UNIVERSIDADE FEDERAL DO ACRE
PRÓ-REITORIA DE GRADUAÇÃO

PLANO DE CURSO

Centro Centro de Ciências Exatas e Tecnológicas		
Curso Bacharelado em Sistemas de Informação		
Disciplina: CCET 189 – Segurança e Auditoria em sistemas de informação		**Créditos: 4-0-0**
Pré-requisitos:	**Co-requisitos:**	
Carga Horária: 60 horas	**CH de Acex:**	**Encontros: 72**
Semestre Letivo/Ano: 02 / 2023		
Professor(a): Wilker Luiz Gadelha Maia (Mestre)		

I- Ementa:
Auditoria de sistemas de informação. Ambiente de auditoria. A pirâmide de tecnologia de auditagem. Posicionamento na organização. Descrição das fases. Análise e desenvolvimento do processo. Segurança física e lógica da informação. Qualidade de Software. Infraestrutura. Normas para certificação de processos de desenvolvimento. Normas parar certificação de processos de desenvolvimento. Normas para certificação de produtos de software.

II- Objetivos de Ensino

1- Objetivos Gerais
O objetivo deste curso é dispor sobre os temas de segurança da informação sob as abrangências de infraestruturas em redes e sistemas de informação, identificar normas, padrões e rotinas para as melhores práticas para gestão em segurança da informação.

2- Objetivos Específicos

a) Discutir Sistemas de Informação, suas formas, classificações e abrangências sob a visão de segurança;

b) Apresentar normas e padrões norteadores para proceder autorias em SI e segurança da informação;

c) Identificar, definir infraestruturas de redes, equipamentos, sistemas operacionais e aplicativos sob a ótica da segurança da informação;

d) Utilização de sistemas de apoio a auditorias em SI;

e) Aspectos da segurança da informação em redes de computadores para monitoramento, caracterização de tráfego;
f) Aspectos de conectividade e convergências de tecnologias sob a visão de segurança;
g) Observar legislações específicas para as áreas da segurança da informação;

h) Abordagem de novas tecnologias.

III- Conteúdos de Ensino

Unidades Temáticas	C/H
Unidade 1 – Apresentação da disciplina; Conceitos e fundamentos Dado, informação, conhecimento; Classificação da Informação (Interna; externa; pública; confidencial); Sistemas de informação; conceitos sobre segurança e auditoria	04
Unidade 2 – Segurança da Informação Confidencialidade; integridade; disponibilidade. Ativos; Vulnerabilidades; Ameaças; Firewall e Gateway	04

Unidade 3 – SGSI (Sistemas de gestão para segurança da informação) Metodologias; composição; Documentos PETI (Plano estratégico em TI); PDTI (Plano Diretor de TI); PCA (Plano de controle de acesso)	08
Unidade 4 – PSI – Política de Segurança da Informação Fundamentos; Conceito; composição; construção; Aplicação; normas; Modelos e padrões	08
Unidade 5 – Firewall pfSense e OPNSense Características; projeto; Fundamentos, Instalação, configuração inicial; Topologias para segurança ; equipamentos; Configurações em laboratório (Regras de firewall, VPN, NAT, Gateway, interfaces ...)	10
Unidade 6 – - Auditoria em SI Introdução, histórico; Tipos; Equipes, perfil de profissionais; Atuação práticas; Ferramentas de auditoria assistida por computador; Noções sobre COBIT e ITIL	10
Unidade 7 - Gestão de riscos Normas e padrões e Conformidades Legais Família normas ISO/IEC 27.000 (27.001, 27.002, 27.003, 27.005) Norma ISO 31.000 e 31.010 (Gestão de riscos)	08
Unidade 8 - Criptografia Histórico; Fundamentos e conceitos; Simétricas; Assimétricas; Algoritmos; Certificado e assinatura digital; ICP BR; PKI (Infraestrutura de chaves) GnuPG – fundamentos e práticas	08

IV- Metodologia de Ensino

A metodologia para esta disciplina está relacionada a proceder maior motivação e participação do aluno, utilizando aulas expositivas, aulas práticas em laboratório, debates em sala de aula, trabalhos em sala e extra sala (na forma individual e em grupo), interpretação de artigos e textos diversos, exercícios, provas e seminários..

V- Recursos Didáticos

Computador; projetor multimídia; slides, quadro branco e laboratório. Simulador para ambiente de redes Cisco PacketTracer; uso de máquinas virtuais em Linux no VirtualBox; pfSense; OPNSense

VI- Avaliação da Aprendizagem

Cada avaliação Bimestral (N1 e N2) será composta da seguinte maneira:1 – Prova escrita: Valor 7,0 pontos; 2 – Atividade Prática (Listas de exercícios, algoritmos, programas e Laboratórios): Valor 3,0 pontos;.

VII- Bibliografia

1- Bibliografia Básica

- TANENBAUM, Andrew S. J. Wetherall, David; Redes de Computadores - 4ª Ed. Rio de Janeiro: Elsevier - 2003
- KUROSE, J. F., ROSS, K. W. Redes de Computadores e a Internet, 5a Ed., Editora Addison-Wesley, 2010.
- FOROUZAN, Behrouz A. Comunicação de Dados e Redes de Computadores. 4ª. Ed., McGraw-Hill, São Paulo, 2008.
- COMER, Douglas E. Redes de computadores e internet. 4ª. Ed., Porto Alegre. Editora Bookman, 2007.
- COMER, Douglas E. Interligação em redes com TCP/IP. Ed. Campus. Rio de Janeiro, 1998.
- CARISSIMI, Alexandre da Silva. Et alii. Redes de computadores. Porto Alegre. Editora Bookman, 2009.

2- Bibliografia Complementar

CAMPOS, André. **Sistema de Segurança da informação: Controlando os Riscos**. 2 ed. Florianópolis, SC. Visual Books, 2007.

Periódicos da Capes:	**- http://www.periodicos.capes.gov.br/**
. Google Acadêmico:	**- https://scholar.google.com.br/**
. Kali Linux	**- https://www.kali.org/**
. Debian Linux	**- https://www.debian.org/index.pt.html**
. Kernel Linux	**- https://www.kernel.org/**
. GRSecurity	**- https://grsecurity.net/**
. SANS	**- https://www.sans.org/**
. CERTbr	**- https://www.cert.br/**
. GnuPG	**- https://www.gnupg.org/**
. Firewall pfSense	**- https://www.pfsense.org/**

3- Bibliografia Sugerida

- SAUVE, Jacques Phillipe, LOPES, Raquel V., NICOLLETTI, Pedro S. **Melhores Práticas para Gerência de Redes de Computadores, 3a ed. Ed. Campus, 2003. SP.**
- SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visao executive da Segurança da Informação. Aplicada ao Security Officer**. Rio de Janeiro-RJ, Elsevier, 2003.
- IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informação**. 3ª. Ed. 2016. Editora Atlas, São Paulo-SP.
- BRAZ, Márcio Rodrigo. **Auditoria de TI: O Guia de Sobrevivência**. 1ª. Ed. Editora Márcio Braz. Brasília-DF.

VIII- Cronograma da Disciplina

Período de realização: 10/10/2023 a 12/03/2024
Dia e Horário de Execução: segunda-feira, 09:20 às 11:00 e quarta-feira, das 07:30 às 09:10

Unidades Temáticas	Início	Término
Unidade 1: Apresentação da disciplina; Conceitos e fundamentos	09/10/2023	11/10/2023
Unidade 2**:** Segurança da Informação	16/10/2023	18/10/2023
Unidade 3: SGSI (Sistemas de gestão para segurança da informação)	23/10/2023	01/11/2023
Unidade 4: PSI – Política de Segurança da Informação	06/11/2023	20/11/2023
Unidade 5: Firewall pfSense e OPNSense	22/11/2023	20/12/2023
Unidade 6: Auditoria em SI	17/01/2024	05/02/2024
Unidade 7: Gestão de riscos	07/02/2024	19/02/2024
Unidade 8: Criptografia	21/02/2024	04/03/2024

Avaliação da aprendizagem	Data de Realização
Avaliação1-N1 – conteúdos das unidades 01 e 02	18/10/2023.
Avaliação2-N1 – conteúdos das unidades 03 e 04	20/11/2023
Avaliação1-N2 – conteúdos da unidade 05 e 06	05/02/2024
Avaliação2-N2 – conteúdos da unidade 07 e 08	06/03/2024
Realização da Prova Final	13/03/2024

Aprovação do Colegiado de Curso (Regimento Geral da UFAC, Artigo 70, incisos II).

Plano de Curso elaborado nos termos do §2º, Art. 243 do Regimento Geral da Ufac, apreciado e homologado pelo Colegiado do Curso de Bacharelado em Engenharia Civil, em reunião realizada em :

…..... de .....……..... de 2023 , conforme estabelecido no Regimento da Ufac, Art. 70, II.

Rio Branco-Acre, 16 de outubro de 2023.

Wilker Luiz Gadelha Maia.
Professor.