Etec Sylvio de Mattos Carvalho Matão

Centro Paula Souza 50 anos 1969 - 2019

SÃO PAULO GOVERNO DO ESTADO

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 SYLVIO DE MATTOS CARVALHO	
Código: **103**	Município: **MATÃO**
Eixo Tecnológico: **INFORMAÇÃO E COMUNICAÇÃO**	
Habilitação Profissional: **HABILITAÇÃO PROFISSIONAL DE TÉCNICO EM INFORMÁTICA**	
Qualificação: **HABILITAÇÃO PROFISSIONAL DE TÉCNICO EM INFORMÁTICA**	
Componente Curricular: **SEGURANÇA DIGITAL**	
Módulo: **3º MÓDULO - B**	C. H. Semanal: **2,5**
Professor: **LUIZ FERNANDO SABINO DE OLIVEIRA**	

I – Atribuições e atividades profissionais relativas à qualificação ou à habilitação profissional, que justificam o desenvolvimento das competências previstas nesse componente curricular.
➢ Selecionar componentes de hardware e ferramentas de software adequadas às necessidades apresentadas.
➢ Estabelecer conexões entre os equipamentos de forma a garantir a segurança, confiabilidade e disponibilidade.
➢ Operar os serviços e funções dos sistemas operacionais
➢ Instalar e configurar programas.
➢ Agir em conformidade com as leis e a ética pessoal e profissional.

Unidade de Ensino Médio e Técnico - Cetec

II – Competências, Habilidades e Bases Tecnológicas do Componente Curricular

Componente Curricular: **SEGURANÇA DIGITAL** Módulo: **3º MÓDULO**

Nº	Competências	Nº	Habilidades	Nº	Bases Tecnológicas
1.	Propor e aplicar soluções visando à proteção das informações de determinadas empresas ou pessoas, garantindo confidencialidade, integridade e disponibilidade.	1.1	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, ntegrity and Availability)
				3.	Certificações de segurança: Órgãos reguladores nacionais e internacionais:CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil;CSIRT – Computer Security IncidentResponse Team (Equipe de Resposta a Tratamento de Incidentes de Segurança)Certificado digital;Assinatura digital.
				4.	Cartilha de Segurança para Internet
				5.	Mecanismos de Segurança:Controles físicos e controles lógicos
				6.	Políticas de Segurança
				7.	Técnicas para identificar vulnerabilidades:Footprint: Descoberta de informações,Varredura/ análise;Enumeração:Testes de penetração e testes de vulnerabilidadesEngenharia social;Negação de serviço (DoS e DDoS);injections SQL
				8.	Criptografia
				9.	Firewall
				10.	Segurança de Redes
				11.	Segurança em Dispositivos Móveis

Unidade de Ensino Médio e Técnico - Cetec

III – Procedimento Didático e Cronograma de Desenvolvimento

Componente Curricular: **SEGURANÇA DIGITAL** Módulo: **3º MÓDULO**

Habilidades	Bases Tecnológicas	Procedimentos Didáticos	Cronograma / Dia e Mês
➢ 1.1 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	➢ Aula expositiva com projeção de slides	05/02 a 15/02
➢ 1.1 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.	➢ 2. Características de informação segura:Confidencialidade, integridade e disponibilidade (CIA – Confidentiality, ntegrity and Availability) ➢ 3. Certificações de segurança: Órgãos reguladores nacionais e internacionais:CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil;CSIRT – Computer Security IncidentResponse Team (Equipe de Resposta a Tratamento de Incidentes de Segurança)Certificado digital;Assinatura digital.	➢ Aula expositiva dialogada. Atividade prática: composição de infográfico sobre os orgãos reguladores brasileiros	18/02 a 01/03
➢ 1.1 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	➢ Exposição da cartilha de segurança para internet por projeção. Leitura de algumas porções. Aula prática por projeto elaboração de animações, vídeo ou slides sobre algumas seleções de temas da cartilha.	07/03 a 15/03
➢ 1.1 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	➢ Aula prática por projeto: Finalização de animações, vídeo ou slides sobre algumas seleções de temas da cartilha.	18/03 a 29/03
➢ 1.1 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.	➢ 5. Mecanismos de Segurança:Controles físicos e controles lógicos	➢ Aula expositiva com projeção de slides. Demonstrações por animações.	01/04 a 12/04
➢ 1.1 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.	➢ 6. Políticas de Segurança	➢ Aula expositiva dialogada. Pesquisa por legislação em direito digital.	15/04 a 26/04
➢ 1.1 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:Footprint: Descoberta de informações,Varredura/ análise;Enumeração:Testes de penetração e testes de vulnerabilidadesEngenharia social;Negação de serviço (DoS e DDoS);injections SQL	➢ Aula com projeção de slides. Demonstração por animações ou vídeos.	29/04 a 10/05

➢ 1.1 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.	➢ 8. Criptografia	➢ Aula expositiva. Trabalho de pesquisa sobre métodos antigos de criptografia.	13/05 a 24/05
➢ 1.1 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.	➢ 8. Criptografia	➢ Aula por projeto: elaboração de método criptográfico e envio de mensagem cifrada entre alunos.	27/05 a 07/06
➢ 1.1 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.	➢ 9. Firewall	➢ Aula expositiva dialogada. Demonstração de firewall no Windows e alternativas em Linux.	10/06 a 19/06
➢ 1.1 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.	➢ 10. Segurança de Redes	➢ Aula expositiva dialogada. Atividade prática interdisciplinar com o componente de Redes de Comunicação de Dados	24/06 a 28/06
➢ 1.1 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.	➢ 11. Segurança em Dispositivos Móveis	➢ Aula prática com aparelhos dos alunos; Demonstração de app em segurança digital para smartphones; Boas práticas para manter seguro os dados no smartphone.	01/07 a 02/07

Etec Sylvio de Mattos Carvalho Matão

Centro Paula Souza 50 anos 1969 • 2019

SÃO PAULO GOVERNO DO ESTADO

Unidade de Ensino Médio e Técnico - Cetec

IV - Plano de Avaliação de Competências

Componente Curricular: **SEGURANÇA DIGITAL** Módulo: **3º MÓDULO**

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.	➢ Assiduidade	➢ Assiduidade	➢ Comparecer as aulas
	➢ Avaliação Teórica(Prova de multipla escolha)	➢ Trabalho em Equipe ➢ Trabalho Prático (em grupo)	➢ Conseguir explicar as técnicas utilizadas para execução do projeto assim como suas metodologias de execução ➢ Senso de percepção, resolução de problemas e comunicação. Saber relacionar ideias a fim de interpretar e analisar as questões propostas. ➢ Capacidade de posicionar-se em situações específicas de mercado.
	➢ Participação em Sala de Aula	➢ Organização ➢ Disciplina	➢ Capacidade de posicionar-se em situações específicas de mercado. ➢ Senso de percepção, resolução de problemas e comunicação com seus pares.
	➢ Trabalho Prático (Individual)	➢ Pontualidade ➢ Compreensão ➢ Construção de Conceito	➢ Montar um sistema simples de criptografia ➢ Interpretar a lógica da sistematização do código. ➢ Determinar sistemas simples de criptografia.

Unidade de Ensino Médio e Técnico - Cetec

V – Plano de atividades docentes

Componente Curricular: **SEGURANÇA DIGITAL** Módulo: **3º MÓDULO**

Atividades 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	Recepção dos alunos e apresentação da disciplina, metodologia de ensino, Habilidades e competências.			Organização e revisão do material de apoio visando atender as necessidades da turma.	Planejamento; Reunião Didático-pedagógica.
MARÇO	Acompanhamento dos alunos faltantes e com dificuldades de aprendizado.	Levantamento das lacunas de aprendizagem e organização de recuperação dessas lacunas.	Organização e correção de trabalhos desenvolvidos e avaliações.	Organização e revisão do material de apoio visando atender as necessidades da turma.	Reunião pedagógica
ABRIL	Acompanhamento dos alunos faltantes e com dificuldades de aprendizado.	Levantamento das lacunas de aprendizagem e organização de recuperação dessas lacunas.		Organização e revisão do material de apoio visando atender as necessidades da turma.	Conselho de classe intermediário. Reunião de curso
MAIO	Acompanhamento dos alunos faltantes e com dificuldades de aprendizado.		Organização e correção de projetos desenvolvidos e avaliações.		Reunião pedagógica
JUNHO			Organização e correção de trabalhos desenvolvidos em laboratórios e avaliações.	Organização e revisão do material de apoio visando atender as necessidades da turma.	Reunião de curso
JULHO	Acompanhamento dos alunos faltantes e com dificuldades de aprendizado.	Levantamento das lacunas de aprendizagem e organização de recuperação dessas lacunas.			Conselho de classe final

Unidade de Ensino Médio e Técnico - Cetec

VI – Material de Apoio Didático para Aluno (inclusive bibliografia)
MORAES, Alexandre Fernandes de, Segurança em Redes: Fundamentos, Editora Érica, 2013.
ULBRICH, Henrique César; VALLE, James Della, Universidade Hacker, 3ª edição, Editora Digerati Books, 2003.
Cartilha deSegurança da informação na internet - CERT
GORDON, Steven R.; GORDON, Judith R. Sistemas de informação: uma abordagem gerencial. Rio de Janeiro: LTC, 2006
TURBAN, Efrain; et al. Administração de tecnologia da informação: teoria e prática. Rio de Janeiro: Elsevier, 2005
SÊMOLA, Marcos; Gestão da segurança da informação: visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003

VII – Propostas de Integração e/ou Interdisciplinares e/ou Atividades Extra
06/05 à 10/05 - Semana Paulo Freire
Atividade interdisciplinar com o componente de Redes de Comunicação de Dados.

VIII – Estratégias de Recuperação Contínua (para alunos com baixo rendimento/dificuldades de aprendizagem)
Após levantamento quinzenal das dificuldades de aprendizagem, propor revisão dos pontos importantes para o avanço do aluno. A revisão objetivando a recuperação poderá ser realizada: com a participação da turma, oralmente e expositivamente; através da proposta de aprendizagem por projetos em grupo; individualizada e com suporte de exercícios que proporcionem melhor compreensão dos assuntos tratados.

IX – Identificação:

Nome do Professor: **LUIZ FERNANDO SABINO DE OLIVEIRA**

Assinatura: Data:____/____/_____

X – Parecer do Coordenador de Curso:

O planejamento deste componente curricular apresenta metodologias de ensino diversificadas, trabalhando a teoria e a prática, contextualizando os conceitos com o dia a dia do aluno e valorizando o trabalho em equipe. Os instrumentos e critérios de avaliação, bem como de recuperação, possibilitam que o aluno possa ser avaliado de maneira holística e de forma contínua. Também está em consonância com o projeto pedagógico dessa Unidade Escolar através de propostas de integração e/ou interdisciplinares. Diante do exposto, manifesto-me favorável a execução desse plano de trabalho.

Nome do Coordenador: **PRISCILA APARECIDA ARTHUR**

Assinatura: Data:____/____/_____

_____

Data e ciência do Coordenador Pedagógico

XI– Replanejamento: