FIAP

PROJETO PEDAGÓGICO DO CURSO

MBA EM CYBER SECURITY – FORENSICS, ETHICAL HACKING & DEVSECOPS

SUMÁRIO

ORGANIZAÇÃO DIDÁTICO-PEDAGÓGICA

Projeto Pedagógico do Curso: aspectos gerais

Contexto educacional

A FIAP está localizada na Grande São Paulo, a maior e mais importante região metropolitana do Brasil, com quase 20 milhões de habitantes, distribuídos em 38 municípios em intenso processo de evolução tecnológica. De acordo com o IBGE (2010), a região metropolitana de SP é o maior polo de riqueza nacional. A metrópole concentra a maioria das sedes brasileiras dos mais importantes complexos industriais, comerciais e, principalmente, financeiros. Esses fenômenos fizeram surgir e fixar, na cidade, uma série de serviços sofisticados, definidos pela dependência da circulação de informações. A região exibe um Produto Interno Bruto (PIB) de R$ 450 bilhões. São Paulo seria a 36ª economia mundial, se fosse um país. Sua economia é maior que a de países como Portugal (US$ 229 bilhões), Finlândia (US$ 237 bilhões) e Hong Kong (US$ 224 bilhões).

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, dos riscos mencionados, a perda de integridade de dados pode conferir, entre outros aspectos, a 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 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 a 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 alinhada a 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. Devendo ainda ser destacado em período que compreende a pandemia (Sars-CoV-2), cresce a busca por profissionais da área de cibersegurança [Valor Econômico], sendo essa uma tendência crescente ao longo dos próximos anos.

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 alto porte. O curso ainda possibilita que demais profissionais sejam preparados na atuação em Segurança da Informação, como áreas de Tecnologia de empresas, assim como áreas de apoio, como Auditoria, *Compliance* e Risco.

Sabe-se ainda que o Brasil é o sétimo país que mais gerou ciberataques no mundo, segundo pesquisa realizada em 2017, de acordo com o Relatório de Ameaças à Segurança na Internet (ISTR, na sigla em inglês), que analisa 157 países, divulgado em março de 2019 pela empresa de segurança digital Symantec. O país, que fica atrás de Estados Unidos, China, Índia, Rússia, Alemanha e Japão, é o terceiro que mais disseminou ameaças por *spam* e o quarto por *bots* (robôs virtuais) no mundo. De todos os e-mails que circulam no Brasil, 64% são *spam*, mensagem de cunho comercial não autorizada [O Globo], e contata-se que os ataques cibernéticos aumentaram com pandemia e já atingem companhias elétricas no Brasil e no mundo [Globo.com], fato noticiado em julho de 2020.

Sabe-se ainda que as leis de proteção de dados e os escândalos aparentemente intermináveis do 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 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 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.

A região metropolitana de SP é altamente industrializada, possuidora de forte atividade comercial e prestação de serviços. Sendo assim, necessita de mão de obra qualificada para o desempenho de funções na área de cibersegurança.

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 2020 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 recairá 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 em modalidade Home Office, pois diversos trabalhadores terão que conviver com o uso da tecnologia em ambiente externo ao ambiente anteriormente adotado no 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. A necessidade de o 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, a visão deste projeto pedagógico já conta com essa visão de futuro, permitindo formar hoje o profissional que irá atuar com esses desafios amanhã.

A inteligência artificial deve ainda ser 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. 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, 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 irão ocorrer 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:

Especializar profissionais nos aspectos de gestão na área de segurança da informação, propiciando condições para que desenvolvam as competências necessárias para atuar no contexto da proteção de informações nos aspectos de integridade, disponibilidade e confidencialidade. Para isso, o profissional terá oportunidade de aprofundar seus conhecimentos nos aspectos tecnológicos, legais e de gestão que abrangem os sistemas de 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.

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 desafiadores, 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 deve se 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, passos e etapas, sendo importantes para a compreensão da devida importância de cada disciplina e sua contribuição às distintas etapas da vida do profissional em cibersegurança. Cada novo conhecimento está intimamente relacionado às demais disciplinas presentes em módulos, que permitem 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 módulos 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 irá mostrar capacidade de adaptação às novas situações que constituem um desafio contínuo da área de segurança de informações. 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

O Projeto Pedagógico pressupõe, inicialmente, a elaboração dos planos de ensino tático e operacional realizados pelos professores, que são, em sua maioria, profissionais das áreas em que lecionam. Complementam os planos de ensino as atividades de extensão, pesquisa e outras atividades. Essa ação inclui a participação ativa dos alunos e professores junto à sociedade exterior ao ambiente da faculdade. Sempre que possível, inclui-se e incentiva-se a participação de empresas relacionadas ao foco do curso, seja por meio de palestras, PBLs (*Project Based Learning*), GBLs (*Game Based Learning*), oficinas e fornecimento de casos para análise e discussão no grupo.

A metodologia, na FIAP, baseia-se num modelo que privilegia o uso das novas tecnologias da informação, oferecendo aos alunos ambientes ricos em possibilidades de aprendizagem.

Os alunos são orientados não só sobre onde encontrar as informações, mas também sobre como avaliá-las, analisá-las e organizá-las, tendo em vista os objetivos pedagógicos do curso.

No modelo para o curso são disponibilizadas as unidades curriculares em um formato que privilegia a formação dos estudantes, de acordo com os objetivos do curso. A oferta das unidades curriculares é norteada para atender as competências e habilidades propostas no curso, visando sempre a flexibilização curricular, de modo que todos os conteúdos sejam contemplados no período de dois anos. Durante o ano, serão disponibilizadas as unidades curriculares correspondentes ao ano em que o aluno está matriculado, totalizando 360 horas. Tal metodologia está aderente às diretrizes para os cursos presenciais, que são:

- Os cursos devem reunir teoria e prática, sendo a construção do saber coletiva e o professor entendido como um facilitador da aprendizagem;
- Modelo de ensino organizado, no qual o aluno é considerado o centro do processo de aprendizagem e sujeito ativo de sua formação, sendo respeitado o seu ritmo de aprendizagem;

- A instituição se compromete em oferecer ao aluno, em termos de recursos, diversas possibilidades de acompanhamento, permitindo-lhe elaborar conhecimentos/saberes, adquirir hábitos, habilidades e atitudes, de acordo com suas possibilidades;
- O aprendizado se dará a partir da interação com materiais didáticos especialmente elaborados para proporcionar um ambiente adequado, sendo analisados o potencial de cada meio de comunicação/informação e a sua compatibilidade e adaptabilidade com a natureza dos cursos e características do aluno;
- Toda definição da tecnologia de comunicação a ser empregada deve estar alicerçada em um sólido modelo pedagógico, existindo a necessidade de uma equipe multidisciplinar (docentes de diversas áreas do conhecimento, pedagogos, dentre outros) capaz de produzir conhecimento coletivamente;
- O apoio docente é condição indispensável para a aprendizagem. Esse docente é um facilitador do processo de construção do conhecimento e deve estar à disposição do aluno para, junto com ele, contextualizar os conteúdos e, assim, aproximar tais conteúdos das experiências concretas desse aluno, de seus acúmulos teóricos e práticos e dos desafios com os quais ele se defronta em seu cotidiano, acompanhando-o durante todo o processo de ensino/aprendizagem.
- É essencial um processo contínuo de avaliação no que concerne:
    - Às práticas educacionais dos tutores;
    - Ao material didático;
    - Ao currículo;
    - À infraestrutura que dá suporte tecnológico, científico e instrumental ao curso; e
    - À realização de convênios e parcerias com outras instituições, empresas ou organizações.

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. Outros recursos, como aulas expositivas motivacionais, pesquisa em livros, prática em laboratórios de software, hardware e redes, projetos multidisciplinares e interdisciplinares, avaliações continuadas, cursos e treinamentos extracurriculares, participação em eventos como congressos, palestras e competições são amplamente utilizados e incentivados. A internet é, hoje, e promete ser no futuro, um grande repositório que armazena todo tipo de informação tornada pública no mundo todo. Professores e alunos são incentivados a recorrer a ela para buscar e trocar informações. A FIAP provê os recursos tecnológicos de acesso à internet (inclusive através de rede Wireless) e seus professores transmitem aos alunos as informações de forma organizada e consistente, buscando criar ambientes de aprendizagem em que os alunos são orientados, não só sobre onde encontrar as informações, mas, também, sobre como avaliá-las, analisá-las e organizá-las, tendo em vista os objetivos pedagógicos do curso.

O fato de que os alunos podem obter as informações de que necessitam fora da sala de aula, seja em suas residências ou locais de trabalho, em momentos em que tenham mais disponibilidade para o estudo, reforça o potencial oferecido pela internet. As tecnologias de acesso remoto facilitam a

comunicação dos alunos com a administração da faculdade, com a coordenação e com os professores do curso, que é enriquecida com a troca de informações que não se restringem a textos, podendo incorporar som, filmes e imagens que são transmitidos pela rede. O acesso a documentos, transferência instantânea de arquivos, comunicação via correio eletrônico, dentre outros, aumentam a eficácia do processo de aprendizagem.

Assim, a tecnologia passa a ajudar os próprios alunos a organizarem as informações de que dispõem, por meio de sites na internet, seja pelo portal da FIAP, seja pelo ambiente de aprendizagem fornecido pela FIAP para suas turmas, servindo de ponto de convergência para os seus contatos com os interessados nas informações ali disponibilizadas, aumentando significativamente o potencial de comunicação.

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-se 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;
- 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.

Desde a concepção do curso, foram e continuam sendo grandes os desafios de se trabalhar num ambiente centrado na tecnologia. Entende-se, dessa forma, que as práticas pedagógicas, realizadas sob uma reflexão crítica, pela compreensão e análise da realidade do curso e da própria instituição,

poderá projetar-se na realidade da sociedade da qual participamos. O curso ainda está projetado para integrar a realidade do profissional de mercado com as atividades acadêmicas.

Baseado no conceito de aprendizagem significativa, tudo o que é abordado em sala de aula deve ter alguma relação com a solução de problemas reais do mercado de trabalho. Dessa forma, é necessário que os alunos participem de projetos integradores que lhes permitam vislumbrar a aplicabilidade de cada conceito ministrado e analisado em sala de aula.

Os projetos que são desenvolvidos no decorrer do curso guardam grande semelhança com os aplicados no mundo corporativo. O perfil docente deve ser, portanto, formado preferencialmente por profissionais atuantes no mercado de trabalho. Com isso, fica garantida a adequação dos conceitos com a prática e a consequente capacidade de problematização por parte do corpo docente. 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.

Conexão entre os módulos e as 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, e 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.

Para os projetos desenvolvidos pelos alunos (Avaliação Multidisciplinar – AM), é sugerida a utilização de um ambiente colaborativo. Os professores funcionam como especialistas que interagem, propõem e cobram resultados dos alunos. Um professor é escolhido como gestor do projeto e fica responsável pela administração do projeto como um todo.

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 (AM), 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 específicos, com acesso permanente à Internet;
- Professores com grande experiência no mercado de trabalho e formações específicas para trazer à sala de aula as necessidades reais solicitadas dos profissionais de Gestão da Tecnologia 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 através 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;
- Utilização de recursos como projetores multimídia e computadores com acesso à Internet em todas as salas de aula.

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.

Nos laboratórios específicos do curso, os alunos conseguem, dentro de um ambiente que simula uma empresa, estabelecer o vínculo entre a teoria e a prática. A partir daí diversos exercícios são propostos, incluindo a contratação e demissão de alunos das “empresas”. Esses trabalhos fazem com que um grande laboratório de testes de soluções seja estabelecido pelos alunos, com ampla simulação de situações reais que os alunos enfrentarão no mercado de trabalho. As diversas soluções são acompanhadas pelos demais alunos do curso, promovendo o intercâmbio de informações e soluções propostas.

Com isso, o aluno consegue simular o ambiente da empresa dentro da FIAP, sob orientação dos professores. Os equipamentos disponibilizados aos alunos são de última geração e são encontrados nas organizações. O objetivo é fazer com que os alunos possam testar seus conhecimentos, inferir novas práticas e aplicar os conceitos dentro da faculdade.

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 MBA em Cyber Security conta com uma disciplina denominada Leadership Skills, que apresenta e discute aspectos relacionados à liderança e gestão de profissionais 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 em sala de aula, 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 irá conduzir 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	
Disciplina	**CH**
Introdução à Cibersegurança	08h
Innovation and Digital Transformation	20h
Financial management	16h
CyberSecurity Strategy & Governance	24h
Leadership Skills	20h
Cyberlaw: Tecnologia, Inovação e Segurança	16h
Risk Assessment	20h
Tecnologias em Cibersegurança	20h
Cloud Computing Security, DevOps e DevSecOps	20h
Physical and Environmental Security	16h
Ethical Hacking e Ransomware	24h
Data Loss Prevention	16h
Computer Forensics	20h
Inteligência e Espionagem	16h
Cybersecurity Incident Response	16h
Defesa Cibernética	20h
Business Continuity Management	20h
Inteligência Artificial & Machine Learning	16h
Critical infrastructure security	12h

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.
As aulas serão divididas em dois encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à cibersegurança.
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

GALVÃO, M. de C. **Fundamentos em Segurança da Informação**. Londres: Pearson, 2015.
JUNIOR, A. K. **Sistemas de segurança da informação na era do conhecimento**. Curitiba: InterSaberes, 2016.
CAPRINO, W. **Trilhas em Segurança da Informação**. São Paulo: Brasport, 2015.

Bibliografia Complementar

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

Disciplina	Innovation and Digital Transformation

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados à inovação e transformação digital. Busca-se conceituar os elementos básicos que compõem a dinâmica de temas como marketing digital (*Digital Marketing*), processos de identificação de *leads* e aceleração do processo de vendas em meios digitais (*SEO Inbound e Marketing Mobile*), assim como a gestão de mídias sociais, conceitos relacionados ao *Design Thinking*, análise e geração de *Insights*, desenvolvimento do tema de negócios digitais (Digital Business) e seus respectivos aspectos relacionados à inovação (*Innovation Management*), bem como sua aplicação nos negócios.
As aulas serão divididas em cinco encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados aos processos de inovação de transformação digital.

Bibliografia Básica

ZULA, G. G.; WECHSLER, S. M.; BRAGOTO, D. **Da criatividade à Inovação.** São Paulo: Papirus, 2016.
PAIXÃO, M. V. **Inovação em produtos e serviços**. Curitiba: InterSaberes, 2014.
POSSOLLI, G. E. **Gestão da inovação e do conhecimento**. Curitiba: InterSaberes, 2012.
FERREIRA JUNIOR, A. B. **Marketing digital: uma análise do mercado 3.0**. Curitiba: InterSaberes, 2015.

Bibliografia Complementar

COUTINHO, D.; FOSS, M. C.; MOUALLEN, P. S. B. **Inovação no Brasil: avanços e desafios jurídicos e institucionais.** São Paulo: Blucher, 2017.

Disciplina	Financial Management

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados à gestão financeira aplicada à cibersegurança. Busca-se capacitar o aluno a compreender a gestão financeira em cibersegurança (*Information Security Budget*), possibilitando identificar, dentre seus investimentos em ativos corporativos, o que deve ser classificado como CAPEX e OPEX, assim como o devido planejamento financeiro que possibilitará aplicação de esforços efetivos aos riscos mais significativos em cibersegurança.
As aulas serão divididas em quatro encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados aos processos de gestão financeira.

Bibliografia Básica

MEGLIORINI, E.; VALLIN, M. A. **Administração Financeira**. Londres: Pearson, 2018.
GITMAN, L. J. **Princípios de administração Financeira**. 10 ed. Londres: Pearson, 2004.
MENEGHETTI NETO, A. **Educação Financeira**. Rio Grande do Sul: EdiPUC-RS, 2014.

Bibliografia Complementar

MARQUES, J. A. V. da C. **Análise Financeira das empresas: da abordagem financeira convencional às medidas de criação de valor: um guia prático de crédito e investimento.** 2 ed. Rio de Janeiro: Freitas Bastos, 2015.

Disciplina	CyberSecurity Strategy & Governance

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados à estratégia de governança em cibersegurança. Busca-se preparar o estudante para 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.

Ainda, são abordados 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.

As aulas serão divididas em seis encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados aos processos de governança em cibersegurança.

Bibliografia Básica

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

BLOK, M. **Compliance e governança corporativa:** atualizado de acordo com a Lei Anticorrupção Brasileira (Lei 12.846) e o Decreto-Lei 8.421/2015. Rio de Janeiro: Freitas Bastos, 2017.

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

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

OLIVEIRA, B. S. de. **Métodos Ágeis e Gestão de Serviços de TI**. São Paulo:

Brasport, 2018.

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

Bibliografia Complementar

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

DALLA COSTA, A. J. **Estratégias e negócios das empresas diante da internacionalização**. Curitiba: Ibpex, 2011.

Disciplina	Leadership Skills

Ementa

Esta disciplina tem o objetivo apresentar e discutir aspectos relacionados à liderança e gestão de profissionais em cibersegurança. Busca-se preparar o aluno para tornar-se um gestor potencial de profissionais que atuem em um time de cibersegurança, por meio de conteúdos que irão desenvolver as habilidades interpessoais, tais como a comunicação e motivação no processo de liderança; *coaching* e *feedback*; administração de conflitos. Ainda, espera-se preparar o estudante para que ele possa identificar e formar equipes de alto desempenho, sendo ainda capaz de atuar liderando as mudanças constantes e exigidas dentro do mundo corporativo.

As aulas serão divididas em cinco encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados aos processos de gestão de profissionais e talentos.

Bibliografia Básica

SELMAN, J. **Liderança**. Londres: Pearson, 2018.

ESCORSIN, A. P.; WAGNER, C. **Liderança e desenvolvimento de equipes.** Curitiba: InterSaberes, 2017.

ALENCASTRO, M. S. C. **Ética empresarial na prática: liderança, gestão e responsabilidade corporativa**. Curitiba: InterSaberes, 2016.

Bibliografia Complementar

KLUYVER, C. A. de. **Estratégia: uma visão executiva**. Londres: Pearson, 2010.

Disciplina	Cyberlaw: Tecnologia, Inovação e Segurança

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados ao Direito quanto à sua aplicação na realidade corporativa, governamental e também relevante ao próprio profissional que atua em cibersegurança. Busca-se preparar o aluno para a tomada de decisões e devida interpretação dos marcos regulatórios da era digital no Brasil e no mundo. Ainda, serão discutidas as 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 estudante 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 LDPD), assim como a aplicação do direito em inteligência artificial e IoT (Internet das Coisas) e a regulamentação das moedas eletrônicas e blockchain.

As aulas serão divididas em quatro encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados aos processos legais que permeiam a cibersegurança.

Bibliografia Básica

LUZ, V. P. da. **Manual do advogado:** advocatícia prática (civil, trabalhista e criminal). São Paulo: Manole, 2016.

FERRAZ JR, T. S. **Argumentação jurídica**. São Paulo: Manole, 2016.

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

Bibliografia Complementar

BLOK, M. **Compliance e governança corporativa:** atualizado de acordo com a

Lei Anticorrupção Brasileira (Lei 12.846) e o Decreto-Lei 8.421/2015. Rio de Janeiro: Freitas Bastos, 2017.

Disciplina	**Risk Assessment**

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados à gestão de riscos em âmbito da cibersegurança. Busca-se preparar o aluno quanto aos conceitos relacionados à gestão de riscos, sendo ainda capaz de identificá-la, produzir um mapa de risco (*Risk Map*), assim como a matriz de riscos (*Risk Assessment Matrix*).

O estudante ainda será familiarizado com as melhores práticas a padrões de acordo com normas de Gestão de Riscos (ISO 31000) e Riscos em Segurança da Informação (ISO 27005), assim como melhores práticas adotadas no mercado de cibersegurança como COSO, NIST, CRAMM, ITScore, FRAP.

As aulas serão divididas em cinco encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados aos processos de gestão de riscos em cibersegurança.

Bibliografia Básica

ARAI, C. **Gestão de Riscos**. Londres: Pearson, 2015.

KAERCHER, A. R. **Gerenciamento de riscos: do ponto de vista da gestão da produção**. Rio de Janeiro: Interciência, 2016.

CCPS. **Diretrizes para segurança de processo baseada em risco**. Rio de Janeiro: Interciência, 2014.

Bibliografia Complementar

HABERFELD, S. **ALCA: riscos e oportunidades**. São Paulo: Manole, 2003.

Disciplina	Tecnologias em Cibersegurança

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às tecnologias em cibersegurança, aplicados em empresas privadas e públicas. Busca-se familiarizar a aluno com as tecnologias atualmente utilizadas em cibersegurança, assim como a aplicação dessas tecnologias dentro do ambiente corporativo, no qual o estudante será capaz de compreender a aplicação dessas tecnologias, assim como propor e readequar arquiteturas tecnológicas em cibersegurança. As tecnologias apresentadas são aplicadas às redes de computadores, sistemas e dispositivos informáticos.
As aulas serão divididas em cinco encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à adoção dessas tecnologias em cibersegurança.

Bibliografia Básica

STALLINGS, W. **Criptografia e segurança de redes:** princípios e práticas. 6 ed. Londres: Pearson, 2015.
STALLINGS, W. **Criptografia e segurança de redes.** 4 ed. Londres: Pearson, 2008.
VERAS, M. **Computação em Nuvem.** São Paulo: Brasport, 2015.

Bibliografia Complementar

JUNIOR, A. K. **Sistemas de segurança da informação na era do conhecimento**. Curitiba: InterSaberes, 2016.

Disciplina	Cloud Computing Security, DevOps e DevSecOps

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às tecnologias baseadas em nuvem, assim como as atividades relacionadas ao desenvolvimento seguro de aplicações e respectiva operacionalização desses ambientes. Busca-se familiarizar o aluno com as tecnologias atualmente utilizadas em nuvem, sendo possível identificar os distintos tipos de modelos aplicados em Cloud Computing, assim como as principais aplicações disponíveis nesse ambiente. O estudante ainda será capaz de fazer a gestão de ambientes em nuvem, incluindo a gestão de custos nesse ambiente.
Visando atender às necessidades normativas e regulatórias existentes no mercado em cibersegurança, o aluno 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 Pressises* para ambiente em *Cloud*.
Ainda, o aluno compreenderá as atribuições e responsabilidades quanto à atuação do profissional denominado DevOps e DevSecOps, responsável pelo desenvolvimento, operação e pela cibersegurança desse ambiente.
As aulas serão divididas em cinco encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à adoção de boas práticas de cibersegurança aplicáveis aos ambientes de nuvem.

Bibliografia Básica

VERAS, M. **Computação em Nuvem**. São Paulo: Brasport, 2015
LEE, V. **Aplicações Móveis: arquitetura, projeto e desenvolvimento**. Londres: Pearson, 2005
OLIVEIRA, B. S. de. **Métodos Ágeis e Gestão de Serviços de TI**. São Paulo: Brasport, 2018.

Bibliografia Complementar

STALLINGS, W. **Criptografia e segurança de redes:** princípios e práticas. 6 ed. Londres: Pearson, 2015.

Disciplina	Physical and environmental security

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos pertinentes às tecnologias relacionadas à proteção de ambientes físicos. Busca-se familiarizar o aluno com as tecnologias atualmente utilizadas em ambientes físicos, tornando-os capazes de entender os conceitos da segurança física e ambiental e respectivas legislações aplicáveis.

O estudante ainda conhecerá os dispositivos e elementos de detecção e monitoramento em segurança física e ambiental, assim como os riscos e controles em segurança físicos e ambientais (que tangem à segurança patrimonial). Ainda, serão apresentadas as melhores práticas relacionadas a esse ambiente, como estruturas de segurança física em ambiente corporativo.

As aulas serão divididas em quatro encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à adoção de boas práticas de cibersegurança aplicáveis em ambientes físicos.

Bibliografia Básica

ALMEIDA, C. A. B. de. **Tecnologias aplicadas à segurança: um guia prático**. Curitiba: InterSaberes, 2018.

AGILBERT, C. **Segurança executiva de autoridades**. Curitiba: InterSaberes, 2017.

SOUZA, C. A. **Segurança Pública: histórico, realidade e desafios**. Curitiba: InterSaberes, 2017.

Bibliografia Complementar

CARVALHO, C. F. de. **A evolução da segurança pública municipal no Brasil**. Curitiba: InterSaberes, 2017.

Disciplina	Ethical Hacking e Ransomware

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às ferramentas e técnicas utilizadas em processos de análise de vulnerabilidade e testes de intrusão. Busca-se familiarizar o aluno com as metodologias e tecnologias atualmente utilizadas em cibersegurança, relacionadas à análise de vulnerabilidade, incluindo padrões como NIST 800-155, OSSTMM e OWASP.
As etapas de identificação de fragilidades são levadas ao conhecimento e à prática do estudante, incluindo as etapas de coleta de informações (*footprint* and *fingerprint*) com Google Hacking, Engenharia Social, análise, exploração e mitigação de vulnerabilidades, além de capacitação para a preparação do relatório de vulnerabilidade técnica.
O estudante ainda conhecerá tecnicamente ameaças como o *Ransomware*, identificando potenciais medidas que evitem o atingimento de negócios a essa e demais ameaças atreladas às fragilidades técnicas.
As aulas serão divididas em seis encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à aplicação de técnicas e ferramentas, que permite a identificação de fragilidades técnicas em tecnologias e sistemas.

Bibliografia Básica

ADDISON, W. **Conheça o seu inimigo:** The Honeynet Project. Londres: Pearson, 2002.
STALLINGS, W. **Criptografia e segurança de redes:** princípios e práticas. 6 ed. Londres: Pearson, 2015.
CAPRINO, W. **Trilhas em Segurança da Informação**. São Paulo: Brasport, 2015.

Bibliografia Complementar

VERAS, M. **Computação em Nuvem.** São Paulo: Brasport, 2015.

Disciplina	**Data Loss Prevention**

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às ferramentas e técnicas utilizadas em processos de prevenção ao vazamento de dados. Busca-se familiarizar o aluno com as tecnologias atualmente utilizadas em cibersegurança, relacionadas aos processos, modelos e políticas aplicadas à classificação de informações.

Partindo do conhecimento preliminar quanto à classificação de informações, o estudante compreenderá os controles existentes que visam a proteção de informações, assim como as tecnologias de prevenção à perda de dados (*Data Loss Prevention*).

As aulas serão divididas em quatro encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à aplicação de técnicas e ferramentas que permitam a devida tomada de ações, visando evitar vazamento de dados em âmbito corporativo e governamental.

Bibliografia Básica

CAPRINO, W. **Trilhas em Segurança da Informação**. São Paulo: Brasport, 2015.

JUNIOR, A. K. **Sistemas de segurança da informação na era do conhecimento**. Curitiba: InterSaberes, 2016.

STALLINGS, W. ***Criptografia e segurança de redes*: princípios e práticas**. 6 ed. Londres: Pearson, 2015.

Bibliografia Complementar

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

Disciplina	**Computer Forensics**

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às ferramentas e técnicas utilizadas em processos investigativos em meios informáticos. Busca-se familiarizar o aluno com as tecnologias atualmente utilizadas em cibersegurança, relacionadas aos processos investigativos, em que são apresentados os padrões periciais como a ISO 27037 e RFC 3227.
As etapas do processo investigativo são apresentadas ao estudante, bem como os processos de identificação, coleta e preservação, análise e apresentação de evidências digitais em dispositivos informáticos, por meio de laudo pericial. O aluno ainda conhecerá ferramentas que permitem a realização de engenharia reversa, assim como a perícia em dispositivos móveis.
As aulas serão divididas em cinco encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à aplicação de técnicas e ferramentas que permitem a investigação em meios informáticos.

Bibliografia Básica

KARSPINSKI, M. T. **Arquitetura contra o crime: prevenção, segurança e sustentabilidade.** Curitiba: InterSaberes, 2016.
SERAFIM, A. de P. **Psicologia e práticas forenses**. São Paulo: Manole, 2014.
BARRETO, G.; WENDT, E.; CASELLI, G. **Investigação Digital em fontes abertas**. São Paulo: Brasport, 2017.

Bibliografia Complementar

YATIRAJ, S. **Quick Review of Forensic Medicine**. Nova Deli: Jaypee Brothers, 2013.

Disciplina	Inteligência e Espionagem

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às técnicas e práticas utilizadas em processos de inteligência e espionagem. Busca-se familiarizar o aluno com as técnicas e tecnologias atualmente utilizadas em cibersegurança, relacionadas aos processos de inteligência, contrainteligência terrorismo, contraterrorismo, espionagem, contraespionagem e engenharia social. O estudante será levado a conhecer a doutrina da Inteligência no Brasil (ABIN), assim como as fontes de informações, como fontes humanas, abertas, de imagens e de sinais. O aluno ainda conhecerá, na prática, a aplicação da segurança em dispositivos pessoais e redes sociais.
As aulas serão divididas em quatro encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à aplicação de técnicas relacionadas à inteligência e espionagem.

Bibliografia Básica

BARRETO, G.; WENDT, E.; CASELLI, G. **Investigação Digital em fontes abertas**. São Paulo: Brasport, 2017.
WOLOSZYN, A. L. **Guerra nas sombras: os bastidores dos serviços secretos internacionais**. São Paulo: Contexto, 2013.
CAROTA, J. C. **Inteligência empresarial**. Rio de Janeiro: Freitas Bastos, 2018.

Bibliografia Complementar

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

Disciplina	Cybersecurity Incident Response

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às técnicas e práticas utilizadas em processos de resposta a incidentes em cibersegurança. Busca-se familiarizar o aluno com as técnicas e tecnologias atualmente utilizadas em cibersegurança, relacionadas aos processos de resposta a incidentes, por meio de conhecimento dos times de resposta a incidentes denominados CSIRTs, conhecendo a composição desses times no Brasil e no mundo.

O estudante será apresentado ao processo de estabelecimento e manutenção de um CSIRT, assim como à prática em processo de detecção, triagem, notificação, análise e resposta de um incidente.

As aulas serão divididas em quatro encontros presenciais com cada turma, com a abordagem dos assuntos principais referentes à aplicação de protocolos relacionados à resposta em incidentes.

Bibliografia Básica

CAMPOS, J. F. M. **Bombeiro civil e gerenciamento de desastres e crises**. Curitiba: InterSaberes, 2017.

CAPRINO, W. **Trilhas em Segurança da Informação**. São Paulo: Brasport, 2015.

BARRETO, G.; WENDT, E.; CASELLI, G. **Investigação Digital em fontes abertas**. São Paulo: Brasport, 2017.

Bibliografia Complementar

ADDISON, W. **Conheça o seu inimigo: The Honeynet Project**. Londres: Pearson, 2002.

Disciplina	Defesa Cibernética

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às técnicas e práticas utilizadas em processos de ações de preparação e resposta em defesa cibernética. Busca-se familiarizar o aluno com as técnicas e tecnologias atualmente utilizadas em defesa cibernética, sendo introduzido o conceito de segurança cibernética, e, ainda, apresentados os controles de segurança aplicados às infraestruturas críticas de comunicação, saúde, transporte, energia, economia e demais infraestruturas.

O estudante ainda será apresentado aos aspectos de segurança dos componentes críticos dispostos no ciberespaço, assim como os aspectos relacionadas às infraestruturas tecnológicas que contribuem com as questões de conflito em ambiente virtual. O aluno será preparado para modelar ameaças cibernéticas e controles críticos, assim como identificar e preparar o plano estratégico para proteção cibernética.

Serão ainda apresentados os órgãos e departamentos de defesa cibernética, em que será possível vivenciar, na prática, a simulação desses processos por meio de jogos de guerra (War Games).

As aulas serão divididas em cinco encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à aplicação de ações de preparação e resposta em defesa cibernética.

Bibliografia Básica

VISACRO, A. **A guerra na Era da Informação**. São Paulo: Contexto, 2018.

TZU, S.; PIN, S. **A arte da guerra**. Rio de Janeiro: Vozes, 2014.

CLARKE, R. A.; KNAKE, R. K. **Guerra Cibernética**. São Paulo: Brasport, 2015.

Bibliografia Complementar

WOLOSZYN, A. L. **Guerra nas sombras: os bastidores dos serviços secretos**

internacionais. São Paulo: Contexto, 2013.

Disciplina	Business Continuity Management

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às práticas utilizadas em processos de continuidade de negócios em cibersegurança. Busca-se a familiarização do aluno com os processos atualmente utilizados em cibersegurança, relacionados aos processos de continuidade de negócios, por meio da gestão de crises e continuidade de negócios. O estudante será apresentado às melhores práticas e padrões adotados, como a ISO 22301 – Continuidade de Negócios e NIST 800-34 – Guia de Planejamento de Contingenciamento. Serão ainda apresentados protocolos de recuperação em cenários de catástrofes, assim como as tecnologias de contingenciamento e continuidade de negócios. Como processo de continuidade de negócios, serão abordados os planos, documentação e processos de *Business Continuity Management.*

As aulas serão divididas em cinco encontros presenciais com cada turma, com a abordagem dos assuntos principais referentes à aplicação de boas práticas relacionadas à continuidade de negócios em cibersegurança.

Bibliografia Básica

KLETZ, T. A. **O que houve de errado? casos de desastres em plantas de processo e como eles poderiam ter sido evitados.** Rio de Janeiro: Interciência, 2013.

CAMPOS, J. F. M. **Bombeiro civil e gerenciamento de desastres e crises**. Curitiba: InterSaberes, 2017.

LINO, A. G. H. **Proteção e defesa civil**. Curitiba: InterSaberes, 2018.

Bibliografia Complementar

NUNES, L. H. **Urbanização e desastres naturais**. São Paulo: Oficina de Textos, 2015.

Disciplina	**Inteligência Artificial & Machine Learning**

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às tecnologias e práticas utilizadas em processos de inteligência artificial. Busca-se familiarizar o aluno com os processos atualmente utilizados em cibersegurança, relacionados aos processos de inteligência artificial, em que o estudante será introduzido aos temas de I.A. e Machine Learning, conhecendo ainda as diferenças entre esses conceitos. O aluno ainda conhecerá o funcionamento do Deep Learning, método utilizado para o aprendizado de em sistemas autônimos. As aulas serão divididas em quatro encontros presenciais com cada turma, com a abordagem dos assuntos principais referentes à aplicação de boas práticas relacionadas à inteligência artificial, quando aplicados em cibersegurança.

Bibliografia Básica

LUGER, G. **Inteligência artificial**. Londres: Pearson, 2013.
MEDEIROS, L. F. de. **Inteligência artificial aplicada: uma abordagem introdutória**. Curitiba: InterSaberes, 2018.
CAROTA, J. C. **Inteligência empresarial**. Rio de Janeiro: Freitas Bastos, 2018.

Bibliografia Complementar

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

Disciplina	Critical infrastructure security

Ementa

Esta disciplina tem o objetivo de apresentar e discutir aspectos relacionados às tecnologias e práticas utilizadas em processos de proteção de infraestruturas críticas. Busca-se familiarizar o aluno com os processos atualmente utilizados em cibersegurança, relacionados aos dispositivos pessoais e correlatos, incluindo aqueles relacionados à consumerização.

O estudante ainda conhecerá técnicas e tecnologias, visando a proteção de ambientes de Big Data, IoT e sistemas embarcados, ambientes industriais (SCADA) e Ethernet Industrial. Ainda, o aluno será apresentado ao tema das criptomoedas e Bitcoin, assim como as tendências do mercado em Cibersegurança.

As aulas serão divididas em três encontros presenciais com cada turma, com a abordagem dos assuntos principais referentes à aplicação de boas práticas relacionadas à cibersegurança em infraestruturas críticas.

Bibliografia Básica

JUNIOR, A. K. **Sistemas de segurança da informação na era do conhecimento**. Curitiba: InterSaberes, 2016.

ALMEIDA, C. A B. de. **Tecnologias aplicadas à segurança: um guia prático**. Curitiba: InterSaberes, 2018.

LINO, A. G. H. **Proteção e defesa civil**. Curitiba: InterSaberes, 2018.

Bibliografia Complementar

VERAS, M. **Computação em Nuvem**. São Paulo: Brasport, 2015.

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

BROWN, T. **Design Thinking - Uma Metodologia Poderosa para Decretar o Fim das Velhas Ideias**. São Paulo, Alta Blocks, 2017.

CARVAJAL JÚNIOR, C. J, SANCHEZ, W. M, e outros. **Empreendedorismo, Tecnologia e Inovação**. São Paulo, Editora Livrus, 2015.

DYER, J; CHRISTENSEN, C. M; GREGERSEN, H. **DNA do inovador - dominando as 5 habilidades dos inovadores de ruptura**. São Paulo: HSM, 2012.

RIES, E. **A startup enxuta: como os empreendedores atuais utilizam a inovação contínua para criar empresas extremamente bem-sucedidas**. São Paulo, Editora 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. São Paulo: 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**. ST: Martin's Press, 2013.

OSTERWALDER, A., PIGNEUR, Y. **Businnes Model generation: The handbook for visionaries, game changers, and challengers**. New Jersey, Wiley 2010.

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 interação constante com esse público, recorrendo a diversos meios de comunicação disponíveis em mídias expositivas e mídias interativas, permite que a informação chegue aos alunos de forma fluida, trazendo a experiência concreta da cibersegurança, que vai além da abstração dos conceitos apresentados.

A fluidez em sala de aula traz discussões maduras sobre diversos temas, respeitando aspectos de privacidade exigidos aos casos identificados e apresentados em sala de aula, garantindo aos alunos resposta imediata às questões atuais que circundam as problemáticas em cibersegurança.

Dessa forma, o aluno não se torna apenas um receptáculo de informações, mas o real detentor do conhecimento, levando consigo elementos

sólidos para serem usados na defesa de seus respectivos pontos de vista em sua vida pessoal e profissional.

A dinâmica aplicada em sala de aula ainda permite aos alunos identificarem as diferenças humanas e pessoais, respeitando-as, garantindo um ambiente diverso, entendo os mais variados pontos de vista e os diversos cenários aos quais estamos inseridos em sociedade.

Garante-se, em sala de aula, que o conhecimento confira poder àquele que saiba usá-lo de forma adequada segundo seus propósitos. Entretanto, alerta-se também ao uso desse conhecimento segundo princípios éticos e morais, preparando o cidadão para as necessidades do uso legítimo desse conhecimento, visando o bem de toda a sociedade.

A garantia de alcance desses objetivos 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 desempenho do grupo de alunos em cada disciplina é avaliado segundo três critérios presentes no portal FIAP, disponível para os professores ao final do curso. Além destes três critérios (cuja média aritmética leva à nota da disciplina) soma-se a possibilidade do professor conferir avaliação por participação em sala de aula, permitindo ao aluno destacar-se junto aos demais colegas presentes.

As avaliações levam em consideração a qualidade dos trabalhos e não somente sua entrega. A média desses três critérios somada aos pontos de participação (facultativo) compõe, portanto, uma avaliação acadêmica para a obtenção da nota final da disciplina, constituindo-se como uma obrigação legal ao final do ano letivo de um MBA.

Na disciplina de Empreendedorismo e Inovação, há também a possibilidade de o professor indicar ou não o projeto da Startup para a competição do Startup One.

Todos os projetos (TCC – Trabalhos de Conclusão de Curso) relacionados à disciplina de Empreendedorismo e Inovação são entregues pelos alunos com o prazo médio de 30 dias após o fechamento da última aula (em data informada pela coordenação do MBA). Isso permite que haja tempo hábil de finalização de todas as iniciativas construídas durante o ano letivo. A participação na competição Startup One não é obrigatória e é totalmente facultativa, conforme decisão dos alunos e de acordo com indicação dos professores.

Caso o grupo decida participar da competição, o projeto da startup será submetido a uma avaliação inicial do professor da disciplina, que pode ou não fazer a indicação por meio de formulário de avaliação, disponível no portal da FIAP.

A avaliação dos projetos indicados no TOP30 é realizada por um grupo de professores designados pela Diretoria do MBA da FIAP. Esse grupo escolhe, com a utilização de critérios específicos, a seleção de trinta projetos que passarão para uma segunda fase.

Nessa segunda fase, as trinta startups escolhidas internamente pela equipe de professores da 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, também, de submeter os alunos a uma situação mais próxima da realidade do mercado (não há influência da FIAP nesse processo). Esses projetos submetidos à segunda fase receberão treinamento extra específico para estarem preparados para a apresentação de seus projetos à banca julgadora (*Pitch*).

Projeto Integrador - Startup One MBA FIAP

O Startup One é integrado aos cursos através da disciplina de empreendedorismo e inovação, ministrada em todos os cursos de MBA da FIAP, com horário e alocação de professores alinhados com os coordenadores de cada curso. As aulas serão divididas em 5 encontros presenciais ou virtuais com cada turma, incluindo também a utilização de materiais digitais (FIAP On), com a abordagem dos assuntos principais relacionados e divididos de acordo com um *framework* próprio da disciplina. 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 4 alunos.

O projeto pode ser inscrito no Startup One – ST1, competição que ocorre semestralmente 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).

Quanto aos conteúdos, eles são ministrados nas 5 aulas expositivas presenciais ou virtuais e incluem dinâmicas e mentorias. Estes conteúdos são ministrados aos alunos em intervalos suficientes para que possam ser incorporados ao projeto.

Além das aulas presenciais o aluno também tem à sua disposição (de forma voluntária, não obrigatória e, portanto, não incluídos na carga horária da disciplina) um material didático eletrônico, composto por apostilas, vídeos e *podcasts*, existente na Plataforma Digital (FIAP ON).

As orientações (ou mentorias) dos professores quanto ao desenvolvimento do projeto (TCC) estão segmentadas de acordo com as divisões de aulas, na distribuição da grade da disciplina.

O programa de aulas e conteúdo da disciplina Empreendedorismo e Inovação está dividido em 5 módulos. Cada módulo corresponde a cada uma das 5 aulas presenciais ou presenciais e segue uma estrutura de 3 etapas, conforme a seguir:

1. A primeira etapa das aulas presenciais ou virtuais é de fixação dos conceitos ligados a jornada do projeto e ocorre com a exposição de conteúdo.
2. A segunda etapa das aulas presenciais ou virtuais corresponde a alguma dinâmica de fixação dos conceitos da primeira etapa. Chamamos esta etapa da aula de "*hands on*".
3. A terceira etapa das aulas presenciais ou virtuais da aula refere-se à apresentação do desafio de validação em campo desta ferramenta, que os grupos terão de executar e trazer para a aula seguinte.

A seguir, encontram-se o detalhamento para cada um dos 5 módulos (aulas):

Aula 1 – Identificação e Validação Problema

Este módulo apresenta a abertura da disciplina, que acontece aproximadamente no segundo mês do ano letivo, e é executada a cada semestre para todas as turmas que iniciam suas aulas.

Seguindo os conceitos de *Design Thinking*, esta etapa contempla as fases de Introdução dos conceitos e entendimento do empreendedorismo, apresentando formas de como os alunos identificam e validam os problemas a serem resolvidos por sua solução (projeto) que será resolvido pelo seu grupo (startup).

Objetivos da Aula 1

Esta aula tem como objetivo a ampliação da visão sobre as principais tendências mundiais e do Brasil, tomando conhecimento de seus principais problemas e formas de identificar oportunidades para a criação do projeto da startup, fomentando os alunos a visualizarem os principais conceitos relacionados à inovação e ao empreendedorismo. Além disso, o objetivo desta aula também é a identificação do problema que a startup irá abordar em seu projeto.

Propostas de temas abordados

Para este módulo, serão abordados as megatendências e visão do mundo exponencial e emergente, com conceitos e ferramentas relacionados aos temas, como por exemplo:

- Funcionamento do Startup One e disciplina de empreendedorismo e inovação (regulamentos que regerão o programa da disciplina).
- Competição Startup One.
- Grandes problemas e desafios do mundo e Brasil.
- Propósito das startups.
- Como identificar problemas a serem resolvidos.
- Exemplos de Startup (Top 10).

Ferramentas apresentadas

A expectativa para este módulo da disciplina de Empreendedorismo e Inovação é que o aluno tenha contato com os principais conceitos atrelados ao ambiente de empreendedorismo e inovação e que ele esteja conectado com o ecossistema do empreendedorismo, sendo capacitado a buscar inspirações em diversas dimensões de negócios existentes, como também apresentar métodos para a identificação de problemas e prospecção de oportunidades.

Espera-se que os alunos, após apresentação deste módulo, estejam aptos a entender o conceito das grandes demandas mundiais e brasileiras, e que tenham sido apresentados aos cases e apresentações de alguma das

Startup TOP 10 (jornada do grupo) e que tenham entendimento pleno do funcionamento e próximos passos da disciplina ST1.

Material EaD

Em consonância com a proposta de material didático da disciplina deste módulo, será disponibilizado ao aluno o conteúdo na plataforma FIAP On, sintetizado pelo “Capítulo 1 - O mundo exponencial e emergente”.

O conteúdo foi embasado com a utilização dos conceitos da fase de Entendimento da metodologia de Design Thinking e com a utilização de conceitos de Validação da Identificação do Problema e Público-Alvo da metodologia de Lean Startup.

Também estarão disponíveis na plataforma FIAP On, os conteúdos referentes à segmentação intitulada “Capítulo 2 - Introdução ao Empreendedorismo Inovador”, incluindo: O conceito de empreendedorismo; Empreendedor e Intraempreendedor; O que são startups?; Casos de empreendedorismo tecnológico (intraempreendedorismo e extraempreendedorismo).

Aula 2 – Proposta de Valor e Modelo de negócio

Esta aula foi desenhada para que seja inserida no calendário do ano letivo (de preferência) dois meses após a apresentação da aula 1, com desenvolvimento de aula expositiva pelo professor, inclusão de dinâmicas em classe, apresentação de ferramentas específicas e estruturação de mentorias para a criação da startup.

O conteúdo deste módulo foi embasado com a utilização dos conceitos da fase de Observação da metodologia de *Design Thinking* e com a utilização de conceitos de Validação da Proposta de Valor da metodologia de *Lean Startup*. Pontos de Vista / Ideação da metodologia de Design Thinking e com a utilização de conceitos de Validação do Modelo de Negócios da metodologia de Lean Startup.

Desafios para aula 2

Para este módulo, durante o fechamento da aula, o professor propõe um desafio para cada grupo, fazendo com que os alunos apliquem os conceitos apresentados em aula e desenvolvam as habilidades de pesquisa em campo e apresentação dos achados quanto ao problema que o grupo irá resolver com seu projeto. Este desafio deverá ser apresentado e discutido em aula posterior, com a avaliação da entrega do trabalho parcial do grupo.

Objetivos da Aula 2

A segunda aula expositiva tem como principal objetivo o entendimento e construção da proposta de valor e modelo de negócio da startup, auxiliando os alunos na construção inicial dos projetos que queiram desenvolver, bem como na identificação da proposta de valor que oferecerão ao mercado.

A segunda aula também tem como principal objetivo a identificação do mercado alvo e do entendimento e desenvolvimento do modelo de negócios da startup, auxiliando os alunos na construção da visão geral do negócio que queiram desenvolver, bem como na construção do modelo de negócio que oferecerão ao mercado.

Propostas de temas abordados

Para esta etapa do programa, o principal assunto abordado será a continuidade da fixação do conceito de Proposta de Valor e Modelo de Negócios através da apresentação dos modelos do Canvas, que são recursos/ferramentas para a melhor compreensão das perspectivas do cliente e o relacionamento da proposta de valor de seu produto ou serviço, enquadrando as necessidades existentes em seu mercado de atuação, suportando a avaliação e mensuração de entrega da solução ideal para o cliente e mensurando se realmente existe um problema solucionado que o cliente queira pagar pela solução.

Para esta etapa do programa, o principal assunto abordado será a construção do Canvas de Modelo de Negócios, com o direcionamento dos alunos para o pensamento crítico na elaboração de todas as interfaces que

envolverão a iniciativa desenhada, através da compreensão de todas as possíveis limitações e dificuldades encontradas. É importante nesta etapa a exploração da importância na construção dos detalhes de todas a nove dimensões do Canvas, bem como na interação entre estas áreas para a consolidação de toda a empresa.

Ferramentas apresentadas

Para a criação dos conceitos deste módulo, deverão ser apresentadas e utilizadas todas as dimensões existentes no Canvas Proposta de Valor e Canvas Modelo de Negócios, elucidando aos estudantes a importância da aplicação da metodologia, bem como na instrução da utilização dos recursos com a ferramenta do modelo. Canvas Modelo de Negócio.

Material EaD

Para esta etapa do processo, estarão disponíveis na plataforma FIAP On, os conteúdos referentes à segmentação intitulada “Capítulo 3 - Como boas ideias nascem” e “Capítulo 4 - Business Model Generation”, incluindo: De onde surgem as boas ideias?; Princípios da criatividade; Processos criativos; Estimulando a criatividade; Quais ferramentas podemos utilizar?; Design Thinking; Da ideia ao negócio; a jornada do empreendedor; Como uma ideia se transforma em um bom negócio?; A importância do time empreendedor (sócios) e Casos reais: como nasceram bons negócios?.

Também estarão disponíveis na plataforma FIAP On, os conteúdos referentes à segmentação intitulada “Capítulo 4 - Business Model Generation”, incluindo: O que é o BMG?; BMG vs Plano de Negócios; O que é um MVP? O que é um MLP?; Como usar o BMG?; Exemplos de preenchimento; Como um BMC evolui? e Testes e prototipação rápida e dicas para a construção de um Canvas de Modelo de Negócios.

Mentorias e Dinâmicas

Para a aula 2, a mentoria deverá ser conduzida para o suporte e localização das ideias do projeto (solução) que serão desenvolvidos pelos

grupos formados, bem como a discussão do Canvas Proposta de Valor (exemplo da Top 10 ou startup externa) e demais implicações para o projeto.

Para este tópico, o trabalho poderá ser desenvolvido através da discussão dos grupos formados, para elaboração inicial do Canvas de Proposta de Valor, bem como a consolidação e ajuste das atividades elencadas na aula 1 referente a identificação do problema. O papel do professor nesta etapa da aula é acompanhar o desenvolvimento da visão do grupo quanto a aplicação do estudo de caso em seu próprio projeto e auxiliá-lo a entender a utilizar as ferramentas apresentadas.

Aula 3 – Prototipação

Esta aula foi desenhada para que seja inserida no calendário do ano letivo (de preferência) dois meses após a apresentação da aula 2, com desenvolvimento de aula expositiva pelo professor, inclusão de dinâmicas em classe, apresentação de ferramentas específicas e estruturação de mentorias para a criação da startup.

O conteúdo deste módulo foi embasado com a utilização dos conceitos da fase de Validação de Protótipo da metodologia de Lean Startup.

Desafios para a aula 3

Para este módulo, durante o fechamento da aula, o professor deverá propor um desafio para a turma, fazendo com que os alunos apliquem os conceitos apresentados em aula e desenvolvam as habilidades de pesquisa e apresentação de conceitos. Este desafio deverá ser apresentado e discutido em aula posterior, com a avaliação dos trabalhos parciais entregues e com observações do professor em relação a qualidade do trabalho executado.

Nesta etapa, o desafio proposto será a validação da proposta de valor e modelo do negócio da proposta do projeto (startup).

Objetivos da Aula

A terceira aula expositiva tem como principal objetivo a apresentação de conceitos e ferramentas para o desenvolvimento de um protótipo da startup e

a elaboração da perspectiva desta iniciativa no ecossistema de startups, ou seja, apresentar aos alunos quais serão os prováveis ambientes encontrados no mercado de atuação na qual ela estará inserida.

Propostas de temas abordados

Para esta etapa do programa, o principal assunto abordado será a prototipação da ideia de empresa construída até então, com o objetivo claro de apresentar a necessidade de se testar a iniciativa junto ao mercado, validando o conceito.

Nesta aula serão apresentadas ferramentas para a conceituação e validação da startup, tais como: Mochup, Wireframe entre outras ferramentas de prototipação.

Ferramentas apresentadas

Serão apresentadas as ferramentas de prototipagem como Wireframe, Mochup, Desenvolvimento de Apps, Protótipos físicos (como Arduíno e dispositivos de IoT). Ferramentas para a construção de protótipos como por exemplo FIGMA, MARVEL e INVISION.

Material EaD

Para esta etapa do processo, estarão disponíveis na plataforma FIAP On, os conteúdos referentes à segmentação intitulada “Capítulo 5 - Como testar e evoluir sua ideia de negócios?”, incluindo os temas: Conceitos de prototipação - física e digital; Para que serve um protótipo?; Técnicas para testar protótipos com usuários; O que devemos perguntar?; Casos de aplicação; Ganhando escala e relevância; Scale-up e tração; Growth Hacking; Gestão do desenvolvimento do negócio.

Mentorias e Dinâmicas

Nesta aula são apresentadas as formas da startup tangibilizar através da construção de protótipos. Para isso, o professor apresenta algumas

ferramentas de prototipação virtual existentes, exemplificando alguns modelos de startups.

Para a aula 4, a mentoria deverá ser conduzida para o suporte na elaboração do Protótipo e Validação de Testes da empresa, explicitando a importância da obtenção do feedback dos potenciais clientes e usuários da solução fornecida (validação), bem como na identificação de potenciais limitações que possam existir com o desenvolvimento do trabalho.

Para facilitar a condução, nesta etapa, deverão ser apresentadas alguns cases Top 10 (cases de sucesso existentes no mercado), com o acompanhamento das discussões pelo professor-mentor.

Aula 4 – Análise financeira e Pitch

Esta aula foi desenhada para que seja inserida no calendário do ano letivo (de preferência) dois meses após a apresentação da aula 3, em torno do nono mês do ano letivo do programa de pós-graduação, com desenvolvimento de aula expositiva pelo professor, inclusão de dinâmicas em classe, apresentação de ferramentas específicas e estruturação de mentorias para a criação da startup.

O conteúdo deste módulo foi embasado com a utilização dos conceitos da fase de Teste da metodologia de Design Thinking e com a utilização de conceitos de Validação de Análise Financeira da metodologia de Lean Startup.

Ainda neste mesmo módulo, serão abordados os assuntos relacionados à construção do Pitch da startup (que será apresentado pelos grupos na aula 5), apresentando aos alunos as principais técnicas relacionadas às melhores práticas para se vender a ideia da empresa em um discurso convincente.

Desafios para a aula 4

Para este módulo, durante o fechamento da aula, o professor deverá propor um desafio para a turma, fazendo com que os alunos apliquem os conteúdos apresentados em aula e desenvolvam as habilidades de pesquisa e apresentação de conceitos (validação de seu modelo de negócios). Este

desafio deverá ser apresentado e discutido na aula seguinte, com a avaliação das entregas dos grupos.

Nesta etapa, o desafio proposto será a imersão, entendimento, construção e validação do protótipo do projeto (startup).

Objetivos da Aula

Também é o objetivo desta aula a apresentação de conceitos e ferramentas para o desenvolvimento de uma estruturação financeira e jurídica da empresa, ressaltando os aspectos necessários para a construção de todas as atividades pertinentes ao negócio, compreendendo aspectos financeiros e monetização.

Também é objetivo desta aula apresentar o processo de elaboração de pitches e a preparação do esboço do projeto da disciplina (trabalho de conclusão de curso - TCC).

Também serão apresentadas ferramentas e técnicas de elaboração de Pitches.

Propostas de temas abordados

Para esta etapa do programa, serão abordados assuntos referentes à estruturação financeira propriamente dita, abordando conceitos de finanças corporativas e de investimentos (fluxo de caixa, balanço financeiro, estruturação e captação de capital etc) e abordando também assuntos jurídicos, tais como: elaboração de contratos de parcerias e com investidores, aspectos legais relacionados a abertura da empresa, regimes tributários, direito societário, dentre outros.

Ferramentas apresentadas

Planilha para análise financeira de uma startup. Modelos de pitches de startups (Top 10 e externas).

Material EaD

Para esta etapa do processo, estarão disponíveis na plataforma FIAP On, os conteúdos referentes à segmentação intitulada “Capítulo 6 - Aspectos Financeiros e Jurídicos e Mercado de uma startup”.

Também estará disponível na plataforma o “Capítulo 7 - Storytelling e Pitches Venturing”, incluindo o conteúdo sobre O que é Storytelling?; Pitches - O que são e como fazer bons pitchies?!; Tipos de pitches; Vendendo o seu peixe!; Estrutura de um bom pitch; Técnicas mais utilizadas; Golden Circle; Templates vencedores.

Mentorias e Dinâmicas

O foco desta aula é trazer o entendimento da importância da análise financeira para uma startup, bem como a formação dos custos e receitas, assim com formas de monetização e precificar a solução e dimensionar o mercado total e mercado alvo.

O papel do Professor nesta etapa da aula é acompanhar o desenvolvimento da visão do grupo quanto a aplicação do estudo de caso em seu próprio projeto e auxiliá-lo a entender a utilizar a ferramenta apresentada.

Descrição da Mentoria: após a aula expositiva (revisão executiva do conteúdo disponível na plataforma digital) ocorre a reunião dos grupos já definidos no ST1 para discutir a planilha financeira e melhorias sugeridas na apresentação do Pitch e TCC, sendo a discussão acompanhada pelo Professor.

Aula 5 – Pitch e Mentoria final do Projeto (TCC)

Esta aula foi desenhada para que seja inserida no calendário do ano letivo (de preferência) um mês após a apresentação da aula quatro, com desenvolvimento de aula expositiva pelo professor, inclusão de dinâmicas em classe, apresentação de ferramentas específicas e estruturação de mentorias para a criação da startup.

O conteúdo deste módulo foi embasado com a utilização dos conceitos da fase de viabilização da metodologia de Design Thinking.

Desafios para aula 5

Para este módulo, durante o fechamento da aula, o Professor deverá propor um desafio para a turma, fazendo com que os alunos elaborem uma versão inicial do projeto (esboço do projeto final). O esboço do trabalho final de cada grupo (startup) é analisado pelo professor que envia um feedback de melhorias.

O projeto de cada startup é apresentado e discutido na aula 5, no formato de Pitch, recebendo as observações e sugestões de melhoria do professor que faz o papel de banca.

Nesta etapa, o desafio proposto será a imersão e definição da iniciativa, com a construção e validação do protótipo (conceitual ou funcional) do projeto (startup), tendo como ponto de partida todo o material desenvolvido até esta etapa. Também está incluso no desafio a preparação do Pitch da startup que será apresentada na aula seguinte (aula 5 – última aula).

O papel do Professor nesta etapa da aula é acompanhar o desenvolvimento da visão do grupo quanto a aplicação do estudo de caso financeiro em seu próprio projeto e auxiliá-lo a entender a utilizar a ferramenta apresentada.

Objetivos da Aula

A quinta aula expositiva tem como principal objetivo a apresentação do pitch da startup e sua avaliação por parte do professor (observações e sugestão de melhorias). Também é objetivo desta aula realizar a mentoria do projeto final (TCC).

Material EaD

O “Capítulo 8 - Ecossistema empreendedor e Corporate” também estará disponível com o conteúdo sobre O que são ecossistemas empreendedores; - Principais atores; - Tipos de investidores (Anjos, Estratégicos, Financeiros, etc);

- Incubadoras: Relação entre grandes empresas e startups e - Espaços de interação.

Mentorias e Dinâmicas

Apresentação das startups: Os grupos apresentam o pitch de seus projetos.

Também é objetivo desta mentoria fazer o fechamento sobre dúvidas do pitch e do projeto final (TCC) que será entregue no mês 12.

Desafios para entrega final do projeto (TCC)

A partir da apresentação do Pitch e entrega do esboço do projeto Final, o grupo deverá evoluir a entrega final do projeto (Entregas finais: Arquivos do Pitch, Análise financeira e Plano de negócio - Projeto).

O desempenho do grupo de alunos na disciplina Empreendedorismo e Inovação é avaliado segundo 3 critérios presentes no portal FIAP, disponível para os Professores ao final do curso.

Além destes três critérios (cuja média aritmética leva a nota da disciplina) soma-se a possibilidade de o Professor conferir até um (1) ponto extra na média final, referente as entregas parciais de trabalhos solicitados durante o curso (desafios para a aula seguinte).

Este ponto é facultativo e o professor titular de cada turma deve conferi-lo levando em conta a qualidade dos trabalhos e não somente a sua entrega. A média destes 3 critérios, mais o ponto extra (facultativo) trata-se, portanto, de uma 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. Cabe ao Professor a decisão de indicar ou não o projeto a concorrer ao Startup One.

O projeto desenvolvido pelos grupos (startups) na disciplina de Empreendedorismo e Inovação será avaliado sob a perspectiva acadêmica, podendo ser ou não indicado para a competição do Startup One.

Caso o grupo decida participar da competição, o projeto da startup será submetido a uma avaliação inicial do Professor da disciplina, que pode ou não indicá-lo através de um formulário de avaliação, disposto no portal da FIAP.

A avaliação dos projetos indicados ao “TOP30” (10 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 submetidos a uma segunda fase de avaliação, recebendo mentorias e treinamentos específico para aprimorarem seus projetos e ficarem aptos para a apresentação do projeto (Pitch) para uma banca externa final que escolhe a startup ganhadora.

Coordenador do curso

Prof. Msc. Marcelo Lau

Diretor executivo da Data Security. Atuou por mais de 12 anos em instituições financeiras em áreas de segurança da informação e prevenção de fraude. Engenheiro pela Escola de Engenharia Mauá, pós-graduado em Administração pela Fundação Getúlio Vargas, pós-graduado em Comunicação e Arte pelo SENAC-SP e Mestre em Ciência Forense pela Escola Politécnica na Universidade de São Paulo.

Atuou por mais de 3 anos como pesquisador da POLI/USP. É o atual coordenador no MBA em CyberSecurity – Forensics, Ethical Hacking & DevSecOps e professor em diversas outras disciplinas de pós-graduação e graduação na FIAP. Também é professor em instituições de ensino como IPOG, UNIFOR e IBG. Foi professor da Universidade Presbiteriana Mackenzie e da FATEC. Foi instrutor da FEBRABAN em cursos na área de *Compliance* e Segurança da Informação, além de diversos outros centros de ensino no Brasil e no exterior. Conta com dezenas de Entrevistas em Rádio, TV, Mídia Impressa e publicações on-line nos mais diversos canais de comunicação de cobertura nacional e internacional, como Argentina e Colômbia e em meios como TV Globo, SBT, Valor Econômico, O Estado de São Paulo, entre outros.