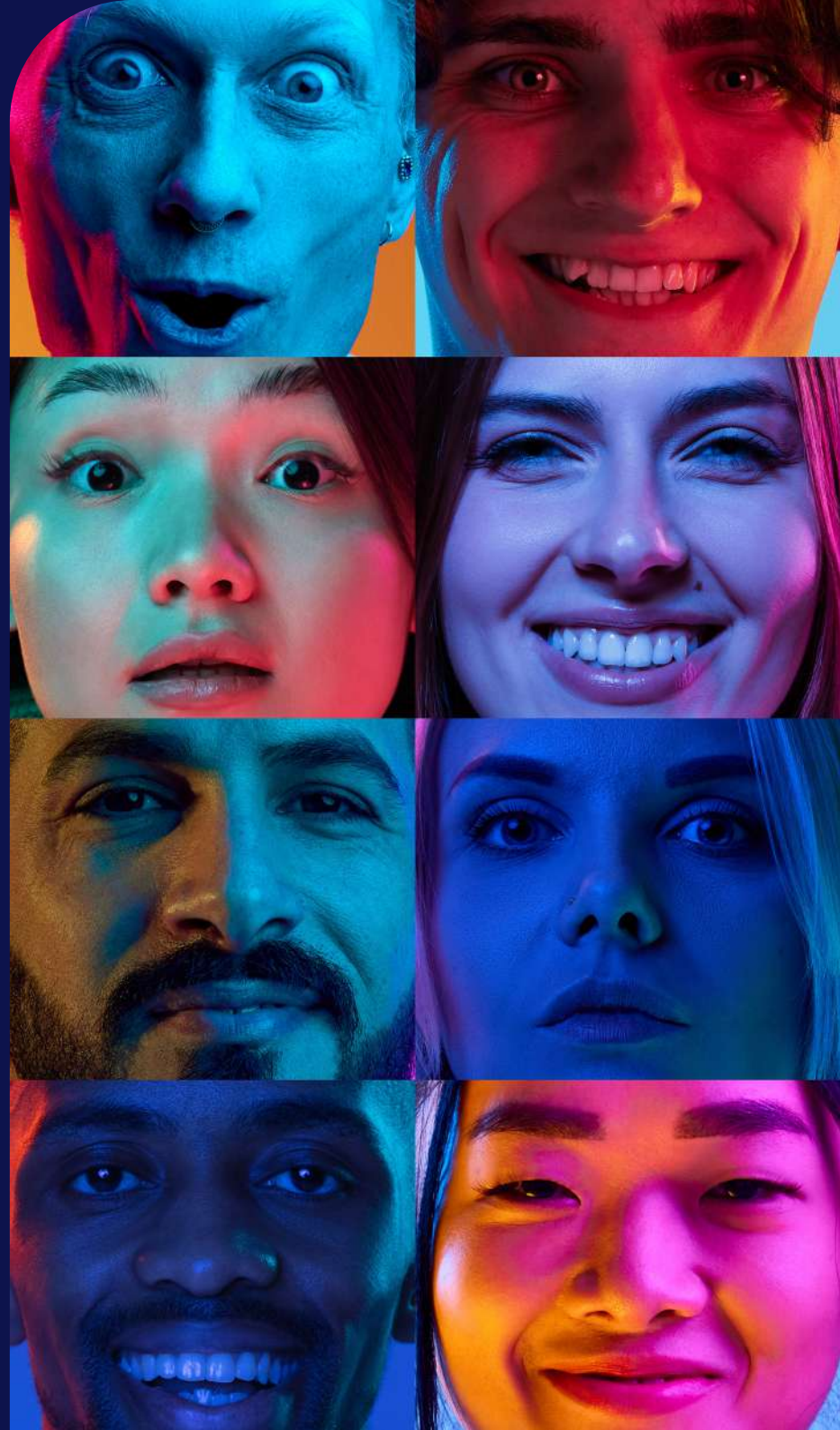


GRAN
FACULDADE

PÓS-GRADUAÇÃO

Pós-Graduação em Direito Digital e Proteção de Dados





Sumário

Por que estudar com o método GRAN de ensino?	3
Conheça nossa metodologia.....	4
Coordenação pedagógica	5
Direito Digital e Proteção de Dados.....	6
Destaques do curso.....	6
Público-Alvo	7
Duração do curso	7
Matriz curricular	8
Conteúdo programático	10
FAQ do curso	14
Diferenciais tecnológicos	15
Ingresso	16

POR QUE ESTUDAR COM O MÉTODO GRAN DE ENSINO?

Disciplinas produzidas em multiformatos, para proporcionar um estudo com mais agilidade, foco e rendimento.

Conteúdo útil para o mercado de trabalho, unindo a teoria à prática, de forma equilibrada, para você poder se desenvolver como um profissional completo e requisitado.

Equipe didática, com professores renomados que oferecem conteúdos alinhados às práticas de mercado, exatamente como você precisa para impulsionar sua carreira.

Plataforma de ensino que acelera o seu aprendizado, por meio de recursos intuitivos e ferramentas tecnológicas, para você estudar no seu ritmo, a qualquer hora e em qualquer lugar, mesmo sem internet.

Certificado emitido por uma instituição reconhecida com nota máxima no MEC.

Valores que cabem no seu bolso, para você estudar o que quer, não o que dá.

Ferramentas de inclusão e acessibilidade para que pessoas que possuam alguma necessidade especial tenham a oportunidade de cursar uma pós-graduação EaD.

EdTech que você já conhece e que é referência em ensino e tecnologia, recomendada por mais de 2 milhões de alunos.

CONHEÇA NOSSA METODOLOGIA

Cursos 100% EaD
compostos por três
módulos, liberados
progressivamente a cada
60 dias.

Avaliação feita por disciplina
no sistema de provas da Gran
Faculdade, com sistema de notas
em valores numéricos, numa escala
de 0 (zero) a 100 (cem) pontos,
considerando-se aprovado aquele
que alcançar a nota mínima de 70
(setenta) pontos.

Disciplinas multiformatos,
com videoaulas, aulas
interativas ao vivo, *slides* e
artigos acadêmicos.

Trabalho de Conclusão de Curso
opcional, conforme Resolução CNE/
CES n. 01, de 06 de abril de 2018.



COORDENAÇÃO PEDAGÓGICA



Prof. Miguel Carvalho
Coordenador

Cientista da Computação e Mestre Informática (2011) pela Universidade Federal do Rio de Janeiro. Há doze anos, atua como professor universitário, consultor de T.I. e palestrante de diversos eventos. Atua, principalmente, nos seguintes temas: Engenharia de Software, Desenvolvimento de Sistemas, Testes de Software, Ciência de Dados, Tecnologia de Web Services, Engenharia de Sistemas IoT, Cultura Maker e Educação STEAM.

DIREITO DIGITAL E PROTEÇÃO DE DADOS



As denominadas novas tecnologias têm gerado desafios que acabam por vindicar a ingerência do Direito. Isso porque, com o crescimento progressivo do acesso à internet, as atividades realizadas nesse ambiente necessitam de análise e regulamentação. As possíveis querelas entre valores como segurança, privacidade e neutralidade da rede são exemplos disso. Assim, dada a sua aplicabilidade, multidisciplinaridade e transversalidade é que o Direito Digital é de importância fundamental para a vida profissional de todo jurista, quer ele atue no setor público, quer no privado.

DESTAQUES DO CURSO

Demonstrar a importância das atividades ocorridas no ambiente cibernético para o Direito

Aprofundar os estudos dos direitos subjetivos e de sua fruição no ambiente digital

Examinar alguns dos desafios que surgiram para o Direito com o despontamento das “novas tecnologias”

Analisar a legislação e a regulamentação brasileira sobre o direito digital, em especial sobre a Estratégia Nacional de Segurança da Informação



PÚBLICO-ALVO

Graduados e pós-graduados em Direito, estudantes e profissionais que queiram se aprofundar em Direito Digital e Proteção de Dados.

DURAÇÃO DO CURSO

O curso de Direito Digital e Proteção de Dados tem duração de 6 (seis) a 18 (dezoito) meses. É ofertado na modalidade EaD com o uso das melhores tecnologias do mercado das *EdTechs*.

MATRIZ CURRICULAR

	Unidade Curricular	Carga Horária
01	Direitos Humanos	25h
02	Crimes Virtuais	20h
03	Gestão de Segurança da Informação e Normas 27001-27002 e 27005	25h
04	Legislação Aplicada à Segurança da Informação	25h
05	Governança e Regulação da Internet	12h
06	Regulação das Plataformas Digitais, Anonimato, Liberdade de Expressão e Fake News	8h
07	Tecnologias Emergentes e Inovação Digital	10h
08	Blockchain e Soluções Descentralizadas	7h
09	Startups, SandBox Regulatório, Open Banking e Fintechs	7h
10	Política Nacional de Segurança da Informação e Cibernética	25h
11	Segurança Cibernética – Histórico, Desconfusão Conceitual, Definições e Natureza Jurídica	22h
12	Mecanismos Constitucionais para Efetivação de Direitos Frente às Novas Tecnologias	10h
13	Marco Legal da Proteção de Dados: Cenário Global, Europeu e Regional	15h
14	Marco Legal da Proteção de Dados no Brasil	15h
15	Proteção de Dados Pessoais e Direitos do Titular	17h

16	Bases Legais do Tratamento de Dados Pessoais no Âmbito da LGPD: Consentimento e Legítimo Interesse	12h
17	Relatórios de Impacto de Dados Pessoais, Agentes de Tratamento e o Papel do Encarregado	20h
18	Tratamento de Dados Pessoais pelo Poder Público e a Autoridade Nacional de Proteção de Dados	25h
19	Transferências Internacionais de Dados Pessoais	15h
20	Boas Práticas de Segurança da Informação à Luz da LGPD e Comunicação de Incidentes	20h
21	Tópicos Especiais em Proteção de Dados	12h
22	Tópicos Especiais em Proteção de Dados II	5h
23	Tópicos Especiais em Proteção de Dados III	5h
24	Tópicos Especiais em Proteção de Dados IV	3h
TOTAL DAS DISCIPLINAS		360 horas
Trabalho de Conclusão de Curso (OPCIONAL)		40 horas
TOTAL DO CURSO		400 horas

CONTEÚDO PROGRAMÁTICO

Conteúdo Programático do Curso	
Disciplina	Conteúdo
DIREITOS HUMANOS	Aspectos históricos dos Direitos Humanos. Fundamentação Religiosa, filosófica e científica dos Direitos Humanos. Dignidade Humana e vulnerabilidade. Fontes dos Direitos Humanos. Características e Dimensões dos Direitos Humanos. As Nações Unidas. As Declarações e os Tratados Internacionais sobre Direitos Humanos. Responsabilidade internacional por violação aos Direitos Humanos. Sistemas de proteção aos Direitos Humanos. Direitos Humanos e o ordenamento jurídico brasileiro. A proteção aos diversos grupos vulneráveis. A proteção à cultura afro-brasileira e indígena na evolução dos Direitos Humanos. Órgãos de Direitos Humanos no Brasil. Questões e problemas atuais de aplicação dos Direitos Humanos. Direitos Humanos, Democracia e Cidadania. Educação e Cultura em Direitos Humanos.
CRIMES VIRTUAIS	Gestão de Segurança da Informação. Análise e avaliação de riscos da informação. Cibersegurança, proteção de dados e segurança da informação. Direito Penal Cibernético (Autoria, materialidade, tipicidade e local do crime). Crimes de Informática. Crimes eletrônicos. Crimes sexuais virtuais. Investigação e provas no ambiente cibernético. Elaboração de laudos periciais. Estudo de casos.
GESTÃO DE SEGURANÇA DA INFORMAÇÃO E NORMAS 27001-27002 E 27005	Definições e conceitos de segurança. Visão geral das Normas. Estrutura. Políticas de segurança da informação. Organização da segurança da informação. Segurança em recursos humanos. Gestão de ativos. Controle de acesso. Criptografia. Segurança física e do ambiente. Segurança nas operações. Segurança nas comunicações. Aquisição, desenvolvimento e manutenção de sistemas. Relacionamento na cadeia de suprimento. Gestão de incidentes de segurança da informação. Aspectos da segurança da informação na gestão da continuidade do negócio. Conformidade. Definições e conceitos de segurança. Visão geral das Normas. Estrutura. Descrição do processo do ISRM. Estabelecimento de contexto. Informações sobre avaliação de riscos de segurança. Tratamento de riscos à segurança da informação. Admissão de riscos. Segurança da informação. Comunicação de riscos à segurança da informação. Rastreamento e revisão de riscos de informações de segurança.
LEGISLAÇÃO APLICADA À SEGURANÇA DA INFORMAÇÃO	LEI GERAL DE PROTEÇÃO DE DADOS e LEI DE ACESSO À INFORMAÇÃO: Conceitos, tratamento dos dados pessoais, direitos do titular, tratamento de dados pessoais pelo poder público, transferência internacional de dados, agentes de tratamento de dados pessoais, segurança e boas práticas, fiscalização, autoridade nacional de proteção de dados, conselho nacional de proteção de dados pessoais e da privacidade. Acesso à informação e sua divulgação, procedimento de acesso à informação, restrições de acesso à informação, responsabilidades. GESTÃO DA CONTINUIDADE DE NEGÓCIOS: Sistemas de gestão de continuidade de negócios, plano de continuidade de negócios.

GOVERNANÇA E REGULAÇÃO DA INTERNET	Definição e evolução da governança da Internet. Ferramentas, abordagens e padrões. Infraestrutura de telecomunicações e da internet. Transmission Control Protocol/ Internet Protocol (TCP/IP). Sistema de nomes de domínio (DNS). Computação em nuvem. Acesso à internet. Instrumentos jurídicos. Regulação da internet: âmbito global e nacional. Princípios garantidores de uma internet livre, aberta e inclusiva.
REGULAÇÃO DAS PLATAFORMAS DIGITAIS, ANONIMATO, LIBERDADE DE EXPRESSÃO E FAKE NEWS	Espaços de decisão no âmbito das plataformas digitais. Direitos dos usuários das plataformas digitais. Regulação das plataformas digitais. Direito ao anonimato e direito ao esquecimento. Desinformação e ameaça ao princípio democrático. Fake News: aspectos jurídicos relevantes.
TECNOLOGIAS EMERGENTES E INOVAÇÃO DIGITAL	Definição e fundamentos da Inteligência Artificial. Inteligência Artificial e direitos de personalidade. Inteligência Artificial e responsabilidade civil. A regulamentação da IA no Brasil e a Estratégia Brasileira de Inteligência Artificial. Histórico, definição e enquadramento legal da tecnologia móvel de 5ª Geração. Origem, definição e importância. Segurança e privacidade no âmbito da IoT. IoT e proteção de dados pessoais. Cidades Inteligentes.
BLOCKCHAIN E SOLUÇÕES DESCENTRALIZADAS	Análises conceituais da tecnologia blockchain e das criptomoedas. Oferta inicial de moedas, sistema bancário, meios de pagamento pela internet, regulação, big data, smart contracts. Aplicações baseadas em Blockchain. Contratos inteligentes (Smart Contracts). NFT. Questões tributárias. Questões criminais.
STARTUPS, SANDBOX REGULATÓRIO, OPEN BANKING E FINTECHS	Marco Regulatório das Startups. Regulação da Proteção de Dados para Agentes de Tratamento de Pequeno Porte. Regulação e Inovação. Sandbox Regulatório. Dinâmicas únicas do mercado da revolução FinTech. Impactos nas indústrias relacionadas. OpenBanking. Aspectos jurídicos relevantes.
POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Decreto n. 10.222, de 5 de fevereiro de 2020, que estabelece a Estratégia Nacional de Segurança Cibernética. Ações e objetivos estratégicos. Eixos temáticos. Análise da Política Nacional de Segurança da Informação.
SEGURANÇA CIBERNÉTICA – HISTÓRICO, DESCONFUSÃO CONCEITUAL, DEFINIÇÕES E NATUREZA JURÍDICA	Conceito jurídico de cibersegurança. Conceitos básicos: confidencialidade, integridade, disponibilidade, garantia, autenticidade e anonimato. Princípios de segurança. Conceitos criptográficos: encriptação, assinaturas digitais, funções hash criptográficas e certificação dos digitais. Programas maliciosos (malware). Natureza jurídica da cibersegurança. Normativos, acordos e tratados internacionais sobre cibersegurança. A cibersegurança e as suas vertentes. A cibersegurança como uma questão transnacional e os dilemas da soberania.

MECANISMOS CONSTITUCIONAIS PARA EFETIVAÇÃO DE DIREITOS FRENTE ÀS NOVAS TECNOLOGIAS	A globalização como contexto de um constitucionalismo multinível. A segurança cibernética como munus de um constitucionalismo multinível. Constitucionalismo multinível. O constitucionalismo multinível aplicado aos direitos fundamentais. Transconstitucionalismo. Interconstitucionalidade. Constitucionalismo global ou societal. Constitucionalismo em rede.
MARCO LEGAL DA PROTEÇÃO DE DADOS: CENÁRIO GLOBAL, EUROPEU E REGIONAL	Conhecer a proteção de dados pessoais na Alemanha: a decisão da Corte Constitucional Alemã relativa à Lei do Censo de 1982 e o surgimento de um direito fundamental autônomo à proteção dos dados pessoais. Conhecer a proteção de dados pessoais nos Estados Unidos da América: o reconhecimento do direito à privacidade, o sistema americano de proteção de dados pessoais e os instrumentos para a transferência internacional de dados (Safe Harbor e Privacy Shield). Conhecer a proteção de dados segundo instrumentos internacionais de cooperação: Convenção 108 do Conselho Europeu; Diretrizes sobre a privacidade e os fluxos transfronteiriços de dados pessoais da Organização para a Cooperação e Desenvolvimento Econômico (OCDE); Padrões de Proteção de Dados Pessoais para os Estados Ibero-Americanos da Rede Ibero-Americana de Proteção de Dados (RIPD). Conhecer a proteção de dados pessoais no Direito comunitário europeu – da Diretiva 95/46 ao Regulamento Geral de Proteção de Dados (GDPR em inglês).
MARCO LEGAL DA PROTEÇÃO DE DADOS NO BRASIL:	Análise da Lei n. 12.527, de 18 de novembro de 2011, a Lei de Acesso à Informação (LAI) e os direitos e deveres dela decorrentes relativos à proteção de dados pessoais. Análise da Lei nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet (MCI), nos aspectos relacionados à proteção de dados pessoais. Análise da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), e os direitos e deveres dela decorrentes. Conhecer a influência de normais internacionais na elaboração desses normativos. Conhecer aspectos relacionados à tramitação dos projetos de lei que deram origem à LAI, ao MCI e à LGPD. Conhecer as disposições da LAI, do MCI e da LGPD que se interconectam na proteção de dados pessoais.
PROTEÇÃO DE DADOS PESSOAIS E DIREITOS DO TITULAR	Princípio da finalidade. Princípio da adequação. Princípio da necessidade. Livre acesso. Qualidade dos dados. Transparência. Segurança. Prevenção. Não discriminação. Responsabilização e prestação de contas. Âmbito de aplicação territorial da LGPD. Direito à privacidade x proteção de dados pessoais. Ameaça à proteção de dados e o risco de influência das redes sociais. Legislação internacional concernente à privacidade e à proteção de dados, em especial o RGPD (União Europeia). Fundamentos da LGPD, em especial o respeito à privacidade e à autodeterminação.
BASES LEGAIS DO TRATAMENTO DE DADOS PESSOAIS NO ÂMBITO DA LGPD: CONSENTIMENTO E LEGÍTIMO INTERESSE	Bases legais. Consentimento do titular. Cumprimento de obrigação legal ou regulatória pelo controlador. Tratamento de dados para execução de políticas públicas. Realização de estudos por órgãos de pesquisa. Execução contratual. Exercício regular de direito. Proteção da vida. Tutela da saúde. Legítimo interesse. Proteção do crédito.

RELATÓRIOS DE IMPACTO DE DADOS PESSOAIS, AGENTES DE TRATAMENTO E O PAPEL DO ENCARREGADO	O papel do controlador. O papel do operador. O papel do encarregado. Obrigações dos agentes de tratamento. Da Responsabilidade e do ressarcimento de danos. Relatório de Impacto à proteção de dados pessoais: documentação, medidas, salvaguardas e mecanismos de mitigação de riscos. Programa de Governança em Privacidade.
TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO E A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS	Analisar as regras e limites que a LGPD impõe para o tratamento de dados pessoais pelo poder público. Conhecer as competências da ANPD – fiscalizadora, sancionadora e orientadora. Conhecer os limites materiais e jurídicos para a atuação da ANPD.
TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS	Definição de transferências internacionais de dados pessoais. Diferenciação de transferências internacionais e trânsito de dados pessoais. Decisão de adequação. Cláusulas-padrão contratuais. Normas corporativas globais. Cláusulas contratuais específicas. Selos, certificados e códigos de conduta. Outras possibilidades.
BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO À LUZ DA LGPD E COMUNICAÇÃO DE INCIDENTES	A importância das medidas de segurança por parte dos agentes de tratamento de dados pessoais. Anonimização e pseudonimização. O papel da Autoridade Nacional de Proteção de Dados na regulamentação de padrões técnicos e medidas de segurança. Proteção de dados pessoais e privacidade by design e by default. Formulação de regras de boas práticas e de governança. Comunicação de Incidentes de Segurança de Dados Pessoais à ANPD. Da fiscalização por parte da ANPD. Das sanções administrativas.
TÓPICOS ESPECIAIS EM PROTEÇÃO DE DADOS	Proteção de dados no âmbito das Relações de Trabalho. Proteção de dados na Saúde. Proteção de dados pessoais na Educação. Proteção de dados pessoais no âmbito das relações de consumo. Proteção de dados pessoais, Processo Civil e resoluções online de disputas.
TÓPICOS ESPECIAIS EM PROTEÇÃO DE DADOS II	Proteção de dados no âmbito das Relações de Trabalho. Proteção de dados na Saúde. Proteção de dados pessoais na Educação. Proteção de dados pessoais no âmbito das relações de consumo. Proteção de dados pessoais, Processo Civil e resoluções online de disputas.
TÓPICOS ESPECIAIS EM PROTEÇÃO DE DADOS III	Proteção de dados no âmbito das Relações de Trabalho. Proteção de dados na Saúde. Proteção de dados pessoais na Educação. Proteção de dados pessoais no âmbito das relações de consumo. Proteção de dados pessoais, Processo Civil e resoluções online de disputas.
TÓPICOS ESPECIAIS EM PROTEÇÃO DE DADOS IV	Proteção de dados no âmbito das Relações de Trabalho. Proteção de dados na Saúde. Proteção de dados pessoais na Educação. Proteção de dados pessoais no âmbito das relações de consumo. Proteção de dados pessoais, Processo Civil e resoluções online de disputas.

FAQ DO CURSO

O curso de Pós-Graduação em Direito Digital e Proteção de Dados é EaD?

Sim. Nosso curso é EaD, com aulas, materiais de apoio e avaliações disponibilizadas no nosso Ambiente Virtual de Aprendizagem (AVA).

O curso de Pós-Graduação em Direito Digital e Proteção de Dados é um curso de Pós-Graduação *Lato Sensu*. O que isso significa?

As pós-graduações *lato sensu* compreendem programas de especialização e incluem os cursos designados como MBA (*Master Business Administration*). Com duração mínima de 360 horas, ao final do curso, o aluno obterá certificado. Ademais, são abertos a candidatos diplomados em cursos superiores e que atendam às exigências das instituições de ensino.

Preciso realizar Trabalho de Conclusão de Curso (TCC)?

A realização de TCC é opcional, conforme Resolução CNE/CES n. 01, de 06 de abril de 2018.

O curso de Pós-Graduação em Direito Digital e Proteção de Dados é autorizado pelo MEC?

Sim. Todos os cursos do Gran Centro Universitário são autorizados pelo Ministério da Educação (MEC).

É possível aproveitar unidades curriculares cursadas anteriormente?

Sim, você pode aproveitar unidades curriculares de disciplinas cursadas ou em curso na pós-graduação da Gran Faculdade. Para isso, é necessário ter obtido aprovação na disciplina que deseja aproveitar e ter finalizado o módulo que a contempla.

O curso conta com calendário de atividades e avaliações?

Sim. O calendário de programações, com as respectivas datas previstas, está disponível no Ambiente Virtual de Aprendizagem (AVA).

DIFERENCIAIS TECNOLÓGICOS

Videoaulas, aulas interativas, artigos acadêmicos, audioaulas e muito mais para você estudar do seu jeito, no seu próprio ritmo.

Secretaria acadêmica virtual: o atendimento à distância de um clique.

Ambiente Virtual de Aprendizagem inovador para estudar de onde e quando quiser, por computador, *tablet*, TV, celular.

Download de materiais para estudo *offline*. Assim você estuda até mesmo nos seus momentos *off*.

App compatível com iOS e Android para você estudar sem distrações.

Player de videoaulas similar ao do YouTube, com legendas, tela escura, anotações e muito mais.

Gran Audiobooks: milhares de audiolivros disponíveis para você.



INGRESSO

A Pós-Graduação evoluiu, e o seu jeito de estudar também! Ter você com a gente nesta jornada de aprendizagem será sensacional.

Comece hoje sua Pós-Graduação e venha conosco revolucionar a educação no Brasil!



Você a poucos



passos de muitos

futuros

gran.com.br

