# Plano de Trabalho Docente – 2017

# Ensino Técnico

| | | |
|---|---|---|
| Plano de Curso nº 160 aprovado pela portaria Cetec nº 138 de 04/10/2012 | | |
| **Etec Sylvio de Mattos Carvalho** | | |
| Código: 103 | Município: Matão | |
| Eixo Tecnológico: ***Informação e Comunicação*** | | |
| **Habilitação Profissional de TÉCNICO EM INFORMÁTICA** | | |
| Qualificação: Técnica de Nível Médio de TÉCNICO EM INFORMÁTICA | | |
| Componente Curricular: Segurança Digital | | |
| Módulo:3º | C. H. Semanal:2,5 | |
| Professor: Maria Célia Barbosa | | |

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

**ATRIBUIÇÕES/ RESPONSABILIDADES**

- Instalar, codificar, compilar e testar programas estruturados, orientados a eventos e objetos.

**ÁREA DE ATIVIDADES**

**A – PLANEJAR E PROJETAR SISTEMAS E APLICAÇÕES**

- Projetar o modelo do sistema e aplicações.

**B – DESENVOLVER SISTEMAS E APLICAÇÕES**

- Codificar, compilar e testar sistemas e aplicações.
- Documentar sistemas e aplicações.

**D – DEMONSTRAR COMPETÊNCIAS PESSOAIS**

- Demonstrar flexibilidade.
- Trabalhar em equipe.

**II – Competências, Habilidades e Bases Tecnológicas do Componente Curricular.**

Componente Curricular: Segurança Digital Módulo:3º

| 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 | 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.<br>2.<br>3.<br>4.<br>5.<br>6. | Conceitos de Segurança Digital<br>Características de informação segura:<br>• Confidencialidade, integridade e disponibilidade (CIA – Confidentiality, Integrity and Availability)<br>Certificações de segurança:<br>• Órgãos reguladores nacionais e internacionais:<br>  • CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil;<br>  • CSIRT – Computer Security Incident<br>  • Response Team (Equipe de Resposta a Tratamento de Incidentes de Segurança)<br>• Certificado digital;<br>• Assinatura digital.<br>Cartilha de Segurança para Internet<br>Mecanismos de Segurança:<br>• Controles físicos e controles lógicos<br>Políticas de Segurança |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 7. | Técnicas para identificar vulnerabilidades:<br>• Footprint:<br>  • Descoberta de informações<br>• Varredura/ análise;<br>• Enumeração:<br>  • Testes de penetração e testes de vulnerabilidades<br>• Engenharia social;<br>• Negação de serviço (DoS e DDoS);<br>• injections SQL |
| | | | | 8. | Criptografia |
| | | | | 9. | Firewall |
| | | | | 10. | Segurança de Redes |
| | | | | 11. | Segurança em Dispositivos Móveis |

**III – Procedimento Didático e Cronograma de Desenvolvimento**

Componente Curricular: Segurança Digital Módulo: 3º

| Habilidade | Bases Tecnológicas | Procedimentos Didáticos | Cronograma / Dia e Mês |
|---|---|---|---|
| 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. | Criptografia | **Conteúdo:**<br>Introdução à Criptografia. Breve histórico.<br>Métodos criptográficos.<br>Hashing.<br><br>**Procedimentos Didáticos:**<br>Estudo dirigido sobre Criptografia. Trabalho em grupo onde cada equipe deve produzir um método criptográfico inédito e expor para a sala. | 24/07 a 04/08 |
| 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. | Características de informação segura:<br>• Confidencialidade, integridade e disponibilidade (CIA – Confidentiality, Integrity and Availability) | **Conteúdo:**<br>Introdução a CIA.<br>Funcionamento da CIA por atribuição de valores.<br><br>**Procedimentos Didáticos:**<br>Exposição teórica e dinâmica em grupo para atribuição de valores CIA aos ativos; exercício proposto pelo professor. | 07/08 a 18/08 |
| 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. | Conceitos de Segurança Digital | Conteúdo:<br>Apresentação da Disciplina, Habilidades, Competências e Bases Tecnológicas. Critérios de Avaliação.<br><br>Introdução à Segurança Digital, conceito de ativo digital.<br>Procedimentos Didáticos:<br>Aula expositiva com uso de projeção de slides para apresentação das definições. | 21/08 a 01/09 |

| | | | |
|---|---|---|---|
| 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. | Certificações de segurança:<br>• Órgãos reguladores nacionais e internacionais:<br>  • CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil;<br>  • CSIRT – Computer Security Incident<br>  • Response Team (Equipe de Resposta a Tratamento de Incidentes de Segurança)<br>• Certificado digital;<br>• Assinatura digital. | **Conteúdo:**<br>O que são certificações de segurança.<br>Os órgãos nacionais e internacionais reguladores de segurança.<br>CSIRT e Response Team no Brasil.<br><br>**Procedimentos Didáticos:**<br>Aula dialogada com exposição dos sites de órgãos reguladores.<br>Elaboração de relatórios com as principais atuações/atividades de cada órgão. | 04/09 a 15/09 |

| | | | |
|---|---|---|---|
| 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. | Certificações de segurança:<br>• Órgãos reguladores nacionais e internacionais:<br>  • CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil;<br>  • CSIRT – Computer Security Incident<br>  • Response Team (Equipe de Resposta a Tratamento de Incidentes de Segurança)<br>• Certificado digital;<br>• Assinatura digital. | **Conteúdo:**<br>Certificado Digital e Assinatura Digital<br>Apresentação da Cartilha de Segurança para Internet.<br><br>**Procedimentos Didáticos:**<br>Aula expositiva com uso de projeções gráficas para demonstrar a organização e funcionamento das chaves de assinatura digital. | 18/09 a 29/09 |
| 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. | Cartilha de Segurança para Internet | **Conteúdo:**<br>Apresentação da Cartilha de Segurança para Internet.<br>**Procedimentos Didáticos:**<br>Propor Painel Seletivo aos alunos onde cada grupo escolherá um tema abordado na cartilha e deverão expor/discutir/amplia este tema com a turma. | 02/10 a 13/10 |
| 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. | Mecanismos de Segurança:<br>• Controles físicos e controles lógicos | **Conteúdo:**<br>Mecanismos de Segurança: Controles Físico e Lógicos<br>**Procedimentos Didáticos:**<br>Aula expositiva Mecanismos de Segurança.<br>Pesquisa na Internet sobre custos de implementação física destes mecanismos. | 16/10 a 27/10 |

| | | | |
|---|---|---|---|
| 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. | Níveis de Segurança:<br>• Física e lógica<br>Políticas de Segurança | **Conteúdo:**<br>Níveis de segurança física e lógica.<br>Políticas de Segurança.<br><br>**Procedimentos Didáticos:**<br>Exposição de slides com projeção e atividade em grupo para resolução de situações-problema. | 30/10 a 10/11 |
| 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. | Técnicas para identificar vulnerabilidades:<br>• Footprint:<br>  • Descoberta de informações<br>• Varredura/ análise;<br>• Enumeração:<br>  • Testes de penetração e testes de vulnerabilidades<br>• Engenharia social;<br>• Negação de serviço (DoS e DDoS);<br>• injections SQL | **Conteúdo:**<br>Apresentar as principais vulnerabilidades e técnicas de identificação.<br><br>**Procedimentos Didáticos:**<br>Elaborar Painel Seletivo onde a turma se organiza em grupos que selecionam uma das técnicas de identificação de vulnerabilidades e, emulam em laboratório a demonstração prática para a sala. | 13/11 a 24/11 |
| 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. | Firewall<br>Segurança de Redes<br>Segurança em Dispositivos Móveis | **Conteúdo:**<br>Definições sobre Firewall e Segurança de Redes.<br>Apresentação da segurança para dispositivos móveis<br>**Procedimentos Didáticos:**<br>Aula Expositiva com projeção de slides.<br>Demonstração prática do uso de firewalls integrada com a participação dos alunos. | 27/11 a 08/12 |

| | | | |
|---|---|---|---|
| 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. | Segurança em Dispositivos Móveis | **Conteúdo:**<br>Apresentação da segurança para dispositivos móveis<br>**Procedimentos Didáticos:**<br>Aula Expositiva com projeção de slides.<br>Demonstração prática com a participação dos alunos. | 11/12 a 18/12 |

**IV - Plano de Avaliação de Competências**

| Competência | Instrumentos e Procedimentos de Avaliação | Critérios de Desempenho | Evidências de Desempenho |
|---|---|---|---|
| Propor e aplicar soluções visando à proteção das informações de determinadas empresas ou pessoas, garantindo confidencialidade, integridade e disponibilidade | Prova Dissertativa<br>Prova Prática<br>Estudo de Caso<br>Trabalho Dissertativo<br>Trabalho Prático<br>Debates em Grupo | Habilidades:<br>Trabalho em Equipe<br>Destreza<br><br>Comportamentos:<br>Organização<br>Pontualidade<br><br>Conhecimentos:<br>Construção de Conceito<br>Compreensão | Capacidade de implementar políticas de segurança. |

**V – Plano de atividades docentes***

| 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 |
|---|---|---|---|---|---|
| **Julho** | Acompanhamento da frequência quinzenalmente. Diálogo com alunos com faltas excessivas para o período. | Revisão de conteúdos para alunos que demonstrarem dificuldades de aprendizagem. | | Elaboração de material didático digital - Apostila | Reunião Didático Pedagógica, planejamento e reunião de área. |
| **Agosto** | Acompanhamento da frequência quinzenalmente. Diálogo com alunos com faltas excessivas para o período. | Revisão de conteúdos para alunos que demonstrarem dificuldades de aprendizagem. | Elaboração/correção de atividades avaliativas aplicadas em sala de aula | Elaboração atividades complementares aos exercícios da apostila | Reunião de curso |
| **Setembro** | Acompanhamento da frequência quinzenalmente. Diálogo com alunos com faltas excessivas para o período. | Revisão de conteúdos para alunos que demonstrarem dificuldades de aprendizagem. Disponibilização de atividades extraclasse. | Elaboração/correção de atividades avaliativas aplicadas em sala de aula | Elaboração atividades complementares aos exercícios da apostila e atividades extraclasse. | Conselho de classe intermediário |
| **Outubro** | Acompanhamento da frequência quinzenalmente. Diálogo com alunos com faltas excessivas para o período. | Revisão de conteúdos para alunos que demonstrarem dificuldades de aprendizagem. Disponibilização de atividades extraclasse. | Elaboração/correção de atividades avaliativas aplicadas em sala de aula | Elaboração atividades complementares aos exercícios da apostila e atividades extraclasse. | |
| **Novembro** | Diálogo com alunos com faltas excessivas para o período ou com dificuldades de aprendizagem. | Revisão de conteúdos para alunos que demonstrarem dificuldades de aprendizagem. Disponibilização de atividades extraclasse. Recuperação contínua | Preparo de meios de avaliação de conceitos e de habilidades prático operacionais. | Elaboração atividades complementares aos exercícios da apostila e atividades. | Reunião Didático Pedagógica Letiva<br><br>Reunião de Curso |
| **Dezembro** | - Identificação e contato com alunos com faltas consecutivas; | Revisão de conteúdos para alunos que demonstrarem dificuldades de aprendizagem. Disponibilização de atividades extraclasse. Recuperação contínua | Preparo e correção da Atividades finais | Lista com links para pesquisa e finalização de apresentações de seminários | Conselho de classe final |

**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.

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

- **25/11 – Apresentação – Mostra de TTCs aberta a comunidade.**

- Atividade interdisciplinar com o componente curricular Redes de Comunicação de Dados - Exercício: desenvolvimento de diagrama e descrição do projeto com base no conteúdo teórico e prático desenvolvido até o momento.

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

Os discentes com aproveitamento insatisfatório constituir-se-ão de atividades, recursos e metodologias diferenciadas e individualizadas com a finalidade de eliminar e/ou reduzir a deficiência de aprendizagem que inviabilizou o desenvolvimento das competências visadas neste componente curricular.
Para isso, serão realizadas:

- Revisão dos conteúdos ministrados, utilizando-se de situações motivadoras, associadas a experiências reais produtivas e gratificantes, de preferência que fazem parte do cotidiano do discente, possibilitando-lhe um maior entusiasmo no processo sistemático da construção do conhecimento.
- Reutilização de critérios diferenciados de avaliação que possibilitem verificar em que medida as estratégias de recuperação adotadas pelo docente tiveram êxito, a partir das competências e habilidades evidenciadas pelo discente a partir de então.

**IX – Identificação:**

**Nome do professor:** Maria Célia Barbosa

**Assinatura: _____** **Data:____/____/ 2017**

**X – Parecer do Coordenador de Curso:**

*O Plano de Trabalho Docente está de acordo com o Plano de Curso definido para esse Componente Curricular, pois planeja a execução de rotinas que objetivam identificar as principais vulnerabilidades, falhas de segurança e portas de entrada de códigos maliciosos com intuito de proteger os sistemas computacionais.*

Nome do coordenador (a): Priscila Aparecida Arthur Data: ___/___/2017

**Priscila Aparecida Arthur**
**RG 41.522.405-6**
**Coordenadora do Curso de Informática**

Data e ciência do Coordenador Pedagógico

**XI – Replanejamento**