UNIVERSIDADE ESTADUAL DE CIÊNCIAS DA SAÚDE DE ALAGOAS - UNCISAL
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
CENTRO DE EDUCAÇÃO A DISTÂNCIA

PROJETO PEDAGÓGICO DO CURSO

ESPECIALIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO E ANÁLISE FORENSE

Maceió, AL
2024

ESPECIALIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO E ANÁLISE FORENSE

REITORIA
Prof. Dr. Henrique de Oliveira Costa

VICE-REITORIA
Profa. Dra. Ilka do Amaral Soares

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
Profa. Dra. Mara Cristina Ribeiro

SUPERVISORA DE PÓS-GRADUAÇÃO LATO SENSU
Prof. Me. Maria Cecilia dos Santos Marques

DIRETOR DO CENTRO DE EDUCAÇÃO A DISTÂNCIA
Prof. Dr. Vagner Herculano de Souza

COORDENADOR GERAL DA UAB-UNCISAL
Prof. Me. Marcelo Santana Costa

COORDENADOR DA ESPECIALIZAÇÃO
Prof. Me. Reinaldo Alves da Silva

SUMÁRIO

1 IDENTIFICAÇÃO DA INSTITUIÇÃO

CNPJ	12.517.793/0001-08
RAZÃO SOCIAL	Universidade Estadual de Ciências da Saúde de Alagoas
ESFERA ADMINISTRATIVA	Autarquia Estadual
E-MAIL	ascom@uncisal.edu.br
SITE	https://www.uncisal.edu.br/
ENDEREÇO	Avenida Jorge de Lima, 113, Trapiche da Barra. CEP. 57010-382
TELEFONE	(82) 3315-6703

2 IDENTIFICAÇÃO DO CURSO

NOME DO CURSO	**Segurança da Informação e Análise Forense**
ÁREA DE CONHECIMENTO (CAPES)	Computação
CONVÊNIO	UNCISAL/UAB
FORMA DE OFERTA	EAD
TURMAS/POLOS EAD	Arapiraca (25), Boca da Mata (25), Coruripe (25), Maceió (50) e Maragogi (25)
PÚBLICO ALVO	Estudantes de computação/Exatas; profissionais com atuação no mercado de TI.
NÚMERO DE VAGAS	150
CARGA HORÁRIA TOTAL	465 h
PERÍODO DE DURAÇÃO	18 meses (15 convencional e 3 de repercurso)
PROCESSO SELETIVO	A ser realizado
REQUISITOS DE ACESSO	Graduação

3 INTRODUÇÃO

3.1 Instituição promotora

A instituição promotora se refere à Universidade Estadual de Ciências da Saúde de Alagoas – UNCISAL, condicionada como Universidade a partir da Lei nº 6.660, de 28 de dezembro de 2005 e criada pela Lei nº 6.660, de 28 de dezembro de 2005, com sede e foro na cidade de Maceió, Estado de Alagoas, no Campus Governador Lamenha Filho, situado à Rua Jorge de Lima, 113, no bairro do Trapiche da Barra.

A UNCISAL é uma Instituição de Ensino Superior – IES – pública de esfera administrativa estadual, constituída pelo princípio da autonomia didático-pedagógica, científica e administrativa, de gestão financeira e patrimonial, com vistas à Constituição Federal e Estadual.

Conforme seu Estatuto, alguns de seus objetivos são:

> I – promover, de forma indissociável, o ensino, a pesquisa e a extensão e aperfeiçoar a educação superior como também educação profissional;
>
> II – estimular a criação cultural e o desenvolvimento do espírito científico e do pensamento reflexivo;
>
> III – aplicar-se ao estudo da realidade brasileira, em busca de soluções para os problemas do desenvolvimento social e econômico, contribuindo com os recursos à sua disposição para o desenvolvimento do bem-estar social; [...].

Com base no documento atual do Plano de Desenvolvimento Institucional – PDI/2020-2024, sua missão consiste em: desenvolver atividades integradas de ensino, pesquisa, extensão e assistência, produzindo e socializando conhecimento para a formação de profissionais aptos a implementar e gerir ações que promovam o desenvolvimento sustentável, atendendo às demandas da sociedade alagoana. E sua visão é ser reconhecida pela sociedade alagoana como referência de qualidade no ensino, pesquisa, extensão e assistência. Com os valores de: integração ensino-serviço; respeito à integralidade do ser; gestão pública sustentável; transparência e ética.

A composição da IES se dá por meio de órgãos de apoio às suas atividades acadêmicas, com unidades administrativas, acadêmicas e assistenciais, conforme quadro a seguir:

QUADRO 1. UNIDADES QUE COMPÕEM A UNCISAL.

UNIDADE	ATIVIDADES	ENDEREÇO
Prédio-sede	Acadêmica, Administrativa e Assistencial	Rua Jorge de Lima, nº. 113, Trapiche da Barra – CEP 57010-382.
Escola Técnica de Saúde Professora Valéria Hora – ETSAL	Acadêmica e Administrativa	Rua Dr. Pedro Monteiro, 347, Centro – CEP 57020-380.
Centro de Patologia e Medicina Laboratorial – CPML	De Apoio Assistencial	Rua Cônego Fernando Lyra, S/N, Trapiche da Barra – CEP 57017-420.
Serviço de Verificação de Óbitos – SVO	De Apoio Assistencial	Rua Cônego Fernando Lyra, S/N, Trapiche da Barra – CEP 57017-420.
Maternidade Escola Santa Mônica – MESM	Assistencial	Av. Comendador Leão, S/N, Poço – CEP 57025-000.
Hospital Escola Dr. Hélvio Auto – HEHA	Assistencial	Rua Cônego Fernando Lyra, S/N, Trapiche da Barra – CEP 57017-420.
Hospital Escola Portugal Ramalho – HEPR	Assistencial	Rua Oldemburgo da Silva Paranhos, S/N, Farol – CEP 57055-000
Centro Especializado em Reabilitação – CER	Acadêmica e Assistencial	Rua Cônego Fernando Lyra, S/N, Trapiche da Barra – CEP 57017-420
Ambulatório de Especialidades Médicas -AMBESP	Acadêmica; Assistencial.	Rua Dr. Pedro Monteiro, 347, Centro – CEP 7020-380.
Centro de Diagnósticos - CEDIM	Acadêmica; Assistencial.	Rua Jorge de Lima, nº. 113, Trapiche da Barra – CEP 57010-382.

FONTE: CEARQ/UNCISAL.

Integrando a estrutura organizacional da UNCISAL, tem-se: o Conselho Superior, a Reitoria, os Órgãos de Assessoramento Superior do Gabinete da Reitoria, os Órgãos de Planejamento e Gestão Administrativa, os Órgãos de Apoio Acadêmico, as Unidades

Acadêmicas, as Unidades Assistenciais e as Unidades de Apoio Assistencial. É no âmbito das Unidades Acadêmicas que se encontram os Centros e Núcleos de Ensino, a exemplo do Centro de Educação a Distância – CED, de onde emerge a proposta desta pós-graduação aqui exposta neste PPC.

No âmbito da estrutura acadêmica de pesquisa e pós-graduação a Pró-reitora de Pesquisa e Pós Graduação – PROPEP – é o órgão responsável pelas práticas de planejamento, elaboração, organização, execução e acompanhamento das políticas e dos projetos de pesquisa e pós-graduação, em articulação com as demais Pró-reitoras, as Unidades Acadêmicas, as Unidades Assistenciais, as Unidades de Apoio Assistencial e os Órgãos de Assessoramento Superior do Gabinete da Reitoria, conforme registrado no Regimento Geral da IES.

Já o CED é um centro que consolida um dos eixos da política de inovação educacional da UNCISAL, prevendo a expansão de cursos e/ou programas na modalidade a distância, com uso de Tecnologias Digitais de Informação e Comunicação na Educação – TDIC, seja no entorno do prédio sede ou nos polos de apoio conveniados pela Universidade Aberta do Brasil – UAB, descentralizando a oferta de cursos apenas na região metropolitana de Maceió.

A UAB é um programa do Ministério da Educação - MEC, com gerenciamento pela Diretoria de Educação a Distância – DED, no âmbito da Coordenação de Aperfeiçoamento de Pessoal de Ensino Superior – CAPES - e pela Secretaria de Educação a Distância - SEED.

O convênio UNCISAL/UAB, consolidado por práticas de trabalhos no CED, surgiu a partir do ano 2017 em observância a edital da CAPES para oferta de cursos superiores, sendo em 2022 a implementação de propostas de cursos de pós-graduação a distância no âmbito da UNCISAL, também entre esta parceria com a UAB.

3.2 Nome do curso e área do conhecimento

O curso Especialização em Segurança da Informação e Análise Forense pertence à área ampla de Computação e Informática, com foco específico nas subáreas de Segurança da Informação e Ciência Forense Digital.

Este curso aborda a gestão e a proteção de dados e sistemas computacionais contra ameaças digitais, além de capacitar os profissionais na investigação de incidentes cibernéticos. Envolve o uso de metodologias e ferramentas de análise forense para coleta, preservação e análise de evidências digitais.

O programa explora:

- **Criptografia, controle de acesso e auditoria de sistemas**, fundamentais na proteção de dados;
- **Análise de vulnerabilidades e segurança ofensiva** (pentest), essenciais para identificar e corrigir falhas de segurança;
- **Métodos forenses digitais** que possibilitam a investigação de incidentes, com foco na coleta e preservação de provas;
- **Aspectos legais e regulamentares** relacionados à proteção de dados e perícia digital, capacitando os profissionais para atuar em conformidade com legislações nacionais e internacionais.

Com este enfoque, o curso oferece uma formação completa para atuar em **empresas públicas e privadas**, prestando serviços em governança de TI, segurança de sistemas, auditoria, e análise forense digital, promovendo uma atuação ética e eficiente diante de incidentes cibernéticos.

3.3 Justificativa de oferta do curso

A crescente demanda por profissionais especializados em segurança da informação e análise forense se intensifica diante da evolução digital e do aumento de ameaças cibernéticas, que impactam tanto organizações públicas quanto privadas. Com o aumento da complexidade dos sistemas de informação, a segurança deixou de ser apenas uma medida preventiva para se tornar estratégica, garantindo a continuidade dos negócios e a conformidade legal, especialmente diante de legislações como a LGPD (Lei Geral de Proteção de Dados) no Brasil e o GDPR na União Europeia.

Além disso, o avanço das tecnologias digitais e a adoção de inteligência artificial e computação em nuvem trazem novos desafios de segurança, como ataques mais sofisticados e a necessidade de proteger grandes volumes de dados em ambientes heterogêneos. Em paralelo, a Análise Forense Digital se mostra essencial na investigação de incidentes cibernéticos, possibilitando a coleta e preservação de evidências que podem ser utilizadas judicialmente.

Diante deste cenário, há uma lacuna a ser preenchida por profissionais com habilidades técnicas em segurança ofensiva e defensiva, conhecimento das melhores práticas de governança de TI, e *expertise* em análise forense digital. O curso também se justifica pela carência de profissionais com competências integradas que aliem aspectos técnicos, legais e

de gestão, capazes de prevenir e responder a incidentes de forma eficiente e em conformidade com as regulamentações vigentes.

A modalidade totalmente EaD facilita o acesso a essa formação por um público mais amplo, incluindo profissionais em atuação que buscam se atualizar sem comprometer suas agendas. O formato também atende às novas demandas de educação continuada e às expectativas por modelos de aprendizagem flexíveis, que permitam a personalização do aprendizado.

Por fim, o projeto aplicado ao final do curso substitui o TCC tradicional, valorizando a prática e garantindo que o aluno aplique, de forma integrada, os conhecimentos adquiridos, preparando-o para enfrentar os desafios reais do mercado.

4 OBJETIVOS

4.1 Geral

Capacitar profissionais para proteger e gerenciar infraestruturas digitais, atuando na prevenção e mitigação de riscos cibernéticos e na análise forense de incidentes. O curso desenvolve habilidades técnicas e estratégicas em segurança da informação e conformidade legal, preparando os alunos para enfrentar desafios reais do mercado por meio de um projeto aplicado de conclusão.

4.2 Específicos

- Desenvolver competências técnicas em segurança da informação, abrangendo conceitos como criptografia, controle de acesso e segurança em redes.
- Capacitar os alunos na realização de análises forenses digitais, com foco na coleta, preservação e análise de evidências para investigação de incidentes cibernéticos.
- Preparar os profissionais para a aplicação de normas e regulamentações legais, como a LGPD e outras legislações de proteção de dados.
- Promover habilidades em segurança ofensiva e defensiva, incluindo a realização de testes de invasão (*pentest*) e a implementação de contramedidas.
- Incentivar a aplicação prática do conhecimento adquirido por meio de projetos aplicados e desafios reais, integrando as diversas áreas de segurança da informação e forense digital.

- Desenvolver habilidades de análise crítica e tomada de decisão para a prevenção e mitigação de riscos, visando a continuidade dos negócios e a proteção de infraestruturas digitais.
- Capacitar para o uso de tecnologias emergentes, como inteligência artificial, no contexto da segurança e da investigação forense.

5 PERFIL PROFISSIONAL

5.1 Público Alvo

O curso é voltado a profissionais de TI e segurança da informação que desejam atuar na proteção de dados e na análise forense digital. Inclui: Analistas, gestores e consultores de TI focados em governança e segurança cibernética; Peritos e auditores digitais interessados em *compliance* e investigação de incidentes; Docentes, pesquisadores e profissionais de áreas afins, como engenharia e direito, que buscam especialização em segurança digital.

O curso atende a quem busca enfrentar os desafios atuais de proteção de dados e conformidade legal, com aplicação em setores públicos e privados.

5.2 Perfil que se objetiva formar

O curso de Especialização em Segurança da Informação e Análise Forense tem como objetivo formar profissionais capazes de proteger e gerenciar infraestruturas digitais, atuando na prevenção e mitigação de riscos cibernéticos. Esses profissionais serão habilitados a realizar investigações forenses digitais, aplicando metodologias para a coleta, preservação e análise de evidências em casos de incidentes de segurança.

Além disso, espera-se que desenvolvam habilidades tanto em segurança ofensiva quanto defensiva, incluindo a identificação de vulnerabilidades e a aplicação de testes de invasão para fortalecer sistemas. A formação também foca na conformidade com normas e regulamentações, como a LGPD, preparando os alunos para garantir a proteção de dados e aderência a boas práticas.

Com um enfoque prático e atualizado, o curso incentiva o uso de tecnologias emergentes, como inteligência artificial, aplicadas à segurança da informação e à análise forense. Ao final, o profissional será capaz de desenvolver soluções inovadoras e eficientes para desafios reais, integrando conhecimentos técnicos, estratégicos e legais. Esses especialistas estarão aptos a atuar em organizações públicas e privadas, órgãos

governamentais, consultorias, e instituições financeiras, desempenhando papéis essenciais na proteção e governança de TI.

6 ORGANIZAÇÃO CURRICULAR E FUNCIONAMENTO

A estrutura curricular do Curso apresenta uma carga horária total de 490 horas. O curso será disposto numa organização de 5 módulos de 3 meses cada. Os componentes curriculares terão no mínimo 20% de sua carga horária ofertada de maneira síncrona, com calendário geral previsto e disponibilizado no início do curso. Os encontros síncronos são de participação obrigatória do estudante.

Tais encontros serão sempre aos sábados, dando prioridade ao turno da manhã, com participação dos professores e tutores. Toda organização didática e disponibilização de materiais do curso será a partir do AVA Moodle da UNCISAL, com acesso pelo endereço https://ced.uncisal.edu.br/.

Os componentes curriculares possuem, em sua maioria, 30h e 45h e serão compostos por duas unidades didáticas, cada unidade prevendo um momento síncrono. Elas seguem a seguinte organização: aula, referencial teórico, tutoria (fórum de interação e de dúvidas) e avaliação.

Cabe ressaltar que as disciplinas funcionarão no formato online (com momentos síncronos e assíncronos). Entretanto, o curso possui um momento presencial de caráter obrigatório: a aula inaugural do curso de especialização.

6.1 Matriz Curricular

MÓDULO E COMPONENTE CURRICULAR	CARGA HORÁRIA
1° SEMESTRE	
MÓDULO 1	
Fundamentos de Segurança da Informação	45h
Gestão de Riscos em Segurança da Informação	30h
MÓDULO 2	
Segurança em Redes e Infraestrutura	30h
Auditoria, Legislação e Conformidade em Segurança da Informação	30h

Técnicas de *Pentest* e Segurança Ofensiva - *Red Team*	45h
2° SEMESTRE	
MÓDULO 3	
Técnicas de *Pentest* e Segurança Defensiva - *Blue Team*	45h
Segurança em Aplicações Web e Desenvolvimento Seguro	30h
Fundamentos de Análise Forense	30h
MÓDULO 4	
Investigação Forense de Redes	30h
Computação Forense em Sistemas Operacionais	45h
IA aplicada à Segurança da Informação	30h
3° SEMESTRE	
MÓDULO 5	
Direito Digital e aspectos Legais da Segurança da Informação	30h
Projeto Aplicado: Práticas de Mercado	45h
TOTAL: 465h	

6.2 Cronograma

2025													**2026**			
MÓDULOS	**COMPONENTES CURRICULARES**	**FEV.**	**MAR.**	**ABR.**	**MAIO**	**JUN.**	**JUL.**	**AGO.**	**SET.**	**OUT.**	**NOV.**	**DEZ.**	**JAN.**	**FEV.**	**MAR.**	**ABR.**
1	Fundamentos de Segurança da Informação	X	X	X												
	Gestão de Riscos em Segurança da Informação	X	X													
2	Segurança em Redes e Infraestrutura				X	X										

	Auditoria, Legislação e Conformidade em Segurança da Informação				X	X										
	Técnicas de *Pentest* e Segurança Ofensiva - *Red Team*				X	X	X									
3	Técnicas de *Pentest* e Segurança Defensiva - *Blue Team*							X	X	X						
	Segurança em Aplicações *Web* e Desenvolvimento Seguro							X	X							
	Fundamentos de Análise Forense							X	X							
4	Investigação Forense de Redes										X	X				
	Computação Forense em Sistemas Operacionais										X	X	X			
	IA aplicada à Segurança da Informação										X	X				
5	Direito Digital e aspectos Legais da Segurança da Informação													X	X	
	Projeto Aplicado: Práticas de Mercado													X	X	X

6.3 Critérios e procedimentos para avaliação da aprendizagem

Os materiais de estudo de cada componente curricular, as atividades avaliativas e as interações entre estudantes, professores, tutores e entre os próprios estudantes serão disponibilizados exclusivamente no Moodle. A avaliação de desempenho será realizada por componente curricular, utilizando provas online, trabalhos, projetos ou outras metodologias adotadas pelo docente responsável, sempre com o uso das ferramentas disponíveis no Moodle e em conformidade com o estabelecido neste Projeto Pedagógico. O aproveitamento da aprendizagem será expresso por meio de nota, sendo considerado aprovado em cada componente curricular o estudante que obtiver nota final igual ou superior a 7,0 pontos.

As disciplinas possuem diferentes cargas horárias, e os modos de avaliação são organizados conforme a seguinte estrutura: nas disciplinas com 30 horas e 45 horas, serão realizadas duas atividades avaliativas (uma por unidade), cada uma valendo de 0 a 10 pontos, sendo a nota final a média aritmética.

Os componentes curriculares não preveem recuperação de nota. No entanto, ao final dos 15 meses de curso, haverá um período de repercurso, que ocorrerá de maio a julho de 2026. O repercurso é uma medida acadêmica destinada às disciplinas pendentes ao longo do curso. Será oferecido exclusivamente de forma online e assíncrona, com caráter autoinstrucional. Após o período previsto para o repercurso, não será ofertada nova oportunidade aos discentes que não alcançarem a integralização da carga horária obrigatória para obtenção do título de especialista.

Especificamente em casos nos quais houver a oferta do componente curricular com pendências em qualquer outro curso de especialização ofertado pela UNCISAL, o discente poderá solicitar por escrito (através do setor de protocolo) para refazer o componente curricular com fins de integralização da carga horária, desde que haja similaridade em termos de carga horária e conteúdos. Para solicitar esse benefício, o estudante deverá ter concluído e obtido aprovação em pelo menos 70% das disciplinas.

O curso também prevê a reprovação por falta, considerando o único momento presencial e encontros síncronos. A ausência destes momentos precisa ter justificativa encaminhada ao docente e coordenador de curso, desde que se encontre em uma das situações abaixo:

- Impossibilidade de comparecimento comprovada por atestado médico;
- Impossibilidade de comparecimento comprovada por declaração de trabalho formal;
- Impossibilidade de comparecimento comprovada por declaração de transporte intermunicipal;
- Exercício de atividade militar comprovada através de declaração da Entidade;
- Exercício de atividades a serviço da justiça comprovada pelo órgão;
- Óbito de membro de família até 3º grau, mediante atestado ou declaração;
- Participação em encontro científico, com solicitação requerida antecipadamente e com comprovação de aceite do evento;
- Participação em eventos relacionados ao processo de ensino-aprendizagem de sua área, com aprovação prévia da Coordenação do Curso.

7 GESTÃO DO CURSO

NOME COMPLETO	Reinaldo Alves da Silva
CADASTRO DE PESSOA FÍSICA:	605.462.044-49
E-MAIL	reinaldo.alves@uncisal.edu.br
FORMAÇÃO	Graduação em Engenharia Química e Tecnólogo em Análise e Desenvolvimento de Sistemas com Mestrado em sistemas de processos químicos e informática.
CURRÍCULO LATTES	http://lattes.cnpq.br/6391322173247824

ANEXO I – EMENTÁRIO DE DISCIPLINAS

Componente curricular: Fundamentos de Segurança da Informação
Carga Horária: 45h
Ementa: Apresenta os princípios fundamentais da segurança da informação, abordando os conceitos de confidencialidade, integridade e disponibilidade (CIA). Explora políticas e normas de segurança, ameaças e vulnerabilidades, e mecanismos de controle de acesso. A disciplina também introduz conceitos de criptografia básica e aplicada, autenticação e auditoria, além de regulamentações e padrões de segurança como a ISO/IEC 27001 e a LGPD. A aplicação prática da criptografia é explorada para garantir a proteção de dados e comunicações, com foco em algoritmos de criptografia simétrica e assimétrica, infraestrutura de chave pública (PKI) e certificados digitais.
Objetivo: Fornecer uma base sólida sobre os princípios e práticas essenciais da segurança da informação, capacitando os alunos a compreender os principais conceitos e desenvolver políticas e procedimentos para proteger sistemas e dados.
Referências básicas: Stallings, W. **Cryptography and Network Security: Principles and Practice**. Pearson, 2017. Pfleeger, C. P.; Pfleeger, S. L. **Security in Computing**. Prentice Hall, 2015 Barretos, J.; Zanin, Fundamentos de Segurança da Informação. Porto Alegre: Grupo A, 2018 (Plataforma Biblioteca A)
Referências complementares: ISO/IEC 27001. **Tecnologia da Informação — Técnicas de Segurança — Sistemas de Gestão da Segurança da Informação**. ISO, 2013. Bishop, M. **Introduction to Computer Security**. Addison-Wesley, 2005 Harris, S. **CISSP All-in-One Exam Guide**. McGraw-Hill, 2018

Componente curricular: Gestão de Riscos em Segurança da Informação
Carga Horária: 30h
Ementa: A disciplina aborda os princípios e práticas de gestão de riscos em segurança da informação, apresentando metodologias para identificação, análise e mitigação de riscos. São discutidas as ameaças e vulnerabilidades associadas a sistemas de informação, além das estratégias de controle e gestão de incidentes. O curso também aborda o mapeamento e avaliação de riscos, com ênfase em frameworks como ISO 31000, ISO/IEC 27005, e NIST SP 800-30, além de técnicas de resposta e recuperação de incidentes.

Objetivo: Capacitar os alunos a identificar, avaliar e mitigar riscos em ambientes de tecnologia da informação. Desenvolver planos de gerenciamento de riscos, aplicar controles adequados e implementar processos de monitoramento contínuo para a mitigação de riscos cibernéticos. Analisar vulnerabilidades e elaborar estratégias de resposta a incidentes, minimizando impactos sobre as organizações.

Referências básicas:

ABNT. **NBR ISO/IEC 27005: Gestão de Riscos de Segurança da Informação**. Associação Brasileira de Normas Técnicas (ABNT), 2019.

Stallings, William. **Segurança de Computadores: Princípios e Prática**. Pearson, 2012.

Alberts, C.; Dorofee, A. **Gerenciamento de Riscos de Segurança da Informação**. LTC, 2009.

Referências complementares:

Harris, S. **CISSP All-in-One Exam Guide**. McGraw-Hill, 2018.

Kossakowski, K. P.; Allen, J. H.; Christie, A. **Gestão de Incidentes e de Riscos de Segurança da Informação**. Campus, 2008.

ISO 31000: **Gestão de Riscos - Princípios e Diretrizes**. ABNT, 2018.

Componente curricular: Segurança em Redes e Infraestrutura

Carga Horária: 30h

Ementa: A disciplina aborda os princípios e práticas de segurança em redes de computadores e infraestruturas de TI, com foco em protocolos de segurança, configuração de firewalls, VPNs, e IDS/IPS. O curso explora a detecção e mitigação de ataques cibernéticos, como DoS, phishing e malware, além de conceitos de segurança em redes sem fio e ambientes de computação em nuvem. A disciplina também discute boas práticas de gerenciamento de redes seguras, criptografia de rede e políticas de controle de acesso.

Objetivo: Capacitar os alunos a projetar, implementar e gerenciar redes seguras, aplicando técnicas de segurança para proteger a infraestrutura de TI contra ameaças internas e externas. Desenvolver a habilidade de detectar, prevenir e responder a incidentes de segurança em redes, além de ensinar como aplicar protocolos de segurança e ferramentas de monitoramento em redes corporativas

Referências básicas:

Stallings, W. **Segurança de Redes: Aplicações e Padrões**. 5ª edição. Pearson, 2015.

Tanenbaum, A. S. **Redes de Computadores**. 5ª edição. Pearson, 2011.

Kurose, J. F.; Ross, K. W. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 7ª edição. Pearson, 2017.

Referências complementares:

Behrouz A. F. **Segurança de Redes de Computadores**. 4ª edição. McGraw-Hill, 2013.

Scarfone, K.; Souppaya, M.; Hoffman, P. **Guia de Segurança para Redes**. NIST Special Publication, 2012.

Silva, M. **Segurança em Redes de Computadores**. Novatec Editora, 2018.

Componente curricular: Auditoria, Legislação e Conformidade em Segurança da Informação

Carga Horária: 30h

Ementa: A disciplina explora os princípios de auditoria em segurança da informação, abordando *frameworks* e normas internacionais, como ISO/IEC 27001 e COBIT, que são aplicados na auditoria de sistemas e infraestruturas de TI. São apresentados os aspectos legais e de conformidade com legislações nacionais e internacionais, como a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (GDPR). A disciplina também abrange metodologias de auditoria de segurança, avaliação de riscos, e desenvolvimento de políticas de *compliance*.

Objetivo: Realizar auditorias de segurança da informação, garantindo a conformidade com normas, regulamentos e leis vigentes. Aplicar *frameworks* de auditoria, identificar falhas de conformidade e elaborar relatórios de auditoria. Implementar políticas e práticas de *compliance* com base em legislações de proteção de dados, tanto nacionais quanto internacionais.

Referências básicas:

ABNT. **NBR ISO/IEC 27001:** Sistemas de Gestão de Segurança da Informação. Associação Brasileira de Normas Técnicas, 2019.

Batista, E. **LGPD - Lei Geral de Proteção de Dados:** Aplicação Prática e Teórica. Editora Juspodivm, 2020.

Moura, M. **Auditoria de Sistemas de Informação:** Guia Prático. Novatec, 2018.

Referências complementares:

Carbone, P. **Gestão de Segurança da Informação:** Auditoria e Gestão de Riscos. Atlas, 2017.

Braz, D. **Proteção de Dados Pessoais:** Teoria e Prática sobre a LGPD. Editora D'Plácido, 2021.

ISACA. **COBIT 2019:** Framework de Governança e Gestão de TI. ISACA, 2019.

Componente curricular: Técnicas de *Pentest* e Segurança Ofensiva - *Red Team*
Carga Horária: 45h
Ementa: A disciplina aborda as técnicas e ferramentas utilizadas em testes de penetração (*pentest*) para avaliar a segurança de sistemas e redes. Os alunos serão introduzidos às práticas de segurança ofensiva, com enfoque no papel do *Red Team* na simulação de ataques reais, identificando vulnerabilidades antes que sejam exploradas por invasores. As principais técnicas incluem varredura de rede, *exploits* de vulnerabilidades, *phishing* e movimentação lateral dentro de redes corporativas. A disciplina também foca em metodologias e ferramentas como *Metasploit, Nmap* e *Burp Suite*, além de práticas de pós-exploração e relatórios de vulnerabilidades.
Objetivo: Realizar testes de penetração e aplicar técnicas de segurança ofensiva para identificar e explorar vulnerabilidades em sistemas de informação. Executar simulações de ataques, elaborar relatórios detalhados sobre vulnerabilidades e fornecer recomendações para mitigação. Compreender as táticas, técnicas e procedimentos (TTPs) utilizados por atacantes reais, preparando os alunos para atuarem como parte de equipes Red Team em simulações de ameaças avançadas.
Referências básicas: Stuart M.; Joel S.; George K. **Hacking Exposto 7: As Técnicas de Ataque de Segurança de Computadores Mais Recentes**. McGraw-Hill, 2012. Ferreira, B. **Guia Prático de Pentest: Testes de Intrusão com Ferramentas de Código Aberto**. Novatec, 2020. Malcom, P. **Segurança Ofensiva: Testes de Invasão e Red Teaming**. Alta Books, 2018.
Referências complementares: Logan, K.; Stackpole, B. **Red Teaming: O Jogo de Guerra da Segurança da Informação**. Novatec, 2016. Engebretson, P. **The Basics of Hacking and Penetration Testing**. Elsevier, 2013. Harris, S. **CISSP: Guia Completo para Certificação**. McGraw-Hill, 2018.

Componente curricular: Técnicas de *Pentest* e Segurança Defensiva - *Blue Team*
Carga Horária: 45h
Ementa: A disciplina explora as técnicas e estratégias de segurança defensiva aplicadas por equipes de *Blue Team* para proteger sistemas e redes contra ameaças cibernéticas. O conteúdo inclui monitoramento contínuo, detecção de intrusões, resposta a incidentes e implementação de políticas de segurança. Os alunos aprenderão a utilizar ferramentas como SIEM (*Security Information and Event Management*), *firewalls*, IDS/IPS e sistemas

de monitoramento de rede para identificar e mitigar vulnerabilidades. O foco será em como proteger a infraestrutura de TI e aplicar técnicas de defesa contra ataques conhecidos, bem como conduzir a análise de logs e a investigação de incidentes.
Objetivo: Aplicar técnicas de defesa cibernética com foco na prevenção, detecção e mitigação de ataques. Preparar os alunos para atuar em equipes de *Blue Team*, garantindo a segurança de redes e sistemas, analisando padrões de comportamento anômalo, implementando medidas de segurança e desenvolvendo planos de resposta a incidentes.
Referências básicas: Northcutt, S.; Zeltser, L. **Guia Completo de Defesa Cibernética**. Alta Books, 2017. Harris, S. **CISSP All-in-One Exam Guide**. McGraw-Hill, 2018. Matta, M. **Segurança Cibernética: Ferramentas e Técnicas de Defesa**. Novatec, 2019.
Referências complementares: Anderson, R. **Security Engineering: A Guide to Building Dependable Distributed Systems**. Wiley, 2020. Davis, J.; Schiller, C. **Segurança Cibernética para Blue Teams: Defesas, Detecção e Resposta**. Alta Books, 2018. Scarfone, K.; Mell, P. **Guia NIST de Defesas em Profundidade**. NIST Special Publication, 2018.

Componente curricular: Segurança em Aplicações *Web* e Desenvolvimento Seguro
Carga Horária: 30h
Ementa: A disciplina explora os princípios e práticas de segurança em desenvolvimento de aplicações web, abordando as principais vulnerabilidades conforme o *OWASP* Top 10, incluindo SQL *Injection*, *Cross-Site Scripting* (XSS) e *Cross-Site Request Forgery* (CSRF). O curso foca em técnicas de desenvolvimento seguro, com ênfase na aplicação de políticas de controle de acesso, criptografia e validação de entradas do usuário. Também são abordadas as melhores práticas para ciclo de vida de desenvolvimento seguro (SDLC), testes de segurança em aplicações *web* e mitigação de riscos em ambientes de produção.
Objetivo: Identificar, mitigar e evitar vulnerabilidades em aplicações *web*, aplicando práticas seguras de codificação e desenvolvimento. Fornecer as habilidades necessárias para criar aplicações robustas e seguras, integrando a segurança desde o início do ciclo de desenvolvimento (*DevSecOps*). Realizar testes de segurança em aplicações e aplicar mecanismos de proteção contra as vulnerabilidades mais comuns no desenvolvimento web.
Referências básicas: OWASP Foundation. **OWASP Top 10: Vulnerabilidades Mais Comuns em Aplicações**

Web. OWASP, 2021.

Stuttard, D.; Pinto, M. **The Web Application Hacker's Handbook: Descobrindo e Exploitando Vulnerabilidades em Aplicações Web**. Alta Books, 2018.

Esposito, D. **Segurança no Desenvolvimento de Aplicações Web**. Novatec, 2017.

Referências complementares:

Anderson, R. **Security Engineering: A Guide to Building Dependable Distributed Systems**. Wiley, 2020.

Harris, S. **CISSP All-in-One Exam Guide**. McGraw-Hill, 2018.

Fagan, M. **Desenvolvimento Seguro e DevSecOps: Integrando Segurança no Ciclo de Vida de Desenvolvimento de Software**. Alta Books, 2020.

Componente curricular: Fundamentos de Análise Forense

Carga Horária: 30h

Ementa: A disciplina apresenta os conceitos fundamentais da análise forense digital, abordando os processos de coleta, preservação e análise de evidências digitais. Os alunos serão introduzidos aos procedimentos de investigação de incidentes cibernéticos, com foco em sistemas de arquivos, logs de sistemas, e memória volátil. A disciplina também explora o uso de ferramentas forenses, além das melhores práticas de preservação de cadeia de custódia e integridade de evidências.

Objetivo: Entender e aplicar os princípios e técnicas da análise forense digital, realizando investigações em dispositivos e sistemas comprometidos. Deixar os alunos aptos a coletar, preservar e analisar evidências digitais, além de elaborar relatórios periciais e atuar em investigações forenses e resposta a incidentes cibernéticos em conformidade com requisitos legais e regulatórios.

Referências básicas:

Casey, E. **Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet**. Elsevier, 2011.

Amorim, H. **Perícia Forense Computacional**. Novatec, 2019.

Carrier, B. **File System Forensic Analysis**. Addison-Wesley, 2005.

Referências complementares:

Sammons, J. **Manual de Investigação Forense Digital**. Alta Books, 2015.

Nelson, B.; Phillips, A.; Steuart, C.: **Fundamentos de Computação Forense**. Cengage Learning, 2017.

Mandia, K.; Prosise, C.; Pepe, M.: **Incident Response and Computer Forensics**.

McGraw-Hill, 2014.

Componente curricular: Investigação Forense de Redes

Carga Horária: 30h

Ementa: A disciplina explora as técnicas e ferramentas utilizadas na investigação forense de redes, abordando a coleta, análise e preservação de evidências digitais em ambientes de rede. Foca no monitoramento de tráfego, captura de pacotes e análise de logs para a detecção de atividades maliciosas. Os alunos aprenderão a utilizar ferramentas como *Wireshark*, *tcpdump* e *Snort* para identificar e mitigar ameaças em redes corporativas, além de técnicas de rastreamento de intrusões e mapeamento de eventos.

Objetivo: Realizar análises forenses em redes de computadores, utilizando metodologias e ferramentas apropriadas para a coleta e preservação de evidências digitais. Investigar incidentes de segurança, identificando comportamentos anômalos e elaborando relatórios detalhados sobre atividades suspeitas e ataques.

Referências básicas:

Bejtlich, R. O Tao da Segurança em Redes. Pearson, 2015.

Amorim, H. Perícia Forense Computacional. Novatec, 2019.

McClure, S.; Scambray, J.; Kurtz, G. Hacking Exposto: Redes. Alta Books, 2018.

Referências complementares:

Carrier, B. File System Forensic Analysis. Addison-Wesley, 2005.

Engebretson, P. The Basics of Hacking and Penetration Testing. Elsevier, 2013.

Stallings, W. Segurança de Redes: Aplicações e Padrões. Pearson, 2015.

Componente curricular: Computação Forense em Sistemas Operacionais

Carga Horária: 45h

Ementa: A disciplina aborda as técnicas e metodologias de computação forense aplicadas a sistemas operacionais, com foco na investigação e análise de incidentes em ambientes Windows e Linux. Explora a coleta e preservação de evidências digitais, análise de logs de sistemas, memória volátil e arquivos de sistema. Os alunos aprenderão a utilizar ferramentas forenses como *Autopsy, FTK Imager* e *Volatility* para investigar atividades maliciosas, rastrear alterações e recuperar dados em sistemas comprometidos. A disciplina também cobre práticas de preservação da cadeia de custódia e documentação detalhada das evidências.

Objetivo: Capacitar os alunos a realizar investigações forenses em sistemas operacionais, aplicando técnicas adequadas para a coleta, preservação e análise de evidências digitais em ambientes Windows e Linux. Ao final do curso, os alunos serão capazes de utilizar ferramentas forenses para identificar atividades suspeitas, analisar logs e memória volátil, e elaborar relatórios periciais completos, respeitando as melhores práticas e os padrões legais de preservação de evidências.

Referências básicas:

Amorim, H. Perícia Forense Computacional. Novatec, 2019.

Casey, E. Digital Evidence and Computer Crime. Elsevier, 2011.

Mandia, K.; Prosise, C.; Pepe, M. Resposta a Incidentes e Computação Forense. McGraw-Hill, 2014.

Referências complementares:

Carrier, B. File System Forensic Analysis. Addison-Wesley, 2005.

Nelson, B.; Phillips, A.; Steuart, C. Fundamentos de Computação Forense. Cengage Learning, 2017.

Sammons, J. Manual de Investigação Forense Digital. Alta Books, 2015.

Componente curricular: IA aplicada à Segurança da Informação

Carga Horária: 30h

Ementa: A disciplina explora o uso de Inteligência Artificial (IA) na segurança da informação, apresentando técnicas e algoritmos de machine learning e deep learning aplicados à detecção de ameaças cibernéticas, análise de anomalias e resposta automatizada a incidentes.

Objetivo: Capacitar os alunos a aplicar técnicas de Inteligência Artificial na proteção e monitoramento de infraestruturas de TI, utilizando algoritmos de *machine learning* e *deep learning* para detecção proativa de ameaças e resposta automatizada a incidentes. Desenvolver e implementar modelos de IA que auxiliem na mitigação de riscos cibernéticos, analisando anomalias em tempo real e melhorando a segurança de sistemas e redes.

Referências básicas:

Russell, S.; Norvig, P. Inteligência Artificial. Pearson, 2020.

Zamboni, D. Machine Learning e Análise de Dados Aplicados à Segurança da Informação. Novatec, 2020.

Goodfellow, I.; Bengio, Y.; Courville, A. Deep Learning. MIT Press, 2016.
Referências complementares: Amorim, H. Segurança Cibernética com Machine Learning. Alta Books, 2019. Harris, S. CISSP: Guia Completo para Certificação. McGraw-Hill, 2018. Bishop, C. M. Pattern Recognition and Machine Learning. Springer, 2016.

Componente curricular: Direito Digital e aspectos Legais da Segurança da Informação
Carga Horária: 30h
Ementa: A disciplina aborda os fundamentos do direito digital e sua aplicação na segurança da informação, explorando as legislações nacionais e internacionais que regulamentam a proteção de dados. Serão discutidos os direitos e responsabilidades das organizações e dos profissionais de TI no tratamento e proteção de dados, além das implicações legais em casos de incidentes de segurança e crimes cibernéticos.
Objetivo: Capacitar os alunos a compreenderem os aspectos legais e regulamentares da segurança da informação, aplicando o direito digital no contexto da proteção de dados e da resposta a incidentes cibernéticos.
Referências básicas: Opice B., R.; Doneda, D. Lei Geral de Proteção de Dados Comentada. Revista dos Tribunais, 2019. Sousa, P. P. P. Direito Digital. Saraiva, 2021. Chaves, E. M. Privacidade, Proteção de Dados e Cibersegurança. Forense, 2020.
Referências complementares: Doneda, D. Proteção de Dados Pessoais: A Função e os Limites do Consentimento. Atlas, 2019. Pinheiro, P. P. Manual de Direito Digital e Internet. Saraiva, 2018. Assis, A. Compliance Digital: Estratégias para Proteção e Conformidade. Novatec, 2020.

Componente curricular: Projeto Aplicado: Práticas de Mercado
Carga Horária: 45h
Ementa: A disciplina visa a aplicação prática dos conhecimentos adquiridos ao longo do curso, proporcionando aos alunos a oportunidade de utilizar, de forma integrada, as

principais ferramentas e técnicas de segurança da informação e análise forense em cenários realistas. Por meio de projetos aplicados, os alunos irão simular situações reais de mercado, desenvolvendo soluções que envolvem auditoria, pentest, análise forense, criptografia e conformidade regulatória.
Objetivo: Capacitar os alunos a utilizar de forma prática e integrada as ferramentas e técnicas de segurança da informação e análise forense estudadas ao longo do curso, em cenários que simulam o ambiente corporativo real. Projetar, implementar e avaliar soluções de segurança, aplicando habilidades adquiridas em situações complexas, que envolvem desde a identificação de vulnerabilidades até a resposta a incidentes e a elaboração de relatórios técnicos e periciais detalhados.
Referências básicas: Northcutt, S.; Zeltser, L. Guia Prático de Defesa Cibernética. Alta Books, 2017. Harris, S. CISSP All-in-One Exam Guide. McGraw-Hill, 2018. Opice B., R. Segurança da Informação: Guia para Empresas e Profissionais. Saraiva, 2020.
Referências complementares: Stallings, W. Segurança de Redes: Aplicações e Padrões. Pearson, 2015. Esposito, D. Segurança no Desenvolvimento de Aplicações Web. Novatec, 2017. Casey, E. Digital Evidence and Computer Crime. Elsevier, 2011.

Maceió, Novembro de 2024

_____

Assinatura do Coordenador do Curso de Especialização