologia ativa onde problemas reais são a base do processo de aprendizagem, por isso, a composição das fases nasce da junção de disciplinas da grade curricular do curso que demonstram sinergia entre si, proporcionando ao nosso aluno a aplicação direta dos conteúdos apresentados. Cada fase reúne arcabouço teórico e um conjunto de ferramentas para resolução de problemas que são/serão vivenciados pelos nossos alunos em sua vida profissional real, equilibrando soft e hard skills necessários para formar líderes protagonistas do futuro.

Os conteúdos entregues via plataforma são criados exclusivamente para os alunos do MBA ON, e para que atendam todos os requisitos necessários (atualização, informação relevante de mercado, base teórica consistente e uso de linguagem amigável) um time de especialistas participa desde a concepção da ideia até a revisão final.

- Coordenador de curso – identificação da necessidade do conteúdo e definição da ementa e busca de profissionais no mercado.
- Conteudista – responsável pela escrita dos materiais equilibrando base teórica sólida e cases de mercado.
- Professores especialistas – gravação de vídeos em formatos que variam de acordo com o perfil de consumo da persona do curso: vídeo aula, podcast, talks (TED), painéis de discussão etc.
- Profissionais de mercado – gravação de vídeos com a visão das empresas em formatos de cases.

Todo projeto de criação de conteúdo é acompanhado e validado pelo coordenador de curso que conta com o apoio do time de professores (mentores) de cada curso. Por isso, é tão importante que além de formação acadêmica, nosso time acadêmico tenha experiência de mercado também.

A partir do desenho da persona do curso, e da geração de indicadores que monitoram os acessos aos mais variados formatos de conteúdo, conseguimos desenhar uma experiência de consumo personalizada para cada um de nossos MBAs ON (no momento da produção do conteúdo). Atualmente contamos com 4 formatos que podem ser combinados entre si: HTML, vídeo, áudio e PDF.

Os quatro formatos se complementam, e trazem ênfases diversificadas. Para os cursos com maior enfoque em business temos aulas com aplicações práticas para formatação de modelos/estratégias de negócio e também cases para fornecer benchmarking aos nossos alunos. A ideia é que eles aprendam com profissionais que já erraram e acertaram na prática, e hoje são referências no mercado.

Já em nossos cursos técnicos, a ênfase está no hands on. Mostramos como fazer, fazendo.

Os podcasts geralmente são utilizados para trazer informações relevantes do mercado discutindo boas práticas e experiência de carreira.

Para os alunos que ainda preferem estudar de maneira mais tradicional, temos também o formato PDF que organiza o conteúdo por meio dos textos e imagens, formando uma apostila que pode ser baixada, e acessada off-line.

Existem ainda cursos em que percebemos uma maior apreciação dos alunos, por exemplo, por vídeos em detrimento à leitura de textos, nesses casos, o número de páginas diminui, e o total de horas de vídeo aumentam.

Hoje, além de todo o conteúdo digital, entregamos aproximadamente 80 horas de aulas ao vivo nas 5 fases e no Startup One.

As aulas apresentam formatos diferentes que vão desde aulas de experimentação focadas em hands on, dinâmicas e aplicação de conteúdos, bate-papos com profissionais de mercado, até mentorias com especialistas das empresas

parceiras. Todas as aulas são gravadas e disponibilizadas na plataforma para consumo caso o aluno não tenha conseguido participar ao vivo.

O Solution Sprint é adotado nas fases 1 a 4 dos cursos como forma de avaliação e experimentação de conteúdo. Nesse formato, convidamos uma empresa parceira para trazer uma dor que será a base do desafio entregue ao aluno, para que ele explorando o conteúdo da fase, crie soluções. Durante o processo de criação de soluções, os alunos recebem mentoria das empresas nas aulas ao vivo agendadas e a validação dessa solução com visão de mercado é feita pelas empresas por meio de pitches ou teste de entregáveis no caso dos cursos mais técnicos (validação técnica de aplicações, modelos analíticos, microsserviços, cloud etc).

Por meio dessa metodologia, a retenção e aplicação de conceitos por parte de aluno é avaliada pelo nosso time acadêmico e a validação das soluções pelo mercado é fornecida pelos nossos parceiros em forma de feedback ao vivo proporcionando ao aluno a experiência e segurança necessária para que ele realmente replique as soluções no seu cotidiano profissional.

Na fase 5 o aluno já possui conhecimento e maturidade suficiente para atuar em desafios mais complexos e é aí que entram os challenges, que reúnem os conteúdos do curso todo.

Por serem mais complexos e exigirem uma dedicação maior do aluno, além de ser o fechamento da experiência do curso, as empresas parceiras e a FIAP oferecem premiação para os melhores projetos.

A escolha dos melhores projetos é realizada pelos parceiros e a avaliação acadêmica é realizada pelo nosso time. Assim, garantirmos que nosso aluno foi munido de base teórica consistente e desenvolveu competências em resolução de problemas. Com isso, pretendemos que ele se torne um profissional capaz de analisar novos cenários e entregar soluções, sendo protagonista da sua carreira.

É importante ressaltar que para o público de MBA, a avaliação precisa ser parte do processo de aprendizado para entregar conhecimento ao aluno valorizando o tempo investido por ele na jornada do curso.

Dentro do portfólio do MBA ON temos cursos com públicos bem diferentes, que demandam não só formatos diferentes de conteúdo, mas também dinâmicas avaliativas e experiências customizadas.

Como variação dos challenges de final de curso, atualmente temos os hackathons, CTFs (Capture The Flag – uma competição de conhecimentos muito valorizada pelo mercado de Cyber Security) e os Datathons.

Durante todo o curso, nossos alunos contam com mentorias que podem ser agendadas sob demanda com nossos professores especialistas, além do contato com o time de professores e coordenador do curso, disponíveis sempre que precisarem.

Diante dos diversos formatos de conteúdo e interações que oferecemos nos MBAs ON, nosso aluno pode escolher a forma que mais se adequa ao seu perfil para se conectar com professores, colegas e profissionais de mercado, criando sua própria rotina de estudos, no seu ritmo e dentro das suas necessidades.

Baseado nas constantes evoluções do mercado e nas crescentes demandas de profissionais cada vez mais especializados nas áreas de atuação profissional em Segurança da Informação, o MBA ON em Cyber Security conta com duas trilhas de especialização, as quais são escolhidas pelos alunos durante o curso. Ao término da primeira fase do curso, onde são abordadas as disciplinas basilares do curso, os alunos são direcionados a escolher uma entre as duas trilhas disponíveis: trilhas de Red Team Operations – onde são vistas todas as disciplinas que formam os profissionais responsáveis por atuar nas áreas de Ethical Hacking e Cyber Security Advisory, ou a trilha de Blue Team Operations – onde são vistas as disciplinas que formam os profissionais responsáveis por atuar nas áreas de Security Operations Center e Perícia Forense Computacional.

O processo didático-pedagógico no qual o aluno estará inserido é plenamente comprometido com a interdisciplinaridade, com o desenvolvimento do espírito científico, com a formação de sujeitos autônomos e cidadãos, não havendo também pré-requisitos para o aluno iniciar qualquer disciplina.

A legitimidade deste projeto pedagógico depende basicamente da participação efetiva de todos os atores do processo de ensino-aprendizagem, a saber: coordenação, corpo docente, corpo técnico-administrativo e corpo discente, no seu processo de construção. Este projeto pedagógico pressupõe a participação coletiva, fruto do debate e da consistência de propósitos que envolvem as perspectivas e as intenções sociais dos atores protagonistas deste processo. A ação coletiva não estará limitada à FIAP, porque é necessário que haja interação do ambiente acadêmico com o exterior da faculdade para que o processo de formação se dê de maneira integral e consistente.

Nossa metodologia baseia-se num modelo que privilegia o uso das novas tecnologias da informação, oferecendo aos alunos ambientes ricos em possibilidades de aprendizagem, com a internet, a web e a mobilidade, tendo um papel fundamental nesse processo, sem, no entanto, limitar-se a eles.

Para a concepção desse ambiente educacional centrado na tecnologia, foi necessário o planejamento de uma pedagogia específica, que considerou os seguintes aspectos: cada vez mais se exigem, hoje, profissionais e cidadãos capazes de trabalhar em grupo, interagindo em equipes reais ou virtuais. Mais do que pessoas autônomas ou autodidatas, a sociedade hoje solicita profissionais que saibam contribuir para o aprendizado do grupo do qual fazem parte, seja ensinando, incentivando, respondendo ou perguntando. É a inteligência coletiva do grupo que se deseja pôr em funcionamento, a combinação de competências distribuídas entre seus integrantes, mais do que a genialidade de um só. Dentro desse quadro, aprender a aprender de forma colaborativa é mais importante do que aprender a aprender sozinho. A colaboração, nesse contexto, é essencial. Também dentro desse quadro, os papéis de professor e aluno se modificam significativamente. Nesse cenário pedagógico, a organização do processo de ensino e aprendizagem assume os seguintes aspectos:

- O aluno deixa de ser visto como mero receptor de informações ou assimilador de conteúdos a serem reproduzidos em testes ou exercícios;

- O professor deixa de ser apenas um provedor de informações ou um organizador de atividades para a aprendizagem do aluno;
- Aluno e professor passam a ser companheiros de aprendizagem: o professor com uma função de liderança, de incentivar as iniciativas individuais e coletivas, de despertar o interesse dos alunos;
- Os alunos contagiam uns aos outros, procurando colaborar para o aprendizado e o crescimento de todos;
- O professor torna-se um gestor do ambiente de aprendizagem;
- A organização das disciplinas procura facilitar e estimular os grupos de discussão, de modo a encorajar e viabilizar a interação e o processo de aprendizagem em grupo;
- O material didático das disciplinas é organizado de forma que os conceitos sejam construídos de forma lógica e incremental, evoluindo de exemplos simples para problemas mais elaborados, exigindo os conhecimentos adquiridos para a sua solução;
- Os novos conceitos e conteúdos são apresentados pelos professores, que devem procurar fazer os alunos associarem-nos aos princípios e conceitos anteriormente aprendidos, na busca de um aprendizado crescente e consistente;
- As avaliações são elaboradas para testar a compreensão dos alunos e a aplicação correta dos conceitos trabalhados, variando entre testes formativos, que permitem aos alunos estabelecer o seu nível de conhecimento, e testes compreensivos, que permitem aos professores avaliar a competência dos alunos em utilizar os conceitos ensinados; e
- Todas as atividades procuram explorar ao máximo os recursos multimídia da faculdade, disponíveis nos laboratórios, biblioteca, acervos vivos e textuais, dentre outros, todos dentro dos ambientes de aprendizado criados pela instituição.

O curso privilegia o uso de laboratórios para que o aluno consiga colocar em prática, avaliar, testar e implementar soluções específicas do curso. Sempre que possível, os casos utilizados e desenvolvidos pelos alunos devem ser extraídos da própria comunidade empresarial, seja ela parceira ou não da FIAP.

Ferramentas colaborativas como o Microsoft Teams e Zoom são utilizados para aproximar os alunos nos encontros realizados de forma síncrona, permitindo utilizar além da interação visual e auditiva, a experiência por meio de métodos de gamificação como a prática de exercícios de “Capture The Flag” (CTF) – exercícios de simulação de ataque e defesa cibernética em plataforma exclusiva da FIAP, os quais desenvolvem as habilidades técnico-práticas necessárias a atuação dos profissionais na área de segurança da informação.

Conexão entre as fases e disciplinas

As unidades curriculares que compõem cada um dos conteúdos estão completamente integradas para favorecer a compreensão e a aplicação dos conceitos abordados pelos professores.

Dessa forma, foram idealizados desafios aos alunos em ordem crescente de complexidade, favorecendo a ambientação por parte dos estudantes sobre as reais necessidades do mercado de trabalho. Nesses desafios, os alunos formam equipes e cada equipe deve apresentar sua proposta, atendendo aos requisitos básicos de segurança da informação durante as disciplinas ministradas.

Ao propor um trabalho, indica-se ao aluno que esse seja realizado em grupo. Atualmente, no mercado profissional, não se trabalha isoladamente. Com isso, algumas competências, como negociação, abordagem, exposição e argumentação são subliminarmente e transversalmente desenvolvidas nos alunos.

Assim, um fator importante na metodologia aplicada diz respeito ao trabalho colaborativo. Não se entende a educação como uma ilha de conhecimento, isolada das demais pessoas e fatos. É necessário estabelecer o diálogo, a participação, a interação, a troca de ideias e a discussão das alternativas. Isso só se dá por meio da colaboração. Colaborar é integrar as pessoas extraindo um resultado maior do que a soma das partes. A colaboração não precisa nem deve estar restrita ao ambiente presencial. Ela

se dá em qualquer lugar, tempo ou espaço. Equipes reais ou virtuais são estabelecidas constantemente pelo mercado de trabalho. Além disso, o trabalho em casa (*home office*) é uma realidade cada vez mais presente nas organizações.

A colaboração favorece a autonomia a partir do instante em que faz com que o aluno busque as soluções para problemas reais sem estar o tempo todo com um tutor a sua volta. Por meio da colaboração, as pessoas interagem mais, incentivam-se, motivam-se e trocam experiências. O trabalho colaborativo é, portanto, incentivado como metodologia e técnica para alcançar a excelência em ensino-aprendizagem.

A formação social do aluno será motivada pelos professores para transpor as fronteiras do currículo, sem fugir do apelo profissional do programa. Dessa forma, fazem parte a produção científica, atividades culturais e iniciativas sociais, tais como prestação de serviços à comunidade dentro do perfil do curso (especialmente ONGs e entidades sem fins lucrativos) e participação em eventos comunitários.

No processo de ensino-aprendizagem são utilizados mecanismos diferenciados de avaliação, que pode ocorrer na forma de provas semestrais, mas, principalmente, por meio da prática profissional na forma de projetos interdisciplinares (exercícios de CTF), que oferecem a visão da formação específica na área de formação do curso. Outros instrumentos também são utilizados, como avaliações periódicas para medir o grau de compreensão dos conteúdos abordados. Isso se dá tanto pela prática em laboratório quanto por meio de pequenas atividades solicitadas no decorrer do semestre.

A fim de estabelecer uma estratégia para que o aluno possa motivar-se à manutenção e atualização dos conceitos específicos em cibersegurança, os professores propõem e incentivam os alunos à pesquisa, empregando os mais modernos meios e técnicas que são utilizadas no mercado profissional, incluindo a Internet, revistas especializadas e artigos científicos. As principais estratégias pedagógicas utilizadas no curso são:

- Aulas práticas em laboratórios online exclusivos da FIAP;

- Professores com grande experiência no mercado de trabalho e formações específicas para trazer aos alunos as necessidades reais solicitadas dos profissionais de Segurança da Informação;
- Recursos bibliográficos disponíveis na biblioteca da FIAP;
- Unidades Curriculares com conteúdos motivadores, altamente focados no mercado profissional e que despertem interesse no aluno;
- Atividades (*hands-on*) desenvolvidas no laboratório específico do curso, integrando em um único laboratório várias matérias de um mesmo semestre a fim de possibilitar situações de rápido raciocínio e tomada de decisões a fim de solucionar problemas.

Para dar suporte à metodologia adotada, são disponibilizados recursos e executadas ações como:

- Laboratórios de computação gerais e específicos, biblioteca, acesso à internet e recursos pedagógicos usuais;
- Reuniões pedagógicas com a participação do corpo docente, nas quais são analisados e discutidos os planos tático e operacional de ensino, com objetivo de garantir a interdisciplinaridade do curso;
- Criação de Grupo de Estudos, coordenados por um docente do curso, com o principal objetivo de promover discussão e pesquisas em áreas específicas de interesse do curso;
- Cursos de extensão extraclasse para que os alunos possam manter-se atualizados sobre as novas tecnologias e tendências do mercado de trabalho;
- Divulgação do curso por meio de diversos meios de comunicação (jornais, rádio, televisão e internet), palestras realizadas em colégios de Ensino Médio para mostrar a área de atuação do profissional de computação;
- Análise periódica da bibliografia disponível na biblioteca para que haja atualização constante do acervo em relação às disciplinas ministradas.

Uma importante atividade desenvolvida ao longo do curso é a montagem de um grupo de até cinco alunos que devem atuar como uma empresa. Todas as propostas elaboradas pelo grupo devem ser testadas no ambiente

disponibilizado pela FIAP (laboratórios específicos) e ganham, naturalmente, consistência prática, além da conceituação e fundamentação teórica.

Competências e Ferramentas

As competências desenvolvidas ao longo do MBA possibilitam, ao aluno, desenvolver-se completamente por meio de *Soft Skills* e *Hard Skills*. Nas *Soft Skills*, o estudante é levado a desenvolver as habilidades pessoais, interpessoais e comportamentais exigidas para os profissionais que atuam nos mais diversos desafios em cibersegurança.

O objetivo é preparar o aluno para se tornar um potencial gestor de profissionais que atuem em um time de cibersegurança por meio de conteúdos que irão ajudá-lo a desenvolver as habilidades interpessoais, tais como a comunicação e motivação no processo de liderança, *coaching* e *feedback* e administração de conflitos. Além disso, espera-se preparar o aluno para que ele identifique e forme equipes de alto desempenho, sendo ainda capaz de, liderando, acompanhar as mudanças constantes exigidas dentro do mundo corporativo.

Não exclusivo a uma única disciplina, o conteúdo apresentado, assim com a dinâmica oferecida em sala de aula, visa também aprimorar algumas competências como:

- **Comunicação eficaz:** o estudante é estimulado a falar em público (fazendo apresentações e questionamentos ao longo das disciplinas), defendendo seus pontos de vista junto aos demais colegas, correlacionando e fazendo analogias entre os assuntos técnicos, processos administrativos e os assuntos voltados ao negócio, para que todos consigam compreender seu ponto de vista e a importância daquele tema para as necessidades em cibersegurança;
- **Resolução de problemas:** a cada aula ministrada, novos problemas são apresentados para que que sejam indicadas e sugeridas soluções em Segurança da Informação. Para isso, estimula-se o desenvolvimento da capacidade de lidar com os problemas de forma estruturada, analisando o

contexto, estruturando o pensamento com a apresentação de soluções necessárias, sempre visando a avaliação da relação 'custo x benefício' para o negócio e, sempre que possível, expondo os riscos envolvidos, as ações necessárias, as ações já realizadas, dentre outras informações relevantes para o contexto do problema ou da questão;

- **Ética no trabalho:** o profissional que atua em segurança da informação tem acesso às mais diversas informações confidenciais e sigilosas da organização. Com isso, o aluno é levado a compreender que as informações a que tiver acesso devem ser utilizadas somente para desempenhar suas atividades corporativas;
- **Proatividade:** ciente de que a área de cibersegurança evolui muito rapidamente por meio de novas legislações sancionadas, novos *frameworks* e ferramentas técnicas, novas vulnerabilidades são detectadas a cada dia, devendo o estudante ser capaz de reconhecer como deve se destacar nessa área, precisando dedicar-se também ao auto estudo, ao autodesenvolvimento, entendendo quais são as mudanças que estão ocorrendo em Segurança da Informação e reconhecendo como aplicar seus conhecimentos nesse ambiente, antecipando-se a possíveis problemas e/ou incidentes na área;
- **Gestão do tempo:** o estudante é levado a estabelecer métodos e ferramentas para a devida gestão de seu tempo, caso contrário, as atividades não serão concluídas, cronogramas serão atrasados e/ou atividades serão realizadas de forma incompleta ou não atendendo às expectativas do negócio. O aluno é levado a melhorar a gestão do tempo por meio dos desafios, trabalhos e atividades que são apresentados ao longo das diversas disciplinas. Dessa forma, o profissional é levado a conciliar o tempo dispendido aos estudos, em seu trabalho e junto às demais atividades concorrentes;
- **Trabalho em equipe:** o aluno é levado a entender sua relação e suas atividades em comparação às demais áreas diretas ou indiretamente relacionadas à cibersegurança. Um dos desafios deste modelo de trabalho é apresentado por meio da estruturação da Política de Segurança da

Informação, que exigirá esforços com o envolvimento de diversas áreas da empresa, alcançando níveis hierárquicos superiores, como o conselho de administração de uma grande corporação;

- **Liderança:** o gestor em cibersegurança pode ter diversos profissionais para liderar, gerenciar e delegar funções, o que exige uma postura de liderança perante a equipe. O estudante é levado a entender seu papel como um potencial gestor de equipes, precisando ter a devida postura de liderança, uma vez que conduzirá ações relevantes para o negócio, vindo a participar de reuniões estratégicas;
- **Negociação:** A capacidade de negociação é de fundamental importância para um profissional da área de cibersegurança, uma vez que, frequentemente, estará apresentando e defendendo pontos de vista relacionados à proteção de dados e informações, devendo convencer os colaboradores, gestores e a diretoria acerca da importância que o tema tem para a organização.

Dentro desse processo, as *Hard Skills* serão exigidas desse profissional por meio do desenvolvimento relacionado às competências e habilidades técnicas do aluno. No caso da área de cibersegurança, diversas disciplinas exigem o desenvolvimento profissional quanto ao conhecimento das normas, leis, boas práticas, além de conhecimentos visando o domínio de tecnologias e processos que envolvam tecnologias *firewall*, antivírus, *backup* em sistemas, desenvolvimento seguro, realização de análise de vulnerabilidade, investigação de crimes informáticos e demais outros assuntos tratados em diversas ementas.

Matriz Curricular

MATRIZ CURRICULAR – Trilha Red Team Operations	
Introdução à Cibersegurança	20h
CyberSecurity Strategy & Governance	20h
Cyberlaw: Tecnologia, Inovação e Segurança	40h

Fundamental Skills	40h
Cyber Intel & Social Engineering	40h
Red Team Operations	60h
Welcome to Offensive Security	40h
Advanced Exploitation	50h
Cloud Computing Security, DevOps e DevSecOps	20h
Purple Team Exercise	10h
Empreendedorismo e Inovação	20h
CARGA HORÁRIA TOTAL DO CURSO	**360h**

MATRIZ CURRICULAR – Trilha Blue Team Operations	
Introdução à Cibersegurança	20h
CyberSecurity Strategy & Governance	20h
Cyberlaw: Tecnologia, Inovação e Segurança	40h
Fundamental Skills	40h
Cyber Intel & Social Engineering	40h
Threat Hunting & Incident Response	30h
Forensics Fundamentals	40h
Malware Analysis	40h
Network Forensics	10h
Cloud Computing Security, DevOps e DevSecOps	20h
Purple Team Exercise	10h
Empreendedorismo e Inovação	20h

CARGA HORÁRIA TOTAL DO CURSO	360h

Ementas e Bibliografias

Disciplina	Introdução à Cibersegurança

Ementa

Esta disciplina tem o objetivo de apresentar e discutir o panorama atual da cibersegurança em empresas e em relação ao mercado de trabalho no Brasil e no Mundo. Busca-se conceituar os elementos básicos que compõem a dinâmica da cibersegurança, discutindo, no cenário atual, as ameaças a empresas e governos, bem como sua aplicação nos negócios.

Tratando-se de uma disciplina relacionada à abertura e ao fechamento do curso, espera-se que o aluno possa trazer suas percepções preliminares atreladas ao universo da cibersegurança, assim como trazer suas percepções ao término deste curso.

Bibliografia Básica

BAARS, H., HINTZBERGEN, K., HINTZBERGEN, J., SMULDERS, A. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.** Rio de Janeiro: Brasport, 2018.

CAPRINO, W. **Trilhas em Segurança da Informação**. Rio de Janeiro: Brasport, 2015.

JUNIOR, A. K. **Sistemas de segurança da informação na era do conhecimento**. [s.l.]. Contentus, 2020.

Bibliografia Complementar

ROSSETE, C. A. **Segurança e Higiene do Trabalho**. São Paulo: Pearson, 2015.

Disciplina	Network Forensics

Ementa

Redes de computadores e a internet. Modelos de referência OSI e TCP/IP. Redes LAN, MAN, WAN e PAN, Conceitos básicos de transmissão de dados. Configuração de um Sistema Operacional de Rede. Conceitos do Endereçamento IPv4 e IPV6. Tecnologias de Cabeamento. Tecnologia Ethernet e sua evolução. Conceitos básicos de segurança física e lógica. Conceitos de cloud.

Conhecer os princípios básicos de funcionamento das redes de computadores, sua finalidade, dispositivos, tecnologias de cabeamento, segurança da informação e os princípios do Endereçamento IPv4; elaborar um ambiente de infraestrutura para hospedagem de uma aplicação web; desenvolver conceitos para infraestrutura em nuvem.

Bibliografia Básica

DA SILVA, C. F. **Projeto estruturado e gerência de redes**. São Paulo: Contentus, 2020.

FILIPETTI, M. A. **CCNA 6 Guia Completo de Estudo**. São Paulo: Visual Books, 2017.

KUROSE, J. F., ROSS, K. W. **Redes de computadores e a Internet**. 8°ed. São Paulo: Editora Pearson,2021.

Bibliografia Complementar

BASSO, D. E. **Administração de Redes de Computadores.** São Paulo: Contentus, 2020.

DE GRACIA, Y., I. **Geografia das Redes**. São Paulo: Contentus, 2021.

GUERRA, A. R. **Redes Sem Fio**. São Paulo: Contentus, 2020.

ROHLING, L. J. **Segurança de redes de computadores**. São Paulo: Contentus,2021.

TANENBAUM, A. S. **Organização estruturada de computadores**. 6ª ed. São Paulo: Pearson Prentice Hall, 2013.

Disciplina	**Fundamental Skills**

Ementa

Testes e Documentação. Fundamentos de Segurança da Informação (SI) e Cibersegurança. Administração do tempo na gestão de projetos. Estimativa de custos e orçamento. Conhecimento básico de gestão de riscos e vulnerabilidades. Crescente ameaça de fraudes e ataques cibernéticos ao ambiente operacional. Como evitar ser hackeado. Necessidade de inovação na postura de Cibersegurança.

Conhecer, compreender e desenvolver conhecimentos referentes aos processos de gestão de projetos, com foco em cibersegurança. Analisar o impacto da gestão de projetos no desenvolvimento das empresas, observando a importância do escopo, da administração do tempo, dos custos, riscos e vulnerabilidades. Promover a capacidade do estudante de identificar a importância da aplicação de técnicas de gestão de projetos às peculiaridades da cibersegurança, considerando o papel do ser humano como um elo forte e ao mesmo tempo fraco no sucesso.

Bibliografia Básica

BUENO, G. **Gestão de projetos para cibersecurity**. São Paulo: Editora Contentus, 2020.

RICHARD, A. C.; ROBERT, K. K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito.** Rio de Janeiro: Editora Brasport, 2015.

STALLINGS, W. **Criptografia e Segurança de Redes Princípios e Práticas**. São Paulo: Pearson, 2015.

Bibliografia Complementar
BERTHOLDI, J. **Cooperação internacional e o combate aos cibercrimes**. São Paulo: Editora Contentus,2020. DE ARAÚJO, S. **Ethical Hacker**. São Paulo: Editora Contentus,2020. JÚNIOR, A. K. **Desafios estratégicos para a segurança e defesa cibernética**. São Paulo: Editora Contentus,2020. SANTIAGO, L. A. de O. **Sistema de segurança e defesa cibernética nacional**. São Paulo: Editora Contentus,2020. STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 6a São Paulo: Editora Pearson, 2015.

Disciplina	CyberSecurity Strategy & Governance
Ementa	
Apresentar e discutir aspectos relacionados à estratégia de governança em cibersegurança. Esta disciplina tem o objetivo de preparar o egresso a compreender a gestão por meio dos processos de Governança, Risco e Compliance, além de compreender as estruturas e modelos de governança aplicados no mundo corporativo, conhecendo padrões e regulamentações como a ISO 38500, ISO 15504, ISO27001, ISO 27002, ISO 27014, COBIT 5, BACEN 4.658 e PCI-DSS. Trazendo ainda importantes conceitos sobre a natureza bimodal da Gestão dos Negócios e da TI, Sourcing de Serviços de Segurança da Informação, OPBOK – Outsourcing Professional Body of Knowledge e RFP – Processo, Estrutura, Seleção, Negociação e Contratação de Serviços SI.	
Bibliografia Básica	
BAARS, H., HINTZBERGEN, K., HINTZBERGEN, J., SMULDERS, A. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018.	

BLOK, M. **Compliance e governança corporativa.** 3ª Ed. Rio de Janeiro: Freitas Bastos, 2020.

JOÃO, B. N. **Tecnologia da informação gerencial**. São Paulo: Pearson, 2015.

MANOEL, S. da S. **Governança de Segurança da Informação.** Como criar oportunidades para seu negócio. Rio de Janeiro: Brasport, 2014.

OLIVEIRA, B. S. de. **Métodos Ágeis e Gestão de Serviços de TI**. Rio de Janeiro: Brasport, 2018.

STATDLOBER, J. **Gestão do Conhecimento em Serviços de TI**: Guia Prático – Base de conhecimento para atendimento a usuários e clientes. Rio de Janeiro: Brasport, 2016.

TAMMENHAIN, A. C. **Gestão de operações de segurança: estratégia e tática**. Curitiba: Intersaberes, 2020.

Bibliografia Complementar

FROTA, A. **Globalização e governança internacional: fundamentos teóricos**. Curitiba: InterSaberes, 2017.

MUNHOZ, A. S. **Fundamentos de tecnologia da informação e análise de sistemas para não analistas**. Curitiba: InterSaberes, 2017.

Disciplina	Advanced Exploitation

Ementa

Introdução a Segurança da Informação, Segurança no Ambiente Web e Mobile, Segurança em Banco de Dados, Controle de acesso e autenticação, Certificação Digital, Plano de Testes, Desenvolvimento Sustentável e Políticas de Segurança. A disciplina tem como objetivos capacitar o aluno a compreender os fundamentos da segurança da informação e a boa prática que deve ser utilizada em programação e banco de dados. Além disso, os alunos têm contato com os conceitos de controle de acesso, certificação digital, criptografia e outros tópicos da segurança da informação. Compreender, discutir, analisar e aplicar os conceitos de segurança nos mais diferentes ambientes, aprimorando os sistemas digitais de defesa e controle.

Bibliografia Básica

DUARTE, W. **Delphi para Android e iOS:** Desenvolvendo Aplicativos Móveis. Rio de Janeiro: Brasport, 2015.

GUEDES, S. **Lógica de Programação Algorítmica**. São Paulo: Pearson, 2014.

STALLINGS, W. **Criptografia e Segurança de Redes Princípios e Práticas**. São Paulo: Pearson, 2015.

Bibliografia Complementar

ASCENCIO, A. F. G. CAMPOS, E. **Fundamentos da Programação de Computadores: algoritmos, Pascal, C/C++ e Java**. São Paulo: Editora Pearson, 2007.

BONATTI, D. **Desenvolvimento de Jogos em HTML5.** Rio de Janeiro: Editora Brasport, 2014.

KUROSE, J. F. **Redes de Computadores e a Internet – Uma abordagem Top/Down**. São Paulo: Addison Wesley, 2013.

LEMAY, L.; COLBURN, R. T. **Aprenda a Criar Páginas Web com HTML e XHTML.** São Paulo: Editora Pearson, 2002.

TOCCI, R. J.; WIDMER, N. S. **Sistemas Digitais: princípios e aplicações**. São Paulo: Pearson, 2003.

Disciplina	**Cyberlaw: Tecnologia, Inovação e Segurança**

Ementa

Apresentar e discutir aspectos relacionados ao direito quanto à aplicação do mesmo à realidade corporativa, governamental e também relevante ao próprio profissional que atual em cibersegurança.

Esta disciplina tem o objetivo de preparar o egresso à tomada de conhecimento e devida interpretação aos marcos regulatórios da era digital no Brasil e no mundo, ainda preparando às questões legais atreladas à investigação dos crimes eletrônicos no ambiente corporativo (abordando assuntos como a interceptação de dados, ata notarial, ransomware e concorrência desleal).

O egresso ainda será capaz de compreender aspectos como responsabilidades civil, criminal e trabalhista, assim como regulamentos Internos em cibersegurança e temas imprescindíveis como a privacidade e proteção dados (por meio da GDPR e LGPD), assim como a aplicação do direito em inteligência artificial e IoT (Internet das Coisas) e a regulamentação das moedas eletrônicas e blockchain.

Bibliografia Básica

BUHRING, M. A.; FUHRMANN, I. R.; TABARELLI, L. **Direitos Fundamentais: direito ambiental e os novos direitos para o desenvolvimento socioeconômico**. Caxias do Sul: Educs, 2018.

COSTA, M. T. de A. **Lógica, comunicação e argumentação jurídica**. Curitiba: Intersaberes, 2021.

POLESEL, J. de O. M. **Cibersegurança, Privacidade e Proteção de Dados Pessoais**. Caxias do Sul: Educs, 2021.

Bibliografia Complementar
BLOK, M. **Compliance e governança corporativa**. Rio de Janeiro: Freitas Bastos, 2018. FERRAZ JR, T. S. **Argumentação jurídica**. São Paulo: Manole, 2016.

Disciplina	Cloud Computing Security, DevOps e DevSecOps
Ementa	
Apresentar e discutir aspectos relacionados às tecnologias baseadas em nuvem assim como as atividades relacionadas ao desenvolvimento seguro de aplicações e respectiva operacionalização destes ambientes. Esta disciplina tem o objetivo de preparar o egresso à familiarização das tecnologias atualmente utilizadas em nuvem, onde será possível identificar os distintos tipos de modelos aplicados em Cloud Computing, assim como as principais aplicações disponíveis neste ambiente. O egresso ainda será capaz de fazer a gestão de ambientes em nuvem, incluindo a gestão de custos neste ambiente. Visando atender necessidades normativas e regulatórias existentes no mercado em cibersegurança, o egresso será levado a identificar e compreender aspectos relacionados ao desenvolvimento seguro de sistemas (*Security Development*) e deverá ser preparado para conhecer as necessidades para a migração do ambiente tecnológico *On Premisses* para ambiente em *Cloud*. O egresso compreenderá as atribuições e responsabilidades quanto à atuação do profissional denominado DevOps e DevSecOps, responsável pelo desenvolvimento, operação e respectivamente a cibersegurança deste ambiente.	
Bibliografia Básica	
JUNIOR, A. K. **Computação em Nuvem**. Curitiba: Contentus, 2020. LEE, V. **Aplicações Móveis: arquitetura, projeto e desenvolvimento**. São Paulo: Pearson, 2005.	

OLIVEIRA, B. S. de. **Métodos Ágeis e Gestão de Serviços de TI**. Rio de Janeiro: Brasport, 2018.

ROSE, C. A. F. De. **O que é esta tal de nuvem e o que pode fazer por você?** Rio Grande do Sul: EdiPUC-RS, 2020.

VERAS, M. **Computação em Nuvem**. Rio de Janeiro: Brasport, 2015.

Bibliografia Complementar

STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 6ª. Ed. São Paulo: Pearson, 2015.

Disciplina	**Red Team Operations**

Ementa

Este módulo do curso tende a demonstrar aos alunos os princípios da segurança da informação, assim como entendimento da engenharia social como uso de ferramenta para obtenção de informações. Além destes itens principais também é passado aos alunos toda a parte prática referente a segurança de sistema operacionais e teste de tentativa de invasão.

Aplicar engenharia social; criar e gerenciar contêineres; entender os ataques à servidores; explorar vulnerabilidades nos protocolos da camada OSI; gerenciar ambientes colaborativos para desenvolvimento. Elaborar relatórios das vulnerabilidades identificadas.

Bibliografia Básica

ARAUJO, S. **Ferramentas hackers: exploração de vulnerabilidades**. São Paulo: Editora Contentus,2020.

ARAÚJO, S. **Ethical hacker**. São Paulo: Editora Contentus,2020.

WEIDMAN, G. **Testes de invasão: uma introdução prática ao hacking**. São Paulo: Novatec Editora, 2018.

Bibliografia Complementar
BUENO, G. **Gestão de projetos para cibersecurity**. São Paulo: Contentus,2020. DE MATTOS, M. S. **Núcleo de combate aos cibercrimes**. São Paulo: Contentus,2020. HOGLUND, G. **Como quebrar códigos: a arte de explorar e proteger software**. São Paulo: Pearson Makron Books, 2006. MARTINS, C. S. **Cibercrime e as organizações criminosas**. São Paulo: Contentus,2020. RIBEIRO, P. B. **Guerra cibernética: cenário mundial de defesa e segurança**. São Paulo: Editora Contentus, 2020.

Disciplina	Welcome to Offensive Security
Ementa	
Apresentar e discutir aspectos relacionados às ferramentas e técnicas utilizadas em processos de análise de vulnerabilidade e testes de intrusão. Esta disciplina tem o objetivo de preparar o egresso à familiarização das metodologias e tecnologias atualmente utilizadas em cibersegurança relacionados à análise de vulnerabilidade incluindo padrões como NIST 800-155, OSSTMM e OWASP. As etapas de identificação de fragilidades são levadas ao conhecimento e prática do egresso, incluindo as etapas de coleta de informações (*footprint* and *fingerprint*) com Google Hacking, Engenharia Social, análise, exploração e mitigação de vulnerabilidades com a capacitação do egresso para a preparação do relatório de vulnerabilidade técnica. O egresso ainda conhecerá tecnicamente ameaças como o Ransomware, identificando potenciais medidas que evitem o atingimento de negócios nesta e demais outras ameaças atreladas às fragilidades técnicas.	

Bibliografia Básica
CAPRINO, W. **Trilhas em Segurança da Informação**. Rio de Janeiro: Brasport, 2015. FRAGA, B. **Técnicas de invasão: Aprenda as técnicas usadas por hackers em invasões reais.** São Paulo: Labrador, 2019. HOGLUND, G., MCGRAW, G. **Como Quebrar Códigos: A arte de explorar (e proteger) software**. São Paulo: Pearson, 2005. STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 4ª. Ed. Pearson, 2007.
Bibliografia Complementar
VERAS, M. **Computação em Nuvem**. Rio de Janeiro: Brasport, 2015.

Disciplina	Malware Analysis
Ementa	
Introdução a malwares; Criação de malwares na prática; Introdução a análise de malwares; Análise de malwares na prática; Tratamento de incidentes; Tecnologias utilizadas na batalha contra os malwares; Tratamento de incidentes e defesa contra malwares na prática. Compreender o que são malwares, como funcionam e se propagam; Realizar a criação de um malware para compreender na prática o seu funcionamento; Compreender as técnicas utilizadas para analisar malwares; Realizar a análise prática de diferentes tipos de malwares utilizando diferentes técnicas para ser capaz de criar estratégias de defesa para a empresa; Compreender as fases do tratamento de um incidente para ser capaz de direcionar a empresa durante um incidente de segurança cibernética.	

Bibliografia Básica
ARAUJO, S. **Ferramentas hackers: exploração de vulnerabilidades**. São Paulo: Editora Contentus,2020. JORGE, H. V. N. **Crimes Cibernéticos**. 3°ed. Rio de Janeiro: Editora Brasport, 2021. TANENBAUM, A. S. **Redes de Computadores.** 5ª ed. Rio de Janeiro: Campus, 2011.
Bibliografia Complementar
DE MATTOS, M. S. **Núcleo de combate aos cibercrimes.** São Paulo: Contentus, 2020. NETO, A. O. K. **Responsabilidade civil: cibercrimes**. São Paulo: Contentus,2020 STALLINGS, W. **Criptografia e Segurança de Redes Princípios e Práticas**. São Paulo: Pearson, 2015. STALLINGS, W. **Criptografia e segurança de redes**. 6°ed. São Paulo: Pearson,2020. TERADA, R. **Segurança de dados.** São Paulo: Editora Blucher, 2008

Disciplina	Forensics Fundamentals
Ementa	
Apresentar e discutir aspectos relacionados às ferramentas e técnicas utilizadas em processos investigativos em meios informáticos. Esta disciplina tem o objetivo de preparar o egresso à familiarização das tecnologias atualmente utilizadas em cibersegurança relacionados aos processos investigativos, onde são apresentados os padrões periciais como a ISO 27037 e RFC 3227.	

As etapas do processo investigativo são apresentadas ao egresso, como os processos de identificação, coleta e preservação, análise e apresentação de evidências digitais em dispositivos informáticos, por meio de laudo pericial.

O egresso ainda conhecerá ferramentas que permitem a realização de engenharia reversa, assim como a perícia em dispositivos móveis.

Bibliografia Básica

BARRETO, G.; WENDT, E.; CASELLI, G. **Investigação Digital em fontes abertas.** Rio de Janeiro: Brasport, 2017.

JORGE, H. V. N. **Investigação Criminal Tecnológica** - **Volume 1**. Rio de Janeiro: Brasport, 2018.

JORGE, H. V. N. **Investigação Criminal Tecnológica - Volume 2.** Rio de Janeiro: Brasport, 2018.

KARSPINSKI, M. T. **Arquitetura contra o crime**: prevenção, segurança e sustentabilidade. Curitiba: InterSaberes, 2016.

MARTINS, D. **Investigação cibernética**. São Paulo: Contentus, 2020.

MATTOS, M. S. de. **Núcleo de combate aos cibercrimes**. São Paulo: Contentus, 2020.

Bibliografia Complementar

SERAFIM, A. de P. **Psicologia e práticas forenses**. São Paulo: Manole, 2018.

Disciplina	**Cyber Intel & Social Engineering**

Ementa

Apresentar e discutir aspectos relacionados às técnicas e práticas utilizadas em processos de inteligência e espionagem.

Esta disciplina tem o objetivo de preparar o egresso à familiarização das técnicas e tecnologias atualmente utilizadas em cibersegurança relacionados aos processos de inteligência, contra inteligência, terrorismo, contraterrorismo, espionagem, contraespionagem e engenharia social.

O egresso será levado a conhecer a doutrina da Inteligência no Brasil (ABIN), assim como a respectiva fonte de informações como fontes humanas, abertas, de imagens e de sinais.

O egresso ainda conhecerá na prática, a aplicação da segurança em dispositivos pessoais e redes sociais.

Bibliografia Básica

BARRETO, G.; WENDT, E.; CASELLI, G. **Investigação Digital em fontes abertas**. Rio de Janeiro: Brasport, 2017.

CAROTA, J. C. **Inteligência empresarial.** Rio de Janeiro: Freitas Bastos, 2018.

MATTOS, M. S. de. **Núcleo de combate aos cibercrimes**. São Paulo: Contentus, 2020.

TAMMENHAIN, A. C. **Gestão de operações de segurança**: estratégia e tática. Curitiba: Intersaberes, 2020.

WOLOSZYN, A. L. **Guerra nas sombras: os bastidores dos serviços secretos internacionais**. São Paulo: Contexto, 2013.

Bibliografia Complementar

CAMARGO, P. S. de. **Liderança e linguagem corporal: técnicas para identificar e aperfeiçoar líderes.** São Paulo: Summus, 2018.

MOREIRA, A. E. **Estratégia empresarial e cross selling**. São Paulo: Contentus, 2020.

Disciplina	**Threat Hunting & Incident Response**

Ementa

Apresentar e discutir aspectos relacionados às técnicas e práticas utilizadas em processos de resposta a incidentes em cibersegurança

Esta disciplina tem o objetivo de preparar o egresso à familiarização das técnicas e tecnologias atualmente utilizadas em cibersegurança relacionados aos processos de resposta a incidentes, por meio de conhecimento dos times de

resposta a incidentes denominados CSIRTs, conhecendo a composição destes times no Brasil e no Mundo. O egresso será familiarizado ao processo de estabelecimento e manutenção de um CSIRT, assim como a prática em processo de detecção, triagem, notificação, análise e resposta de um incidente.
Bibliografia Básica
BARRETO, G.; WENDT, E.; CASELLI, G. **Investigação Digital em fontes abertas.** Rio de Janeiro: Brasport, 2017. CAMPOS, J.; MARTINS, F. **Bombeiro civil, defesa civil e gerenciamento de desastres e crises**. Curitiba: InterSaberes, 2017. CAPRINO, W. **Trilhas em Segurança da Informação**. Rio de Janeiro: Brasport, 2015.
Bibliografia Complementar
THE HONEYNET PROJECT. Conheça seu inimigo. São Paulo: Pearson, 2002.

Disciplina	**Purple Team Exercise**
Ementa	
Apresentar e discutir aspectos relacionados às técnicas e práticas utilizadas em processos de criação de exercícios de Purple Team no contexto de times de Segurança da Informação. Esta disciplina tem o objetivo de preparar o egresso à familiarização das técnicas e tecnologias atualmente utilizadas em Purple Team, sendo introduzido o conceito de segurança cibernética, sendo ainda apresentado os controles de segurança aplicados às infraestruturas críticas de comunicação, saúde, transporte, energia, economia e demais infraestruturas. O egresso ainda será familiarizado aos aspectos de segurança aos componentes críticos dispostos no ciberespaço, assim como os aspectos relacionadas às	

infraestruturas tecnológicas que contribuem às questões de conflito em ambiente virtual. O egresso será preparado para modelar exercícios de ataque e defesa cibernética, assim como identificar e preparar o plano estratégico para proteção cibernética. Serão ainda apresentados os órgãos e departamentos de defesa cibernéticos, onde será possível vivenciar na prática simulação destes processos por meio de jogos de guerra (War Games).
Bibliografia Básica
CLARKE, R. A., KNAKE, R. K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015. RIBEIRO, P. B. **Guerra cibernética: cenário mundial de defesa e segurança**. São Paulo: Contentus, 2020. SUN, T. **A arte da guerra**. 4ª ed. Petrópolis: Vozes, 2011. VISACRO, A. **A guerra na Era da Informação**. São Paulo: Contexto, 2018.
Bibliografia Complementar
WOLOSZYN, A. L. **Guerra nas sombras: os bastidores dos serviços secretos internacionais**. São Paulo: Contexto, 2013.

Disciplina	**Empreendedorismo e Inovação**
Ementa	
Introdução ao empreendedorismo inovador e aos modelos de criação de novas empresas emergentes. Apresentação de métodos e ferramentas para ideação. Técnicas e ferramentas de validação de negócios e análise de mercado. Noções sobre intraempreendedorismo e modelos internos de inovação. Modelos empreendedores para criação, testes e evolução de propostas de valor.	

Modelos e ferramentas de prototipação de negócios. Noções sobre ecossistemas empreendedores e de inovação. Técnicas de storytelling e formatação de apresentações (*pitch*).
Bibliografia Básica
CARVAJAL J. C. J., SANCHEZ, W. M., et. al. **Empreendedorismo, Tecnologia e Inovação.** São Paulo: Editora Livrus, 2015. OSTERWALDER, A.; PIG, Y. **Business Model Generation - inovação em modelos de negócios.** Rio de Janeiro: Alta Books, 2011. RIES, E. **A startup enxuta: como os empreendedores atuais utilizam a inovação contínua para criar empresas extremamente bem-sucedidas**. São Paulo: Lua de Papel, 2012.
Bibliografia Complementar
BESSANT, J. R.; TIDD, J. **Inovação e empreendedorismo**. Porto Alegre: Bookman, 2009. COZZI, A.; JUDICE, V.; DOLABELA, F. **Empreendedorismo de base tecnológica spin-off: criação de novos negócios a partir de empresas constituídas**, **universidades e centros de pesquisa**. Amsterdã: Elsevier Academic, 2012. DRUCKER, P. F. **Inovação e espírito empreendedor (entrepreneurship): prática e princípios.** São Paulo: Cengage Learning, 2014. GOVINDARAJAN, V.; TRIMBLE, C. **Beyond the idea how to execute innovation in any organization.** Nova York: ST. Martin's Press, 2013.

Design Experience FIAP

Questões relacionadas ao cuidado do conteúdo disponibilizado aos nossos alunos exigem o devido zelo por meio de uma cuidadosa curadoria que avalia a relevância do material apresentado às diversas mídias e a satisfação quanto à experiência positiva do resultado desse trabalho, que é o aprendizado,

fixação do conteúdo e garantia quanto à identificação dos valores levados em nível pessoal e profissional.

A sequência dos conteúdos ministrados em todas as aulas obedece a um encadeamento lógico que preza a construção do conhecimento, visando garantir aos alunos excelência em experiência, independente dos meios pelos quais o conteúdo é apresentado e discutido.

Essa experiência ainda se amplifica pelo fato de considerarmos, em nosso corpo docente, profissionais com conhecimento e experiência acadêmica, que apresentam suas respectivas vivências aplicadas no mundo real, pois estes são também profissionais atuantes no mercado de trabalho, atendendo a diversas empresas e atuações no mercado nacional e estrangeiro.

Isso nos permite trazer conteúdos exclusivos que se somam às melhores práticas e metodologias, criando uma experiência única aos estudantes. Para isso, contamos com formadores de opinião sobre os diversos segmentos relacionados à cibersegurança e áreas correlatas.

A garantia de alcance dos objetivos do curso pelos alunos é devidamente oferecida por meio de avaliações concisas, justas e devidamente detalhadas ao discente, permitindo que os objetivos sejam atingidos e bem identificados, assim como as probabilidades de melhorias alcançáveis, quando o potencial aprimoramento desse profissional é visado.

Processo de Avaliação

O processo didático-pedagógico no qual o aluno estará inserido é plenamente comprometido com a interdisciplinaridade, com o desenvolvimento do espírito científico, com a formação de sujeitos autônomos e cidadãos e com a flexibilidade na disponibilização das unidades curriculares, não havendo também pré-requisitos para o aluno iniciar qualquer disciplina.

O curso é anual e o sistema de avaliação é dividido entre **atividades a distância (AD)** e **atividades presenciais obrigatórias (APO)**, totalizando 100 pontos. Para aprovação, o aluno deve alcançar nota superior ou igual a 70 pontos.

As **atividades a distância (AD)** representam 60 pontos (60%) da nota final, e são compostas por avaliações dissertativas e práticas, realizadas individualmente e/ou em grupo, por meio da plataforma FIAP ON. Para o desenvolvimento de atividades práticas a distância, serão disponibilizadas duas formas de acesso:

- O aluno utilizar o próprio computador, pois o conteúdo disponibilizado contém o passo a passo de instalação dos softwares necessários, e que são gratuitos;
- O aluno utilizar, presencialmente, no horário de sua preferência, as estruturas de laboratórios da FIAP, que contam com os softwares necessários para as práticas.

As **atividades presenciais obrigatórias (APO)** representam 40 pontos (40%) da nota final e são compostas por avaliação objetivas, projetos e dinâmicas, pautados na relação prática e teórica, envolvendo todas as unidades curriculares abordadas até a data do encontro que ocorre ao final do curso, sendo assim, tais atividades integram e avaliam todos os conhecimentos e habilidades das disciplinas apresentadas e, por esta razão, os 40 pontos aqui mencionados são usados para compor essas disciplinas (quarenta para cada uma delas).

A respeito das notas finais:

- Caso o aluno obtenha a nota inferior a 70 pontos, estará automaticamente reprovado na disciplina e deverá realizar uma avaliação substitutiva, de forma a substituir a nota deficitária. A avaliação é realizada a distância em formato digital, entregue no Ambiente Virtual de Aprendizagem (AVA).

Projeto Integrador – Startup One MBA FIAP ON

O Startup One é integrado aos cursos por meio da disciplina de empreendedorismo e inovação, ministrada em todos os cursos de MBA da FIAP. Para a modalidade do MBA online (FIAP ON), os conteúdos serão disponibilizados em três (3) fases/períodos distintos do curso, além de encontros on-line ao vivo para mentorias individuais e em grupo com intuito de apoiar os alunos na jornada. O *framework* da disciplina, composto por seu conteúdo, materiais e dinâmicas, foram desenvolvidos com a utilização dos conceitos de *Design Thinking* e *Lean Startup*, aplicando conhecimentos específicos de acordo com a necessidade e respeitando os limites da aplicação de cada método, dado a carga horária.

A disciplina caracteriza-se pela orientação aos alunos de MBA para elaborarem, ao longo do curso, um projeto (plano de negócio prático) para a criação de uma Startup, configurando o trabalho final do curso. Este trabalho final (ou projeto) substitui o TCC (Trabalho de Conclusão de Curso) e é entregue ao final do curso, podendo ser executado em grupos de até quatro (4) alunos.

O projeto pode ser inscrito no Startup One – ST1, competição que ocorre ao final de cada ciclo do MBA FIAP.

Objetivos da disciplina:

- Conceituar os elementos básicos do empreendedorismo;
- Discutir as características principais dos empreendedores, bem como sua aplicação na criação de startups;
- Capacitar o aluno a entender a jornada de um empreendedor, desde a identificação e validação do problema, desenvolvimento da solução,

criação e validação do protótipo, análise financeira do empreendimento e apresentação resumida da solução (pitch).

Estrutura

Os conteúdos dos cursos MBA on-line são separados em fases, onde cada uma tem um propósito e direcionamento. Os conteúdos relacionados ao tema Startup também são apresentados em fases que, por sua vez, se tornam disponíveis para os alunos em três (3) momentos dentro do curso. São no total 3 fases, 6 capítulos, 6 mentorias em grupo/aula ao vivo, 6 atividades intermediárias que não possuem nota (apenas feedback), e uma atividade final (entrega final do Startup One – TCC) organizados da seguinte forma:

STO 1 – Fase 1 do Startup One MBA ON

Conteúdos da fase 1

Capítulo 0 – Welcome to Startup One

Capítulo de instruções iniciais e boas-vindas ao Startup One, modelo integrado de desenvolvimento do trabalho final dos MBAs da FIAP. É baseado na metodologia de Project Base Learning e busca a convergência entre as disciplinas, capacidades e atitudes dos alunos para estimular suas jornadas de aprendizado de maneira inovadora.

Capítulo 1 – Introdução ao empreendedorismo inovador

Este capítulo trata a evolução das tecnologias exponenciais e o fato de que o empreendedorismo vem passando por uma transformação social nos últimos anos e as startups de base tecnológica se tornaram uma opção atraente como alternativa de investimento e carreira, para empreendedores e até mesmo para grandes empresas. Por meio de processos bem definidos e estruturados, e somado à flexibilidade e a um crescimento rápido e contínuo, as startups contribuem significativamente com o desenvolvimento econômico.

Capítulo 2 – Como nascem as boas ideias

Neste capítulo, serão relatadas histórias de startups bem-sucedidas, o padrão que encontramos em boas ideias, tipos de análise, cuidados que se deve tomar ao empreender e entrar em um novo mercado, o que é disfunção e como é a jornada do empreendedor.

Atividades da fase 1

Atividade 1 – Identificando Oportunidades

Desafio e objetivo: Dar início ao projeto de startup. Nesta atividade desafiamos os alunos a buscarem identificação com áreas e segmentos de mercado para, a partir disso, identificar problemas e oportunidades deste segmento. Instruímos os alunos a buscarem ao menos três (3) grandes problemas para serem base de uma análise futura mais profunda, focada em uma pesquisa mais detalhada para compreender o problema em sua essência.

Mentorias em Grupo/Aula ao vivo (on-line)

Mentoria 1 - Aula inaugural do Startup One

Neste encontro on-line nos reunimos pela primeira vez com os alunos para contextualizar sobre o programa Startup One e ajudar nas direções iniciais dos projetos. Explicamos a jornada do Startup One, as fases e entradas de conteúdos durante o curso, as dinâmicas das mentorias em grupo/aulas ao vivo, o apoio dos professores como pontos focais do curso e agenda de mentorias individuais. Além disso, estruturamos palestras de 15 minutos com os professores sobre temas relacionados a diversos segmentos de mercado para inspirar os alunos e dar dicas de como buscar problemas de grande escala e alto impacto. Como segunda fase deste encontro, estimulamos a formação de grupos multidisciplinares entre diferentes cursos para iniciar a jornada de inovação do Startup One.

Mentoria 2 – Validar problema

Nesta mentoria o professor busca despertar nos alunos a importância da validação do problema, os desafios existentes nesta fase do negócio e dicas para não ter análises com vieses que possam gerar riscos para o projeto.

STO 2 – Fase 2 Startup One MBA ON

Conteúdos da fase 2

Capítulo 3 – Business Canvas

O início de um bom negócio começa com um rascunho do modelo de negócio. Com uma ideia levantada, agora é preciso compreender sua estruturação como negócio. Neste capítulo, o objetivo é compreender a lógica do Business Model Canvas e aplicá-lo no projeto do Startup One, permitindo registrar e comunicar decisões do projeto, bem como extrair *insights* e hipóteses para validação.

Capítulo 4 – Como testar e evoluir sua ideia de negócio

Neste capítulo, falamos sobre como validar e desenvolver as ideias nos em empresas e startups sustentáveis, o que é um MVP e quais são as abordagens e desafios na etapa inicial do empreendedor, sua escala e tração. Entre esses desafios está o da prototipação.

Atividades

Atividade 2 – Canvas

Desafio e objetivo: A partir da identificação do problema, iniciar o mapeamento de um modelo de negócio inicial, incluindo formação de equipe e suas habilidades, definição refinada do problema e do cliente, análise de tamanho do mercado, análise de concorrente, mapeamento da proposta de

valor por meio do Canvas Proposta de Valor e modelo de negócio por meio do *Business Model Canvas.*

Atividade 3 – Prototipação

Desafio e objetivo: Efetivamente tirar a ideia da solução do papel, criar um protótipo conceitual da solução por meio de ferramentas de prototipação apresentadas nos conteúdos na plataforma FIAP ON e nas aulas ao vivo, afim de validar hipóteses da solução e saber se realmente ela gera valor para os clientes.

Mentorias em Grupo/Aula ao vivo

Mentoria 3 – Canvas

Nesta mentoria, os professores trazem análises diferentes de modelos de negócio para ajudar os alunos a compreender os prós e contras de cada modelo, os riscos envolvidos de cada um deles com o objetivo de ajudar os alunos a modelarem e validações a estrutura de escala, análise de dependências de fornecedores, estruturas de custo e receita.

Mentoria 4 - Validar MVP

Nesta mentoria os professores discutem sobre estratégias de validação de hipóteses sobre a solução da startup por meio do desenvolvimento do mínimo produto viável (MVP), além de abordar detalhes sobre como garantir uma validação não tendenciosa e que por consequência garanta a evolução do projeto.

STO 3 – Fase 3 Startup One MBA ON

Conteúdos da fase 3

Capítulo 5 - Análise financeira

Este capítulo traz uma análise de projeção de resultados financeiros que precisam ser monitorados para avaliar os investimentos realizados em grandes empresas ou mesmo em startups. Além disso, apresenta a ferramenta para projetar as entradas e saídas e identificar se o modelo de negócio da nossa startup.

Capítulo 6 - Storytelling & pitches

Esse capítulo mostra como o poder de contar histórias pode auxiliar a jornada do empreendedor e o que é e como construir um bom *pitch* para a sua startup.

Atividades

Atividade 4 – Análise Financeira

Desafio e objetivo: com uma planilha modelo, realizar uma projeção financeira para compreender e validar hipóteses de negócio por meio do racional de entradas, saídas e análise de DRE projetados para 5 anos.

Atividade 5 – Pitch

Desafio e objetivo: Desenvolver um *pitch* do negócio, explicando como o problema foi identificado, o tamanho deste mercado, modelo de negócio e estrutura financeira, as validações de hipóteses do problema, modelo de negócio e solução, assim como composição de equipe e definição de *roadmap* da startup. O tempo deste *pitch* é de cinco (5) minutos e deve ser gravado e entregue em vídeo.

Atividade 6 – Entrega final (TCC)

Desafio e objetivo: Consolidar todos as entregas de atividades anteriores em um único modelo de arquivo, demonstrando todos os aspectos da jornada de desenvolvimento da startup, partindo deste a identificação do problema,

evolução do modelo de negócio, solução, validação de hipóteses, análise financeira e *pitch*.

Mentorias em Grupo/Aula ao vivo

Mentoria 5 - Financeiro

Os professores apoiam os alunos a identificar custos fixos, variáveis, linhas de produtos e serviços, precificação e projeção financeira. A partir da análise financeira, é possível identificar se o modelo de negócio e até mesmo o negócio em si pode ser promissor e escalável.

Mentoria 6 – Pitch e dicas para entrega final

Os professores ajudam os alunos a compreender como aplicar o conceito de *storytelling* na definição e apresentação de um *pitch*, a estruturar argumentos de venda e se prepararem para objeções que possam surgir durante a apresentação para uma banca. Informações sobre as expectativas da entrega final do Startup One são passadas para que os alunos consigam evoluir os projetos ao ponto em que as avaliações acadêmicas estejam de acordo com a proposta do programa.

Desafios para entrega final do projeto (TCC)

A partir da entrega final do projeto, o desempenho do grupo de alunos na disciplina Empreendedorismo e Inovação é avaliado segundo critérios comuns estabelecidos:

A ideia	
É relevante?	O problema a ser resolvido é relevante para o público-alvo?
É uma solução?	A proposta apresentada é uma solução adequada ao problema? (Considerar o protótipo apresentado)
É viável?	É viável de ser aplicada? (Considerar o ambiente do mercado)
Foi validado?	A ideia e a solução foram validadas? (Considerar as evidências apresentadas)
Aplicou o conteúdo do MBA?	O conteúdo do MBA foi aplicado durante o desenvolvimento da ideia?
Inovação e uso da tecnologia	
É inovador?	O produto ou serviço desenvolvido é inovador?
Qualidade do projeto?	O projeto foi bem detalhado e com profundidade?
Apresentação e entrega	
Entregáveis adequados?	O grupo detalhou todos os itens obrigatórios do *pitch deck*?
Qualidade do pitch?	Com Clareza/Design/Objetividade/Convencimento?
Avaliação Geral	
Qual sua avaliação geral para a solução apresentada?	

A média destes critérios, representam a avaliação acadêmica para a obtenção da nota final da disciplina, constituindo-se de obrigação legal ao final do ano letivo de MBA.

Competição Startup One

Neste mesmo formulário de avaliação do projeto final há também a possibilidade de o professor indicar ou não o projeto da Startup para a competição do Startup One. Importante ressaltar que a participação na competição não tem impacto na avaliação acadêmica realizada pelos professores. O grupo de alunos também tem a opção de não participar da competição sem nenhum prejuízo na nota da disciplina Empreendedorismo e Inovação ou do Trabalho de Conclusão de Curso (TCC). A avaliação dos projetos indicados ao “TOP30” (30 melhores projetos do ciclo) é realizada por um grupo de professores designados pela Diretoria do MBA da FIAP. Este grupo escolhe, com a utilização de critérios específicos, a seleção de trinta projetos que passarão para uma segunda fase.

Na segunda fase de avaliação, as trinta startups escolhidas internamente pela equipe de Professores FIAP são submetidas a uma banca

externa de avaliação, composta por empreendedores, investidores, gestores de empresas, parceiros e demais convidados, com o intuito de isentar a avaliação e de também submeter os alunos a uma situação mais próxima da realidade do mercado (não há influência da FIAP neste processo). Os projetos selecionados compõem o TOP10 (10 melhores projetos do ciclo) que são submetidos a uma segunda fase de avaliação, recebendo mentorias e treinamentos específicos para aprimorarem seus projetos e ficarem aptos para a apresentação do projeto (*Pitch*) para uma banca externa final que escolhe a startup ganhadora da competição.