IDESP
Instituto Daryus
de Ensino Superior
Paulista

Pós-Graduação

Forense Digital e Investigação Cibernética

MANUAL DO CURSO

ACORDO DE COOPERAÇÃO
TÉCNICO CIENTÍFICO

FACULDADE
FABAD

IDESP
Instituto Daryus
de Ensino Superior
Paulista

Great Place To Work.
Certificado
Set/2021 - Set/2022
BRASIL

APRESENTAÇÃO

O nosso compromisso é transformar a vida das pessoas. E da mesma maneira que fizemos isso com muitos alunos, faremos o melhor para transformar sua vida pessoal e profissional.

Há mais de 15 anos a Daryus, que tornou-se Instituto Daryus no ano de 2020, promove conhecimento e capacitação profissional de alta qualidade para profissionais e empresas atuando nas áreas de Gestão de Riscos e Continuidade de Negócios, Governança e Gestão de Tecnologia da Informação, Privacidade e Proteção de Dados, Segurança da Informação e Cibersegurança.

Seja em um treinamento de certificação internacional, na pós-graduação ou em projetos de consultoria, nossos professores e consultores são instruídos e orientados a buscar, incessantemente, o equilíbrio entre teoria e prática com o intuito de levar o conhecimento para alunos e empresas, potencializando as competências para enfrentar os desafios contemporâneos.

Instituto Daryus: iluminando mentes, potencializando pessoas e protegendo negócios.

NADIA GUIMARÃES

DIRETORA ACADÊMICA

IDESP
Instituto Daryus
de Ensino Superior
Paulista

PALAVRA DA COORDENADORA

ANA MOURA

COORDENADORA TÉCNICA

A transformação digital da sociedade está afetando o crime, os criminosos e a investigação criminal. Ferramentas técnicas cada vez mais avançadas geram oportunidades para os criminosos e desafios para os investigadores e para o combate ao crime cibernético.

Por outro lado, quase qualquer crime pode ter um conjunto abrangente de fontes de evidências digitais, o que gera um desafio para os criminosos ao tentar esconder evidências, e criam oportunidades para os investigadores digitais.

O curso de pós-graduação Aperfeiçoamento em Forense Digital e Investigação Cibernética foi elaborado para atender as necessidades de profissionais que já atuam no mercado de tecnologia da informação, auditores ou quem está diretamente envolvido com segurança da informação e que buscam conhecer mais sobre os desafios e soluções tecnológicas na formação de provas/evidências em crimes digitais.

COORDENADORES DE PÓS-GRADUAÇÃO

Nossa equipe técnica com ampla experiência de mercado

IDESP
Instituto Daryus de Ensino Superior Paulista

Jeferson D'Addario | Coordenador Técnico

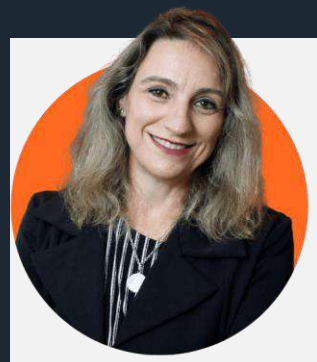
MBA em Gestão e Tecnologia em Segurança da Informação
MBA em Gestão de Riscos e Continuidade de Negócios

Mais de 30 anos de experiência em TI, Riscos e Continuidade de Negócios. Diretor de Consultoria e Presidente IDESP. Certificado como CBCP, ISO 27001 AL, ISO 22301 AL.

André Regazzini | Coordenador Técnico

Pós-graduação em Gestão de Riscos e Compliance

Empresário com mais de 30 anos de experiência em GRC, Auditoria e Compliance. Formação em TI e Direito. Certificado como CISA, CISM e CRISC. Foi Diretor da ISACA.



Ana Moura | Coordenadora Técnica

Pós-graduação Forense Digital e Investigação Cibernética

Profissional de Forense Digital do Governo do Estado de São Paulo há mais de 10 anos. Especialista em Criminalística pelo Exército Brasileiro. Formada em Sistemas da Informação, Pós-graduada em Perícia Forense Digital e Business Project. Certificada como XRI – MSAB, AccessData FTK ACI e MCFE Certification.

Thiago Bordini | Coordenador Técnico

Pós-graduação Cyber Threat Intelligence

Executivo com mais de 20 anos de experiência no mercado de inteligência cibernética. Pós-graduado em MBA Gestão Estratégica de TI e Segurança da Informação. Palestrante em diversos eventos nacionais e internacionais. Membro da HTCIA (High Technology Crime Investigation Association).

Ricardo Tavares | Coordenador Técnico

Pós-graduação Cyber Security

Especialista em Cibersegurança com mais de 16 anos de experiência. Pós-graduado em Forense e MBA em Gestão de Segurança da Informação. Certificado como CISM, CRISC e COBIT (ISACA), GPEN E GIHC (SANS), TOGAF CERTIFIED (TOG) e ITIL e ISMAS (EXIN).

Luiz Ferreira | Coordenador Técnico

Pós-graduação Gestão de Privacidade da Informação

Especialista de Proteção de Dados com mais de 17 anos de experiência atuando em grandes empresas. Pós-graduado em MBA em Gestão de Projetos e Negócios em TI. Certificado como Data Protection Officer – EXIN.

IDESP
Instituto Daryus
de Ensino Superior
Paulista

SOBRE A PÓS-GRADUAÇÃO

OBJETIVOS

Capacitar os profissionais nas mais diversas técnicas de investigação digital, com ampla visão dos aspectos legais envolvidos através de discussão integrada entre as disciplinas.

Capacitar o aluno na ferramenta Forensic Toolkit® (FTK®) e outras ferramentas open source disponíveis no mercado.

Proporcionar ao profissional o desenvolvimento de suas habilidades de investigação em um estudo de caso prático sobre análise de dados e conteúdo de perícia, possibilitando a junção de provas e consequente conclusão do caso.

PÚBLICO-ALVO

- Profissionais atuantes na área de Tecnologia da Informação, com formação acadêmica na área de informática, que desejem especializar-se nos aspectos legais, normativos, regulamentares e tecnológicos referentes à Resposta a incidentes e Forense Digital. Profissionais envolvidos em processos de auditoria e segurança que desejam conhecer mais sobre os desafios e soluções tecnológicas na formação da prova em crimes de ambiente cibernético.

PRÉ REQUISITO

Diploma: De acordo com a Resolução CNE/CES n°1/2018, o acesso em um curso de pós-graduação é exclusivo para portadores de diploma de nível superior e documento que comprove.

Conhecimentos: É necessário ter leitura e compreensão do idioma inglês, operação de computador e familiaridade com o ambiente MS Windows e conhecimentos básicos de investigação digital e procedimentos de análise forense.

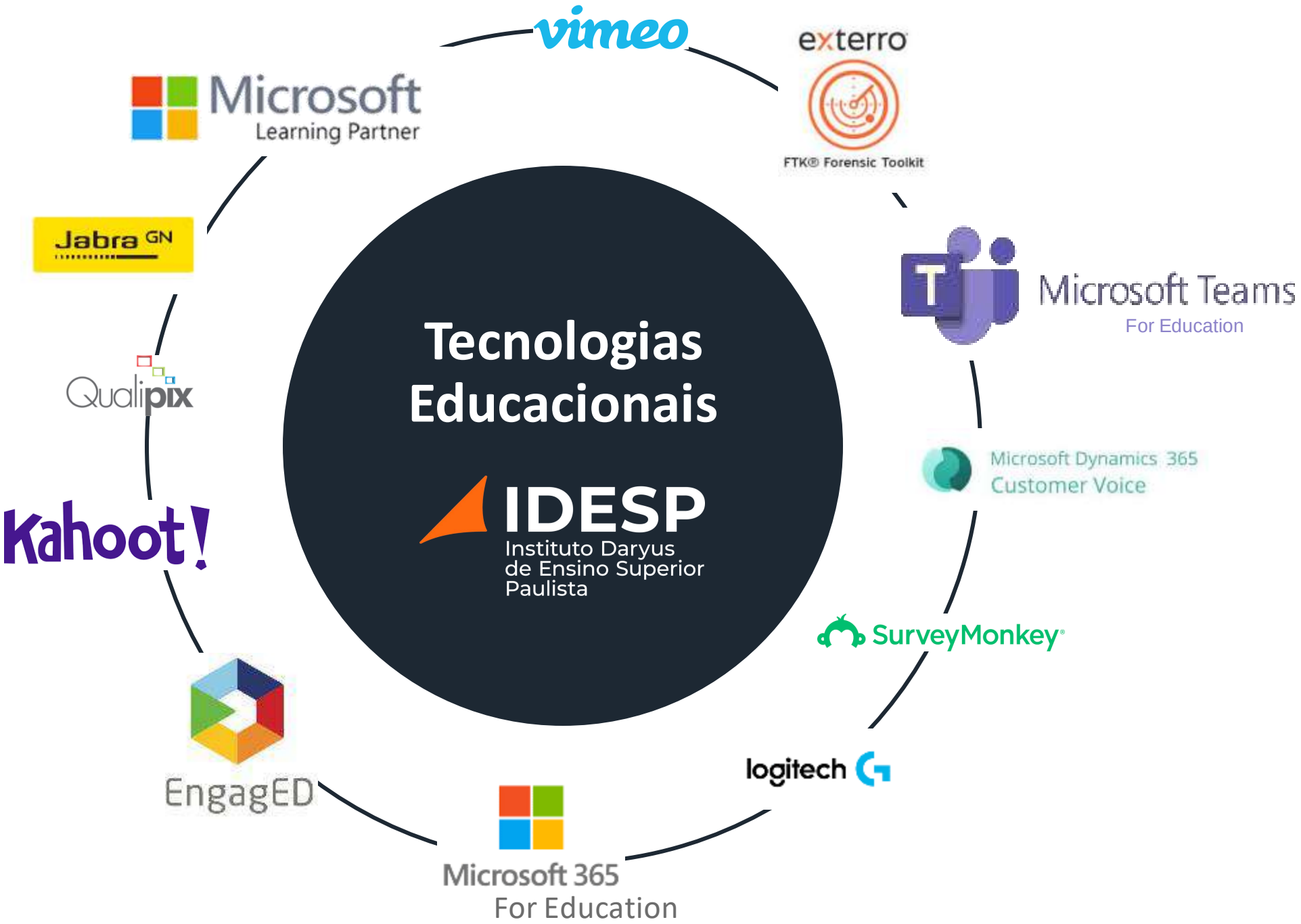
Equipamentos: É necessário possuir notebook com as seguintes configurações mínimas: mínimo 8 GB de RAM, processador i7 e pelo menos 60 GB de espaço livre em disco rígido.

Para efeitos de comprovação do nível de escolaridade como graduação completa é necessário que você tenha o seu diploma em mãos.
O recém-graduado recebe seu diploma oficialmente após a realização da colação de grau.

ECOSSISTEMA DE
ENSINO E QUALIDADE

IDESP
Instituto Daryus de Ensino Superior Paulista

- Material didático de qualidade
- Professores referência de mercado
- Técnicas modernas de aprendizagem
- ★★★ Parcerias internacionais
- Tecnologias educacionais alinhadas ao propósito
- Acompanhamento acadêmico especializado
- Debates e *networking*
- Aplicação prática do conhecimento
- Gamificação
- Satisfação do aluno medida em toda a jornada
- Paixão por ensinar
- Tecnologia robusta e segura


vimeo
exterro
FTK® Forensic Toolkit
Microsoft
Learning Partner
Jabra GN
Qualipix
Kahoot!
Tecnologias
Educacionais
IDESP
Instituto Daryus
de Ensino Superior
Paulista
Microsoft Teams
For Education
Microsoft Dynamics 365
Customer Voice
SurveyMonkey
logitech
EngagED
Microsoft 365
For Education

ACESSOS E BENEFÍCIOS

IDESP
Instituto Daryus de Ensino Superior Paulista

- Biblioteca Pearson
- Pacote de normas ABNT oficiais
- Aulas gravadas
- Conta Microsoft 365 Education com e-mail, OneDrive e Office 365 web
- Sistema acadêmico do aluno
- Aulas com a ferramenta Forensic Toolkit Academic ® (FTK®)
- Grupo de whatsapp exclusivo

DESTAQUES DO CURSO

Corpo docente de destaque e atuante de Mercado.

Aulas com a ferramenta Forensic Toolkit Academic ® (FTK®) – ferramenta de investigação utilizada pelo serviço secreto da Polícia Federal e pelo FBI.

Aplicação da ferramenta em um estudo de caso, onde você executará uma investigação nas oficinas integradoras.

Aulas práticas e teóricas.

Mais de 350 alunos formados.

IDESP
Instituto Daryus de Ensino Superior Paulista

SÃO 180 HORAS DE MUITO APRENDIZADO

MÓDULO 1 - FUNDAMENTAÇÃO À FORENSE DIGITAL

1 - CIÊNCIA DO CRIME: TEORIA, PRINCÍPIOS E FONTES DE INTELIGÊNCIA - 10 HORAS

Apresentar o conceito e origem da ciência forense, adaptação para o conteúdo digital e fonte de inteligência disponível para estudo do dado/informação, tais como navegadores, aplicativos, interceptação telefônica e OSINT.

2 - METODOLOGIA CIENTÍFICA - LEIS, POLÍTICAS E EVIDÊNCIA DIGITAL - 10 HORAS

Apresentar a Legislação, literatura internacional, tipo de aquisição em local de incidente, tipo de ferramenta forense e trato com a coleta e custódia do dado digital e dispositivo físico.

3 - PRÁTICAS APLICADAS À EVIDÊNCIA INVESTIGATIVA - 20 HORAS

Apresentar ao aluno como realizar a identificação da potencial evidência em local de crime, atuar na preservação do dado (teoria de Locard) e condução do dispositivo para análise, além dos tipos de aquisição disponíveis para aplicação.

MÓDULO 2 - ANÁLISE DE INVESTIGAÇÃO CIBERNÉTICA: RESPOSTA À INCIDENTES

1 - IDENTIFICAÇÃO, COLETA, AQUISIÇÃO E PRESERVAÇÃO DE EVIDÊNCIA DIGITAL - 10 HORAS

Uma vez conhecedor do arcabouço legal que cerca a forense digital, o perito passa a lidar com a imagem forense e a potencial evidência digital de modo a entender a importância do processo e seus impactos legais e técnicos, sob a ótica da integridade e autenticidade.

2 - CICLO DE VIDA DO INCIDENTE E PROCESSO DO TRATAMENTO DE INCIDENTES - 10 HORAS

Ciclo de vida de um incidente e suas quatro etapas: Ameaças, Incidente, Dano e Recuperação; tipos de controles que uma organização necessita; processo de gerência de riscos.

3 - ANÁLISE DE DADOS EM SISTEMAS OPERACIONAIS (IOS, LINUX) - 10 HORAS

Estudar os métodos utilizados no processo de dados coletados, identificando os principais artefatos de cada sistema operacional, tornando possível a condução da investigação de modo assertivo.

IDESP
Instituto Daryus de Ensino Superior Paulista

SÃO 180 HORAS DE MUITO APRENDIZADO

4 - ANÁLISE DE DADOS EM SISTEMAS OPERACIONAIS (WINDOWS) - 10 HORAS

Estudar os métodos utilizados no processo de exame de dados coletados, identificando artefatos relevantes que possam conduzir a investigação de modo assertivo, com o estudo de navegadores, logs de registro do Windows e arquivos apagados para eliminação de vestígios digitais.

MÓDULO 3 - TÉCNICAS DE ANÁLISE DE FORENSE DIGITAL

1 - APLICAÇÕES DE DATA ANALYTICS PARA PROCESSOS EM DFIR - 10 HORAS

Estratégias para agregar informações, identificar o perfil do fraudador, utilizar as ferramentas necessárias e estar preparado para receber e analisar essas informações; combinação de várias fontes de dados e a melhoria da qualidade dos processos de análise; conhecimento necessário para analisar os resultados gerados e trabalhar dentro da prevenção à fraude com análises aprofundadas.

2 - PERÍCIA FORENSE DIGITAL: COLETA E ANÁLISE EM DISPOSITIVOS MÓVEIS E IOT - 20 HORAS

Técnicas de extração de dados, recuperação de dados e engenharia reversa em perícia de dispositivos móveis; mecanismos de segurança do iOS, Windows e Android; análise dos arquivos confidenciais em diferentes plataformas; extração de dados das plataformas iOS, Android e Windows; técnicas de recuperação de dados em todas as três plataformas móveis.

Desafios da perícia em novas tecnologias: dados armazenados em diversos tipos de dispositivos como relógios inteligentes e as diversas ferramentas que hoje podem auxiliar no trato com a organização do artefato de origem variada.

3 - COLETA E ANÁLISE DE AMBIENTES CLOUD COMPUTING - 10 HORAS

Metodologia para o trato de evidências; implicações legais das investigações forenses de dados armazenados em ambiente cloud e a evolução do armazenamento em nuvem e seu impacto na perícia digital.

4 - COLETA E ANÁLISE EM AMBIENTES DE REDE - 10 HORAS

Apresentar e discutir como o tráfego de rede entre computadores e ambientes externos se tornou um alvo de grande importância. Identificar potenciais artefatos resultantes de crimes praticados em ambiente de rede é de suma importância para o conhecimento do analista.

5 - COLETA E ANÁLISE DE ARTEFATOS VIA ENDPOINT - 10 HORAS

Com o home office, decorrente da pandemia, um novo cenário corporativo trouxe mais uma inovação: a captura dos dados remotamente, com o conteúdo exibido na ferramenta forense de modo à permitir ao analista uma visão geral das ações suspeitas. Monitorar, coletar o dado de interesse, e analisar remotamente artefatos relevantes para o foco da investigação, é um recurso cada vez mais necessário e utilizado para prevenção de ataques e investigação de ameaças cibernéticas.

SÃO 180 HORAS DE MUITO APRENDIZADO

MÓDULO 4 - OFICINA INTEGRADORA

1 - OFICINA: ENTREGA E PLANEJAMENTO DO ESTUDO DE CASO DE INVESTIGAÇÃO CIBERNÉTICA - 10 HORAS

Estudo de caso: discussão da estratégia e planejamento da investigação. O escopo investigativo organizado para entrega.

2 - OFICINA: DOCUMENTAÇÃO DA CENA DO CRIME E PREPARAÇÃO DAS PROVAS DIGITAIS - 20 HORAS

Toda a órbita de documentos e formalidades necessárias para a composição da entrega do relatório, como formação robusta do elemento de informação até a autoridade para sequência do trâmite jurídico.

3 - OFICINA: APRESENTAÇÃO DO RESULTADO DA INVESTIGAÇÃO: PARECER TÉCNICO E LAUDO PERICIAL - 10 HORAS

Parecer técnico com base nas análises realizadas no material entregue para estudo de caso; síntese de todo o conhecimento absorvido no curso.

AVALIAÇÃO E FREQUÊNCIA

Em cada disciplina o aluno será avaliado, sendo que a nota mínima para aprovação é 7 (sete). A avaliação poderá incluir participação em sala de aula, trabalhos individuais e/ou em grupo, provas, entre outros.

É necessário manter uma frequência mínima de 75% em cada disciplina, sendo que a presença é registrada por meio da ferramenta Teams for Education.

CRONOGRAMA DAS AULAS

180 HORAS

15 DISCIPLINAS

4 MÓDULOS

Integral: aulas quinzenais, aos sábados, das 08h00 às 18h00.

Noturno: aulas uma vez por semana, das 18h30 às 23h00.

O curso tem duração aproximada de 12 meses, podendo sofrer alteração devido ao período de férias, feriados e/ou cancelamentos de aulas por motivo de força maior.

COMO É O PROCESSO SELETIVO?

IDESP
Instituto Daryus de Ensino Superior Paulista

ETAPA 1	ETAPA 2	ETAPA 3	ETAPA 4
Efetue sua inscrição no Processo Seletivo e realize o pagamento da taxa. (não reembolsável em caso de reprovação ou desistência).	Preencha o formulário e a avaliação técnica que seguirão por e-mail e submeta juntamente com o seu currículo para análise.	Aguarde o resultado do processo seletivo que será enviado por e-mail, em até 7 dias corridos. Após o resultado proceda com as instruções que receberá para garantir sua vaga.	Realize a assinatura do contrato, efetue o pagamento da primeira parcela e envie os documentos obrigatórios para efetivar sua matrícula conosco.

MAS FIQUE ATENTO!

O preenchimento da ficha de inscrição no p rocesso seletivo tem o investimento de R$ 220,00 (duzentos e vinte reais) para fins de análise curricular. **Em caso de desistência e/ou não aprovação curricular, o valor não será reembolsado.**

Caso a Coordenação Acadêmica julgue necessário, será feito uma **entrevista por telefone ou pessoalmente/online com o candidato** para **assegurar** as expectativas e os objetivos em relação ao curso.

O **resultado do processo seletivo será enviado por e-mail em até 7 (sete) dias** após o recebimento da inscrição no processo seletivo.

Confira também **outras condições e possibilidades de negociação** com nosso departamento comercial pelo telefone (11) 3285-6539 ou via atendimento *online* acessando nosso website www.idesp.com.br.

PROCESSO DE MATRÍCULA

Após aprovação no processo seletivo, você deverá efetuar o pagamento da **matrícula**. Após o pagamento da matrícula e a assinatura do contrato, os **seguintes documentos serão solicitados** para a real efetivação da sua matrícula conosco:

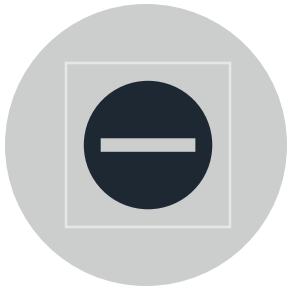
- Cópia do diploma de graduação (frente e verso);
- Cópias da cédula de identidade (RG) e do CPF (a CNH não substitui o RG e o CPF);
- Cópia do comprovante de residência (data até 60 dias);
- 1 Foto 3x4 recente colorida;
- Xerox da Certidão de Nascimento ou Casamento.

SOBRE O MINISTÉRIO DA EDUCAÇÃO - MEC

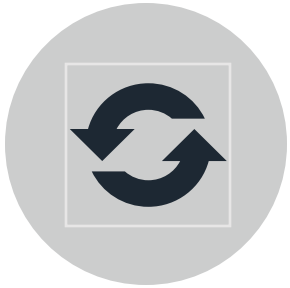
Carga horária: o Ministério da Educação (MEC) qualifica como Pós-graduação *Lato Sensu* em nível de "Especialização", os cursos com igual ou mais de 360 (trezentas e sessenta) horas. Já os cursos com carga horária inferior a 360 (trezentas e sessenta) horas são considerados Pós-graduação em nível de "Aperfeiçoamento", de acordo com a Resolução do CNE/CSE 1/2001, emitida em 3/4/2001 e publicada no Diário Oficial da União de 9/4/2001.

Certificação: os cursos ofertados estão regulados pelo acordo de cooperação técnico-científica entre o IDESP e FABAD, sendo a FABAD regulamentada nos termos da Resolução CNE/CES nº 1 de 06 de abril de 2018, com respaldo no Regimento Geral da Instituição e estão devidamente inseridos no Cadastro Nacional de Oferta do E-MEC, conforme preconiza a Resolução nº 2 de 12 de fevereiro de 2014.

SOBRE CANCELAMENTO OU ADIAMENTO



A instituição **reserva a si o direito de cancelar ou mesmo adiar o curso** por falta de *quórum*, com até 1 (um) dia de antecedência da data prevista para seu início ou por motivo de força maior.



Na hipótese de **adiamento**, serão devolvidos, mediante requerimento expresso do aluno endereçado ao e-mail secretaria@idesp.com.br, 100% (cem por cento) do valor pago, exceto o valor referente ao processo seletivo no valor de R$ 220,00 (duzentos e vinte reais), também por meio de depósito em conta bancária indicada pelo aluno em até 15 (quinze) dias úteis após a informação dos dados bancários.

Na hipótese de **cancelamento**, serão devolvidos automaticamente, 80% (oitenta por cento) do valor pago, sujeito a uma multa de 20%. Além disso, o valor referente ao processo seletivo não será reembolsado.A devolução será realizada por meio de depósito em conta bancária indicada pelo aluno em até 15 (quinze) dias úteis após a informação dos dados bancários.

O **IDESP não se responsabiliza** por quaisquer outros valores que eventualmente tenham sido despendidos pelo aluno, seja a que título for, tais como passagens aéreas ou rodoviárias, combustível, hospedagem, etc., em virtude do cancelamento ou adiamento do curso.


IDESP
Instituto Daryus
de Ensino Superior
Paulista