Cibersegurança

O Curso de Especialização em Cibersegurança da PUCPR está organizado em dois principais eixos de formação. O primeiro fornece a capacitação do estudante na área de Segurança de
Infraestrutura de Rede, focando no currículo de formação e certificação Cisco CyberOPS com treinamentos práticos e oficiais em parceria com a empresa, onde os estudantes do curso ganham acesso ao sistema web da academia Cisco (netacad.com), com acesso ao material on-line, simuladores, redes sociais, materiais adicionais, etc.., disponibilizados pela própria Cisco, além de terem direito a fazer uma prova no final dos módulos que dará desconto na prova de certificação, conforme política da Cisco. O segundo eixo segue os currículos de certificação da EC-COUNCIL por meio da parceria oficial estabelecida pela PUCPR (EC-COUNCIL Partner). No caso, são 6 módulos nos eixos Ethical Hacking Essentials (EHE), Network Defense Essentials (NDE) e Digital Forensics Essentials (DFE). A parceria permite o compartilhamento com os estudantes do livro (ebook) oficial, sem custo, e vouchers para obtenção de desconto na prova de certificação, conforme política vigente e definida pela EC-COUNCIL. Por fim, outros módulos abordam aspectos legais da gestão da informação, importante no momento da implantação da LGPD no Brasil, normas e padrões de segurança, Fundamentos de Ciência de Dados, entre outros. Aulas práticas são viabilizadas pelo fornecimento de máquinas virtuais e uso de plataformas online, conforme necessidade de cada módulo.
O egresso do curso de Cibersegurança é um profissional consciente da relevância da segurança cibernética na sociedade, capaz de atuar de forma autônoma ou em corporações, na implantação e uso de sistemas, plataformas e metodologias relacionadas, bem como realizar a integração no campo das tecnologias da informação e comunicação.

O que é cibersegurança?

A Cibersegurança é frequentemente referida como proteção de tecnologia da informação (TI), enfatizando a necessidade de proteger máquinas, redes, serviços e dados contra acesso não autorizado. A segurança cibernética e os ataques cibernéticos estão se tornando mais relevantes no mundo digital em constante mudança, intensificando a necessidade de especialistas nesta área.

Quem pode fazer uma especialização em Cibersegurança?

O curso de Cibersegurança pode ser feito por profissionais de tecnologia da informação e comunicação, engenharia e áreas afins que tenham interesse em se especializar na gestão e implantação da cibersegurança em ambientes corporativos.

Destina-se tanto a recém-formados quanto a profissionais atuantes no mercado de trabalho, no início ou em fase de consolidação de suas carreiras, quando o curso irá proporcionar atualização de conhecimentos ou aquisição de novas habilidades e competências para atuar em um mercado em constante expansão.

Por que fazer uma especialização em Cibersegurança na PUCPR?

Na PUCPR, a Especialização em Cibersegurança forma profissionais consciente da relevância da segurança cibernética na sociedade, capazes de atuar de forma autônoma ou em corporações, na implantação e uso de sistemas, plataformas e metodologias relacionadas, bem como realizar a integração no campo das tecnologias da informação e comunicação.

A Pós-Graduação da PUCPR pode ser feita à distância, com aulas online e ao vivo, facilitando o acesso de alunos em

todo o país.Público-AlvoProfissionais de tecnologia da informação e comunicação, engenharia e áreas afins que tenham interesse em se especializar na gestão e implantação da Cibersegurança em ambientes corporativos. Destina-se tanto a recém-formados quanto a profissionais atuantes no mercado de trabalho, no início ou em fase de consolidação de suas carreiras, quando o curso irá proporcionar atualização de conhecimentos ou aquisição de novas habilidades e competências dentro de sua área de atuação.

Campus:
Curitiba

Modalidade:
EAD

Formato:
Aula Online ao Vivo

Duracao:
19 meses

Periodicidade:
Quinzenal

Mensalidade:
R$ 499.00

Inscricao:
Clique aqui

Disciplinas

Gestão Ágil de Projetos

Esta disciplina aborda assuntos relacionados às práticas e ferramentas da Gestão Ágil de Projetos. Serão discutidos conceitos sobre a origem da gestão, contexto ágil nas organizações, cultura e liderança ágil e os frameworks ágeis Scrum, Kanban e SAFe. Ao final da disciplina, o participante é capaz de analisar a adoção de um framework ágil de acordo com o contexto das organizações e, também, aplicar as práticas da agilidade na liderança e processos gerencias da organização.

Sistemas de Virtualização e Orquestração de Containers

Esta disciplina trata da virtualização de recursos e das arquiteturas de cloud computing. Ao final, os estudantes são capazes de desenvolver projetos em ambientes multi-tenant, envolvendo containers e orquestração de recursos.

Fundamentos de Ciência de Dados: Análise, Seleção e Visualização

Administração de Sistemas Linux

Esta disciplina aborda os fundamentos da administração de Sistemas Linux. Ao final, os estudantes são capazes de realizar os procedimentos básicos de administração, envendo o uso do shell e dos sistemas de arquivos.

Aspectos Legais de Segurança e Privacidade

Esta disciplina é destinada a compreender os impactos que a Lei Geral de Proteção de Dados (LGPD) traz para os processos de governança de TI. Nela, os estudantes conhecem os conceitos, implicações, regras, stakeholders e processos envolvidos na LGPD aplicados à TI. Ao final, os estudantes podem analisar os impactos da LGPD relacionados aos processos de governança de TI e de gerenciamento de serviços com base na legislação vigente.

TCC - Especialização

Seminários Avançados em TICs

Tópicos especiais em Tecnologia da Informação e Comunicação. Cases Corporativos. Tendências e Tecnologias.

Projeto de Aplicação

Esta disciplina trata da estrutura do trabalho científico, bem como dos tipos e métodos de pesquisa. Ao final, o estudante desenvolve seu trabalho de conclusão de curso com base na temática definida pelo desafio de aplicação proposto.

Cisco CCNA CyberOps I

Esta disciplina aborda os fundamentos associados à cybersecurity. Ao final, os estudantes compreendem a relevância da utilização de técnicas de segurança, bem como a arquitetura de protocolos e serviços relacionados.

Cisco CCNA CyberOps II

Esta disciplina trata dos sistemas de criptografia e da proteção de endpoints. Ao final, os estudantes são capazes de utilizar plataformas e softwares para a implementação de processos de segurança baseados em confidencialidade.

Python Scripting

Esta disciplina trata dos fundamentos de Programação Python. Ao final, o estudante é capaz de desenvolver projetos com a linguagem utilizando recursos básicos e de orientação a objetos.

Ethical Hacking Essentials I

Esta disciplina aborda os fundamentos de segurança ofensiva, onde os estudantes apendem sobre as principais ameaças e vulnerabilidades de sistemas computacionais. Neste primeiro módulo, são apresentadas técnicas e contramedidas para a quebra de senhas, engenharia social e ataques na camada de rede.

Ethical Hacking Essentials II

Esta disciplina aborda ataques e contramedidas de segurança em diversos cenários como aplicações web, redes sem fio, dispositivos móveis, Internet das Coisas e computação em nuvem. No final do módulo, são apresentados fundamentos de testes de invasão (pentest). No final do módulo, os alunos poderão obter um voucher com desconto para realização da prova de certificação EHE – Ethical Hacking Essentials, , conforme política vigente da EC-COUNCIL.

Network Defense Essentials I

Esta disciplina aborda os fundamentos de segurança de redes. São abordados temas como Identificação, Autenticação e Autorização, controles de rede administrativos, físicos e técnicos, segurança em virtualização e computação em nuvem.

Network Defense Essentials II

Esta disciplina aborda a proteção de diferentes cenários como redes sem fio, dispositivos móveis, Internet das Coisas, controles criptográficos, segurança de dados e monitoração de tráfego de rede. No final do módulo, os alunos poderão obter um voucher com desconto para realização da prova de certificação NDE – Network Defense Essentials, conforme política vigente da EC-COUNCIL.

Normas e Padrões de Segurança

Normas da Família ISO 27000. Controles e Políticas de Segurança. Normas NIST. Frameworks de segurança.

Digital Forensics Essentials I

Esta disciplina aborda os fundamentos de forense digital. São abordados temas como o processo de investigação forense, disco rígido e sistemas de arquivos, aquisição e duplicação de dados, combate a técnicas anti forense, e forense em ambiente Windows.

Digital Forensics Essentials II

Esta disciplina aborda a análise forense em ambientes Linux, Mac e redes de computadores. Também apresenta detalhes sobre a análise forense em cenários como ataques web, dark web, e-mail e malwares. No final do módulo, os alunos poderão obter um voucher com desconto para realização da prova de certificação DFE – Digital Forensics Essentials, conforme política vigente do EC-COUNCIL.

Gestão De Segurança E Auditoria De Sistemas

A disciplina trata da gestão de segurança de sistemas e do gerenciamento de Riscos. Ao final, o estaudante é capaz de implementar processos de cibersegurança associados e construir planos de contigência e de recuperação.

Ética.

Analisar os problemas éticos atuais, privilegiando controvérsias relacionadas às atividades profissionais. Ao final, os alunos serão capazes de tomar decisões responsáveis e sustentáveis, de acordo com princípios éticos.

Administração de Sistemas Linux

Esta disciplina aborda os fundamentos da administração de Sistemas Linux. Ao final, os estudantes são capazes de realizar os procedimentos básicos de administração, envendo o uso do shell e dos sistemas de arquivos.

Aspectos Legais de Segurança e Privacidade

Esta disciplina é destinada a compreender os impactos que a Lei Geral de Proteção de Dados (LGPD) traz para os processos de governança de TI. Nela, os estudantes conhecem os conceitos, implicações, regras, stakeholders e processos envolvidos na LGPD aplicados à TI. Ao final, os estudantes podem analisar os impactos da LGPD relacionados aos processos de governança de TI e de gerenciamento de serviços com base na legislação vigente.

TCC - Especialização

Seminários Avançados em TICs

Tópicos especiais em Tecnologia da Informação e Comunicação. Cases Corporativos. Tendências e Tecnologias.

Projeto de Aplicação

Esta disciplina trata da estrutura do trabalho científico, bem como dos tipos e métodos de pesquisa. Ao final, o estudante desenvolve seu trabalho de conclusão de curso com base na temática definida pelo desafio de aplicação proposto.

Cisco CCNA CyberOps I

Esta disciplina aborda os fundamentos associados à cybersecurity. Ao final, os estudantes compreendem a relevância da utilização de técnicas de segurança, bem como a arquitetura de protocolos e serviços relacionados.

Huawei HCIA - Security

Esta disciplina aborda fundamentos de segurança da informação. Ao final, o estudante é capaz de compreender as principais técnicas e processos associados à segurança de hosts, de redes e à análise e operação de segurança em ambientes corporativos.

Python Scripting

Esta disciplina trata dos fundamentos de Programação Python. Ao final, o estudante é capaz de desenvolver projetos com a linguagem utilizando recursos básicos e de orientação a objetos.

Ethical Hacking Essentials I

Esta disciplina aborda os fundamentos de segurança ofensiva, onde os estudantes apendem sobre as principais ameaças e vulnerabilidades de sistemas computacionais. Neste primeiro módulo, são apresentadas técnicas e contramedidas para a quebra de senhas, engenharia social e ataques na camada de rede.

Ethical Hacking Essentials II

Esta disciplina aborda ataques e contramedidas de segurança em diversos cenários como aplicações web, redes sem fio, dispositivos móveis, Internet das Coisas e computação em nuvem. No final do módulo, são apresentados fundamentos de testes de invasão (pentest). No final do módulo, os alunos poderão obter um voucher com desconto para realização da prova de certificação EHE – Ethical Hacking Essentials, , conforme política vigente da EC-COUNCIL.

Network Defense Essentials I

Esta disciplina aborda os fundamentos de segurança de redes. São abordados temas como Identificação, Autenticação e Autorização, controles de rede administrativos, físicos e técnicos, segurança em virtualização e computação em nuvem.

Network Defense Essentials II

Esta disciplina aborda a proteção de diferentes cenários como redes sem fio, dispositivos móveis, Internet das Coisas, controles criptográficos, segurança de dados e monitoração de tráfego de rede. No final do módulo, os alunos poderão obter um voucher com desconto para realização da prova de certificação NDE – Network Defense Essentials, conforme política vigente da EC-COUNCIL.

Normas e Padrões de Segurança

Normas da Família ISO 27000. Controles e Políticas de Segurança. Normas NIST. Frameworks de segurança.

Digital Forensics Essentials I

Esta disciplina aborda os fundamentos de forense digital. São abordados temas como o processo de investigação forense, disco rígido e sistemas de arquivos, aquisição e duplicação de dados, combate a técnicas anti forense, e forense em ambiente Windows.

Digital Forensics Essentials II

Esta disciplina aborda a análise forense em ambientes Linux, Mac e redes de computadores. Também apresenta detalhes sobre a análise forense em cenários como ataques web, dark web, e-mail e malwares. No final do módulo, os alunos poderão obter um voucher com desconto para realização da prova de certificação DFE – Digital Forensics Essentials, conforme política vigente do EC-COUNCIL.

Ética

Analisar os problemas éticos atuais, privilegiando controvérsias relacionadas às atividades profissionais. Ao final, os alunos serão capazes de tomar decisões responsáveis e sustentáveis, de acordo com princípios éticos.

Gestão Ágil de Projetos

Esta disciplina aborda assuntos relacionados às práticas e ferramentas da Gestão Ágil de Projetos. Serão discutidos conceitos sobre a origem da gestão, contexto ágil nas organizações, cultura e liderança ágil e os frameworks ágeis Scrum, Kanban e SAFe. Ao final da disciplina, o participante é capaz de analisar a adoção de um framework ágil de acordo com o contexto das organizações e, também, aplicar as práticas da agilidade na liderança e processos gerencias da organização.

Sistemas de Virtualização e Orquestração de Containers

Esta disciplina trata da virtualização de recursos e das arquiteturas de cloud computing. Ao final, os estudantes são capazes de desenvolver projetos em ambientes multi-tenant, envolvendo containers e orquestração de recursos.

Fundamentos de Ciência de Dados: Análise, Seleção e Visualização