ORGANIZAÇÃO DIDÁTICO-PEDAGÓGICA

PROJETO PEDAGÓGICO DO CURSO: ASPECTOS GERAIS

CONTEXTO EDUCACIONAL

A FIAP está inserida 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 a fragilidades exploradas nos domínios de pessoas, processos e tecnologia.

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

Os alunos preparados por esta formação atenderão demandas já existentes e reprimidas deste mercado. As oportunidades geradas por este curso poderão aumentar 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 deste mercado em empresas no exterior, já que 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, quanto em produtos que podem surgir em oportunidades geradas pelo mercado de trabalho local (Brasil), aplicáveis a diversas partes do mundo.

Este curso se diferencia das demais formações em meios acadêmicos, por estar alinhada a normas do mercado de segurança aplicado hoje em empresas privadas e órgãos governamentais, atendendo as 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 um mercado ainda requer mais profissionais com conhecimentos e vivência em segurança da informação, em um ambiente cada vez mais vulnerável a ataques, em razão da descoberta de novas fragilidades em processos, pessoas e tecnologia que influenciam diretamente os negócios de uma empresa.

O curso prepara os profissionais de mercado 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].

Sabe-se ainda que as leis de proteção de dados e os escândalos aparentemente intermináveis do Facebook relacionados à privacidade do consumidor 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 Cybersegurança. Este profissional tem um campo de trabalho que tem aumentado consideravelmente nos últimos anos devido a fatores como a globalização da economia e expansão das grandes corporações, ao surgimento de serviços e processos cada vez mais específicos e especializados e à informatização de pequenas e micros empresas.

Este curso 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.

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 isto, 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 cybersegurança, 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 Cybersegurança.

Neste 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 2019, exigindo que o mercado de trabalho possa contar com profissionais cada vez mais capacitados.

OBJETIVOS DO CURSO

O Curso de Pós-graduação – Especialização em Cyber Security – Forensics, Ethical Hacking & DevSecOps deriva do conhecimento aplicado da área de exatas. A área de Segurança da Informação surgiu com o advento da tecnologia, que pode ser considerado como primórdio as tecnologias primitivas, dentre elas o fogo, que tem suas origens possivelmente há 800.000 anos. Entretanto nos aspectos tecnológicos, podemos mencionar que o ábaco, surgido na Mesopotâmia em torno de 2.400 A.C. é considerado como a primeira tecnologia relacionada à computação que hoje dão lugar à segurança da informação. A segurança da informação somente tem sua normatização em 1995 através do documento **British Standard 7799** e com o avanço nos processamento de dados e informatização de processos, tornou-se necessário se preservar a segurança destes ambientes através de outros mecanismos e tecnologias que estão presentes nos dias atuais. A Gestão, que é o elemento complementar do curso tem sua origem na área de humanas, por meio da Administração clássica, e que por meio deste curso, oferece todos os elementos para que o aluno reconheça os aspectos tecnológicos a administrativos necessários para a atuação neste segmento.

O curso parte da premissa de que a segurança é propriedade de um Sistema de Informação cuja existência depende da cooperação de especialistas e de conhecimentos de diversas áreas. Daí sua natureza multidisciplinar. Em função desse princípio, os componentes curriculares do curso abrangem aspectos técnicos, de gestão, forenses e de recursos formulação e implementação de uma política de segurança eficiente.

Esta última frase antecipa e resume os objetivos do programa: possibilitar aos participantes a definição de uma política de segurança corporativa, compreendendo objetivos e ações concretas, avaliar sistemas de informação do ponto de vista da sua segurança, escolher e combinar ferramentas que permitam a implementação das políticas propostas.

O programa não objetiva ensinar os participantes a programar, instalar e operar produtos na área de segurança, nem se vincula a uma determinada linha de produtos e de fornecedor. A necessidade de conhecimento prático de ferramentas é suprida com a utilização de software livre.

Pretende-se complementar as aulas teóricas com aulas realizadas também em laboratório. A função dessas aulas práticas é permitir aos alunos tomar contato com o maior número possível de tipos de tecnologias, ferramentas e processos, avaliando

comparativamente as técnicas de segurança e conhecer suas características, de modo a permitir escolhas conscientes de políticas de segurança.

OBJETIVO GERAL:

Especializar profissionais os 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 isto 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 a realização de análise crítica sobre soluções de segurança, oferecendo um amplo conhecimento de cenários e ferramentas necessárias para atender os 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 custo, prazos, processos, tecnologia disponível 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.

PERFIL DO EGRESSO

Profissionais graduados que participam de decisões, planejamento de soluções, concepção, desenvolvimento e implantação de projetos diretamente relacionados com a área de segurança de redes e de sistemas de informação.

O aluno deverá mostrar capacidade de adaptação às novas situações que constituem um desafio contínuo da área de segurança de informações. Para tanto o aluno 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 as 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 esta 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 incluem 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 adequado 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 egresso poderá atuar em organizações de diferentes tipos, em projetos na área de segurança da informação; no desenvolvimento de sistemas de software corporativos; na coordenação de projetos na área de desenvolvimento de sistemas de software específicos para a segurança, ou 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 que os egressos poderão atender: desde administradores de rede com ênfase na segurança, até administradores de políticas de segurança.

Não se espera dos egressos o conhecimento da instalação e operação de uma determinada linha de produtos, nem a capacidade de desenvolverem produtos voltados a específicas funções de segurança. Entretanto o aluno poderá recomendar soluções existentes no mercado, sendo capaz de indicar as implementações de menor custo em função às 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 na área em que lecionam. Complementa os planos de ensino, atividades de extensão, pesquisa e outras atividades complementares. Esta 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 com o foco do curso, seja através 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 se baseia 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-la, analisá-la e organizá-la, tendo em vista os objetivos pedagógicos do curso.

No modelo para o curso são disponibilizadas as unidades curriculares em um modelo que privilegia a formação do egresso, 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 correspondente ao ano 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 um facilitador da aprendizagem;
- Modelo de ensino organizado onde o aluno é considerado centro do processo de aprendizagem e sujeito ativo de sua formação, sendo respeitado o seu ritmo de aprender;
- 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 compatibilidade e adaptabilidade destes 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 coletivamente conhecimento;

- O apoio docente é condição indispensável para a aprendizagem, este 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 deste aluno, de seus acúmulos teóricos e práticos, e dos desafios com que o mesmo 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;
  - O material didático;
  - O currículo;
  - A infra infraestrutura que dá suporte tecnológico, científico e instrumental ao curso;
  - A realização de convênios e parcerias com outras instituições, empresas ou organizações.

O processo didático-pedagógico do 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 se baseia 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, se limitar 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.

Os 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-la, analisá-la e organizá-la, 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, coordenação e 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, através de sites na internet, seja o portal da FIAP, seja o 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 deste quadro, aprender a aprender de forma colaborativa é mais importante do que aprender a aprender sozinho. A colaboração, neste contexto, é essencial. Também dentro deste quadro, os papéis de professor e aluno se modificam significativamente.

Neste 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 conteúdo, 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, desta forma, que as práticas pedagógicas, realizadas sobre uma reflexão crítica, pela compreensão e análise da realidade do curso e da própria instituição, poderão 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 que é abordado em sala de aula deve ter alguma relação com uma solução de problema real do mercado de trabalho. Desta 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 parceira ou não da FIAP.

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

Desta forma, foram idealizados projetos que são aos alunos em ordem crescente de complexidade, favorecendo a ambientação por parte dos alunos nas reais necessidades do mercado de trabalho. Onde é proposto que os alunos formem equipes de no mínimo três participantes e no máximo 5, onde cada equipe deverá apresentar o projeto completo de uma implantação de infraestrutura computacional com uma rede de computadores que atenda aos requisitos básicos de transmissão e troca de dados com segurança, escalabilidade e disponibilidade.

Ao propor este tipo de trabalho, indica-se ao aluno que este 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.

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 através 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 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 aprendiz busque as soluções para problemas reais sem estar o tempo todo com um tutor a sua volta. Através da colaboração, as pessoas interagem mais, incentivam, motivam 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 sugerido 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 do curso será motivada pelos professores para transpor as fronteiras do currículo, sem fugir do apelo profissional do programa. Desta forma, faz parte a produção científica, atividades culturais, iniciativas sociais, como prestação de serviços à comunidade dentro do perfil do curso, especialmente ONGs e entidades sem fins lucrativos, e em eventos comunitários.

No processo de ensino-aprendizagem são utilizados mecanismos diferenciados de avaliação seja na forma de provas semestrais, mas, principalmente, através da prática profissional, na forma de projetos interdisciplinares (AM) que oferecem a visão da formação específica na área de formação do curso. Outros instrumentos, como avaliações periódicas para medir o grau de compreensão dos conteúdos abordados, tanto através da prática em laboratório quanto através 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 cybersegurança, os professores propõem e incentivam os alunos à pesquisa através dos 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 na sala de aula as necessidades reais utilizadas pelo profissional 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 tais problemas;

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

- Laboratório de computação gerais e específicos, biblioteca, acesso à Internet e recursos pedagógicos usuais. Outros recursos que se pode salientar:
- Reuniões pedagógicas com a participação do corpo docente onde são analisados e discutidos os planos tático e operacional de ensino, com objetivo de garantir a interdisciplinaridade do curso;
- Criação de Grupo de Estudos, coordenado por um docente do curso, com o principal objetivo de promover discussão e pesquisas em áreas específicas de interesse do curso;
- Cursos de extensão extra classe para que os alunos possam manter-se atualizados com relação a 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”. Este trabalho, ao final do semestre, faz com que um grande laboratório de testes de soluções seja estabelecido pelos alunos com ampla simulação da situação real 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.

MATRIZ CURRICULAR

MATRIZ CURRICULAR	
Disciplinas	CH
Introdução à Cibersegurança	04
Innovation and Digital Transformation	20
Financial management	16
CyberSecurity Strategy & Governance	24
Leadership Skills	16
Cyberlaw: Tecnologia, Inovação e Segurança	16
Risk Assessment	20
Security in Bimodal IT & Sourcing	16
Tecnologias em Cibersegurança	16
Cloud Computing Security, DevOps e DevSecOps	16
Physical and environmental security	16
Ethical Hacking e Ransomware	20
Data Loss Prevention	16
Computer Forensics	20
Inteligência e Espionagem	16
Cybersecurity Incident Response	16
Defesa Cibernética	20
Business Continuity Management	20
Inteligência Artificial & Machine Learning	16
Critical infrastructure security	12
Empreendedorismo e Inovação	20
CARGA HORÁRIA TOTAL DO CURSO	**360**

EMENTAS E BIBLIOGRAFIAS

Disciplina	Introdução à Cibersegurança
Ementa	
Apresentar e discutir a sobre o panorama atual da cibersegurança em empresas e em relação ao mercado de trabalho no Brasil e no Mundo. Esta disciplina tem o objetivo de conceituar os elementos básicos que compõem a dinâmica da cibersegurança. Discutindo o cenário atual as ameaças em empresas e governos, bem como sua aplicação nos negócios. As aulas serão divididas em 2 encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à cibersegurança. É uma disciplina relacionada à abertura e fechamento do curso, espera-se que o aluno possa trazer suas percepções preliminares atrelados ao universo da cibersegurança, assim como trazer suas percepções do término deste curso.	
Bibliografia Básica	
GALVÃO, M. de C. Fundamentos em Segurança da Informação. São Paulo: Pearson 2015. JUNIOR, A. K. Sistemas de segurança da informação na era do conhecimento. Curitiba: Editora InterSaberes 2016. CAPRINO, W. Trilhas em Segurança da Informação. Rio Janeiro: Brasport 2015.	
Bibliografia Complementar	
HINTZBERGEN, J. et al. Foundations of information security based: on ISO27001 e ISO27002. Rio Janeiro: Editora Brasport, 2018: 3ª ed. ROSSETE, C. A. Segurança e Higiene do Trabalho. São Paulo: Pearson 2015.	

Disciplina	Innovation and Digital Transformation
Ementa	
Apresentar e discutir aspectos relacionados à inovação e transformação digital. Esta disciplina tem o objetivo de conceituar os elementos básicos que compõem a dinâmica este tema, que trata de assuntos como marketing digital (*Digital Marketing*), processos de identificação de *leads* e aceleração ao 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 ao 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 5 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. Campinas: 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: Editora Blucher, 2017. KELLEY, T. As 10 Faces da Inovação. São Paulo: Elsevier, 2007: 2ª ed. MONTEIRO JR, J. G. Criatividade e Inovação. São Paulo: Pearson, 2011.

Disciplina	Financial management
Ementa	
Apresentar e discutir aspectos relacionados à gestão financeira aplicada à cibersegurança. Esta disciplina tem o objetivo de posicionar o egresso a compreender a gestão financeira em cybersegurança (*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 4 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. São Paulo: Pearson 2018. GITMAN, L. J. Princípios de administração financeira São Paulo: Pearson 2004: 10 ed. MENEGHETTI NETO, A. Educação Financeira. Porto Alegre: EDIPUCRS, 2014.	

Bibliografia Complementar
CRUZ, J. A. W. e ANDRICH, E. G. Gestão Financeira Moderna. Curitiba: Intersaberes, 2013. 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. Rio Janeiro: Ed. Freitas Bastos, 2015.

Disciplina	CyberSecurity Strategy & Governance
Ementa	
Apresentar e discutir aspectos relacionados à estratégia de governança em cibersegurança. Esta disciplina tem o objetivo de preparar o egresso a compreender a gestão através 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 e PCI-DSS. O egresso ainda compreenderá a estrutura e papéis de uma área de Cibersegurança, tal como as ferramentas de apoio à Governança. As aulas serão divididas em 6 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. Rio Janeiro: 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 Janeiro: Editora Freitas Bastos, 2017. FROTA, A. Globalização e governança internacional: fundamentos teóricos. Curitiba: InterSaberes, 2017.	
Bibliografia Complementar	
MANOEL, S. S. Governança de segurança da informação: como criar oportunidades para o seu negócio. Rio Janeiro: Brasport, 2014. MUNHOZ, A. S. Fundamentos de tecnologia da informação e análise de sistemas para não analistas. Curitiba: InterSaberes, 2017.	

Disciplina	Leadership Skills
Ementa	

Apresentar e discutir aspectos relacionados à liderança e gestão de profissionais em cibersegurança. Esta disciplina tem o objetivo de preparar o egresso a se tornar potencialmente um gestor de profissionais que atuem em um time de cibersegurança, por meio de conteúdos que irão prepará-lo às habilidades interpessoais, tal como a comunicação e motivação no processo de liderança; *coaching* e *feedback*; administração de conflitos; ainda espera-se preparar o egresso para que o mesmo identifique e forme equipes de alto desempenho, sendo ainda capaz de liderando as mudanças constantes e exigidas dentro do mundo corporativo. As aulas serão divididas em 4 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. São Paulo: Pearson, 2018. ESCORSIN, A. P; WAGNER, C. Liderança e desenvolvimento de equipes. Curitiba: InterSaberes, 2017. ROBBINS, S. P. e JUDGE, T. A. Comportamento Organizacional. São Paulo: Editora Pearson Brasil, 2014, 14ª ed.
Bibliografia Complementar
ALENCASTRO, M. S. C. Ética empresarial na prática: liderança, gestão e responsabilidade corporativa. Curitiba: InterSaberes, 2016. CHIAVENATO, I. Gerenciando com as pessoas: transformando o executivo em um excelente gestor de pessoas. São Paulo: Editora Manole, 2015 – 5ª ed. KLUYVER, C. A. de. Estratégia: uma visão executiva. São Paulo: Pearson, 2010 MANDELLI, P. e LORIGGIO, A. Liderando para alta performance: conceitos e ferramentas. Petropólis, RJ: Vozes, 2017. VERGARA, S. C. Gestão de Pessoas. São Paulo: Atlas, 2016 – 16ª ed.

Disciplina	Cyberlaw: Tecnologia, Inovação e Segurança
Ementa	
Apresentar e discutir aspectos relacionados ao direito quanto à aplicação do mesmo à realidade corporativa, governamental e também relevante ao próprio profissional que atual em cibersegurança. Esta disciplina tem o objetivo de preparar o egresso à tomada de conhecimento e devida interpretação aos marcos regulatórios da era digital no Brasil e no mundo, ainda preparando às questões legais atreladas à investigação dos crimes eletrônicos no ambiente corporativo (abordando assuntos como a interceptação de dados, ata notarial, ransomware e concorrência desleal).	

O egresso ainda será capaz de compreender aspectos como responsabilidades civil, criminal e trabalhista, assim como regulamentos Internos em cibersegurança e temas imprescindíveis como a privacidade e proteção dados (por meio da GDPR e 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 4 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. Caxias do Sul: Editora 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 Janeiro: Freitas Bastos, 2017. TEIXEIRA, T. Startups e inovação: direito no empreendedorismo (entrepreneurship law). São Paulo: Manole, 2017.

Disciplina	Risk Assessment
Ementa	
Apresentar e discutir aspectos relacionados à gestão de riscos em âmbito da cibersegurança. Esta disciplina tem o objetivo de preparar o egresso aos conceitos relacionados à gestão de riscos, sendo ainda capaz de a identificar, produzir um mapa de risco (*Risk Map*), assim como a matriz de riscos (*Risk Assessment Matrix*). O egresso ainda será familiarizado às 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 5 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. São Paulo: Pearson, 2015.	

KAERCHER, A. R.. Gerenciamento de riscos: do ponto de vista da gestão da produção. Rio Janeiro: Editora Interciência, 2016. CCPS. Diretrizes para segurança de processo baseada em risco. Rio Janeiro: Editora Interciência, 2014.
Bibliografia Complementar
ARAI, C. Gestão de Riscos. São Paulo: Pearson, 2015 HABERFELD, Sérgio. ALCA: riscos e oportunidades. São Paulo: Manole, 2003.

Disciplina	Security in Bimodal IT & Sourcing
Ementa	
Apresentar e discutir aspectos relacionados à cibersegurança e seu alinhamento segundo as necessidades de negócio. Esta disciplina tem o objetivo de preparar o egresso à familiarização das necessidades de negócio e a identificação sobre o papel da cibersegurança ao atingimento dos objetivos de negócio (sejam estes corporativos privados ou atrelados a empresas públicas). Neste aspecto, o egresso será familiarizado à natureza bimodal da Gestão dos Negócios e da TI, compreendendo e avaliando questões como o *Sourcing* de Serviços de Segurança da Informação e compreendendo a operacionalização destes processos pelo OPBOK (*Outsourcing Professional Body of Knowledge*), assim como a preparação e avaliação de RFPs em seu processo, estrutura, seleção, negociação e contratação de serviços em cibersegurança. As aulas serão divididas em 4 encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados aos processos de negócios que exigem abordagem junto à cibersegurança.	
Bibliografia Básica	
STATDLOBER, J. Gestão do Conhecimento em Serviços de TI: Guia Prático – Base de conhecimento para atendimento a usuários e clientes. Rio Janeiro: Brasport, 2016. OLIVEIRA, B. S. de. Métodos Ágeis e Gestão de Serviços de TI. Rio Janeiro: Brasport, 2018. JOÃO, B. N. Tecnologia da informação gerencial. São Paulo: Pearson, 2015.	
Bibliografia Complementar	
DALLA COSTA, A. J. Estratégias e negócios das empresas diante da internacionalização. São Paulo: Editora Ibpex, 2011.	

Disciplina	Tecnologias em Cibersegurança
Ementa	
Apresentar e discutir aspectos relacionados às tecnologias em cibersegurança, aplicados em empresas privadas e públicas. Esta disciplina tem o objetivo de preparar o egresso à familiarização das tecnologias atualmente utilizadas em cibersegurança, assim como a aplicação destas tecnologias dentro do ambiente corporativo, onde o egresso será capaz de compreender a aplicação destas tecnologias, assim como propor e readequar arquiteturas tecnológicas em cibersegurança. As tecnologias presentadas são aplicadas às redes de computadores, sistemas e dispositivos informáticos. As aulas serão divididas em 4 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. São Paulo: Ed. Pearson, 2015. STALLINGS, W. Criptografia e segurança de redes: São Paulo: Ed. Pearson, 2008: 4ª ed. VERAS, M. Computação em Nuvem. Rio Janeiro: Editora Brasport 2015.	
Bibliografia Complementar	
JUNIOR, A K. Sistemas de segurança da informação na era do conhecimento. Curitiba: Editora InterSaberes 2016. RUFINO, N. M. O. Segurança em redes sem fio. São Paulo: Editora Novatec, 2014: 4ª ed.	

Disciplina	Cloud Computing Security, DevOps e DevSecOps
Ementa	
Apresentar e discutir aspectos relacionados às tecnologias baseadas em nuvem assim como as atividades relacionadas ao desenvolvimento seguro de aplicações e respectiva operacionalização destes ambientes. Esta disciplina tem o objetivo de preparar o egresso à familiarização das tecnologias atualmente utilizadas em nuvem, onde será possível se identificar os distintos tipos de modelos aplicados em Cloud Computing, assim como as principais aplicações disponíveis neste ambiente. O egresso ainda será capaz de fazer a gestão de ambientes em nuvem, incluindo a gestão de custos neste ambiente. Visando atender necessidades normativas e regulatórias existentes no mercado em cibersegurança, o egresso será levado a identificar e compreender aspectos	

relacionados ao desenvolvimento seguro de sistemas (*Security Development*) e deverá ser preparado para conhecer as necessidades para a migração do ambiente tecnológico *On Pressises* para ambiente em *Cloud*. O egresso compreenderá as atribuições e responsabilidades quanto à atuação do profissional denominado DevOps e DevSecOps, responsável pelo desenvolvimento, operação e respectivamente a cibersegurança deste ambiente. As aulas serão divididas em 4 encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à adoção às boas práticas de cibersegurança aplicáveis aos ambientes de nuvem.
Bibliografia Básica
VERAS, M. Computação em Nuvem. Rio Janeiro: Editora Brasport 2015 LEE, V. Aplicações Móveis: arquitetura, projeto e desenvolvimento. São Paulo: Pearson, 2005 OLIVEIRA, B. S. de. Métodos Ágeis e Gestão de Serviços de TI. Rio Janeiro: Editora Brasport, 2018.
Bibliografia Complementar
FERRERA, A. M. Introdução ao cloud computing: tecnologia, conceito e modelo de negócio. Lisboa: Editora Fca, 2015. STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. São Paulo: Pearson, 2015: 6ª ed.

Disciplina	Physical and environmental security
Ementa	
Apresentar e discutir aspectos relacionados às tecnologias relacionadas à proteção de ambientes físicos. Esta disciplina tem o objetivo de preparar o egresso à familiarização das tecnologias atualmente utilizadas em ambientes físicos, sendo capaz de entender os conceitos da segurança física e ambiental e respectivas legislações aplicáveis. O egresso 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 tange à segurança patrimonial) Ainda serão apresentadas as melhores práticas relacionadas a este ambiente como estruturas de segurança física em ambiente corporativo. As aulas serão divididas em 4 encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à adoção às boas práticas de cibersegurança aplicáveis ambientes físicos.	
Bibliografia Básica	

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

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

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

Bibliografia Complementar

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

HINDSBERGEN, J. et al. Fundamentos de Segurança da Informação. Rio Janeiro: Brasport, 2018.

Disciplina	Ethical Hacking e Ransomware

Ementa

Apresentar e discutir aspectos relacionados às ferramentas e técnicas utilizadas em processos de análise de vulnerabilidade e testes de intrusão.

Esta disciplina tem o objetivo de preparar o egresso à familiarização das metodologias e tecnologias atualmente utilizadas em cibersegurança relacionados à análise de vulnerabilidade incluindo padrões como NIST 800-155, OSSTMM e OWASP.

As etapas de identificação de fragilidades são levadas ao conhecimento e prática do egresso, incluindo as etapas de coleta de informações (*footprint* and *fingerprint*) com Google Hacking, Engenharia Social, análise, exploração e mitigação de vulnerabilidades com a capacitação do mesmo à preparação do relatório de vulnerabilidade técnica.

O egresso ainda conhecerá tecnicamente ameaças como o Ransomware, identificando potenciais medidas que evite o atingimento de negócios à esta e demais outras ameaças atreladas às fragilidades técnicas.

As aulas serão divididas em 5 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

THE HONEYNET PROJECT. Conheça seu inimigo. São Paulo: Pearson, 2002.

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

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

Bibliografia Complementar
HINDSBERGEN, J. et al. Fundamentos de Segurança da Informação. Rio Janeiro: Brasport, 2018. VERAS, Ml. Computação em Nuvem. Rio Janeiro: Editora Brasport 2015.

Disciplina	Data Loss Prevention
Ementa	
Apresentar e discutir aspectos relacionados às ferramentas e técnicas utilizadas em processos de prevenção ao vazamento de dados. Esta disciplina tem o objetivo de preparar o egresso à familiarização das tecnologias atualmente utilizadas em cibersegurança relacionados aos processos, modelos e políticas aplicadas à classificação de informações. Partindo do conhecimento preliminar quanto à classificação de informações, o egresso 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 4 encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à aplicação de técnicas e ferramentas que permite a devida tomada de ações que visam evitar vazamento de dados em âmbito corporativo e governamental.	
Bibliografia Básica	
CAPRINO, W. Trilhas em Segurança da Informação. Rio Janeiro: Editora Brasport 2015. KOLBE JUNIOR, A. Sistemas de segurança da informação na era do conhecimento. Curitiba: Editora InterSaberes 2016. STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. São Paulo: Pearson, 2015: 6ªed.	
Bibliografia Complementar	
HINDSBERGEN, J. et al. Fundamentos de Segurança da Informação. Rio Janeiro: Brasport, 2018. KARSPINSKI, M. T. Arquitetura contra o crime: prevenção, segurança e sustentabilidade. Curitiba: Editora InterSaberes, 2016.	

Disciplina	Computer Forensics
Ementa	
Apresentar e discutir aspectos relacionados às ferramentas e técnicas utilizadas em processos investigativos em meios informáticos. Esta disciplina tem o objetivo de preparar o egresso à familiarização das tecnologias atualmente utilizadas em cibersegurança relacionados aos processos investigativos, onde são apresentados os padrões periciais como a ISO 27037 e RFC 3227. As etapas do processo investigativo são apresentadas ao egresso, como os processos de identificação, coleta e preservação, análise e apresentação de evidências digitais em dispositivos informáticos, por meio de laudo pericial. E egresso ainda conhecerá ferramentas que permitem a realização de engenharia reversa, assim como a perícia em dispositivos móveis. As aulas serão divididas em 5 encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à aplicação de técnicas e ferramentas que permite a investigação em meios informáticos.	
Bibliografia Básica	
KARSPINSKI, M. T. Arquitetura contra o crime: prevenção, segurança e sustentabilidade. Curitiba: Editora 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. Rio Janeiro: Editora Brasport, 2017.	
Bibliografia Complementar	
BARRETO, A. G. e BRASIL, B. S. Manual de investigação cibernética: à luz do marco civil da internet. Rio Janeiro: Editora Brasport, 2016. YATIRAJ, S. Quick Review of Forensic Medicine. New Delhi, India: Jaypee, 2013. WENDT, E. e JORGE, H. V. N. Crimes cibernéticos: ameaças e procedimentos de investigação. Rio Janeiro: Editora Brasport, 2017: 2ª ed.	

Disciplina	Inteligência e Espionagem
Ementa	
Apresentar e discutir aspectos relacionados às técnicas e práticas utilizadas em processos de inteligência e espionagem. Esta disciplina tem o objetivo de preparar o egresso à familiarização das técnicas e tecnologias atualmente utilizadas em cibersegurança relacionados aos processos de inteligência, contra inteligência, terrorismo, contraterrorismo, espionagem, contraespionagem e engenharia social.	

O egresso será levado a conhecer a doutrina da Inteligência no Brasil (ABIN), assim como a respectiva fonte de informações como fontes humanas, abertas, de imagens e de sinais. O egresso ainda conhecerá na prática, a aplicação da segurança em dispositivos pessoais e redes sociais. As aulas serão divididas em 4 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. Rio Janeiro: Editora Brasport, 2017. CAROTA, J. C. Inteligência empresarial. Rio Janeiro: Editora Freitas Bastos, 2018 WOLOSZYN, A. L. Guerra nas sombras: os bastidores dos serviços secretos internacionais. São Paulo: Editora Contexto, 2013.
Bibliografia Complementar
CAMARGO, P. S. de. Liderança e linguagem corporal: técnicas para identificar e aperfeiçoar líderes. São Paulo: Editora Summus, 2018. WENDT, E. e JORGE, H. V. N. Crimes cibernéticos: ameaças e procedimentos de investigação. Rio Janeiro: Editora Brasport, 2017: 2ª ed.

Disciplina	Cybersecurity Incident Response
Ementa	
Apresentar e discutir aspectos relacionados às técnicas e práticas utilizadas em processos de resposta a incidentes em cibersegurança Esta disciplina tem o objetivo de preparar o egresso à familiarização das técnicas e tecnologias atualmente utilizadas em cibersegurança relacionados aos processos de resposta a incidentes, por meio de conhecimento dos times de resposta a incidentes denominados CSIRTs, conhecendo a composição destes times no Brasil e no Mundo. O egresso será familiarizado ao processo de estabelecimento e manutenção de um CSIRT, assim como a prática em processo de detecção, triagem, notificação, análise e resposta de um incidente. As aulas serão divididas em 4 encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à aplicação de protocolos relacionados à resposta em incidentes.	
Bibliografia Básica	

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

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

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

Bibliografia Complementar

THE HONEYNET PROJECT. Conheça seu inimigo. São Paulo: Pearson, 2002.

YATIRAJ, S. Quick Review of Forensic Medicine. New Delhi, India: Jaypee, 2013.

Disciplina	Defesa Cibernética

Ementa

Apresentar e discutir aspectos relacionados às técnicas e práticas utilizadas em processos de ações de preparação e resposta em defesa cibernética.

Esta disciplina tem o objetivo de preparar o egresso à familiarização das técnicas e tecnologias atualmente utilizadas em defesa cibernética, sendo introduzido o conceito de segurança cibernética, sendo ainda apresentado os controles de segurança aplicados às infraestruturas críticas de comunicação, saúde, transporte, energia, economia e demais infraestruturas.

O egresso ainda será familiarizado aos aspectos de segurança aos componentes críticos dispostos no ciberespaço, assim como os aspectos relacionadas às infraestruturas tecnológicas que contribuem às questões de conflito em ambiente virtual.

O egresso será preparado para modelar de 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 cibernéticos, onde será possível vivenciar na prática simulação destes processos por meio de jogos de guerra (War Games).

As aulas serão divididas em 5 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: Editora Contexto, 2018.

SUN T: A arte da guerra. Petrópolis: Editora Vozes, 2014.

CLARKE, R. A.; KNAKE, R.t K. Guerra Cibernética. Rio Janeiro: Editora Brasport, 2015.

Bibliografia Complementar
CAPRINO, W. Trilhas em Segurança da Informação. Rio Janeiro: Editora Brasport 2015. WOLOSZYN, A. L. Guerra nas sombras: os bastidores dos serviços secretos internacionais. São Paulo: Editora Contexto, 2013.

Disciplina	Business Continuity Management
Ementa	
Apresentar e discutir aspectos relacionados às práticas utilizadas em processos de continuidade de negócios em cibersegurança. Esta disciplina tem o objetivo de preparar o egresso à familiarização dos processos atualmente utilizados em cibersegurança relacionados aos processos de continuidade de negócios, por meio da gestão de crises e continuidade de negócios. O egresso será familiarizado 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 5 encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados 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 Janeiro: Editora Interciência, 2013. CAMPOS, J. F. M. Bombeiro civil e gerenciamento de desastres e crises. Curitiba InterSaberes, 2017. HILLER, A. G. Proteção e defesa civil. Curitiba: Editora InterSaberes, 2018.	
Bibliografia Complementar	
NUNES, L. H. Urbanização e desastres naturais. São Paulo: Editora Oficina de Textos, 201 PEREIRA JR, J. H. P. Plano de continuidade de negócios aplicado à segurança da informação. Dissertação de Mestrado: Porto Alegre: Universidade Federal do Rio Grande do Sul, 2008.	

Disciplina	Inteligência Artificial & Machine Learning
Ementa	
Apresentar e discutir aspectos relacionados às tecnologias e práticas utilizadas em processos de inteligência artificial. Esta disciplina tem o objetivo de preparar o egresso à familiarização dos processos atualmente utilizados em cibersegurança relacionados aos processos de inteligência artificial, onde o egresso será introduzido ao tema de I.A. e Machine Learning, conhecendo ainda as diferenças entre estes conceitos. O egresso ainda conhecerá o funcionamento do *Deep Learning*, método utilizado para o aprendizado de em sistemas autônimos. As aulas serão divididas em 4 encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados à aplicação de boas práticas relacionadas à inteligência artificial quando aplicados em cibersegurança.	
Bibliografia Básica	
LUGER, G. Inteligência artificial. São Paulo: Pearson, 2013. MEDEIROS, L. F. de. Inteligência artificial aplicada: uma abordagem introdutória. Curitiba: Editora InterSaberes, 2018. CAROTA, J. C.. Inteligência empresarial. Rio Janeiro: EditoraFreitas Bastos, 2018.	
Bibliografia Complementar	
ANTERO, A. O. Inteligência Artificial: teórica e prática. São Paulo: Livraria da Física, 2009. MUNHOZ, A. S. Fundamentos de tecnologia da informação e análise de sistemas para não analistas. Curitiba: Editora InterSaberes, 2017.	

Disciplina	Critical infrastructure security
Ementa	
Apresentar e discutir aspectos relacionados às tecnologias e práticas utilizadas em processos de proteção de infraestruturas críticas. Esta disciplina tem o objetivo de preparar o egresso à familiarização dos processos atualmente utilizados em cibersegurança relacionados aos dispositivos pessoais e correlatos, incluindo aqueles relacionados à consumerização. O egresso ainda conhecerá técnicas e tecnologias, visando a proteção de ambientes de Big Data, IoT e sistemas embarcados, ambientes industriais (SCADA) e Ethernet Industrial. O egresso ainda será melhor familiarizado ao tema das criptomoedas e Bitcoin, assim como as tendências do mercado em Cibersegurança.	

As aulas serão divididas em 3 encontros presenciais com cada turma, com a abordagem dos assuntos principais relacionados 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: Editora InterSaberes 2016. ALMEIDA, C. A. B. de. Tecnologias aplicadas à segurança: um guia prático. Curitiba: Editora InterSaberes 2018. LINO, A. G. H. Proteção e defesa civil. Curitiba: Editora InterSaberes, 2018.
Bibliografia Complementar
HINDSBERGEN, J. et al. Fundamentos de Segurança da Informação. Rio Janeiro: Brasport, 2018. VERAS, M. Computação em Nuvem. Rio Janeiro: Editora 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	
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: Editora HSM, 2012. OSTERWALDER, A; PIG, Y. Business Model Generation - inovação em modelos de negócios. Rio Janeiro: Editora Alta Books, 2011.	
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.

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.

PROCESSO DE AVALIAÇÃO

O desempenho do grupo de alunos em cada disciplina 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 avaliação por participação em sala de aula que permita destacar-se junto aos demais colegas presentes em sala de aula. As avaliações levam em consideração a qualidade dos trabalhos e não somente a entrega dos mesmos. A média destes 3 critérios mais o ponto de participação (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.

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. Cabe ao Professor a decisão de indicar ou não o projeto a concorrer ao Startup One

Todos os projetos (TCC - trabalhos de conclusão de curso) relacionados a 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 da competição Startup One não é obrigatória e é totalmente a facultativa participação pela decisão dos alunos e pela 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 indicá-lo através de formulário de avaliação, disposto no portal da FIAP.

A avaliação dos projetos indicados ao TOP30 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). Estes projetos submetidos à segunda fase receberão treinamento extra específico para estarem preparados para a apresentação de seus projetos a banca julgadora (*Pitch*).

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 a 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. Atual coordenador no MBA em CyberSecurity – Forensics, Ethical Hacking & DevSecOps e professor em diversas outras disciplinas em pós-graduação e graduação na FIAP. Professor em instituições de ensino como IPOG, UNIFOR e IBG. Foi professor na Universidade Presbiteriana Mackenzie e 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 online nos mais diversos canais de comunicação de cobertura regional e nacional no Brasil e internacional como Argentina e Colômbia em meios como TV Globo, SBT, Valor Econômico, Estado de São Paulo, entre outros.