**1. Por que convém que a Segurança Lógica faça parte da cultura organizacional da empresa?**  
**B)** Porque a informação contida na empresa é muito valiosa.

**2. Quais são os elementos que fazem parte da Segurança Lógica?**  
**B)** Sistemas operacionais e senhas.

**3. O que é considerado uma informação sensível que precisa de proteção na Segurança Lógica?**  
**B)** Dados de clientes.

**4. Quais são algumas das medidas de proteção da Segurança Lógica?**  
**A)** Antivírus e firewall.

**5. O que é criptografia na Segurança Lógica?**  
**C)** Um método para ocultar informações sensíveis.

**6. Qual a importância das assinaturas digitais na Segurança Lógica?**  
**B)** Para validar transações financeiras.

**7. Qual é a função de um firewall na Segurança Lógica?**  
**A)** Bloquear o acesso de pessoas não autorizadas à rede.

**8. O que é um antivírus na Segurança Lógica?**  
**B)** Um programa para proteger contra vírus de computador.

**9. Quais são os tipos de informações que devem ser protegidos na Segurança Lógica?**  
**A)** Dados de clientes e fornecedores.

**10. Por que é importante proteger as informações sensíveis na Segurança Lógica?**  
**A)** Para evitar vazamento de informações.

**11. Marque Verdadeiro ou Falso sobre Segurança Lógica:**

* (V) A Segurança Lógica envolve proteção contra ameaças virtuais, como vírus e hackers.
* (V) As senhas são consideradas informações sensíveis que devem ser protegidas pela Segurança Lógica.
* (V) Um firewall é um dispositivo que protege uma rede de computadores contra acessos não autorizados.
* (V) Criptografia é o processo de tornar informações legíveis apenas para quem tem a chave de decodificação.
* (V) Assinaturas digitais são usadas na Segurança Lógica para garantir a autenticidade e integridade de documentos eletrônicos.

**12. Marque Verdadeiro ou Falso sobre Segurança Lógica:**

* (F) A Segurança Lógica se preocupa apenas com a proteção física dos equipamentos de informática.
* (V) Um antivírus é um software utilizado na Segurança Lógica para proteger contra vírus de computador.
* (V) Um dos objetivos da Segurança Lógica é garantir a disponibilidade das informações quando necessário.
* (V) A criptografia pode ser usada para proteger dados durante a transmissão pela internet.
* (F) A Segurança Lógica não é importante para empresas que não lidam com informações sensíveis.

**13. Relacione a coluna da esquerda com a coluna da direita:**

* (Antivírus) → **A.** Protege contra ameaças virtuais, como vírus e malware.
* (Firewall) → **D.** Utilizado para proteger sistemas contra acesso não autorizado.
* (Criptografia) → **C.** Tornar informações ilegíveis para quem não possui a chave de decodificação.
* (Assinatura Digital) → **B.** Utilizado para autenticar a autoria de um documento eletrônico.
* (Senha) → **E.** Método de autenticação de usuário para acessar sistemas e aplicativos.

**14. Relacione a coluna da esquerda com a coluna da direita:**

* (Backup) → **D.** Cópia de segurança dos dados para recuperação em caso de perda.
* (Autenticação de dois fatores) → **C.** Processo de verificação da identidade de um usuário através de duas etapas distintas.
* (VPN) → **A.** Ferramenta para conexão segura a redes privadas através da internet.
* (Política de Segurança da Informação) → **B.** Estratégia para garantir a confidencialidade, integridade e disponibilidade das informações.
* (Controle de Acesso) → **E.** Regras e diretrizes para proteger as informações da empresa.

**15. Relacione a coluna da esquerda com a coluna da direita:**

* (Token) → **D.** Dispositivo de segurança utilizado para autenticação de usuários.
* (Controle de Acesso) → **C.** Ferramenta de segurança que controla o acesso a sistemas e dados.
* (Phishing) → **A.** Tipo de ataque que visa obter informações confidenciais por meio de engenharia social.
* (Firewall de Aplicação) → **E.** Protege os aplicativos web contra ataques como injeção de SQL e XSS.
* (Política de Senhas) → **B.** Regras e procedimentos para definir a complexidade e a atualização de senhas.