Unidade de Ensino Médio e Técnico - CETEC

Plano de Trabalho Docente - 2019

Ensino Técnico

Plano de Curso no. 160 aprovado pela Portaria Cetec – 738, de 10-09-2015, publicada no Diário Oficial de 11-09-2015 – Poder Executivo – Seção I – página 53.			
ETEC:	Escola Técnica Estadual Rodrigues de Abreu		
Código:	135	Município:	Bauru
Eixo Tecnológico	Informação e Comunicação		
Habilitação Profissional:	Habilitação Profissional de Técnico em Informática		
Qualificação:	Habilitação Profissional Técnica de Nível Médio de TÉCNICO EM INFORMÁTICA		
Componente Curricular:	Segurança Digital		
Módulo:	3	C. H. Semanal:	2,00
Professor:	DANIEL TOETZ DUARTE ;		

I – Atribuições e atividades profissionais relativas à qualificação ou à habilitação profissional, que justificam o desenvolvimento das competências previstas nesse componente curricular.

* Aplicar critérios de navegação em sistemas e aplicações.
* Definir critérios de navegação.
* Definir padronizações de sistemas, aplicações e segurança.
* Estabelecer conexões entre os equipamentos de forma a garantir a segurança, confiabilidade e disponibilidade.
* Implementar rotinas de segurança.

Agir de forma a minimizar os riscos inerentes à segurança de informações, relacionando e aplicando soluções adequadas; Estabelecer conexões entre os equipamentos de forma a garantir a segurança, confiabilidade e disponibilidade

II – Competências, Habilidades e Bases Tecnológicas do Componente Curricular

Competências

1. Propor e aplicar soluções visando à proteção das informações de determinadas empresas ou pessoas, garantindo confidencialidade, integridade e disponibilidade.

Habilidades

1. Identificar as principais vulnerabilidades, falhas de segurança e portas de entrada para códigos maliciosos e/ ou pessoas mal intencionadas, protegendo as informações de sistemas computacionais.

Bases Tecnológicas

1. Conceitos de Segurança Digital
2. Características de informação segura: confidencialidade, integridade e disponibilidade (CIA – Confidentiality, Integrity and Availability)
3. Certificações de segurança:
3.1 órgãos reguladores nacionais e internacionais:
3.1.1 CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil;
3.1.2 CSIRT – Computer Security Incident Response Team (Equipe de Resposta a Tratamento de Incidentes de Segurança)
3.2 certificado digital;
3.3 assinatura digital
4. Cartilha de Segurança para Internet
5. Mecanismos de Segurança e seus níveis: controles físicos e lógicos
6. Políticas de Segurança
7. Técnicas para identificar vulnerabilidades:
7.1 footprint: descoberta de informações
7.2 varredura/ análise;
7.3 enumeração: testes de penetração e testes de vulnerabilidades
7.4 engenharia social;
7.5 negação de serviço (DoS e DDoS);
7.6 injections SQL
8. Criptografia
9. Firewall
10. Segurança de Redes
11. Segurança em Dispositivos Móveis

Aplicar conceitos de Ética e Cidadania Organizacional neste componente

III – Procedimento Didático e Cronograma de Desenvolvimento

Habilidades	Bases Tecnológicas	Procedimentos Didáticos	De	Até
1. Identificar as principais vulnerabilidades, falhas de segurança e portas de entrada para códigos maliciosos e/ ou pessoas mal intencionadas, protegendo as informações de sistemas computacionais.;	1. Conceitos de Segurança Digital; 2. Características de informação segura: confidencialidade, integridade e disponibilidade (CIA – Confidentiality, Integrity and Availability); 3. Certificações de segurança: ;	aula expositiva dialogada com aplicação pratica em computado utilizando aplicativo refente a SD	04/02/19	18/02/19
1. Identificar as principais vulnerabilidades, falhas de segurança e portas de entrada para	3. Certificações de segurança: ; 3.1 órgãos reguladores nacionais e internacionais:; 3.1.1 CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil;; 3.1.2 CSIRT –	aula expositiva dialogada utilizando apostilas e videos refente a SD	18/02/19	11/03/19

códigos maliciosos e/ ou pessoas mal intencionadas, protegendo as informações de sistemas computacionais.;	Computer Security Incident Response Team (Equipe de Resposta a Tratamento de Incidentes de Segurança); 3.2 certificado digital;; 3.3 assinatura digital; 4. Cartilha de Segurança para Internet;			
1. Identificar as principais vulnerabilidades, falhas de segurança e portas de entrada para códigos maliciosos e/ ou pessoas mal intencionadas, protegendo as informações de sistemas computacionais.;	4. Cartilha de Segurança para Internet; 5. Mecanismos de Segurança e seus níveis: controles físicos e lógicos; 6. Políticas de Segurança;	aula com aplicação pratica em computado utilizando aplicativo refente a SD	18/03/19	01/04/19
1. Identificar as principais vulnerabilidades, falhas de segurança e portas de entrada para códigos maliciosos e/ ou pessoas mal intencionadas, protegendo as informações de sistemas computacionais.;	7. Técnicas para identificar vulnerabilidades:; 7.1 footprint: descoberta de informações; 7.2 varredura/ análise;; 7.3 enumeração: testes de penetração e testes de vulnerabilidades; 7.4 engenharia social;; 7.5 negação de serviço (DoS e DDoS);; 7.6 injections SQL;	aula expositiva dialogada com aplicação pratica em computado utilizando aplicativo e lista de exercícios refente SD	08/04/19	22/04/19
1. Identificar as principais vulnerabilidades, falhas de segurança e portas de entrada para códigos maliciosos e/ ou pessoas mal intencionadas, protegendo as informações de sistemas computacionais.;	7. Técnicas para identificar vulnerabilidades:; 8. Criptografia;	aula expositiva com aplicação pratica em computado utilizando aplicativo de segurança e lista de exercícios refente SD	29/04/19	13/05/19
1. Identificar as principais vulnerabilidades, falhas de segurança e portas de entrada para códigos maliciosos e/ ou pessoas mal intencionadas, protegendo as informações de sistemas computacionais.;	7. Técnicas para identificar vulnerabilidades:; 8. Criptografia; 9. Firewall;	aula aplicação pratica em computado utilizando aplicativo refente SD	20/05/19	03/06/19
1. Identificar as principais vulnerabilidades, falhas de segurança e portas de entrada para códigos maliciosos e/ ou pessoas mal intencionadas, protegendo as informações de sistemas computacionais.;	7. Técnicas para identificar vulnerabilidades:; 8. Criptografia; 9. Firewall; 10. Segurança de Redes;	aula expositiva dialogada e lista de exercícios refente SD	10/06/19	24/06/19
1. Identificar as principais vulnerabilidades, falhas de segurança e portas de entrada para códigos maliciosos e/ ou pessoas mal intencionadas, protegendo as informações de sistemas computacionais.;	7. Técnicas para identificar vulnerabilidades:; 10. Segurança de Redes; 11. Segurança em Dispositivos Móveis; Aplicar conceitos de Ética e Cidadania Organizacional neste componente;	aula expositiva dialogada lista de exercícios refente SD	24/06/19	03/07/19

IV - Plano de Avaliação de Competências

Competências	Instrumento(s) e Procedimentos de Avaliação	Critérios de Desempenho	Evidências de Desempenho
1. Propor e aplicar soluções visando à proteção das informações de determinadas empresas ou pessoas, garantindo confidencialidade, integridade e disponibilidade.	Lista de Exercícios ; Recuperação ; Participação em Aula ; Avaliação Prática ;	Argumentação Consistente ; Atendimento às Normas ; Criatividade na Resolução de Problemas ; Cumprimento das Tarefas Individuais ; Interatividade, Cooperação e Colaboração ; Organização ; Execução do Produto ; Relacionamento de Ideias ;	Identificar as principais vulnerabilidades, falhas de segurança e portas de entrada para códigos maliciosos e/ ou pessoas mal intencionadas, protegendo as informações de sistemas computacionais.

V – Plano de atividades docentes

Atividade Previstas	Projetos e Ações voltados à redução da Evasão Escolar	Atendimento a alunos por meio de ações e/ou projetos voltados à superação de defasagens de aprendizado ou em processo de Progressão Parcial	Preparo e correção de avaliações	Preparo de material didático	Participação em reuniões com Coordenador de Curso e/ou previstas em Calendário Escolar
Fevereiro	semana de integração dos alunos."palestra jogos e atividades interclasses "	observar a dificuldade de aprendizagem dos alunos, avaliação diagnostica	organização e correção das atividades projetos e avaliações desenvolvidas nas aulas	oferecer atividades praticas como interpretação dos prefiz dos colaboradores e materialístico para apoio na execução	4/2 inicio semestre/ano letivo; 01 e 20/02 reunião equipe gestora; 13/02 reunião apm; 27/02 reunião de conselho escolar.
Março	interação com os alunos sobre a importância do curso, quais oportunidades oferece no mercado de trabalho.		organização e correção das atividades projetos e avaliações desenvolvidas nas aulas	relatórios com perguntas para pesquisa na internet.sendo enviado por email	1/03 dia da escola-família; 6/03 reunião de cursos, entrega de PTD e publicação da portaria; 16/03 reunião pedagógica; 13-27/03 reunião de equipe; 20/03 reunião direção-discentes.
Abril	atividade em grupo que demonstre as dificuldades	atividades com revisão do conteúdo para observação de	organização e correção das atividades projetos	evidencias os resultados dos relatórios	10e 24/04 reunião de equipe gestora; 15/04 entrega de menções;18 e 22/04 CCI e divulgação; 22 a 26/04 período de reconsiderações;24/04

	de aprendizagem	dificuldades de aprendizagem	e avaliações desenvolvidas nas aulas	para evolução de conteúdo e avaliação	profissional de finanças;29/profissional seg.trabalho.
Maio	apresentação de estímulos aos alunos com atividades diversificadas e aberto a comunidade escolar		organização e correção das atividades projetos e avaliações desenvolvidas nas aulas	atualização de material teórico e de apoio pratico	3/05 final da FIADE;4/05 reunião curso e pais; 6a 10/05 sem.paulo freire; 13/05 profissional de enfermagem; 08 e 22/05 reunião de equipe gestora; 25/05 reunião pedagógica.
Junho	atividades integrando a comunidade, dando destaque a importância da conclusão do curso técnico junto com os alunos formados.	atividades com revisão do conteúdo para observação de dificuldades de aprendizagem	organização e correção das atividades projetos e avaliações desenvolvidas nas aulas	utilização de mídias áudio visuais juntamente com material de apoio	3/06 conselho escolar; 07/06 profissional de logística;14/06 atividade cultural; 24/06a3/07 re matricula.
Julho	finalização do ciclo motivando o aluno citando as disciplinas do próximo ciclo e sua importância		organização e correção das atividades projetos e avaliações desenvolvidas nas aulas	organização e correção das atividades projetos e avaliações desenvolvidas nas aulas	3 e 24/07 reunião de equipe; 01/07 entrega de menções; 4/07 conselho.

VI – Material de Apoio Didático para Aluno (inclusive bibliografia)

- Apostila de exercícios propostos pelo professor. - Microcomputadores; Projetor Multimídia. - Internet – Sites especializados www.cartilha.cert.br/ www.cgi.br

• Material Didático Centro Paula Souza – Livro 2

Apostila confeccionada pelo professor

Apostilas de domínio publico

Bibliografia de apoio: - TANEMBAUM, Andrew S. – Redes de Computadores, Editora Campus. - MORIMOTO, Carlos E. – Redes, Guia Prática, GDH Press e Sul Editores Quadro Branco Internet. Vídeos Aulas Apostila elaborada pelo Professor.

BRASIL: Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 Segurança da Informação em Servidores. Rio de Janeiro, ABNT, 2005.

Cartilha de Segurança para Internet, Golpes na Internet, Ataques na Internet, Códigos Maliciosos, Spam, Mecanismos de Segurança, Contas e Senhas, Privacidade e Criptografia. http://cartilha.cert.br/

Criptografia e Segurança de Redes - William Stallings - Pearson - SP, 2007

VII – Propostas de Integração e/ou Interdisciplinares e/ou Atividades Extra

Atividade Extra

Elaborar sistemas aplicando princípios e paradigmas de seguração de dados. Este programa deve conter dados cadastrais do produto e do cliente.

Propostas de Integração e/ou Interdisciplinares

juntamente com os professores de DS elaborar em grupos um PROGRAMA com temas definidos por livre escolha dos alunos em grupos utilizando ferramentas de BANCO DE DADOS

VIII – Estratégias de Recuperação Contínua (para alunos com baixo rendimento/dificuldades de aprendizagem)

A avaliação da aprendizagem será realizada de forma contínua, tendo como um de seus objetivos o diagnóstico da situação de aprendizagem de cada aluno, em relação à programação prevista. A avaliação envolverá a análise do conhecimento e das técnicas específicas adquiridas pelo aluno.

IX – Identificação:

Nome do Professor DANIEL TOETZ DUARTE ;

Assinatura **Data** 14/02/2019

X – Parecer do Coordenador de Curso:

O Plano de Trabalho Docente (PTD) está de acordo com a proposta do Plano de Curso.

Nome do Coordenador:

Assinatura: **Data:** 27/02/19

Data e ciência do Coordenador Pedagógico

XI - Replanejamento

Data	Descrição
14/02/2019	Na ocorrência de pontos facultativos, palestras eventuais e visitas técnicas, sera realizado o replanejamentos dos conteúdos e solicitado atividades diversas.

Imprimir