UNIVERSIDADE DO OESTE DE SANTA CATARINA
CAMPUS DE JOAÇABA
ÁREA DAS CIÊNCIAS EXATAS E TECNOLÓGICAS
PLANO DE ENSINO E APRENDIZAGEM

1 DADOS DE IDENTIFICAÇÃO

Campus:	CAMPUS DE JOAÇABA
Curso/Matriz/Fase:	620 - ENGENHARIA DE COMPUTAÇÃO/5/8
Componente curricular:	33506 - Cyber Security - Turma: JBA620-5
Professor:	7196 - Guilherme Rossetti Anzollin
Nr. créditos/Carga Horária:	4/80
Período letivo:	2024/2

1.1 Alocação na Matriz de Referência de Formação

Perfil do Egresso que o componente contribui para formar:	Profissional apto a implementar a interoperabilidade na comunicação de sistemas, considerando a utilização da miniaturização de componentes, aplicando à automação, distribuição e a segurança da informação.
Competência(s) que contribui para desenvolver:	Compreender e identificar os fundamentos de segurança da informação e de sistemas de computação. Conhecer e utilizar os fundamentos da ética, da legislação profissional e dos atos normativos no âmbito do exercício da profissão. Implementar e gerenciar a segurança de sistemas de computação.

2 EMENTA

Fundamentos de Segurança Computacional: Princípios e Conceitos de Segurança Computacional, A internet como Meio. Criptografia: Cifras de Transposição, Cifras de Substituição, Criptografia Simétrica, Criptografia Assimétrica, Cifras de Fluxo, Cifras de Bloco, Funções de Hash. Autenticação e Autorização: Fluxos de Autenticação, Navigation Guards e Authentication Guards, Hash de Passwords, JWT - JSON Web Token, OAuth 2.0, Web Storage APIs, Interceptors e Middlewares, Autorização através de Gates, Policies e Token Scopes.

2.1 Unidades de Ensino

Fundamentos de Segurança Computacional. Criptografia. Autenticação e Autorização.

3 JUSTIFICATIVA

É fundamental que o acadêmico possua conhecimento em Cyber Security, pois a crescente dependência de sistemas computacionais e redes de comunicação, bem como a expansão da internet e a proliferação de dispositivos conectados, ampliaram significativamente a superfície de ataque para ameaças cibernéticas. Compreender os princípios e conceitos de segurança computacional, assim como dominar técnicas de criptografia e mecanismos de autenticação e autorização, capacita os futuros engenheiros de computação a proteger dados sensíveis, assegurar a integridade e a confidencialidade das informações, e garantir a resiliência e a confiabilidade dos sistemas. Dessa forma, os profissionais poderão enfrentar os desafios contemporâneos de segurança digital e contribuir efetivamente para a criação de ambientes computacionais mais seguros e robustos.

4 OBJETIVO GERAL

O objetivo geral da disciplina de Cyber Security é capacitar os alunos a compreenderem e aplicarem os principais conceitos, técnicas e ferramentas de segurança computacional, com ênfase em criptografia, autenticação e autorização. Através do estudo aprofundado dos fundamentos de segurança, os alunos serão preparados para identificar, analisar e mitigar ameaças e vulnerabilidades em sistemas e redes de computadores. Além disso, a disciplina visa desenvolver a habilidade de implementar soluções de segurança eficazes, garantindo a proteção de dados e a integridade dos sistemas, capacitando assim os futuros engenheiros a atuarem de forma proativa e competente no campo da segurança cibernética.

5 DESENVOLVIMENTO DO PROCESSO ENSINO APRENDIZAGEM

5.1 Unidades de Ensino

Unidade 1: Fundamentos de Segurança Computacional

Unidade 2: Criptografia

Unidade 3: Autenticação e Autorização

5.2 Metodologias

Entende-se que as metodologias de ensino e aprendizagem mais adequadas e significativas são aquelas que colocam o discente no centro do processo, priorizando práticas pedagógicas que permitam que o acadêmico seja agente ativo da aprendizagem, participando na construção do conhecimento e na mudança da realidade social. Portanto, define-se para este componente curricular metodologias que levarão o acadêmico a estabelecer por meio do diálogo, do debate, da reflexão e resolução de exercícios uma relação ativa e significativa com este componente.

Unidade 1: Fundamentos de Segurança Computacional

De forma a verificar o conhecimento prévio dos estudantes será utilizada a metodologia de debate, onde no início da aula os acadêmicos irão expor seus entendimentos frente aos fundamentos de segurança computacional. Na sequência o nivelamento acontecerá por meio de interações dialogadas em uma breve aula expositiva com a apresentação dos conceitos referentes à unidade de ensino. Para o domínio teórico, os estudantes deverão ler o material proposto na bibliografia básica. A aplicação dos conhecimentos estudados nesta unidade será realizada mediante a resolução de exercícios relacionados ao tema.

Unidade 2: Criptografia
O conhecimento prévio dos estudantes nessa unidade de ensino está diretamente ligado com a unidade anterior, no início da aula os acadêmicos irão expor seus entendimentos frente ao tema da unidade por meio de discussão em grupos. Na sequência, o nivelamento acontecerá por meio de interações dialogadas em uma breve aula expositiva com a apresentação de técnicas de criptografia. Para o domínio teórico, os estudantes deverão ler o material proposto na bibliografia básica sugerida. A aplicação e a problematização dos conhecimentos estudados nesta unidade será realizada mediante a resolução de estudos de caso de média complexidade.

Unidade 3: Autenticação e Autorização
O desenvolvimento dos conteúdos ocorrerá mediante a proposta metodológica que pressupõe a ativa participação do aluno em todas as atividades, possibilitando a associação da teoria e da prática. No primeiro momento será realizada uma aula expositiva por meio de discussão trazendo exemplos de aplicações que utilizam de autenticação e autorização, bem como atividade prática para nivelamento. O domínio teórico será realizado mediante a leitura orientada da bibliografia básica e documentação técnica, bem como o desenvolvimento de um trabalho acerca do tema.

5.3 Avaliação do Processo Ensino Aprendizagem

Tipo	Nome	Peso	Descritivo	Data
A1	A1/1	3	Prova escrita, individual e sem consulta.	27/08/2024
A1	A1/2	3	Prova escrita, individual e sem consulta.	08/10/2024
A1	A1/3	3	Trabalho prático, em equipe e com consulta.	05/11/2024 a 26/11/2024
A1	APEx	1	Trabalho prático, em equipe e com consulta.	10/09/2024 a 03/12/2024

5.3.1 Orientações gerais sobre avaliações:

O processo avaliativo inserido nas atividades de ensino e aprendizagem é formativo e pressupõe uma Matriz de Referência que considera o domínio teórico, a aplicabilidade do conhecimento e a problematização. A avaliação será processual e terá como critérios a participação efetiva do acadêmico, a pontualidade na entrega das tarefas, a consistência e coerência dos conteúdos. Para fins de aferição e promoção da aprendizagem serão utilizadas para a composição da nota da média semestral, denominada A1, trabalhos e provas individuais e em grupo. Em relação à composição de A1, deverão ser realizadas as avaliações conforme descrição e pesos registrados no item 5.3 deste plano de ensino. Não serão realizadas atividades avaliativas fora dos prazos previstos, exceto nos casos previstos no regimento da Unoesc. 5.3.2 Sobre Avaliação A2 Conforme determina o Regimento da Unoesc, os alunos que obtiverem média semestral (A1) igual ou superior a 4,0 (quatro), mas não atingirem a média semestral (A1) igual ou superior a 7,0 (sete) pontos, submeter-se-ão ao exame final (A2), constituída de uma prova abrangente, presencial, individual, cumulativa e sem consulta. Segundo o regimento da Unoesc: o estudante que não realizar avaliação de A2 em data fixada, e cujos motivos sejam justificados e comprovados, pode requerer, via portal de ensino a avaliação fora de prazo, protocolando o pedido em até 48 (quarenta e oito) horas, a contar da data originalmente agendada.

6 PLANEJAMENTO DE CONTEÚDO E CRONOGRAMA

No desenvolvimento das atividades o cronograma poderá ser alterado, com prévio aviso do professor, mediante o caráter dinâmico do processo, ensino e aprendizagem.

Dia(s) letivo(s)	Conteúdo - Unidade de Ensino	Atividade
APEx - Atividades práticas de extensão	APEx.	Desenvolver um material de conscientização sobre Cyber Security (vídeo, folder, palestra, etc.) que contribua para que a sociedade tenha mais conhecimento acerca do assunto. Desenvolver também uma estratégia para entrega/apresentação com objetivo de alcançar o maior número possível de pessoas.
30/07/2024	Fundamentos de Segurança Computacional: Princípios e Conceitos de Segurança Computacional, A internet como Meio.	Aula expositiva, discussão e atividade prática.
06/08/2024	Fundamentos de Segurança Computacional: Princípios e Conceitos de Segurança Computacional, A internet como Meio.	Aula expositiva, discussão e atividade prática.
13/08/2024	Fundamentos de Segurança Computacional: Princípios e Conceitos de Segurança Computacional, A internet como Meio.	Aula expositiva, discussão e atividade prática.
20/08/2024	Fundamentos de Segurança Computacional: Princípios e Conceitos de Segurança Computacional, A internet como Meio.	Aula expositiva, discussão e atividade prática.
27/08/2024	Fundamentos de Segurança Computacional: Princípios e Conceitos de Segurança Computacional, A internet como Meio.	Prova escrita, individual e sem consulta para avaliação A1/1.

03/09/2024	VIII Simpósio Integrado das Engenharias e Arquitetura.	Atividades do Simpósio.
10/09/2024	Criptografia: Cifras de Transposição, Cifras de Substituição, Criptografia Simétrica, Criptografia Assimétrica, Cifras de Fluxo, Cifras de Bloco, Funções de Hash.	Aula expositiva, discussão e atividade prática.
17/09/2024	Criptografia: Cifras de Transposição, Cifras de Substituição, Criptografia Simétrica, Criptografia Assimétrica, Cifras de Fluxo, Cifras de Bloco, Funções de Hash.	Aula expositiva, discussão e atividade prática.
24/09/2024	Criptografia: Cifras de Transposição, Cifras de Substituição, Criptografia Simétrica, Criptografia Assimétrica, Cifras de Fluxo, Cifras de Bloco, Funções de Hash.	Aula expositiva, discussão e atividade prática.
01/10/2024	Criptografia: Cifras de Transposição, Cifras de Substituição, Criptografia Simétrica, Criptografia Assimétrica, Cifras de Fluxo, Cifras de Bloco, Funções de Hash.	Aula expositiva, discussão e atividade prática.
08/10/2024	Criptografia: Cifras de Transposição, Cifras de Substituição, Criptografia Simétrica, Criptografia Assimétrica, Cifras de Fluxo, Cifras de Bloco, Funções de Hash.	Prova escrita, individual e sem consulta para avaliação A1/2.
15/10/2024	Eventos de Inovação, Empreendedorismo e Tecnologia no Estado de Santa Catarina.	Participação do evento Smart Grid With Power Quality - evento que incentiva a cultura de inovação, empreendedorismo e tecnologia para o ecossistema catarinense de inovação.
22/10/2024	Autenticação e Autorização: Fluxos de Autenticação, Navigation Guards e Authentication Guards, Hash de Passwords, JWT - JSON Web Token, OAuth 2.0, Web Storage APIs, Interceptors e Middlewares, Autorização através de Gates, Policies e Token Scopes.	Aula expositiva, discussão e atividade prática.
29/10/2024	Autenticação e Autorização: Fluxos de Autenticação, Navigation Guards e Authentication Guards, Hash de Passwords, JWT - JSON Web Token, OAuth 2.0, Web Storage APIs, Interceptors e Middlewares, Autorização através de Gates, Policies e Token Scopes.	Aula expositiva, discussão e atividade prática.
05/11/2024	Autenticação e Autorização: Fluxos de Autenticação, Navigation Guards e Authentication Guards, Hash de Passwords, JWT - JSON Web Token, OAuth 2.0, Web Storage APIs, Interceptors e Middlewares, Autorização através de Gates, Policies e Token Scopes.	Desenvolvimento de trabalho com acompanhamento.
12/11/2024	Autenticação e Autorização: Fluxos de Autenticação, Navigation Guards e Authentication Guards, Hash de Passwords, JWT - JSON Web Token, OAuth 2.0, Web Storage APIs, Interceptors e Middlewares, Autorização através de Gates, Policies e Token Scopes.	Desenvolvimento de trabalho com acompanhamento.
19/11/2024	Autenticação e Autorização: Fluxos de Autenticação, Navigation Guards e Authentication Guards, Hash de Passwords, JWT - JSON Web Token, OAuth 2.0, Web Storage APIs, Interceptors e Middlewares, Autorização através de Gates, Policies e Token Scopes.	Desenvolvimento de trabalho com acompanhamento.
26/11/2024	Autenticação e Autorização: Fluxos de Autenticação, Navigation Guards e Authentication Guards, Hash de Passwords, JWT - JSON Web Token, OAuth 2.0, Web Storage APIs, Interceptors e Middlewares, Autorização através de Gates, Policies e Token Scopes.	Apresentação do trabalho e discussão para avaliação A1/3.
03/12/2024	Todo o conteúdo.	Discussão e revisão para encerramento do componente curricular.

7 REFERÊNCIAS BIBLIOGRÁFICAS

Referência	Tipo	
FUNDAMENTOS de segurança da informação. Porto Alegre SAGAH 1 recurso online	Básica	eBook
STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. São Paulo: Pearson, 492 p.	Básica	
TERADA, Routo. **Segurança de dados :** criptografia em rede de computador. . São Paulo Blucher 1 recurso online ISBN 97885115400.	Básica	eBook
SEGURANÇA máxima: o guia de um hacker para proteger seu site da internet e sua rede. Rio de Janeiro: Campus, xvi, 686 p.	Complementar	
LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** Campinas, SP: Millennium, vi, 234 p.	Complementar	
MORAES, Alexandre Fernandes de. **Cibersegurança e a nova geração de firewalls.** São Paulo Expressa 1 recurso online	Complementar	eBook
SARLET, Ingo Wolfgang. **Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital.** São Paulo Saraiva Jur 1 recurso online (Direito, tecnologia, inovação e proteção de dados num mundo em transformação).	Complementar	eBook
TEIXEIRA, Tarcísio. **Lei Geral de Proteção de Dados Pessoais (LGPD) :** comentada artigo por artigo. . São Paulo Saraiva Jur 1 recurso online	Complementar	eBook