



Lupa: 🔍 🔍

VERIFICAR E ENCAMINHAR

DGT1353 - DESENVOLVIMENTO DE S

2024.3 EAD (G)

Aluno: DOUGLAS ANTONIO BRAGA NOVATO

202303047479

Prezado(a) Aluno(a),

Responda a todas as questões com atenção. Somente clique no botão **FINALIZAR PROVA** ao ter certeza de que respondeu a todas as questões e que não precisará mais alterá-las.

A prova será SEM consulta. O aluno poderá fazer uso, durante a prova, de uma folha em branco, para rascunho. Nesta folha não será permitido qualquer tipo de anotação prévia, cabendo ao aplicador, nestes casos, recolher a folha de rascunho do aluno.

Valor da prova: 10 pontos.

1 ponto

1. Garantir que um software seja seguro está longe de ser uma atividade trivial. Por isso mesmo, os desenvolvedores precisam utilizar diversas técnicas para reduzir as vulnerabilidades de um sistema e, assim, minimizar a exposição ao risco de ataques. Infelizmente, esse excesso de controles, também pode gerar vulnerabilidades. Nesse sentido, selecione a opção correta que contém a vulnerabilidade associada ao excesso de tentativas de evitar vulnerabilidades.

(Ref.: 202310871080)

- ☐ Defesa contra erros.
- ☐ Mecanismos de privilégio mínimo.
- ☐ Economia de mecanismo.
- ☐ Design aberto.
- ☒ Complexidade do projeto.

1 ponto

2. É um fato que os riscos de ataques a sistemas sempre existiram e sempre vão existir. Isso exige ainda mais esforço da nossa parte para reduzir as chances de que eles se tornem em problemas reais. Neste sentido, selecione a opção correta que apresenta uma forma genérica de reduzirmos as chances de um risco se tornar um problema.

(Ref.: 202310871083)

- ☒ Através do estabelecimento de uma política de avaliação e gerenciamento de riscos.
- ☐ Através da identificação de todos os possíveis riscos de um sistema.
- ☐ Aumentarmos a quantidade camadas de um software até que ele faça a tarefa que lhe for designada.
- ☐ Concentrar-se apenas nos riscos de menor ocorrência.
- ☐ Só permitir acesso ao sistema através de controles biométricos.

1 ponto

3. 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.

(Ref.: 202310886125)

- ☐ Serve para tornar o processo de autenticação mais lento.
- ☐ É uma estratégia para obrigar o usuário a entrar com uma segunda senha.
- ☐ É uma forma do usuário se comprometer a usar o sistema de forma consciente.
- ☒ Esse é um recurso para evitar que um programa se passe por um usuário.
- ☐ É uma alternativa de autenticação quando o usuário esquece a senha.

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.