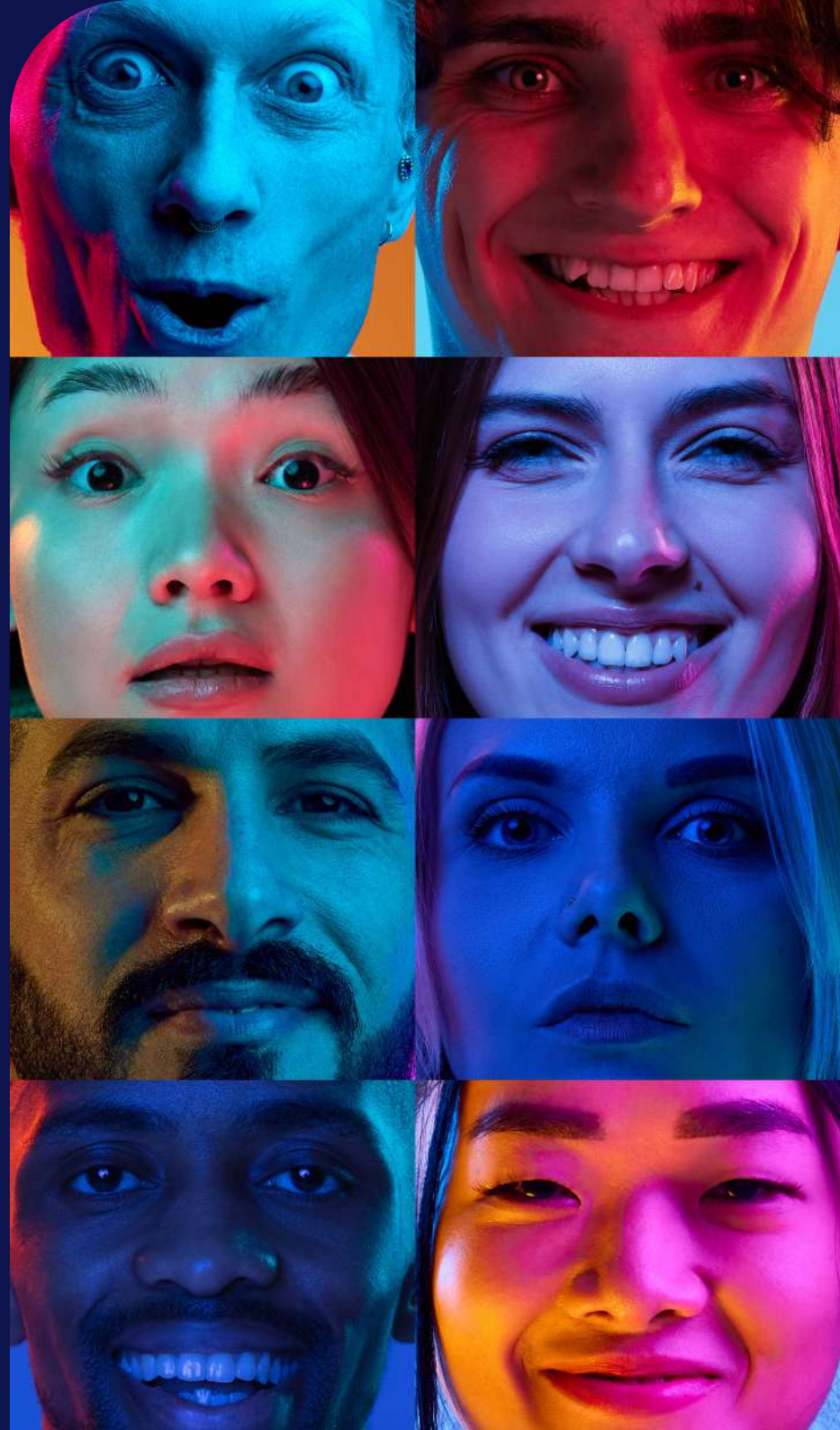


**GRAN**  
FACULDADE

PÓS-GRADUAÇÃO

# Pós-Graduação em Segurança da Informação





# Sumário

Por que estudar com o método GRAN de ensino? .....	3
Conheça nossa metodologia.....	4
Coordenação pedagógica .....	5
Segurança da Informação.....	6
Destaques do curso.....	6
Público-Alvo .....	7
Duração do curso .....	7
Matriz curricular .....	8
Conteúdo programático .....	9
FAQ do curso .....	11
Diferenciais tecnológicos .....	12
Ingresso .....	13

# 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.

# SEGURANÇA DA INFORMAÇÃO



A quantidade de profissionais dessa área é pequena, e sua demanda é crescente. Empresas de todos os portes e áreas de atuação buscam profissionais habilitados e com as competências necessárias ao desempenho das atividades de proteção dos seus ativos, bem como gestão da segurança da informação e continuidade de negócios.

## DESTAQUES DO CURSO

Capacitar e desenvolver habilidades relacionadas à gestão da segurança da informação, continuidade de negócios, desenvolvimento seguro de software, segurança em infraestrutura de T.I, auditoria de sistemas e forense computacional.

Formação em alto nível em relação aos conceitos, tecnologias, normas e frameworks da área de segurança da informação e cibersegurança.



## PÚBLICO-ALVO

Bacharéis, licenciados e tecnólogos, docentes e profissionais da área de tecnologia da informação, profissionais de outras áreas que desejam adquirir conhecimento em uma área de grande relevância na atualidade.

## DURAÇÃO DO CURSO

O curso de Segurança da Informação tem duração de 6 (seis) a 18 (dezoito) meses. Ofertado na modalidade EaD com o uso das melhores tecnologias do mercado das *EdTechs*.

# MATRIZ CURRICULAR

	Unidade Curricular	Carga Horária
01	Fundamentos de Segurança da Informação	22h
02	Organização e Arquitetura de Computadores	27h
03	Gestão de Segurança da Informação e Normas 27001-27002 e 27005	27h
04	Fundamentos de Sistemas Operacionais	22h
05	Segurança em Aplicações Web	27h
06	Forense Computacional	42h
07	Auditoria de Sistemas de Informação	27h
08	Redes de Computadores	47h
09	Segurança da Infraestrutura de TI	27h
10	Criptografia, Certificação Digital e Tópicos Especiais em Segurança da Informação	66h
11	Legislação Aplicada à Segurança da Informação	26h
TOTAL DAS DISCIPLINAS		360 h/a
Trabalho de Conclusão de Curso (OPCIONAL)		40 h/a
TOTAL DO CURSO		400 h/a



# CONTEÚDO PROGRAMÁTICO

Conteúdo Programático do Curso	
Disciplina	Conteúdo
<b>FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO</b>	Conceitos de segurança de computadores. Arquitetura de segurança OSI. Ataques à segurança. Serviços de segurança. Mecanismos de segurança. Política de segurança da informação. Controles de acesso lógico.
<b>ORGANIZAÇÃO E ARQUITETURA DE COMPUTADORES</b>	Introdução à Arquitetura de Computadores. Sistema de Computação. Processadores. Tipos de Memórias. Entrada/Saída. Lógica e Aritmética. Sistemas Numéricos. Aritmética do Computador. Lógica Digital. Unidade Central do Processamento. Conjunto de Instruções. Estrutura e Função do Processador. Paralelismo. Organização Paralela. Processamento Paralelo. Computadores Multicores. Unidades de Processamento Gráfico. Unidade de Controle. Micro-operações. Microarquitetura. Sistema Operacional.
<b>GESTÃO DE SEGURANÇA DA INFORMAÇÃO E NORMAS 27001-27002 E 27005</b>	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. 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.
<b>FUNDAMENTOS DE SISTEMAS OPERACIONAIS</b>	Conceitos básicos. Conceitos de hardware e software. Concorrência. Estrutura do sistema operacional. Processos e threads. Sincronização e comunicação entre processos. Gerência de recursos. Sistemas de arquivos. Virtualização e nuvem.
<b>SEGURANÇA EM APLICAÇÕES WEB</b>	Fundamentos de Segurança em Aplicações Web. Estrutura da Web. Autenticação e Autorização. Mecanismos de Segurança do Navegador. Tipos de Vulnerabilidades. Testes de Segurança. Melhores Práticas para Segurança em Aplicações Web.

<b>FORENSE COMPUTACIONAL</b>	Introdução à Forense Computacional. Produção e Preservação da Prova. Legislação Forense. Cadeia de Custódia. Ferramentas Forenses. Análise Live e Post Mortem. Recuperação de Dados em Dispositivos de Armazenamento. Investigação Computacional. Estrutura do Laudo Pericial.
<b>AUDITORIA DE SISTEMAS DE INFORMAÇÃO</b>	Fundamentos de auditoria de sistemas de informações. Padrões e códigos de ética para auditorias de sistemas de informação. Controles internos e avaliação. Ferramentas e técnicas de auditoria de sistemas de informação. Auditoria de desenvolvimento de sistemas. Auditoria de controle de acesso. Auditoria de operação de sistemas. Auditoria de suporte técnico. Avaliação de software. Emissão de relatórios de auditoria de sistemas de informação.
<b>REDES DE COMPUTADORES</b>	Usos de redes de computadores. Hardware de rede. Software de rede. Modelos de referência. Padronização das redes. Camada física. Camada de enlace de dados. Subcamada de controle de acesso. Camada de rede. Camada de transporte. Camada de aplicação.
<b>SEGURANÇA DA INFRAESTRUTURA DE TI</b>	Conceitos de segurança de computadores. Ameaças, ataques e ativos. Requisitos funcionais de segurança. Autenticação do usuário. Controle de acesso à rede e segurança na nuvem. Segurança na camada de transporte. Segurança em rede wireless. Segurança do correio eletrônico. Segurança IP. Firewall. Arquitetura e projetos de firewall. Intrusion detection system e prevention detection system.
<b>CRİPTOGRAFIA, CERTIFICAÇÃO DIGITAL E TÓPICOS ESPECIAIS EM SEGURANÇA DA INFORMAÇÃO</b>	Cifras Simétricas. Cifras Assimétricas. Funções de Hash. Assinatura Digital. Certificação Digital. Blockchain. Bitcoin. Smart Contracts. Digital Tokens. DApps. IoT
<b>LEGISLAÇÃO APLICADA À SEGURANÇA DA INFORMAÇÃO</b>	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.

# FAQ DO CURSO

## O curso de Pós-Graduação em Segurança da Informação 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 Segurança da Informação 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 Segurança da Informação 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](https://gran.com.br)

