

# CURSO DE ENGENHARIA DE SOFTWARE

## 1. CARACTERIZAÇÃO DA DISCIPLINA

Nome da Disciplina: <b>Segurança e Auditoria em Engenharia de Software</b>	Ano/semestre: <b>2021/2</b>
Código da Disciplina: <b>08937</b>	Período: <b>8º</b>
Carga Horária Total: <b>80h/a</b>	Carga Horária Teórica: <b>80h/a</b> Carga Horária Prática: <b>00h/a</b>
Pré-Requisito: <b>Não se aplica</b>	Co-Requisito: <b>Não se Aplica</b>

## 2. PROFESSOR(ES)

Millys Fabrielle Araujo Carvalhaes, M.e.

## 3. EMENTA

**Compreender:** Princípios de segurança: Confidencialidade, Integridade, Disponibilidade. Ameaças de segurança e softwares maliciosos. Infraestrutura de chaves públicas brasileiras (ICP-Brasil): Certificados digitais, Assinaturas digitais, Auditoria de segurança. ABNT NBR ISO/IEC 27001, 27002 e 27005; **Aplicar:** Ferramentas criptográficas. Controle de acesso: Autenticação, Autorização, Auditoria. Desenvolvimento de software seguro;

## 4. OBJETIVO GERAL

Capacitar o aluno em relação aos conceitos e à prática da segurança da informação, identificando as ameaças, os ataques e as principais práticas de proteção.

## 5. OBJETIVOS ESPECÍFICOS

Unidades	Objetivos Específicos
Princípios de Segurança de Computadores	Compreender os princípios de segurança
Ferramentas criptográficas. Autenticação de usuário. Controle de acesso. Segurança de bancos de dados. Software malicioso. Ataques de negação de serviço. Detecção de intrusão	Compreender as ameaças de segurança e softwares maliciosos.
Infraestrutura de chaves públicas brasileiras (ICP-Brasil).	Compreender a infraestrutura de chaves públicas brasileiras (ICP-Brasil).
Auditoria de segurança	Compreender a auditoria de segurança
Norma NBR 27000	Compreender as normas ABNT NBR ISO/IEC 27001, 27002 e 27005
Desenvolvimento de software seguro	Aplicar Desenvolvimento de software seguro

## 6. HABILIDADES E COMPETÊNCIAS

### Gerais:

- G.2. Conhecer e compreender os limites da computação;
- G.4. Gerir a própria aprendizagem e desenvolvimento pessoal e profissional, realizando trabalho em equipe, com visão trans e interdisciplinar;
- G.5. Desenvolver trabalhos e soluções, adotando metodologias diversificadas;

G.8. Resolver problemas usando ambientes de programação;

**Específicas:**

- E.1. Investigar, compreender e estruturar as características de domínios de aplicação em diversos contextos para a construção de sistemas de software, considerando questões éticas, sociais, legais e econômicas, individualmente e/ou em equipe;  
 E.3. Avaliar a qualidade e evolução de sistemas de software, aplicando adequadamente normas técnicas, através de padrões e boas práticas no desenvolvimento de software;  
 E.4. Identificar e analisar problemas, avaliando as necessidades dos clientes, especificar os requisitos de software, projetar, desenvolver, implementar, verificar, integrar e documentar soluções de software baseadas no conhecimento apropriado de teorias, modelos e técnicas.  
 E.5. Gerenciar projetos de software conciliando objetivos conflitantes, com limitações de custos, tempo e com análise de riscos;

**7. CONTEÚDO PROGRAMÁTICO**

Semana	Data	Conteúdo	Estratégia de ensino-aprendizagem	Aula Teórica/Prática	Local
1	12/08/2021	Apresentação da disciplina e Plano de ensino; Introdução aos conceitos de governança de TI.	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
2	19/08/2021	Visão geral dos conceitos de segurança. Software malicioso. Ataques de negação de serviço.	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
3	26/08/2021	Ferramentas criptográficas. (Parte 1)	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
4	02/09/2021	Ferramentas criptográficas (Parte 2.)	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
5	09/09/2021	Autenticação de usuário e controle de acesso.	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula -	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem

			questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.		
6	16/09/2021	Resolução de questões. Problematização: Falhas de segurança.	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
7	23/09/2021	<b>1ª Verificação de aprendizagem (on- line)</b>	<b>Prova Individual</b>	Teórica	Ambiente Virtual de Aprendizagem
8	30/09/2021	Devolutiva da Verificação de Aprendizagem	<b>Devolutiva qualificada</b>	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
9	07/10/2021	Protocolos de autenticação de usuário.	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
10	14/10/2021	Infraestrutura de chaves públicas brasileiras (ICP-Brasil). Certificados digitais e Assinaturas digitais (Parte 1)	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
11	21/10/2021	Certificados digitais e Assinaturas digitais (Parte 2)	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
12	28/10/2021	Sistemas de detecção e prevenção de intrusão. Firewalls (Parte 1)	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula –	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem

			questionário.		
13	04/11/2021	Firewalls (Parte 2)	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
14	11/11/2021	<b>2ª Verificação de aprendizagem</b>	<b>Prova Individual</b>	Teórica	Sala de aula
15	18/11/2021	Devolutiva da Verificação de Aprendizagem	<b>Devolutiva qualificada</b>	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
16	25/11/2021	Ataque Man-in-the-middle. Ataques à segurança da informação.	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
17	02/12/2021	ABNT NBR ISO/IEC 27000 (Parte 1) Auditoria de segurança.	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
18	09/12/2021	ABNT NBR ISO/IEC 27000 (Parte 2) Auditoria de segurança.	Leitura da referência bibliográfica Objeto de aprendizagem – Apresentação slides. Atividade pré-aula - questionário. Aula síncrona – Meeting Atividade pós-aula – questionário.	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem
19	16/12/2021	<b>3ª Verificação de aprendizagem</b>	<b>Prova Individual</b>	Teórica	Sala de aula
20	23/12/2021	Devolutiva da Verificação de Aprendizagem Encerramento da disciplina.	<b>Devolutiva qualificada</b>	Teórica	Sala de aula e Ambiente Virtual de Aprendizagem

## 8. PROCEDIMENTOS DIDÁTICOS

Atividade avaliativa, aula expositiva dialogada, retomada de conteúdo, problematização, mapa conceitual, seminário, trabalho em grupo e Tecnologias da Informação e Comunicação – vídeos, mapa mental, AVA – plataforma Moodle com Vídeo do YouTube

### Recursos de Acessibilidade disponíveis aos acadêmicos

O curso assegura acessibilidade metodológica, digital, comunicacional, atitudinal, instrumental e arquitetônica, garantindo autonomia plena do discente.

## 9. ATIVIDADE INTEGRATIVA

A interdisciplinaridade no curso de Engenharia de Software é construída com o amparo das disciplinas de Projeto Interdisciplinar. Estas promovem a associação entre os diferentes conteúdos, habilidades e cenários em projetos que favoreçam a construção do conhecimento científico, tecnológico e de prática profissional aliado à autoaprendizagem, proatividade, resolução conjunta de problemas, trabalho em equipe, reflexividade, entre outros.

A proposta de cada disciplina de Projeto Interdisciplinar é variável, mas, obrigatoriamente, deve evoluir em uma constante de maturidade pessoal, interpessoal, científica e prática. Para o desenvolvimento dos projetos interdisciplinares o aluno percorre três momentos: ensino – por meio do diálogo entre as áreas de conhecimento; pesquisa - seguindo os rigores metodológicos necessários à construção do conhecimento científico e de extensão – oportunizando o compartilhamento dos projetos desenvolvidos para o público interno e externo.

Em função disto, as atividades de cada Projeto estão detalhadas em Plano de Ensino próprio.

## 10. PROCESSO AVALIATIVO DA APRENDIZAGEM

### 1ª Verificação de aprendizagem (V. A.) – valor 0 a 100 pontos

Avaliação teórica com valor 50 pontos, contemplando questões relacionadas ao componente específico e de formação geral.

Avaliações processuais totalizam 50 pontos distribuídos da seguinte forma:

- Questionário pós-aula síncrona – 0 a 12 pontos. (0 a 2 pontos cada)
- Problemática: Falhas de segurança. – 0 a 38 pontos.

A média da 1ª V. A. será a somatória da nota obtida na avaliação teórica (50 pontos) e as notas obtidas nas avaliações processuais (50 pontos). (a devolutiva será realizada conforme Cronograma).

### 2ª Verificação de aprendizagem (V. A.) – valor 0 a 100 pontos

Avaliação teórica com valor 50 pontos, contemplando questões relacionadas ao componente específico e de formação geral.

Avaliações processuais totalizam 50 pontos distribuídos da seguinte forma:

- Questionário pós-aula síncrona – 0 a 12 pontos. (0 a 2 pontos cada).
- Problemática: Certificado Digital. – 0 a 19 pontos.
- Problemática: Firewalls. – 0 a 19 pontos.

A média da 2ª V. A. será a somatória da nota obtida na avaliação teórica (50 pontos) e as notas obtidas nas avaliações processuais (50 pontos). (a devolutiva será realizada conforme Cronograma).

### 3ª Verificação de aprendizagem (V. A.) – valor 0 a 100 pontos

Avaliação teórica com valor 50 pontos, contemplando questões relacionadas ao componente específico e de formação geral.

Avaliações processuais totalizam 50 pontos distribuídos da seguinte forma:

- Questionário pós-aula síncrona – 0 a 8 pontos. (0 a 2 pontos cada)
- Problemática: Ataques à segurança da informação. – 0 a 12 pontos.
- SITES – 0 a 30 pontos.
- Problemática: Política de segurança da informação – 0 a 30 pontos (**Alunos que não fazem SITES**)

A média da 3ª V. A. será a somatória da nota obtida na avaliação teórica (50 pontos) e as notas obtidas nas avaliações processuais (50 pontos). (a devolutiva será realizada conforme Cronograma).

## ORIENTAÇÕES ACADÊMICAS

- Nas três VAs – O pedido para avaliação substitutiva tem o prazo de 3 (três) dias úteis a contar da data de cada avaliação com apresentação de documentação comprobatória (§ 1º e § 2º do art. 39 do Regimento Geral do Centro Universitário UniEVANGÉLICA). **A solicitação deverá ser feita através do Sistema Acadêmico Lyceum obrigatoriamente.**
- Nas três VAs – O pedido para Revisão de nota tem o prazo de 3 (três) dias úteis a contar da data da publicação, no Sistema Acadêmico Lyceum, do resultado de cada avaliação. (Art. 40 do Regimento Geral do Centro Universitário UniEVANGÉLICA).
- Atribui-se nota zero ao aluno que deixar de submeter-se às verificações de aprendizagem nas datas designadas, bem como ao que nela se utilizar de meio fraudulento. (Capítulo V Art. 39 do Regimento Geral do Centro Universitário UniEVANGÉLICA)

### Participação em eventos científicos:

#### **Portaria – Frequência e nota dos alunos que apresentarem trabalhos em eventos científicos**

Seguir as orientações presentes na Portaria Nº 01, de 7 de fevereiro de 2019, dos Bacharelados em Computação, que dispõe sobre os procedimentos de justificativa de ausência para alunos que apresentarem trabalhos em eventos científicos.

**Condição de aprovação**

Considera-se para aprovação do (a) acadêmico (a) na disciplina, frequência mínima igual ou superior a 75% da carga horária e nota igual ou superior a sessenta (60) obtida com a média aritmética simples das três verificações de aprendizagem.

**11. BIBLIOGRAFIA (deve estar de acordo com o PPC)**


**Básica:**

STALLINGS, W.; BROWN, L., Segurança de Computadores: Princípios e Práticas. 2ª Ed. Campus. 2013;  
BASTA, A.; BASTA, N.; BROWN, M., Segurança de computadores e teste de invasão. Cengage. 2015. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788522121366>.  
HINTZBERGEN, Kees, Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Brasport. 2018.

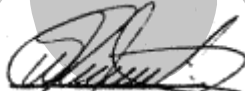
**Complementar:**

MCCARTHY, N. K.. Resposta a incidentes de segurança em computadores: planos para proteção de informação em risco. Porto Alegre, RS, Brasil: Bookman, 2014. 209 p.  
STALLINGS, William. Criptografia e segurança de redes princípios e práticas. 4. ed. São Paulo, SP, Brasil: Pearson Prentice Hall, 2008. 492 p.  
LYRA, Maurício Rocha; Lyra, Maurício Rocha. Segurança e Auditoria em Sistemas de Informação. Ciência Moderna, 2008. 253 p.  
SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. Rio de Janeiro - RJ, Brasil: Elsevier, 2014. 171 p.  
FERREIRA, Fernando Nicolau Freitas. Segurança da Informação. Rio de Janeiro: Editora Ciência Moderna Ltda, 2003.

Anápolis, 09 de agosto de 2021.

  
**Prof. M.e Natasha Sophie Pereira**

COORDENADORA DO CURSO DE ENGENHARIA DE SOFTWARE DA UniEVANGÉLICA

  
**Prof. M.e William Pereira dos Santos Júnior**

COORDENADOR PEDAGÓGICO DO CURSO DE ENGENHARIA DE SOFTWARE DA UniEVANGÉLICA

  
**Prof. M.e Millys Fabielle Araujo Carvalhoes**

PROFESSOR RESPONSÁVEL PELA DISCIPLINA