CERTIFICADO

Certificamos que **ISABELA ELZA TEIXEIRA**, concluiu com rendimento satisfatório o Treinamento online de **Segurança cibernética**, através do site **kmz0u1ep.fixonweb.com.br** com início em **24/10/2026** e sua conclusão em **24/10/2026**, com duração de **40 horas**, com base no Decreto Legal nº 5.154, de julho de 2004, Art. 1º e 3º de acordo com as normas do Ministério da Educação (MEC) pela Resolução CNE nº 04/99, Art. 11°.

sábado, 24 de outubro de 2026

Guilherme Cunha
Coordenador Geral

Isabela Elza Teixeira
Aluno

CONTEÚDO PROGRAMÁTICO

Módulo 1 — Introdução à Segurança Cibernética
Conceitos essenciais e fundamentos da proteção digital.

- Conceitos de segurança cibernética e segurança da informação.
- Confidencialidade, integridade e disponibilidade.
- Ativos digitais, vulnerabilidades, ameaças e riscos.
- Principais responsabilidades dos usuários.
- Panorama das ameaças no ambiente digital.

Módulo 2 — Ameaças e Ataques Digitais
Reconhecimento das principais ameaças cibernéticas.

- Malware, vírus, ransomware e spyware.
- Phishing, smishing e outras fraudes digitais.
- Engenharia social e manipulação de usuários.
- Ataques de negação de serviço: conceitos e impactos.
- Sinais de comprometimento de contas e dispositivos.

Módulo 3 — Senhas e Controle de Acesso
Proteção de identidades e contas digitais.

- Criação e gerenciamento de senhas fortes.
- Uso de gerenciadores de senhas.
- Autenticação multifator (MFA).
- Princípio do menor privilégio.
- Segurança de contas pessoais e corporativas.

Módulo 4 — Proteção de Computadores e Dispositivos
Medidas de proteção para equipamentos e sistemas.

Módulo 6 — Proteção de Dados e Privacidade
Proteção de informações e redução de exposição.

- Classificação e tratamento de informações.
- Princípios de privacidade e proteção de dados.
- Noções da Lei Geral de Proteção de Dados (LGPD).
- Cópias de segurança e recuperação de arquivos.
- Compartilhamento seguro de documentos.

Módulo 7 — Vulnerabilidades e Prevenção
Identificação de riscos e redução da superfície de ataque.

- Conceitos de vulnerabilidade e gestão de riscos.
- Importância de atualizações e correções de segurança.
- Configurações seguras e redução de serviços desnecessários.
- Noções de análise de vulnerabilidades.
- Uso responsável de ferramentas em ambientes autorizados.

Módulo 8 — Incidentes e Continuidade
Primeiras ações diante de eventos de segurança.

- Conceito e classificação de incidentes.
- Identificação, registro e comunicação de ocorrências.
- Isolamento inicial de dispositivos comprometidos.
- Preservação de evidências e encaminhamento técnico.
- Continuidade das operações e recuperação básica.

Módulo 9 — Revisão e Avaliação Final
Consolidação dos conhecimentos e verificação de aprendizagem.

Guilherme Cunha
Instrutor:

- Atualizações de sistemas operacionais e aplicativos.
- Antivírus, firewall e ferramentas de proteção.
- Segurança em dispositivos móveis.
- Bloqueio de tela e criptografia de dispositivos.
- Instalação segura de programas e aplicativos.

Módulo 5 — Segurança em Redes e Internet
Conexões seguras e proteção do tráfego digital.

- Conceitos básicos de redes de computadores.
- Redes Wi-Fi domésticas e corporativas.
- HTTPS, certificados digitais e navegação segura.
- Riscos de redes públicas e uso de VPN.
- Configurações básicas de segurança em roteadores.

- Revisão dos fundamentos de segurança cibernética.
- Análise de situações hipotéticas de risco.
- Boas práticas de prevenção e proteção.
- Questionário de avaliação final.
- Orientações para aplicação dos conhecimentos.

_____

Guilherme Cunha
Instrutor: