PLANO DE APRENDIZAGEM

1. DADOS DE IDENTIFICAÇÃO			
Curso: Bacharelado em Sistemas de Informação			
Disciplina: Auditoria e Segurança da Informação			**Código:** SIF38
Professor: Me. Ronierison de Souza Maciel			**Email:**ronierison.maciel@unirios.edu.br
CH Teórica: 40h	**CH Prática:** 20h	**CH Total:** 40h	**Créditos:** 04
Pré-requisito:			
Período: VII		**Ano:** 2021.1	

2. EMENTA:

Fundamentos de segurança para sistemas de informação. Proteção da informação. Gestão de vulnerabilidade em sistemas de informação. Noções de auditoria de sistemas de informação.

3. COMPETÊNCIAS E HABILIDADES DA DISCIPLINA:

Preparar profissionais que no exercício de suas atividades estejam aptos a:

- Reconhecer e relacionar os principais riscos envolvidos no ambiente de informações;
- Descrever e explicar ferramentas e procedimentos com relação à segurança da informação - nos aspectos de segurança lógica, física e ambiental;
- Reconhecer e relacionar os principais pontos de controle de auditoria da tecnologia da informação no que se refere à auditoria do desenvolvimento e manutenção de sistemas, administração de dados,
- Estabelecer os ativos de sistemas de informação e de sistemas para as organizações.
- Definir, gerenciar e otimizar políticas de segurança.
- Atuar em auditorias de segurança da informação e de sistemas.

4. OBJETIVO GERAL DA APRENDIZAGEM:

Conhecer a tecnologia disponível na área de redes de computadores com a finalidade de identificar a mais adequada no suporte a sistemas distribuídos. Fornecer os princípios básicos de telecomunicações e torná-los capazes de montar e configurar uma rede de computadores em seus aspectos principais.

5. CONTEÚDOS

5.1 -PRIMEIRA ETAPA

5.1.1 CONTEÚDOS PRESENCIAIS (20 aulas)

5.1.1.1 GESTÃO DA SEGURANÇA DA INFORMAÇÃO (5h)

- Considerações para o Executivo da Organização

- pela Existência da Política de Segurança da Informação
- A Segurança necessita de Planejamento
- Planejamento estratégico da segurança da informação.
- Segurança alinha ao negócio!
- A organização que aprende
- ROI, meta-ROI e despesa
- Uma política divina
- Arquitetura corporativa
- Arquitetura de segurança da informação

5.6 PARCEIROS (5h)

- Parceiros
- Serviços com parceiros
- Utilizando o SLA como elemento da segurança
- Novas Tecnologias! Velhos riscos!

5.7 PROCESSOS DE APOIO A SEGURANÇA DA INFORMAÇÃO(5h)

- Flexibilidade operacional para a segurança
- Identifique a raiz do problema!

5.8 CONTINUIDADE DO NEGÓCIO (5h)

- Contingência, crise, desastre, emergência ou descontinuidade do negócio?
- Avaliando o nível de proteção para situações de desastres
- Não dê sorte ao azar!
- A maturidade na continuidade do negócio
- Nossas torres de cada dia
- A necessidade de não parar
- Seu plano de continuidade é pra valer?
- Para entender, analisar e gerenciar os riscos!
- Para Elaborar um plano de continuidade de negócio.
- Para enfrentar crises e outras situações de emergências!
- Indisponibilidade: a ameaça de parar o negócio!
- Diretrizes para testes – continuidade de negócio

5.2 -SEGUNDA ETAPA

5.2.1 CONTEÚDOS PRESENCIAIS (15 Aulas)

5.2.1.1 PCN (10h)

- Processo de Gerenciamento da Continuidade dos Serviços de TI
- Gerenciamento de Riscos
- Estratégia de CONTINUIDADE
- Formação da Equipe
- Análise da Capacidade com as diversas área da organização

- Análise das Vulnerabilidades
- Análise de Impacto
- Potencial Impacto no Negócio
- Medir recursos Internos e Externos
- Elaboração de um PCN
- Estrutura de um PCN

5.2.1.2 AUDITORIA DE SISTEMAS (5h)

- Objetivos da Auditoria
- Importância da Auditoria e suas fases
- Planejamento da Auditoria
- Auditoria Interna vs auditoria externa

5.2.1.3 PBL (5h)

6. METODOLOGIA DO TRABALHO:

6.1 **- 1ª Etapa:**

6.1.1 – Metodologias Ativas Presenciais

A proposta de aulas revisionais debatidas será resultado da sala de aula invertida para prover aulas menos expositivas, mais produtivas e participativas, capazes de engajar os alunos no conteúdo e melhor utilizar o tempo e conhecimento do professor. Sendo assim, será proposto para os alunos, por meio de pesquisas e/ou leituras extraclasse, o estudante terá acesso prévio do conteúdo curricular de Sistemas de Informação e estudar antes de ir para a sala de aula, ocasião em que discutirá com colegas e professor os assuntos já vistos em casa. Além disso, serão utilizadas aulas discursivas.

Conforme as diretrizes a seguir:

- Seminário – 6,0 (seis) pontos

Conforme as seguintes diretrizes:

- A equipe irá entregar o Plano, sobre o tema proposto, antes de iniciar o Seminário contemplando a didática da aula fundamenta por meio de Pesquisa Bibliográfica (50 min).
- Serão analisados:

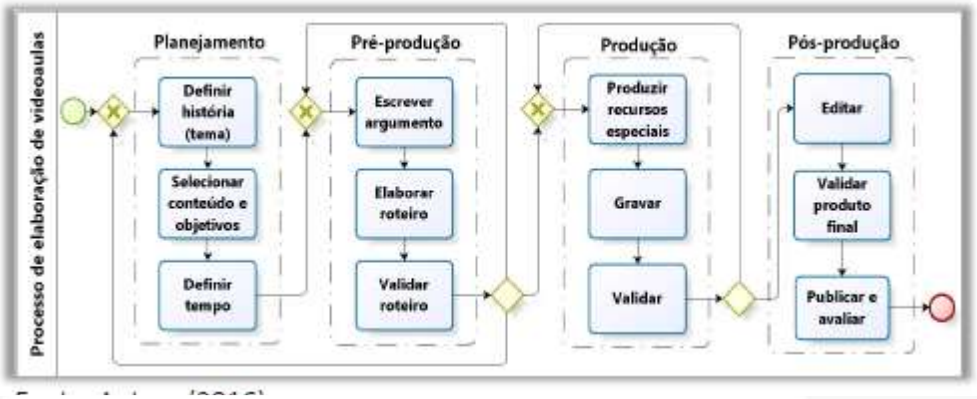
Descrição		Valor	
Desempenho individual	Participação interativa nos demais Seminários;	**0,5**	**2,5 pt**
	Clareza/Coerência na fundamentação teórica e prática;	**1,0**	

	Perfil na apresentação individual (Vestir/Vocabulário)].	**1,0**	
Desempenho em Grupo	1 - Pontualidade	0,5	**3,5 pt**
	2 - Integração da Equipe	0,5	
	3 - Fundamentação Teórica em Power Point	0,5	
	4 - Estética / Organização da Gestão de sala	0,5	
	5 - Recursos Pedagógicos – Música / Vídeo Didático até 5 min / Sinopse de um Filme	0,5	
	6 - Interação do conhecimento da equipe com a turma	1,0	

- Ao término do Seminário, há uma análise verbal com a participação de uma equipe e, logo após, o professor intervirá nos aspectos desenvolvidos como pontos frágeis, em processo e os construídos, como também, potencializar o cognitivo em virtude de alguma lacuna no desenvolvimento da fundamentação teórica e prática. Na oportunidade, será aplicado um instrumento escrito de Análise Avaliativa envolvendo todas as equipes participantes, autoavaliação da equipe que realizou e a avaliação do professor, compreendendo um olhar mais preciso de todo o processo didático.

- Abaixo seguem os temas que serão sorteados no primeiro dia de aula, baseado no Livro Segurança de Computadores e Teste de Invasão (BASTA, 2014)
  Tema 1: Ética de hacker e cracker (Capítulo 1)
  Tema 2: Reconhecimento (Capítulo 2)
  Tema 3: Ferramentas de escaneamento (Capítulo 3)
  Tema 4: Farejadores (Capítulo 4)
  Tema 5: Vulnerabilidades do TCP/IP (Capítulo 5)
  Tema 6: Criptografia e craqueamento de senhas (Capítulo 6)

2ª Experimentos / Vídeos Educativo: Os temas serão sorteados em sala de aula. A construção deverá seguir o modelo de processo de Elaboração de vídeo Aulas abaixo:



- Os mesmos serão avaliados da seguinte maneira:

Descrição	Valor
Clareza/Coerência referente ao Tema	**1,0**
Conteúdo e objetivos	**1,0**
Tempo (3 a 5 minutos)	**0,5**
Roteiro	**1,0**
Integração da Equipe	**0,5**

Tema 1: Como esconder seu IP / Proxy Local com A4Proxy (Capítulo 3 e 4)
Tema 2: Scanners de Rede / híbridos / Vulnerabilidade (Capítulo 7, 8 e 9)
Tema 3: Pesquisando regras de Firewall / Mapeando a rede (Capítulo 10 e 11)
Tema 4: Força Bruta (Windows / Linux) – (Capítulo 13 e 14)
Tema 5: Quebrando Senha (Windows / Linux) – (Capítulo 19 e 20)
Tema 6: Injeção de SQL / Farejando redes (Capítulo 21 e 22)

Obs.: Material do Experimento será disponível no portal Acadêmico.

6.2 **- 2ª Etapa:**

6.1.1 – Metodologias Ativas Presenciais

A proposta de aulas revisionais debatidas será resultado da sala de aula invertida para prover aulas menos expositivas, mais produtivas e participativas, capazes de engajar os alunos no conteúdo e melhor utilizar o tempo e conhecimento do professor. Sendo assim, será proposto para os alunos, por meio de pesquisas e/ou leituras extraclasse, o estudante terá acesso prévio do conteúdo curricular de Sistemas de Informação e estudar antes de ir para a sala de aula, ocasião em que discutirá com colegas e professor os assuntos já vistos em casa. Além disso, serão utilizadas aulas discursivas.

Projeto - Plano de Continuidade de Negócios aplicado a Segurança da Informação – PCN.

Fases	Descrição		Valor
Fase 1	**Escopo do projeto**	**15/10**	**1,0**
Fase 2	**Análise do Impacto**	**22/10**	**1,0**
Fase 3	**Avaliação dos Riscos**	**29/10**	**1,0**
Fase 4	**Plano de Gerenciamento de Crise**	**05/11**	**1,0**
	Plano de Recuperação		**1,0**
Fase 5	**Relatório de Gestão**	**19/11**	**1,0**
	Conclusão		**1,0**
	Apresentação / Impressão		**3,0**

Obs: As equipes deverão desenvolver o PCN em um ambiente real.

8. SISTEMA DE AVALIAÇÃO:

1ª Etapa

a) **Avaliação Processual (20,0) pontos**

1. **Construção de 1(um) Seminário Temático Interativo,** em grupo, no valor de 6,0 (seis) pontos
2. **Experimento / Construção de Vídeo** no valor de 4 (quatro) pontos;

b) **Avaliação Institucional (Modelo ENADE) (10,0) pontos**

3. **Avaliação Institucional Escrita, contemplando 4(quatro) questões dissertativas e 2(duas) questões objetivas, individual, no valor de 10,0 (dez) pontos**.

2ª Etapa:

a) Avaliação Processual

1. **Plano de Continuidade de Negócios aplicado a Segurança da Informação – PCN,** em Grupo, no valor de 10,0 (dez) pontos

b) Avaliação Institucional (Modelo ENADE) (10,0) pontos

Avaliação Institucional Escrita, contemplando 4(quatro) questões dissertativas e 2(duas) questões objetivas, individual, no valor de 10,0 (dez) pontos.

Obs.: detalhes das atividades no item 10. Cronograma de Atividades

FREQUÊNCIA

O aluno deverá ter frequência exigida às aulas e demais atividades de 75% na disciplina. Sua margem de ausência em hipótese alguma deverá ultrapassar os 25%.

9. ATENDIMENTO EXTRA CLASSE:

Em caráter complementar, o professor oferece atendimento, diariamente, através do endereço eletrônico: ronierison.maciel@gmail.com

10. BIBLIOGRAFIA BÁSICA:

ARIMA, Carlos Hideo; SCHMIDT, Paulo; SANTOS, José Luiz dos. **Fundamentos de Auditoria de Sistemas.** v. 9. São Paulo: Atlas, 2006.

IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informações**. São Paulo: Atlas, 2008.

SCHMITZ, Eber Assis; ALENCAR, Antonio Juarez. **Análise de Risco em Gerência de Projetos.** Rio de Janeiro: Brasport, 2006.

11. BIBLIOGRAFIA COMPLEMENTAR:

BADDINI, Francisco. Gerenciamento de redes com o Windows XP. Érica

CARMONA, Tadeu. **Universidade Linux**. Digerati Books.

VIGLIAZZI, Douglas. **Redes Locais com Linux**. Visual Books.

PAINE, Stephen; BURNETT, Steven. **Criptografia e Segurança**: o Guia Oficial RSA. Campus.

SÁ, Josué de. **Dominando Servidores Windows Server 2003**. Alta Books.

THOMPSON, Marco Aurélio. **Proteção e segurança na internet.** São Paulo: Érica, 2002.

WHITTAKER, James A. **How to break software.** EUA: Pearson.

BASTA, Alfred. **Segurança de Computadores e teste de invasão.** São Paulo: Cengage Learning, 2014.

12. CRONOGRAMA DE ATIVIDADES:

Cronograma das atividades será estabelecido conforme andamento da aplicação das metodologias ativas às turmas alvo.

13. INFORMAÇÕES COMPLEMENTARES:

14. APROVAÇÃO:

Aprovado em _____/_____/_____ **homologado em ____/____/_____**

COORDENADOR **GERÊNCIA ACADÊMICA**

OBS: As datas das avaliações poderão sofrer alterações de acordo com o disciplinado pela secretaria acadêmica da UniRios.