MECHANICAL TECNOLOGIA

Plano de Formação em Segurança Cibernética

1. Nome da Instituição Formadora

Mechanical Tecnologia

2. Objectivos

Garantir que o participante saiba definir responsabilidades, identificar, avaliar riscos e estabelecer ações de prevenção, proteção, deteção e respostas a eventuais problemas de segurança em sua empresa que podem provir de crimes cibernéticos do tipo, malware, espionagem, engenharia Social, também visa dar a conhecer os requisitos regulamentares contra problemas de segurança cibernética existentes nas organizações.

3. Publico Alvo

Profissionais na área de tecnologias de Informação, Técnicos e gestores redes e data centres; Gestores de Base de dados, formadores e formados nas áreas de informática ou de engenharia informática e de telecomunicações, profissionais das demais áreas que lidam com TICs em uma empresa.

4. Pré-requisitos

Os estudantes devem ter conhecimento solido sobre o modelo TCP/IP e endereçamento de sub-redes.

5. Metodologia de Ensino

A formação será ministrada em uma sala preparada respeitando a disposição orador-para-participante, serão apresentados cenários práticos e realísticos de situações semelhantes e diversificadas referentes aos temas a ser abordado.

6. Plano Programático

Tópico 1: Fundamentos da Segurança Cibernética

- Introdução à segurança cibernética;
- Princípios de segurança de informações;

6. Plano Programático

- Fundamentos de criptografia;
- Conceitos de redes seguras;
- Identificação e autenticação.

Tópico 2: Segurança de Redes

- Riscos de segurança de rede;
- Tecnologias de firewall;
- Segurança de switch e roteador;
- Implementação de redes seguras;
- Configuração de dispositivos de segurança.

Tópico 3: Tecnologias de Acesso Remoto

- VPN (Virtual Private Network);
- Autenticação multifator;
- Acesso remoto seguro;
- Segurança de terminal.

Tópico 4: Segurança de Sistemas

- Gerenciamento de vulnerabilidades;
- Segurança do sistema operacional;
- Segurança de aplicativos;
- Segurança de dispositivos móveis;
- Hardening de sistemas.

Tópico 5: Segurança em Cloud

- Conceitos de computação em nuvem;
- Segurança de dados em nuvem;
- Desafios de segurança em ambientes de nuvem;
- Controles de segurança em serviços de nuvem.

Tópico 6: Gestão de Incidentes e Resposta a Incidentes

- Planeamento de incidentes de segurança;
- Detecção de incidentes;
- Resposta a incidentes;
- Recuperação de incidentes;
- Lições aprendidas e melhoria contínua.

6. Plano Programático

Tópico 7: Ética e Legislação em Segurança Cibernética

- Ética profissional;
- Regulamentações e legislações relevantes;
- Privacidade de dados;
- Responsabilidade legal.

7. Aptidões ao fim do curso

O formando ao fim deste treinamento estará apto para propor melhores soluções de segurança para a organização, contribuindo na elaboração de políticas robustas de para prevenir a sua organização contra-ataques e crimes cibernéticos na infraestrutura local ou na Web, com a identificação de vulnerabilidades nos sistemas, redes de computadores, e terá domínio de uso de criptografia para uma comunicação segura para a sua organização.

8. Carga Horaria

- 96 Horas

9. Referencias Bibliográficas

Livro Oficial da CompTIA Security+: https://www.comptia.org/training/books/security-sy0-601-study-guide