1 ponto

**4.** Existem diversas fontes de informação que descrevem as vulnerabilidades de segurança de um software. Um exemplo de fonte de informação é a OWASP. Neste sentido, selecione a opção correta a respeito da afirmação:"Um invasor pode utilizar uma fonte oficial de informação para aprender a explorar vulnerabilidades de um software".

(Ref.: 202310886105)

- ○ Está correta, pois é natural que após aprender sobre as vulnerabilidades de um software, um indivíduo passe a explorá-las.
- ○ Está correta, pois um invasor pode usar um conhecimento para explorar sistemas vulneráveis.
- ◉ Está correta, pois o objetivo dessas fontes é que os sistemas vulneráveis sofram as consequências do mau-gerenciamento.
- ○ Está errada, pois essas fontes não fornecem muitos detalhes sobre as vulnerabilidades.
- ○ Está errada, pois essas fontes são explícitas sobre as consequências de usar um conhecimento que elas fornecem de forma indevida.

1 ponto

**5.** Uma situação bastante comum no desenvolvimento de software é fazer chamada a outro programas. Especialmente, quando os programas são de terceiros, há riscos de vulnerabilidade para segurança do nosso software. Nesse sentido, selecione uma opção que apresente um exemplo de risco ao chamarmos um programa de terceiros de dentro do nosso software.

(Ref.: 202310886109)

- ○ Não haver uma documentação detalhada de como realizar a chamada.
- ○ Que o programa seja muito lento.
- ◉ Que o programa não tenha recebido atualizações recentes.
- ○ Os desenvolvedores do nosso sistema sentirem dificuldades para fazer a chamada.
- ○ Um invasor interceptar os dados na chamada do programa.

1 ponto

**6.** O ciclo de vida de desenvolvimento de software seguro engloba atividades diversas divididas em etapas encadeadas que vão da elicitação de requisitos até os testes. Considerando as afirmativas a seguir, assinale a alternativa que melhor representa as lacunas apresentadas.

**I -** O desenho da arquitetura do software as especificações técnicas são formalmente definidas empregando linguagens voltadas à modelagem na fase de _____.

**II -** O principal mecanismo empregado para proteger os dados armazenados e em trânsito é a _____.

**III -** Projetar o software para ser imune a injeções maliciosas de dados corresponde ao passo de _____.

(Ref.: 202310871411)

- ◉ I - projeto; II - criptografia; III - validação das entradas.
- ○ I - requisitos; II - criptografia; III - auditoria.
- ○ I - requisitos; II - criptografia; III - paralelização do processamento.
- ○ I - projeto; II - auditoria; III - validação das entradas.
- ○ I - projeto; II - auditoria; III - criptografia.

1 ponto

**7.** O SDL da Microsoft estabelece testes de três naturezas para encontrar falhas nos seus sistemas. Assinale a alternativa que apresenta os três tipos de teste propostos.

(Ref.: 202310871414)

- ○ Teste de conformidade; teste estático; e teste dinâmico.
- ○ Teste de desempenho; teste estático; e teste dinâmico.
- ○ Teste funcional; teste estático; e teste dinâmico.
- ◉ Teste de penetração; teste estático; e teste dinâmico.
- ○ Teste de penetração; teste de desempenho; e teste funcional.

1 ponto

**8.** Conformidade e Governança são dois conceitos fundamentais de Segurança da Informação onde a conformidade refere-se ao cumprimento das leis, regulamentos e padrões estabelecidos com o objetivo de garantir a segurança dos dados e informações, e a governança trata do conjunto de processos, políticas, normas e diretrizes que devem ser utilizados para gerenciar e controlar a segurança da informação de uma organização. Qual é o objetivo da governança no contexto de Segurança da Informação?

(Ref.: 202310974798)

- ○ Garantir a conformidade com as leis, regulamentos e políticas internas.
- ○ Estabelecer processos claros e bem definidos na organização.
- ◉ Gerenciar e controlar a segurança da informação em uma organização.
- ○ Estabelecimento de processos claros e comunicação efetiva dentro da organização.
- ○ Promover uma cultura de responsabilidade corporativa.