PLANO DE CURSO

1. DADOS DE IDENTIFICAÇÃO			
Curso: Bacharelado em Sistemas de Informação			
Disciplina: Auditora e Segurança da Informação		**Código:** SIF38	
Professor: MSc. Igor Peterson Oliveira Santos		**e-mail:** igor.santos@fasete.edu.br	
CH Teórica: 40h **CH**	**Prática:** 20h	**CH Total:** 40h	**Créditos: 04**
Pré-requisito(s): -			
Período: VII		**Ano:** 2019.1	

2. EMENTA:

Segurança em Informática. Auditoria. Plano Diretor de Informática. Gestão de Recursos Tecnológicos.

3. OBJETIVO GERAL DA DISCIPLINA:

Desenvolver no aluno o senso crítico referente aos aspectos relacionados à segurança da informação, capacitando-o para identificar os pontos vulneráveis em um sistema de informação.

4. OBJETIVO(S) ESPECÍFICOS(S) DA DISCIPLINA:

- ✓ Desenvolver no aluno a compreender o papel do software, rede e usuário para a garantia da segurança da informação;
- ✓ Desenvolver a habilidade para a confecção e implantação de um plano de segurança da informação.
- ✓ Apresentar os principais conceitos da criptografia e o seu papel para a segurança da informação;
- ✓ Capacitar o aluno a realizar uma análise de segurança de um sistema;
- ✓ Introduzir as normas e padrões de segurança da informação.

5. CONTEÚDO PROGRAMÁTICO:

1ª ETAPA

5.1 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

5.1.1 Considerações para o Executivo da Organização
5.1.2 pela Existência da Política de Segurança da Informação
5.1.3 A Segurança necessita de Planejamento
5.1.4 Planejamento estratégico da segurança da informação.
5.1.5 Segurança alinha ao negócio!
5.1.6 A organização que aprende

5.1.7 ROI, meta-ROI e despesa
5.1.8 Uma política divina
5.1.9 Arquitetura corporativa
5.1.10 Arquitetura de segurança da informação

5.2 PARCEIROS

5.2.1 Parceiros
5.2.2 Serviços com parceiros
5.2.3 Utilizando o SLA como elemento da segurança
5.2.4 Novas Tecnologias! Velhos riscos!

5.3 PROCESSOS DE APOIO A SEGURANÇA DA INFORMAÇÃO

5.3.1 Flexibilidade operacional para a segurança
5.3.2 Identifique a raiz do problema!

5.4 CONTINUIDADE DO NEGÓCIO

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

2ª ETAPA

5.5 PCN

5.5.1 Processo de Gerenciamento da Continuidade dos Serviços de TI
5.5.2 Gerenciamento de Riscos
5.5.3 Estratégia de CONTINUIDADE
5.5.4 Formação da Equipe
5.5.5 Análise da Capacidade com as diversas área da organização
5.5.6 Análise das Vulnerabilidades
5.5.7 Análise de Impacto
5.5.8 Potencial Impacto no Negócio
5.5.9 Medir recursos Internos e Externos
5.5.10 Elaboração de um PCN
5.5.11 Estrutura de um PCN

5.6 AUDITORIA DE SISTEMAS

5.6.1 Objetivos da Auditoria
5.6.2 Importância da Auditoria e suas fases
5.6.3 Planejamento da Auditoria
5.6.4 Auditoria Interna vs auditoria externa

6. METODOLOGIA DO TRABALHO:

A disciplina será trabalhada a partir de aulas expositivas e participativas, debates, estudo dirigido, artigos complementares, discussões, Aprendizagem baseada em projetos, avaliação formal e informal.

7. SISTEMA DE AVALIAÇÃO:

AVALIAÇÃO:

1ª ETAPA

a) **Construção de 1(um) Seminário Temático Interativo,** em grupo, no valor de 6,0 (seis) pontos
b) **Experimento / Construção de Vídeo** no valor de 4 (quatro) pontos;
c) **Avaliação Institucional Escrita, contemplando 4(quatro) questões dissertativas e 2(duas) questões objetivas, individual, no valor de 10,0 (dez) pontos**.

2ª Etapa:

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

8. ATENDIMENTO EXTRA CLASSE:

Diariamente, através do endereço eletrônico: igor.santos@fasete.edu.br
Semanalmente, mediante pré-agendamento.

9. BIBLIOGRAFIA BÁSICA:

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

IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informações**. 2ª ed. São Paulo: Atlas, 2008.

SCHMITZ, Eber Assis; ALENCAR, Antonio Juarez. **Análise de Risco em Gerência de Projetos.** Rio de Janeiro: Brasport, 2005.

10. BIBLIOGRAFIA COMPLEMENTAR:

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

Atlas, 2006.

FUNDAMENTOS de segurança da informação: com base na ISO 27001 e na ISSO 27002. Rio de Janeiro: Brasport, 2010.

IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informações**. 2ª ed. São Paulo: Atlas, 2008.

SCHMITZ, Eber Assis; ALENCAR, Antonio Juarez. **Análise de Risco em Gerência de Projetos.** Rio de Janeiro: Brasport, 2005.

WHITTAKER, James A. **How to break software: practical guide to testing.** EUA: Pearson, 2002.

Rua Vereador José Moreira, 1000 - Bairro Prefeito Sérgio Guim
Paulo Afonso / BA - CEP 48.603-004
75 3501.0777 fasete.edu.br atendimento@fasete.edu.br

10. CRONOGRAMA DE ATIVIDADES:

1ª Etapa

1ª Atividade – Seminário – 6,0 (seis) pontos - (24/03) Tarde

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**

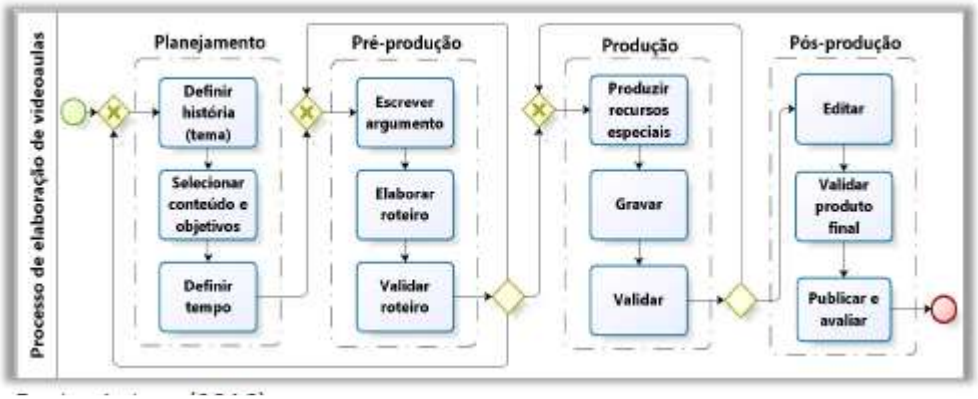
	Clareza/Coerência na fundamentação teórica e prática;	**1,0**	
	Perfil na apresentação individual (Vestir/Vocabulário)].	**1,0**	
Desempenho em Grupo	1 - Pontualidade	0,5	**3,5 pt**
	2 - Integração da Equipe	0,5	
	3 - Fundamentação Teórica em Power Point	0,5	
	4 - Estética / Organização da Gestão de 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 raqueamento e craqueamento (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:
Datas: 22/03 e 29/03



- 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.

2ª Etapa

1ª – Projeto - Plano de Continuidade de Negócios aplicado a Segurança da Informação – PCN.

Fases	Descrição		Valor
Fase 1	**Escopo do projeto**	**19/04**	**1,0**
Fase 2	**Análise do Impacto**	**26/04**	**1,0**
Fase 3	**Avaliação dos Riscos**	**03/05**	**1,0**
Fase 4	**Plano de Gerenciamento de Crise**	**10/05**	**1,0**
	Plano de Recuperação	**17/05**	**1,0**
Fase 5	**Relatório de Gestão**	**17/05**	**1,0**

	Conclusão	**24/05**	**1,0**
		Apresentação / Impressão	**3,0**

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

11. INFORMAÇÕES COMPLEMENTARES:

Serão acrescidas 08 horas aulas para complementação de carga horária e estas serão utilizadas para o desenvolvimento de atividades extraclasse com os discentes.

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