Escola:	Escola Politécnica	**Campus:**	Curitiba
Curso:	Bacharelado em Ciência da Computação e Sistemas de Informação	**Ano/Semestre**:	2021/2
Código/Nome da disciplina:	Segurança da Informação		
Carga Horária:	60 horas-relógio ou 80 horas-aula		
Requisitos:	Não se aplica		
CH/Créditos:	4	**Período:** 2o	**Turma**: U	**Turno:** manhã/noite
Professor Responsável:	Vilmar Abreu Junior		

1. EMENTA

A disciplina de Segurança da Informação é de natureza teórica/prática ofertada a estudantes da área da Computação. Durante a disciplina, o estudante identifica, de forma ética, programas maliciosos responsáveis por ataques e intrusões de sistemas computacionais. Além disso, configura sistemas, aplicando mecanismos de criptografia, autenticação e controle de acesso. Ao final, o estudante é capaz de aplicar mecanismos de segurança que protegem sistemas computacionais contra hackers, vírus e trojans, utilizando mecanismos, normas e padrões de segurança da informação baseado em aspectos legais e éticos.

2. RELAÇÃO COM DISCIPLINAS PRECEDENTES E POSTERIORES

Esta disciplina não possui outras precedentes e pode ser cursada por estudantes de qualquer curso. A disciplina fornece a base necessária de segurança da informação para as seguintes disciplinas:

Bacharelado em Ciência da Computação: Banco de Dados; Experiência Criativa: Pesquisa Aplicada; Programação Distribuída, Paralela e Concorrente; Big Data; Conectividade e Sistemas Ciberfísicos; Experiência Criativa: Inovando Colaborativamente; Performance em Sistemas

Ciberfísicos; Data Science; Sistemas Operacionais Ciberfísicos; Redes Convergentes; Experiência Criativa: Projeto Transformador I; Arquitetura de Sistemas Distribuídos, Paralelos e Concorrentes; Experiência Criativa: Projeto Transformador II.

Bacharelado em Sistemas da Informação: Banco de Dados; Desenvolvimento de Aplicações Multicamadas; Experiência Criativa: Implementando Sistemas de Informação; Big Data; Tecnologias para desenvolvimento Web; Conectividade e Sistemas Ciberfísicos; Desenvolvimento para Dispositivos Móveis; Experiência Criativa: Projetando Sistemas de Informação; Performance em Sistemas Ciberfísicos; Desenvolvimento de Serviços Web Seguros; Projeto Final: Especificação e Design; Projeto Final: Implementação.

3. TEMAS DE ESTUDO

TE1 – Autenticação e controle de acesso	TE3 – Softwares maliciosos e intrusões
TE2 – Sistemas criptográficos	TE4 – Normas e procedimentos de segurança

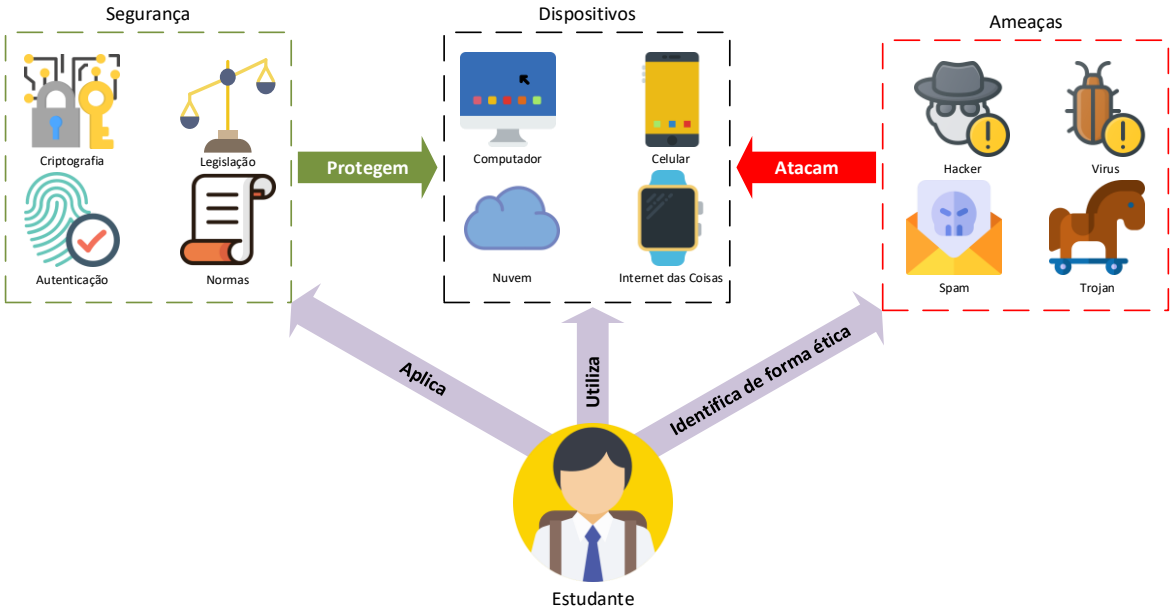
4. RESULTADOS DE APRENDIZAGEM

Quadro 4-1. Resultados de Aprendizagem e Temas de Estudo em relação às Competências do Egresso.

COMPETÊNCIA	ELEMENTO DE COMPETÊNCIA	RESULTADO DE APRENDIZAGEM	TEMAS DE ESTUDO
C1. Projetar soluções computacionais de acordo com especificações de requisitos, utilizando diretrizes da Engenharia de Software, considerando as tecnologias atuais de forma autorregulada	EC1.1 Aplicar mecanismos de segurança a diferentes contextos computacionais de forma ética	RA1. Integrar mecanismos de autenticação e controle de acesso em diferentes contextos computacionais, comprometendo-se com a qualidade do trabalho.	TE1. Autenticação e controle de acesso. TE4. Normas e procedimentos de segurança.
		RA2. Aplicar sistemas criptográficos em diferentes contextos computacionais, com eficácia.	TE2. Sistemas criptográficos. TE4. Normas e procedimentos de segurança.
		RA3. Aplicar mecanismos de detecção de intrusão e softwares maliciosos em sistemas computacionais, de forma eticamente responsável.	TE3. Softwares maliciosos e intrusões. TE4. Normas e procedimentos de segurança.
	EC1.2 Aplicar normas e padrões de segurança e privacidade em projetos de sistemas computacionais	RA1. Integrar mecanismos de autenticação e controle de acesso em diferentes contextos computacionais, comprometendo-se com a qualidade do trabalho.	TE1. Autenticação e controle de acesso. TE4. Normas e procedimentos de segurança.
		RA2. Aplicar sistemas criptográficos em diferentes contextos computacionais, com eficácia.	TE2. Sistemas criptográficos. TE4. Normas e procedimentos de segurança.

COMPETÊNCIA	ELEMENTO DE COMPETÊNCIA	RESULTADO DE APRENDIZAGEM	TEMAS DE ESTUDO
		RA3. Aplicar mecanismos de detecção de intrusão e softwares maliciosos em sistemas computacionais, de forma eticamente responsável.	TE3. Softwares maliciosos e intrusões. TE4. Normas e procedimentos de segurança.

5. MAPA MENTAL



6. METODOLOGIA E AVALIAÇÃO

Os Resultados de Aprendizagem desta disciplina serão desenvolvidos de acordo com o exposto no Quadro 6-1. Nele são apresentados os Resultados de Aprendizagem (RA), os Indicadores de Desempenho (ID), os Métodos ou Técnicas empregados e o Processo de Avaliação.

Serão conduzidos os seguintes tipos de avaliação:

- Diagnóstica: atividade de feedback imediato que permite ao professor acompanhar o aprendizado dos temas e identificar necessidades de reforço. Geralmente será aplicada na forma de questões com respostas imediatas em sala e referente a um tema estudado anteriormente de forma individual ou em grupo.

- Formativa: realizada durante o desenvolvimento das atividades, com intervenção e feedback imediato dado pelo professor ou pelos colegas, reforçando os conceitos, quando necessário.

- Somativa: composta por atividades com nota atribuída a partir de entregas (trabalhos e atividades) e avaliações por pares. A nota atribuída é necessária para aprovação na disciplina, conforme regulamento acadêmico.

- Recuperação: composta por atividades com nota atribuída a partir de entregas (trabalhos e atividades) e avaliações por pares com o objetivo de recuperar resultados de aprendizagem menores que 7,0. A nota atribuída é limitada no máximo em 07.

- Devolutiva: apresentação das avaliações realizadas corrigidas, geralmente uma ou duas semanas após a sua realização. As entregas somativas também possuem devolutivas, com comentários nas entregas.

Os seguintes critérios de aprovação serão considerados:

- Para ser aprovado nesta disciplina, o estudante deverá obter no mínimo nota igual a 7,0 (sete) em cada Resultados de Aprendizagem (RA), considerando todas as avaliações realizadas para este RA.

- Caso o estudante não atinja a nota média 7,0 (sete) para os Resultados de Aprendizagem, será oportunizada uma Semana de Recuperação, na qual o estudante poderá recuperar o(s) resultado(s) não atingido(s), por meio de atividades específicas.

- Caso o estudante, mesmo após a Semana de Recuperação, não consiga atingir a nota média 7,0 (sete) para os Resultados de Aprendizagem, então será considerado reprovado, e deverá cursar novamente a disciplina.

Quadro 6-1. Indicadores de Desempenho, Métodos ou Técnicas Empregados e Avaliações por Resultado de Aprendizagem.

RESULTADO DE APRENDIZAGEM	INDICADORES DE DESEMPENHO	PROCESSOS DE AVALIAÇÃO	MÉTODOS OU TÉCNICAS EMPREGADOS
RA1. Integrar mecanismos de autenticação e controle de acesso em diferentes contextos computacionais, comprometendo-se com a qualidade do trabalho.	RA1-ID1: Diferencia normas e procedimentos, identificando boas práticas de segurança em processos computacionais. RA1-ID2: Diferencia mecanismos de autenticação e mecanismos de controle de acesso, considerando a adequação de uso. RA1-ID3: Aplica mecanismos de autenticação e controle de acesso em diferentes contextos computacionais de forma integrada, comprometendo-se com a qualidade do trabalho.	[**Diagnóstica**] Aplicação de questionário objetivo para avaliação dos conceitos prévios dos estudantes sobre autenticação e controle de acesso. [**Formativa**] Aplicação de atividades práticas para avaliação e fixação dos conceitos vistos durante a aula. [**Somativa**] Avaliação individual com questões discursivas e objetivas sobre os conceitos e correspondente aplicabilidade de mecanismos de autenticação e controle de acesso.	- ConceptTest - Jigsaw - Problem Based Learning (PBL) **Meios de Interação**: Blackboard, Mentimeter e Kahoot.
RA2. Aplicar sistemas criptográficos em diferentes contextos computacionais, com eficácia.	RA2-ID1: Diferencia mecanismos de criptografia simétrica e assimétrica. RA2-ID2: Emprega sistemas criptográficos na proteção de sistemas computacionais com eficácia, considerando técnicas de hash criptográfico utilizadas em assinatura digital e certificados.	[**Diagnóstica**] Aplicação de questionário objetivo para avaliação dos conceitos prévios dos estudantes sobre criptografia. [**Formativa**] Aplicação de atividades práticas avaliação e fixação dos conceitos vistos durante a aula. [**Somativa**] Elaboração de projeto baseado em problemas sobre sistemas criptográficos.	- Flipped Classroom - Problem Based Learning (PBL) - Project Based Learning (PjBL) - Peer review **Meios de Interação**: Blackboard, Mentimeter e Kahoot.

RA3. Aplicar mecanismos de detecção de intrusão e softwares maliciosos em sistemas computacionais, de forma eticamente responsável.	RA3-ID1: Diferencia softwares maliciosos e intrusões em sistemas computacionais. RA3-ID2: Emprega mecanismos de detecção de intrusão e de softwares maliciosos em sistemas computacionais, de forma eticamente responsável.	[**Diagnóstica**] Aplicação de questionário objetivo para avaliação dos conceitos prévios dos estudantes sobre ataques e intrusões. [**Formativa**] Aplicação de atividades práticas avaliação e fixação dos conceitos vistos durante a aula. [**Somativa**] Elaboração de projeto em equipe sobre os conceitos e correspondente aplicabilidade dos sistemas de detecção de intrusão.	- Jigsaw - Problem Based Learning (PBL) - Project Based Learning (PjBL) - Peer review **Meios de Interação**: Blackboard, Mentimeter e Kahoot.

Quadro 6-2. Composição dos pesos dos Resultados de Aprendizagens.

	Peso do resultado de aprendizagem
RA1	35%
RA2	35%
RA3	30%

7. CRONOGRAMA DE ATIVIDADES

Quadro 7-1. Cronograma de atividades previsto, podendo sofrer alterações de acordo com necessidades.

Período (Semana)	**RAs**	**Atividades pedagógicas**	**Em aula / TDE**	**Carga Horária**
1	RA1	Apresentação da disciplina, plano de ensino e visão geral da disciplina	Em aula	4 horas
2	RA1	* Esteganografia	Em aula	4 horas
3	RA1	* Mecanismos de Autenticação	Em aula	4 horas
4	RA1	* Gestão de Identidade e Acesso	Em aula	4 horas
5	RA1	* Controle de Acesso	Em aula	4 horas
6	RA2	Criptografia Simétrica	Em aula	4 horas
7	RA2	* Centro de Distribuição de Chaves	Em aula	4 horas

8	RA2	* Criptografia de chave pública	Em aula	4 horas
9	RA2	Autenticação de mensagens	Em aula	4 horas
10	RA2	* Assinatura Digital e Certificados	Em aula	4 horas
11	RA2	Semana Acadêmica	Em aula	4 horas
12	RA1 e RA2	Recuperação do resultado de aprendizagem 01 e 02	Em aula	4 horas
13	RA3	Normas e procedimentos de segurança	Em aula	4 horas
14	RA3	* Softwares Maliciosos	Em aula	4 horas
15	RA3	* Ethical Hacking	Em aula	4 horas
16	RA3	* Detecção de Intrusão	Em aula	4 horas
17	RA3	Recuperação do resultado de aprendizagem 03	Em aula	4 horas

Quadro 7-2. Relação de atividades pedagógicas que atribuem frequência

Entregas de atividades pedagógicas para atribuição de frequência	CH contabilizada	Data de entrega
Esteganografia	8 horas	3ª semana
Mecanismos de Autenticação	4 horas	4ª semana
Gestão de Identidade e Acesso	4 horas	5ª semana
Controle de Acesso	4 horas	6ª semana
Centro de Distribuição de Chaves	8 horas	8ª semana
Criptografia de chave pública	4 horas	9ª semana
Assinatura Digital e Certificados	8 horas	11ª semana
Softwares Maliciosos	8 horas	13ª semana
Ethical Hacking	4 horas	14ª semana
Detecção de Intrusão	4 horas	15ª semana

8. REFERÊNCIAS

Materiais de apoio serão fornecidos via ambiente BlackBoard.

Básica:

- STALLINGS, William; BROWN, Lawrie. Segurança de computadores: princípios e práticas. Rio de Janeiro: Elsevier Campus, 2014
- STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. São Paulo: Pearson Prentice Hall, 2008.
- HANS BAARS, KEES HINTZBERGEN, JULE HINTZBERGEN, ANDRÉ SMULDERS. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002, 2018.

Complementar:

- NBRISO/IEC27002: TECNOLOGIA DA INFORMAÇÃO - TÉCNICAS DE SEGURANÇA - CÓDIGO DE PRÁTICA PARA CONTROLES DE SEGURANÇA DA INFORMAÇÃO
- Anderson, Ross (2008). Security Engineering: A Guide to Building Dependable Distribuited Systems, 2a. Ed., Ed. Wiley. ISBN: 978-0-470-06852-6. Disponível [online]: https://www.cl.cam.ac.uk/~rja14/book.html
- Amoroso, Edward G. (1994). Fundaments of Computer Security Tecnology. Ed. Prentice-Hall. ISBN: 978-0131089297
- Gollmann, Dieter. ((2011). Computer Security, 3e, Ed. Wiley. ISBN: 978-0-470-74115-3
- Menezes, van Oorschot and Vanstone, Handbook of Applied Cryptography (2001); Ed. CRC Press. Disponível [online] http://cacr.uwaterloo.ca/hac/
- https://www.journals.elsevier.com/computers-and-security/

Alterações por conta da COVID19:

Não se aplica.

9. Acessibilidade**

Não houve necessidade de adaptação.

10. Adaptações para práticas profissionais**

Não se aplica.

** conforme nota técnica conjunta número 17/2020 CGLNRS/DPR/SERES/SERES