Segurança Cibernética

Apresentação e Conceitos de Segurança Cibernética

Prof. Dr. Daniel Caetano

2021 - 2

Compreendendo o problema

- **Situação:** Parques tecnológicos são construídos para manter e processar todas as informações úteis às empresas.

Essas informações existiam antes?

Compreendendo o problema

- Vamos conhecer o Mentimeter!

https:///www.menti.com/

Compreendendo o problema

- **Situação:** Essas informações são mais facilmente comprometidas hoje, pois estão mais acessíveis...

Qual é o impacto desse comprometimento?

Objetivos

- Conhecer o professor
- Conhecer a disciplina
- Compreender o sistema de estudo
- Conhecer a história e evolução da segurança cibernética
- Compreender o valor da informação para os negócios e as pessoas

Apresentação

Quem é o professor?

Chamada, Presença e Contato

- Será controlada a presença
  - Chamada ocorrerá sempre nos 15 minutos finais
    - Em tempo real, na aula – Lista do Teams
  - "Estou frequentando mas a matrícula..."
- Contato

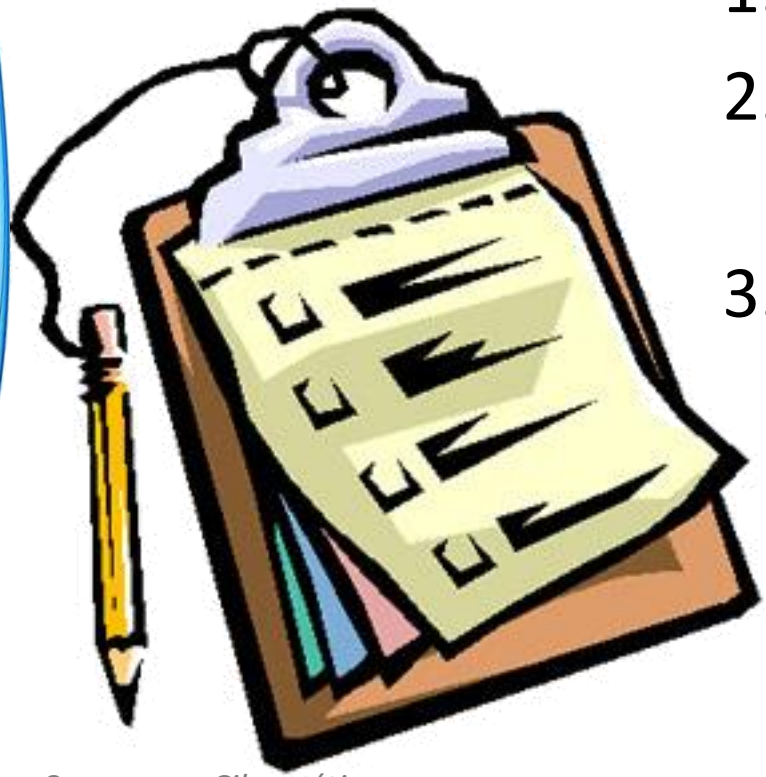
Professor	Informações de Contato
Daniel Caetano	prof@caetano.eng.br

Plano de Ensino e Plano de Aula

Plano de Ensino

Disponível no SIA/YUDQS/AURA

https://estudante.estacio.br/



1. Entre no **Ambiente Virtual**
2. Clique no
   NOME DA DISCIPLINA
3. Clique em
   PLANO DE ENSINO

Plano de Aula – Turma de **2ª**

- 16/08 – 1. Apresentação
- 23/08 – 2. Princípios I
- 30/08 – 3. Princípios II
- 06/09 – 4. Ataques I
- 13/09 – 5. Ataques II
- 20/09 – 6. Ataques III
- 27/09 – 7. Vulnerabilid. I / Rev. I
- **04/10 – P1 (AV1)**
- 11/10 – 8. Vulnerabilidades II
- 18/10 – 9. Contramedidas I
- 25/10 – 10. Contramedidas II
- 01/11 – 11. Resposta a Incidentes
- 08/11 – Revisão II
- **15/11 – [República]**
- **22/11 – P2 (AV2)**
- 29/11 – Vista
- **06/12 – P3 (AV3)**
- 13/12 – Fechamento dos Diários

- **Aulas que possuem conteúdo digital no ambiente AURA**
  Esse conteúdo extra é considerado CRÉDITO DIGITAL e as horas e notas dos mesmos são computadas em separado!

Como Estudar?

- Até o fim do ensino médio...
  - Professor: apresenta os conteúdos completos
  - Teoria-prática: são exercitadas todas as situações em sala
  - Alunos: estudam após a aula, repetindo exercícios.
- E na faculdade...?
  - O procedimento do ensino médio... não é eficiente.
  - Alunos: estudam antes da aula os conteúdos
  - Conjunto: na aula, discutem o conteúdo diante de uma situação-problema
  - Professor: organiza os conceitos principais do conteúdo
  - Teoria-prática: exercitadas situações relevantes em sala.

Disciplina Presencial + Digital

- Como funciona?
  - Aluno se prepara entre as aulas, conhece a teoria
    - Vídeos, textos, desafios...
  - Na aula: discussão e complemento do conteúdo
  - Na aula: teoria-prática com atividades participativas
- Como é a preparação semanal?
  - Varia muito de acordo com o conteúdo... Mas...
  - Toda semana serão passadas atividades
    - **Conteúdo** para absorver e analisar...
    - Complementado por um **desafio**: Atividade Autônoma Aura
  - Algumas aulas têm bastante conteúdo digital
    - Esse conteúdo será **discutido** em sala e cai em prova!

Ambiente Aura

- Você acompanha seus conteúdos...

https://estudante.estacio.br/login

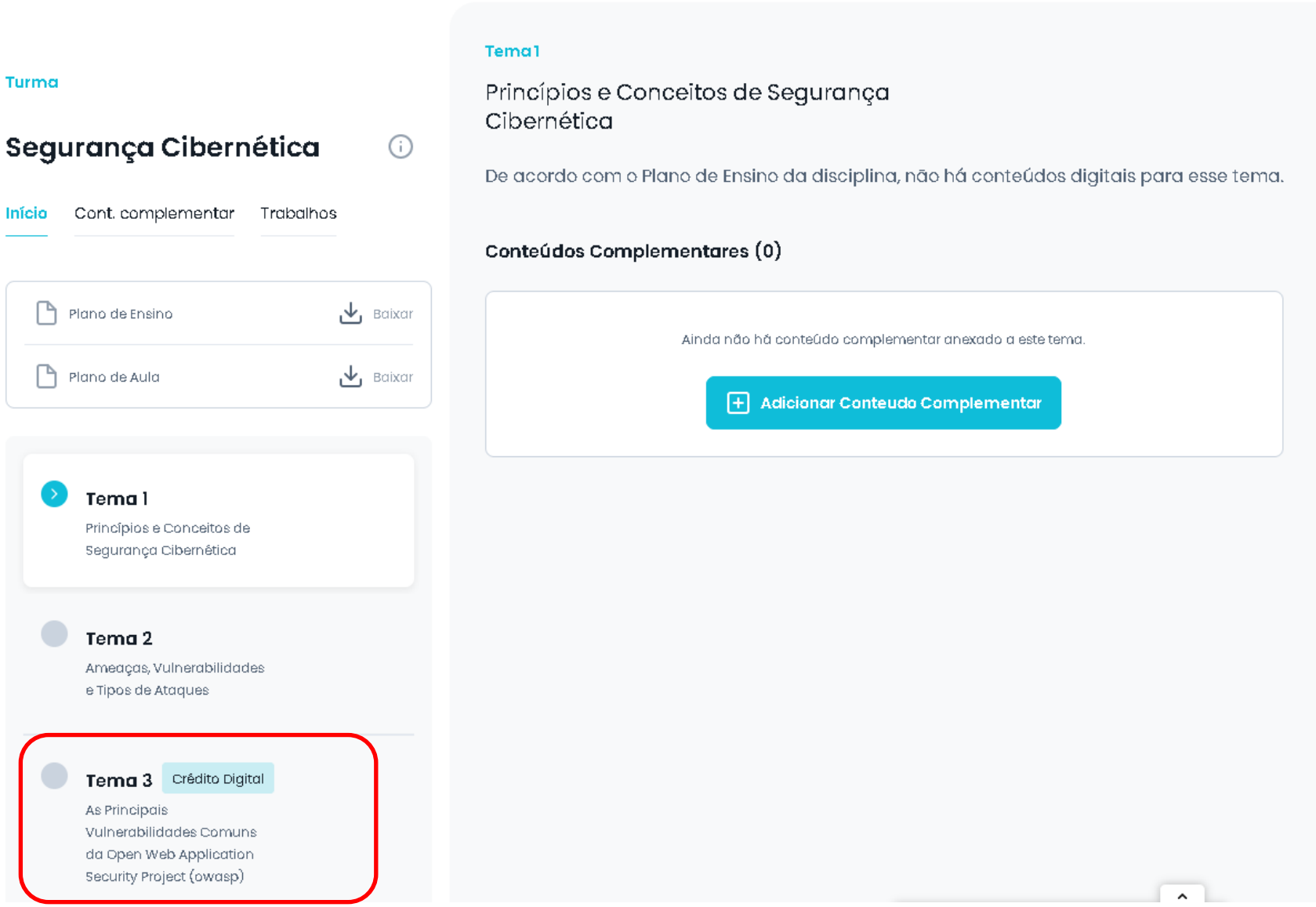
 Turmas

 Fontes de Informação (mais no SIA/YUDQS!)

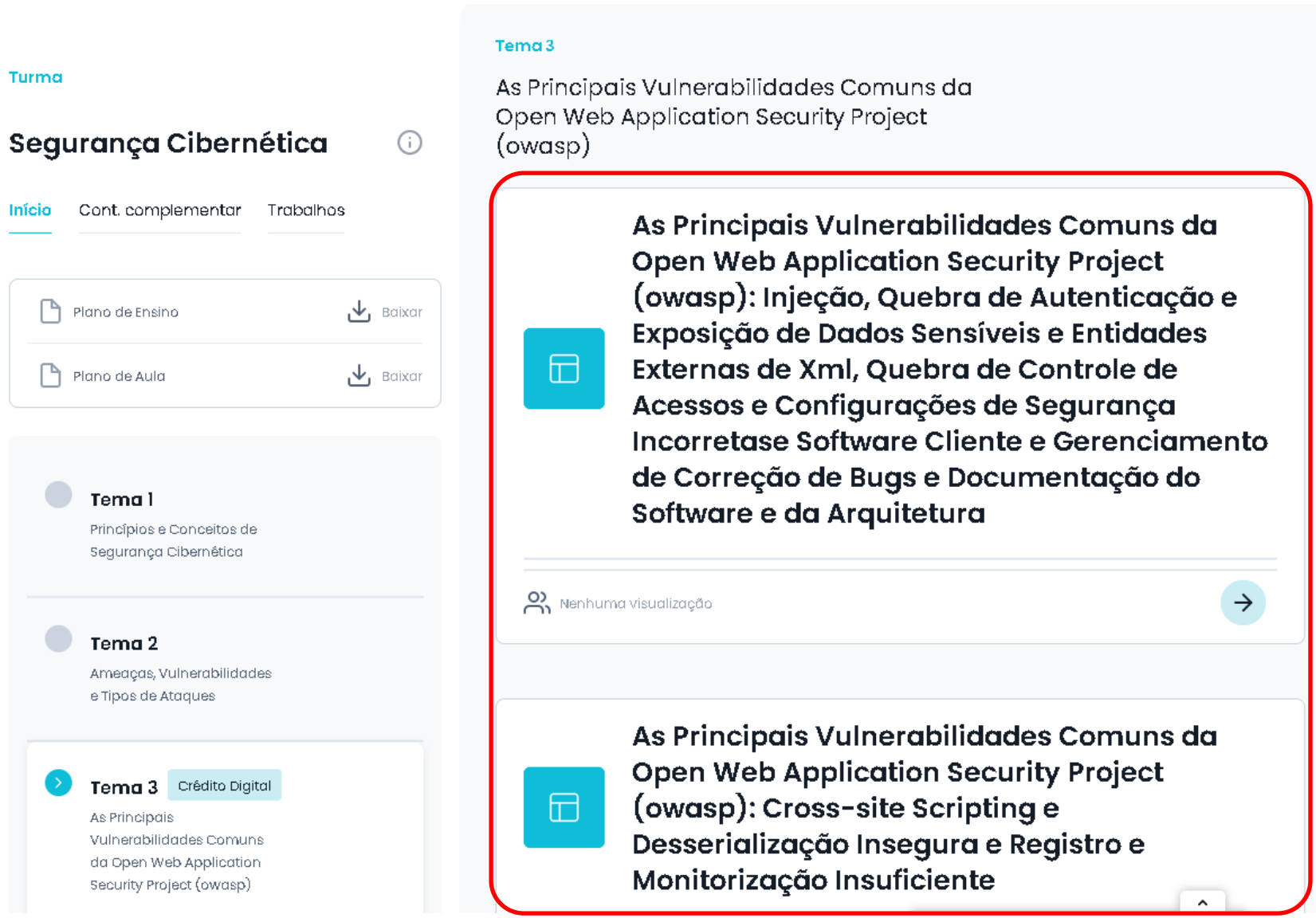
 Calendário Acadêmico (Presencial Centro-Sul)

 Sistema de Avaliações

Ambiente Aura - Turma



Ambiente Aura - Turma



Trabalhos, Datas e Critério de Aprovação

Trabalhos, Datas e Aprovação **(2ª)**

Trabalho	Valor	Data
Desafios até Aula 05	0,5 em Prova	Domingo (Web)
Desafios após Aula 05	0,5 em Prova	Domingo (Web)
Atividade Avaliativa A – Aula 06	3,0 na AV1	20/09
Avaliação P1	**7,0 na AV1**	**04/10 (Aula)**
Atividade Avaliativa B – Aula 09	2,5 na AV2	31/10
Atividade Avaliativa C – Aula 10	2,5 na AV2	07/11
Avaliação P2	**5,0 na AV2**	**22/11 (Aula)**
Avaliação P3	**10,0 na AV3**	**06/12 (Aula)**
Avaliação Digital (AVD)	**10,0 na AVD**	**11~24/11**
Avaliação Digital Substitutiva (AVDS)	**10,0 na AVDS**	**02~08/12**

Os desafios serão sempre postados aqui:
https://padlet.com/djcaetano/segciber

Composição da Nota AV1

- T1: nota que varia de 0,0 a 3,0
- P1: nota obtida na avaliação P1

$$\underbrace{AV1}_{0,0 \text{ a } 10,0} = \overbrace{T1}^{0,0 \text{ a } 3,0} + \overbrace{P1}^{0,0 \text{ a } 7,0}$$

Composição da Nota AV1

- Fiquei com AV1 < 4,0!

Calma!

- Pode ser que tenha **Nova Chance** (Nota AVR)
  - Agendar/Executar: 18/10 a 29/10

$$\underbrace{AV1}_{\text{0,0 a 10,0}} = \text{máx}(\overbrace{T1}^{\text{0,0 a 3,0}} + \overbrace{P1}^{\text{0,0 a 7,0}} , \overbrace{AVR1}^{\text{0,0 a 10,0}})$$

Informações: https://portal.estacio.br/novachance/

Composição da Nota AV2

- T2: nota que varia de 0,0 a 5,0
- P2: nota obtida na avaliação P2

$$\underbrace{AV2}_{0,0 \text{ a } 10,0} = \overbrace{T2}^{0,0 \text{ a } 5,0} + \overbrace{P2}^{0,0 \text{ a } 5,0}$$

Composição da Nota AV2

- Fiquei com AV2 < 4,0!

Calma!

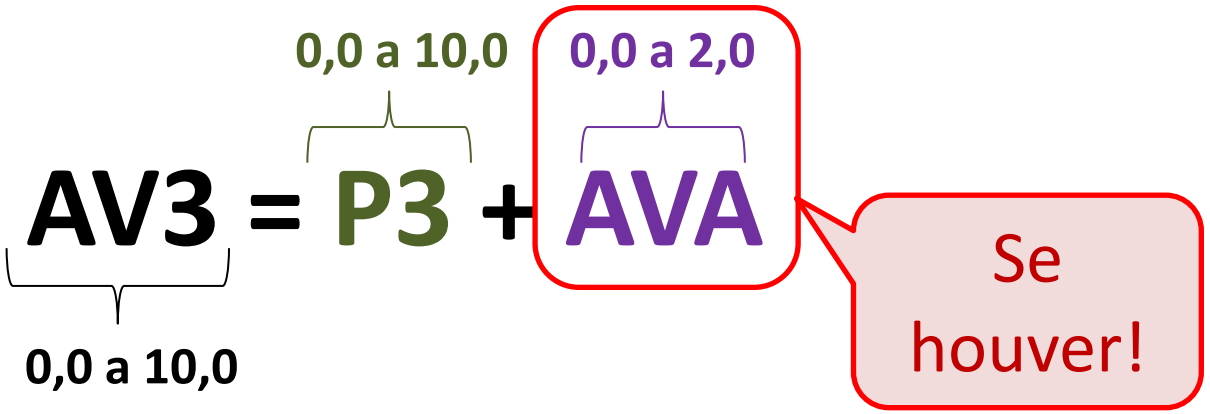
- Se tiver **Nova Chance** (Nota AVR)
  - Agendar/Executar: 19/11 a 01/12

$$\underbrace{AV2}_{\text{0,0 a 10,0}} = \text{máx}(\overbrace{T2}^{\text{0,0 a 5,0}} + \overbrace{P2}^{\text{0,0 a 5,0}} , \overbrace{AVR1}^{\text{0,0 a 10,0}})$$

Informações: https://portal.estacio.br/novachance/

Composição da Nota AV3

- P3 é a nota obtida na avaliação P3 (PNI).
- AVA é a nota do Avaliando o Aprendizado



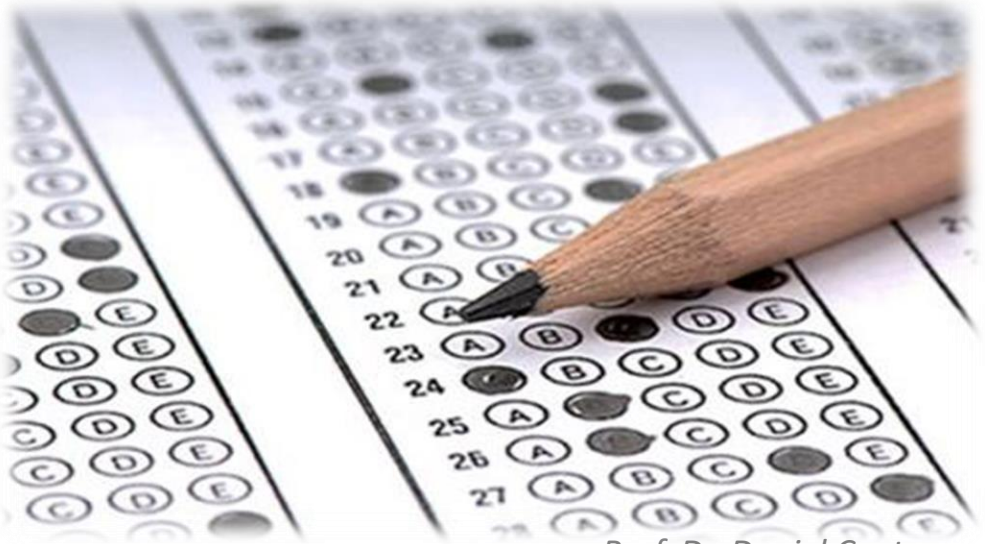
Avaliando o Aprendizado

- Quatro Simulados, 5 questões cada
  - Cada questão vale 0,1 na AV3 (se resposta for correta!)
  - Até 2,0 pontos na AV3

Informações: **https://portal.estacio.br/avaliandoaprendizado**

Avaliação: **https://simulado.estacio.br/alunos/**

- Módulo 1: 01/09~
- Módulo 2: 21/09~
- Módulo 3: 11/10~
- Módulo 4: 04/11~
- Terminar até: 17/11



Composição da Nota AVD

- A AVD é composta simplesmente da nota obtida na avaliação AVD, que é uma Prova que Digital sobre o Conteúdo Digital da Disciplina:
  - AVD: 11/11 a 24/11
  - AVDS: 02/12 a 08/12

$$\underbrace{AVD}_{\text{0,0 a 10,0}} = \text{máx}(\overbrace{AVD}^{\text{0,0 a 10,0}} , \overbrace{AVDS}^{\text{0,0 a 10,0}})$$

Critério de Aprovação

A = Maior nota entre { AV1 , AV2 , AV3 }

B = Segunda maior nota entre { AV1 , AV2 , AV3 }

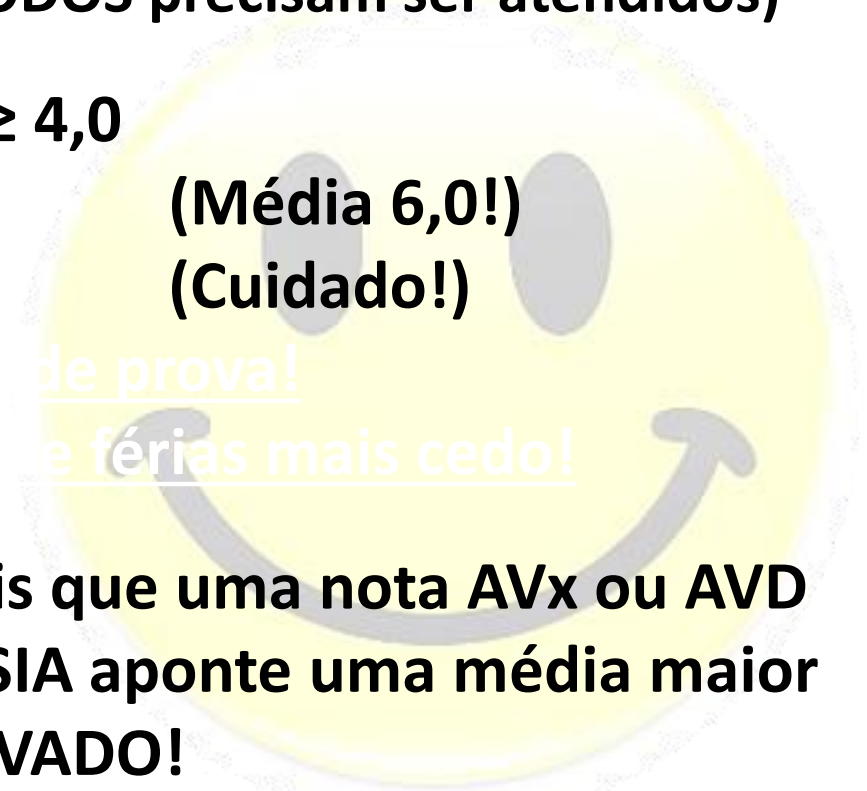
C = Maior nota entre as AVDs

Critérios de Aprovação (TODOS precisam ser atendidos)

1) A ≥ 4,0; B ≥ 4,0; C ≥ 4,0

2) A + B + C ≥ 18,0 (Média 6,0!)

3) Frequência ≥ 75% (Cuidado!)



ATENÇÃO: Se você tiver mais que uma nota AVx ou AVD abaixo de 4,0, ainda que o SIA aponte uma média maior que 6,0, você estará REPROVADO!

Reforço de Estudo

- Aulas complementares de apoio
  - Prepara AV1: 02/10 – Aula ONLINE com hora predefinida!
  - Prepara AV2: 06/11 – Aula ONLINE com hora predefinida!

http://prepara.estacio.br/presencial

- Resumo dos programas de reforço:

https://portal.estacio.br/reforcoacademico/

Bibliografia e Fontes de Informação

Bibliografia Básica

- **Segurança de Computadores – Princípios e Práticas**
  - **Stallings (Minha Biblioteca - 978-85-352-6449-4)**
- **Hackers Expostos: Segredos e Soluções para a Segurança de Redes**
  - **Dscambray; McClure; Kurtz (Minha Biblioteca - 978-0-07-178028-5)**
- **Segurança de Computadores e Teste de Invasão**
  - **Basta; Basta; Brown (Minha Biblioteca - 978-0-8400-2093-2)**

Bibliografia Complementar

- **Redes de computadores: uma abordagem top-down**
  - **Fropuzan; Mosharraf (Minha Biblioteca - 978-85-8055-169-3)**
- **Segurança de Redes sem Fio: Guia do Iniciante**
  - **Wrightson (Minha Biblioteca - 978-0-07-178028-5)**
- **Redes de Computadores e Internet**
  - **Comer (Minha Biblioteca - 978-0-13-358793-7)**

Material de Aula

- **Apresentações e outros itens de estudo**

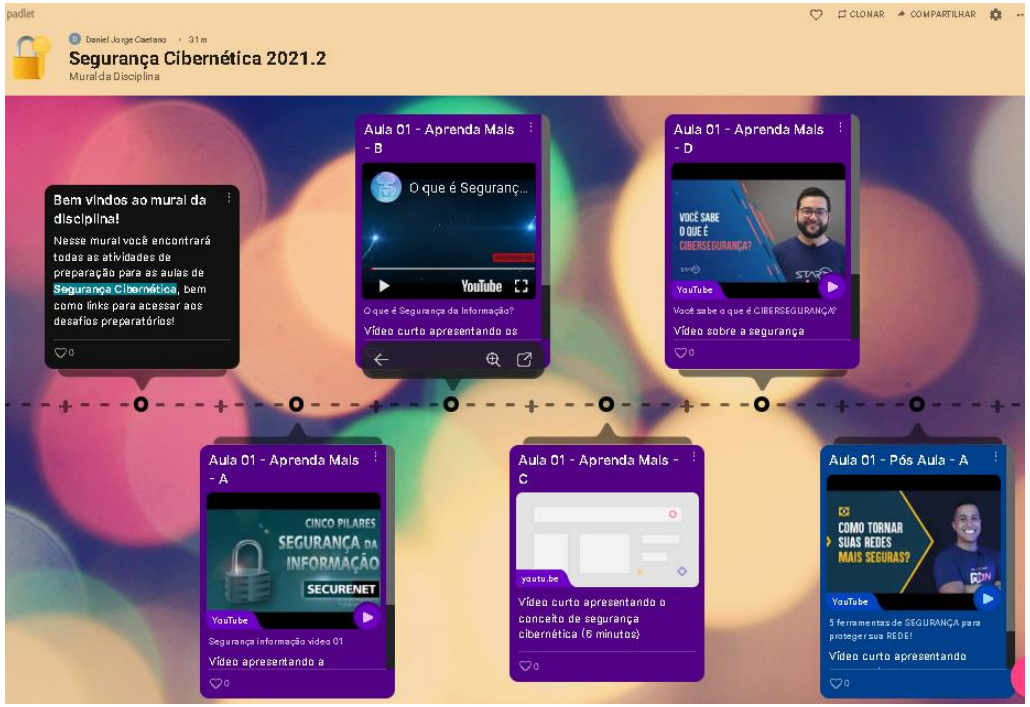
https://www.caetano.eng.br/

- **Selecione o ano/semestre atual**
- **Clique no nome da disciplina**

Material de Estudo

- **Conteúdo e atividades de preparação**

https://padlet.com/djcaetano/segciber



Aula NN
Aprenda Mais

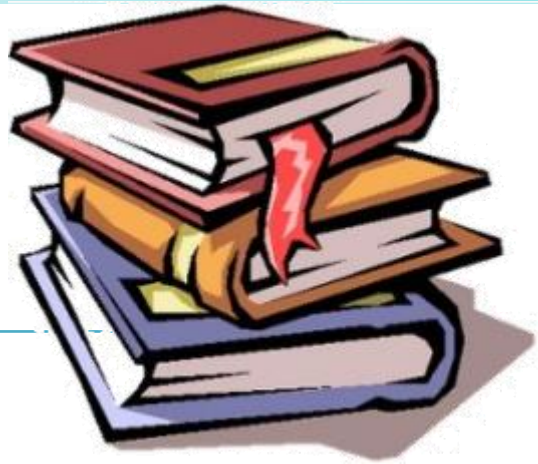
Aula NN
Pós Aula

Aula NN
Desafio

Atividade Autônoma Aura

ATENÇÃO: As postagens mais novas estarão à direita!

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2021b/ara0076.php (Segurança Cibernética – Aula 1)
Minha Biblioteca	• Segurança de Computadores: Princípios e Práticas (ISBN: 978-85-352-6449-4), págs 7 a 9; • Segurança de Computadores e Teste de Invasão (ISBN: 978-0-8400-2093-2), págs 1 a 11.
Material Adicional	1) O que é Segurança da Informação? https://youtu.be/_OrtRqR_mw 2) Segurança informação video 01 https://youtu.be/ZD66EMgB1FA 3) Segurança Cibernética: Funcionamento e Exemplos https://youtu.be/mLWd6kO2Udk 4) Você sabe o que é CIBERSEGURANÇA? https://youtu.be/CU2yQxzkvFg

Importância das Informações

Importância da Informação

- Necessidades das empresas
  - Saber fazer
  - Aprimorar o que faz
  - Conhecer a quem vender
  - Satisfazer aos clientes.

- Tudo isso exige informações
  - São essenciais para os negócios!
  - Informações são ativos!

Importância da Informação

- Informações de pessoas físicas
  - Dados pessoais
  - Informações bancárias
  - Informações operacionais
  - Internet das Coisas (IoT)
    - Automação residencial
    - Sistemas de vigilância
    - ...

Importância da Informação

- O mundo mudou muito nas últimas décadas
  - Documentos e processos são digitais: nuvem
  - Todos os dispositivos “sempre online”!

Importância da Informação

- Informação em constante risco
  - É preciso proteger os negócios!
    - Marco Civil da Internet
    - Lei Geral de Proteção de Dados

- Isso é suficiente?
  - O que fazer?

Mentimeter

Recordando:

Princípios da Segurança da Informação

Princípios Fundamentais

- Equação fundamental da segurança

$$Praticidade = \frac{1}{Segurança}$$

- Objetivo: garantir
  - **Confidencialidade**
  - **Integridade**
  - **Disponibilidade.**

Princípios Fundamentais

- Qual a preocupação em cada caso?
  - Confidencialidade
    - Informação protegida da visualização não autorizada
    - Controle da coleta e compartilhamento de informações
  - Integridade
    - Informação protegida do manuseio não autorizado
    - Sistemas protegidos de adulteração de suas funções
  - Disponibilidade
    - Informação deixa de estar acessível no momento necessário

Princípios Fundamentais

- O que configura a quebra em cada caso?
  - Confidencialidade
    - Exposição de informações a pessoas não autorizadas
  - Integridade
    - Sistema ou informação manipulada/destruída sem autorização
  - Disponibilidade
    - Indisponibilidade do sistema ou informação no momento de uso

Preocupações Adicionais

- Preocupações decorrentes:
  - Autenticidade
    - Confiabilidade do conteúdo e autoria
      - Os autores são quem dizem ser
      - Os dados transmitidos são genuínos
  - Determinação de responsabilidade
    - Irretratabilidade / Não-repúdio
    - Registros para apuração de responsabilidades

Magnitude dos Impactos

- **Baixa**: Efeito adverso limitado nas operações, ativos ou indivíduos
  - Não inviabiliza a execução das tarefas, mas afeta a efetividade das ações
  - Dano desprezível aos ativos organizacionais
  - Perdas financeiras insignificantes
  - Dano reduzido a indivíduos
- **Moderada**: Efeito adverso sério nas operações , ativos ou indivíduos
  - Não inviabiliza a execução das tarefas, mas afeta muito sua efetividade
  - Dano significativo aos ativos organizacionais
  - Perdas financeiras significativa
  - Dano significativo a indivíduos, sem ferimentos sérios ou ameaças à vida
- **Alta**: Efeito adverso catastrófico nas operações, ativos ou indivíduos
  - Praticamente inviabiliza a execução das tarefas
  - Grande dano aos ativos organizacionais
  - Grandes perdas financeiras
  - Dano grave a indivíduos, envolvendo ferimentos sérios ou ameaças à vida

Exemplos de Magnitudes

- Confidencialidade
  - Alta: informações salariais e familiares
  - Média: projetos em que um funcionário trabalhou
  - Baixa: curriculum vitae de um funcionário
- Integridade
  - Alta: informações hospitalares sobre alergias
  - Média: desfiguração de um fórum de *hobbistas*
  - Baixa: informações de votações anônimas online
- Disponibilidade
  - Alta: sistema de refrigeração de reatores nucleares
  - Média: site informativo de uma universidade fora do ar
  - Baixa: site para consulta a lista telefônica online fora do ar

Conhecendo os Adversários

Conhecendo o Adversário

- Crackers
  - Muito conhecimento em TIC
    - Redes com fio
    - Redes sem fio
    - Telefonia
  - Conhecimento avançado de programação
  - Conhecimentos de eletrônica, psicologia etc...
  - Ação: **quebra da legalidade**

Hackers x Crackers

- Público: Hackers = Crackers
  - Mas a comunidade não entende assim
- Hackers
  - Muito conhecimento em TIC
    - Redes com fio
    - Redes sem fio
    - Telefonia
  - Conhecimento avançado de programação
  - Conhecimentos de eletrônica, psicologia etc...
  - Ação: **SEM quebra da legalidade**

Atuação Legal: Hackers

- Identificação e correção de falhas
  - Contratados para isso
- Exemplos de tarefas
  - Análise de código
  - Teste de Invasão (*pentesting*)
    - Exploits
    - Metaexploits

Motivações dos Hackers e Crackers

- Curiosidade
- Paixão por quebra-cabeças
- Reconhecimento e fama
- Vingança
- Ganho financeiro
  - É sempre uma motivação ruim?
- Razões ideológicas (patriotismo etc.)
  - É sempre uma motivação ruim?
- ...

Classificação da Comunidade

- Na terminologia da comunidade
  - Chapéu Branco (White Hat) - Hacker
  - Chapéu Preto (Black Hat) - Cracker
  - Chapéu Cinza (Gray Hat)
    - Meios de Black Hat (destruir ou vazar dados, sem autorização, anti-ética)
    - Motivações “nobres” (atacar uma empresa considerada “má”, revelar crimes etc)



Classificação “Formal”

- Novatos (n00b)
  - Habilidades muito limitadas em conhecimento e capacidade de programação
  - Dependem e confiam em “kits” para os ataques
  - Podem causar mais danos do que imaginam, por ignorância sobre os ataques que praticam
  - Motivação principal é a notoriedade e a fama

Classificação “Formal”

- Cyberpunks (Punks Cibernéticos)
  - Desenvolvem seus próprios softwares
  - Compreendem os sistemas que atacam
  - Envolvem-se em roubos de senha, cartão e fraudes em telecomunicações
  - Motivação principal é a notoriedade, mas em geral possuem também motivação ideológica

Classificação “Formal”

- Internos
  - (Ex-)Funcionários Descontentes
    - Usam seu conhecimento e permissões nos sistemas
    - **Maior fonte de ameaças à segurança**
  - Ladrões menores (funcionários, consultores...)
    - Conhecem computação e falhas do sistema da empresa
    - Motivados por ganância ou necessidade

Classificação “Formal”

- Coders (Codificadores)
  - Mentores dos novatos
  - Escrevem scripts e ferramentas para outros
  - Motivados pelo senso de poder e prestígio
  - Perigosos por suas motivações ocultas
    - Ferramentas que desenvolvem costumam serem *trojans*

Classificação “Formal”

- Criminosos Profissionais
  - Especializados em espionagem corporativa
  - Costumam atuar por contrato (aluguel)
  - Altamente motivados e treinados
    - Não poupam investimentos leitura e equipamentos
  - Atuam com tecnologia de ponta

Classificação “Formal”

- Terroristas Cibernéticos
  - Atuam em todos os tipos de ataques destrutivos
  - Motivações normalmente político-ideológicas
  - Possuem muitos recursos e conhecimento
  - Crescimento grande desde o fim da guerra-fria

Classificação “Formal”

- Hacktivistas
  - Querem erradicar entidades ou causas “do mal”
  - Por definição, agem por ideologia
  - Tentam interferir em questões políticas

Classificação “Formal”

- Hackers da Velha Guarda
  - Normalmente agem pelo desafio intelectual
  - Possuem um desrespeito enorme pela propriedade
  - Muitas vezes parecem não ter intenção criminosa

Histórico da Atuação Hacker/Cracker

- **1940** – Surgem com os computadores
- **1950** – Conceito moderno: uso diferenciado da tecnologia para resolver problemas
- **1960** – Sistemas multiusuário: contornar controle de acesso
- **1970** – Telecomunicação: telefonar de graça
- **1980** – Modems e o *hacking* de comunicações
  - Virus, vermes, trojans... Uso de BBSs e Internet
- **1990** – Internet: difusão maior de vírus
- **2000** – eCommerce: fraudes, scams...

Entidades Certificadoras

- Associação de Controle e Auditoria de Sistemas da Informação (ISACA): www.isaca.org
- EC-Council: www.eccouncil.org/
- ISC2: www.isc2.org
- CompTIA: www.comptia.org/certifications/security
- Certificação de Garantia da Informação Global (GIAC): www.giac.org/certifications/cyber-defense

ATIVIDADE

Atividade

- Discussão
- Alguém tem conhecimento de algum tipo de ataque que tenha impactado a segurança da informação em alguma empresa?
- Quais princípios de segurança da informação foram afetados nesse ataque?
- Qual o impacto que isso teve nos negócios da empresa?

ENCERRAMENTO

Resumo e Próximos Passos

- Planos de Ensino e Aula, datas e critérios
- Principais fontes de informação
- Princípios da Segurança da Informação
- Hackers x Crackers – Questão Ética
- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/segciber

- Principais mecanismos de proteção
  - O que é melhor em cada caso?

PERGUNTAS?