

1

Marcar para revisão

Para utilizar um sistema, precisamos entrar com o nosso login de usuário e senha. Além disso, no caso de sistemas seguros, ainda precisamos confirmar nossa identificação em outro dispositivo pré-cadastrado. Com base nas informações acima, selecione a opção correta que contém o nome dessa técnica.

A

autenticação multifator

B

recursos móveis

C

autenticação móvel.

D

Senha de segurança dupla.

E

Autenticação por criptografia.

00 : 46 : 31

hora min seg



Ocultar

Questão 1 de 10

1

2

3

4

5

6

7

8

9

10

● Respondidas (10) ● Em branco (0)

Finalizar prova



2

Marcar para revisão



Feedback

Um aspecto básico para a construção de um software seguro é aplicar os princípios de segurança. Então, considere a seguinte afirmação:

"O princípio de segurança mais importante é o da confidencialidade."

Nesse sentido, selecione a opção correta a respeito da afirmação.

A Está correta, pois é a partir dela que eliminamos todas as vulnerabilidades de um software.

B Está correta, pois restringe o acesso aos dados apenas para as pessoas que tem a devida autorização de utilizá-los

C Está errada, pois não há como garantir a confidencialidade dos dados através de um software



Está errada, pois o princípio de segurança mais importante é o de autorização.

Está errada, pois existem outros aspectos dos princípios de segurança que se somam para minimizar a exposição a riscos

3

Marcar para revisão

Os dados podem ser classificados como sensíveis ou confidenciais. Nesse sentido, considere a seguinte situação:

“Depois de muita deliberação, os gestores de uma empresa em recuperação decidiram injetar uma grande quantidade de recursos próprios para aumentar a credibilidade dos investidores e marcaram uma data específica para realizar essa ação.”

Com base nessa afirmação, escolha a opção correta.



A

É o caso típico de uma informação sensível, pois ela pode afetar o comportamento dos investidores

B

A afirmação é uma informação sensível, pois é necessário que os gestores tracem uma estratégia para evitar instabilidades no mercado

C

Trata-se de uma informação confidencial, pois está relacionada à estratégia da empresa

D

A afirmação trata de uma informação confidencial, pois expõem os valores que serão injetados na empresa

E

Claramente, é uma informação sensível, pois expõem os nomes dos investidores



Risco em segurança da informação se refere à probabilidade de uma ameaça explorar uma vulnerabilidade em um sistema e causar prejuízos aos ativos de informação. Nesse sentido, considere o seguinte comentário:

"Como não é possível eliminar todos os riscos a que um software está sujeito, pelo menos, tentamos mensurar quais os possíveis danos que podem ser causados por um invasor"

Agora, selecione a opção correta a respeito desse texto.

A

Sempre devemos garantir que não existem riscos para um software, caso contrário, ele não pode ser considerado seguro.

B

Só é possível tomar decisões sobre a mensuração de riscos de um software depois de realizarmos testes.

C

Para mensurar os possíveis danos de um ataque, precisamos utilizar segmentação de funções.



D

A forma ideal para mensurar riscos para um software é estudar o comportamento de cada usuário quando opera o sistema.

E

Uma forma de atingir o objetivo do comentário é usar privilégios mínimos para cada perfil de usuário.

5

Marcar para revisão

Para conseguirmos garantir que os dados sejam seguros, precisamos de um gerenciador deles que ofereça segurança. Esse gestor é o que chamamos de software seguro que pode ter diversas funcionalidades que vão do armazenamento a visualização e processamento dos dados. Neste sentido, selecione a opção correta que viabiliza desenvolvermos um código seguro.



A

Deixar que o próprio programa trate os erros e os exiba para o usuário final.

B

Com o uso de técnicas de embaralhamento de código que dificultam o entendimento deles por parte de invasores.

C

Através de diversos testes antes de entregar o software para o usuário final.

D

Através da aplicação de práticas de codificação segura.

E

Fazer uso de códigos obtidos em fóruns na Internet sem realizar testes.



6

Marcar para revisão

Alguns sistemas utilizam a opção "Não sou um robô". Nesse sentido, selecione a opção correta a respeito de como essa opção pode acrescentar em segurança para um software, uma vez que o

usuário já entrou com o login e a senha.

A

Esse é um recurso para evitar que um programa se passe por um usuário.

B

É uma forma do usuário se comprometer a usar o sistema de forma consciente.

C

É uma estratégia para obrigar o usuário a entrar com uma segunda senha.

D

Serve para tornar o processo de autenticação mais lento.

E

É uma alternativa de autenticação quando o usuário esquece a senha.



7

Marcar para revisão

O processamento dos dados é uma etapa importante de manipulação e construção de resultados úteis para os usuários finais. No entanto, não



existe apenas uma forma de realizar o processamento dos dados. Nesse sentido, selecione a opção que contém o nome do tipo de processamento que é adequado para situações em que lidamos com grandes volumes de dados de uma única vez.

A Processamento no servidor.

B Processamento em nuvem.

C Processamento em lote.

D Processamento de fluxo.

E Processamento em tempo real.



8

Marcar para revisão

A tecnologia de processamento da nuvem está cada vez mais popular. Certamente, existem várias justificativas para isso. Nesse sentido, selecione a opção correta sobre uma das vantagens para segurança

associadas ao processamento de dados na nuvem.

A

As configurações adequadas são escaláveis.

B

Possibilitar a criação de uma infraestrutura similar à da nuvem para criar redundâncias.

C

Usar as configurações padrões do fornecedor do serviço.

D

Usar serviços de rede para fazer chamadas aos programas.

E

Trabalhar com empresas de pequeno porte.



9

Marcar para revisão

Uma boa prática de segurança é manter os sistemas atualizados. Alguns fornecedores disponibilizam essas atualizações nas páginas oficiais deles. Neste sentido, selecione a opção correta que

apresenta o nome de um instrumento de atualização.

A arquivos criptografados.

B arquivo de mapeamento de vulnerabilidades e correções.

C arquivo de testes de estresse.

D arquivos de logs.

E arquivos de patches.



10

Marcar para revisão

Atualmente, é bastante comum trabalharmos com sistemas que utilizam a arquitetura cliente x servidor. O contato de um usuário ocorre com a aplicação do lado do cliente. Nesse sentido, escolha a opção correta sobre a afirmação: "não devemos fazer testes de validação de entrada do lado do servidor".

A

Está certa, pois testes de validação consomem muitos recursos computacionais.

B

Está certa, pois todos os testes de validação de entrada devem ser feitos no lado da aplicação cliente.

C

Está errada, pois apenas o lado da aplicação do servidor é que tem recursos para testar entradas maliciosas.

D

Está errada, pois podem passar dados maliciosos que não foram detectados pelos testes do lado da aplicação cliente.

E

Está errada, pois nunca fazemos testes de validação de entrada do lado da aplicação do cliente.

