

## Avaliação de conhecimento - INFOSEC01 PBs

Este questionário tem como objetivo validar o conhecimento adquirido no curso "Segurança da Informação (Básico). São 15 perguntas e você pode utilizar um tempo médio de 2 minutos para responde-las,

Para dar o curso como concluído é **necessário atingir 80%** de acerto nas respostas, ao final você poderá confirmar seus acertos neste próprio formulário ou enviando as respostas para seu e-mail.

1. São possíveis rótulos pra classificação das informações e assim protege-las adequadamente.

(5 Pontos) \*

- ☐ Secreta, Ultrassecrta, Top Secret, Sigilosa
- ☐ Protegida, Mediana, Pública, Aberta
- ☒ Confidencial, Restrita, Interna e Pública
- ☐ Secreta, Interna, Protegida, Sigilosa

2. Entre as diversa técnica de engenharia social em busca de informações valiosas para elaborar um ataque há uma menos usual, porém, não menos eficiente. Um lugar improvável e rico em informações sobre o alvo do ataque. Identifique-a: (5 Pontos) \*

☒ Dumpster diving

☐ Design thinking

☐ Big data crashing

☐ Denial of service

3. Quais são os fatores de autenticação mais utilizados? (5 Pontos) \*

☐ Token/ SMS/ Usuário

☒ O que sei/ O que tenho/ Quem sou

☐ Senha/ Biometria/ Localização

☐ Onde estou/ Horário do acesso/ Sistema solicitado

4. Ao falar em navegação segura na internet lembre-se de: (5 Pontos) \*

☒ Verificar o uso de certificado digital (HTTPS)

☒ Navegador web está atualizado

☐ Usar a deep web

☐ Abrir anexos de TODOS os e-mails

5. Quais os critérios devem ser avaliados para classificar uma informação corretamente? (5 Pontos) \*

- ☒ Sensibilidade, criticidade e valor
- ☐ Criação, descarte e local de armazenamento
- ☐ Tamanho, quantidade de cópias e tipo do arquivo
- ☐ Local do armazenamento, acesso controlado e tamanho

6. Quanto às credenciais de acessos aos sistemas, é correto afirmar que são de total responsabilidade do time de segurança da informação. (5 Pontos) \*

- ☐ Verdadeiro
- ☒ Falso

7. Sempre que for necessário instalar algum software em seu equipamento, devemos: (5 Pontos) \*

- ☐ Pesquise opções na internet

☒ Consulte a lista de softwares homologados

☐ Faça um banchmark

☐ Analise se há espaço em disco

8. Quando falamos em manter a confidencialidade de uma informação, logo pensamos em informações altamente sigilosas e que se vazarem pode causar danos à empresa. (5 Pontos) \*

☐ Falso

☒ Verdadeiro

9. **É correto** afirmar sobre ferramentas de IA. (5 Pontos) \*

☐ Ferramentas gratuitas e pagas dispensam a supervisão de profissionais experientes

☒ Ferramentas gratuitas e pagas devem ser utilizadas como auxiliares e supervisionadas por profissionais experientes.

☐ Ferramentas pagas trazem melhores respostas.

☐ Ferramentas gratuitas podem ser utilizadas sem limitações ou restrições.

10. Para proteger dados sensíveis ao utilizar ferramentas IA devo: (5 Pontos) \*

- ☒ Trocar dados reais como nomes próprios das empresas ou clientes.
- ☐ Utilizar fontes de dados externos
- ☒ Mascarar os dados informados
- ☒ Remover dados pessoais, senhas ou tokens.

11. É o melhor documento para você encontrar as boas práticas e diretrizes de segurança da informação na Compass? (5 Pontos) \*

- ☐ Formulário de incidentes
- ☐ Termo de conduta
- ☒ Política de segurança da informação (PSI)
- ☐ Dicas de governança

12. Escolha duas opções de abordagem na engenharia social. (5 Pontos) \*

- ☐ Crashing

☐ Smashing

☒ Smishing

☒ Phishing

13. O que melhor descreve a engenharia social? (5 Pontos) \*

☒ Obter informação ou acesso através de persuasão

☐ Brechas em configuração de dispositivos

☐ Benefícios sociais para engenheiros

☐ Técnicas de graduação em exatas

14. Um incidente acontece sempre que um evento ou conjunto deles impactar a confidencialidade, integridade ou disponibilidade de um ativo de informação. E deve ser reportado ao time InfoSec imediatamente. (5 Pontos) \*

☒ Verdadeiro

☐ Falso

15. Quero me proteger de abordagens de engenharia social, o que devo fazer? (múltipla escolha)  
(5 Pontos) \*

- ☒ Descartar documentos físicos de forma que não possam ser recuperados
- ☒ Suspeitar sempre, validar remetente e links
- ☒ Não baixar ou executar arquivos anexos suspeitos.
- ☐ Interagir com os suspeitos



Este conteúdo foi criado pelo proprietário do formulário. Os dados que você enviar serão enviados ao proprietário do formulário. A Microsoft não é responsável pela privacidade ou práticas de segurança de seus clientes, incluindo aqueles do proprietário deste formulário. Nunca forneça sua senha.

**Microsoft Forms** | Pesquisas, questionários e votações com tecnologia de IA [Criar meu próprio formulário](#)

[Política de privacidade](#) | [Condições de uso](#)