Exemplo de Exame - Respostas

Conjunto de Exemplo de Exame – exame escrito
Versão Final

ISTQB ® Security Test Engineer Syllabus Specialist Level

Compatível com a versão 1.0.1 do Syllabus

International Software Testing Qualifications Board

Final 2025-01-31

Aviso de direitos autorais

Responsabilidade pelo documento

O ISTQB® Examination Working Group é responsável por este documento.

Este documento é mantido por uma equipe central do ISTQB®, composta pelo Syllabus Working Group e pelo Exam Working Group.

Agradecimentos

Este documento foi produzido por uma equipe central do ISTQB®: Dr. Frank Simon (presidente), Alain Ribault, Gabriel Firmino Barjollo, Michael Pott, Beata Karpinska, Maria Kispal, Frans Dijkman

A equipe principal agradece à equipe de revisão do Exam Working Group, ao Syllabus Working Group e aos Conselhos Membros por suas sugestões e contribuições.

Histórico de revisões

Versão	Data	Observações
1.0	2024-09-10	Versão final para aprovação da GA
1.0.1	2015-01-31	Versão final após revisão EWG

Histórico da versão de tradução do BSTQB

Data	Observações
07/03/2025	Lançamento da versão na língua portuguesa

Índice

Introdução

Objetivo deste documento

Os exemplos de perguntas e respostas e as justificativas associadas neste exemplo de exame foram criados por uma equipe de especialistas no assunto e redatores de perguntas experientes com o objetivo de:

- Auxiliar os Conselhos de Membros e os Conselhos de Exames do ISTQB® em suas atividades de elaboração de perguntas.
- Fornecer aos provedores de treinamento e candidatos um exemplo de perguntas de exames.

Essas perguntas não podem ser usadas como estão em nenhum exame oficial.

Observe que os exames reais podem incluir uma grande variedade de perguntas, e este exemplo de exame ***não tem*** a intenção de incluir exemplos de todos os tipos, estilos ou durações possíveis de perguntas.

Instruções

Neste documento, você pode encontrar:

- Tabela Respostas, incluindo cada resposta correta:
  - Nível K, objetivo de aprendizado e valor de pontos
- Conjuntos de respostas, inclusive para todas as perguntas:
  - Resposta correta
  - Justificativa para cada opção de resposta (resposta)
  - Nível K, objetivo de aprendizado e valor de pontos
- Conjuntos de respostas adicionais, inclusive para todas as questões [não se aplica a todos os exemplos de exame]:
  - Resposta correta
  - Justificativa para cada opção de resposta (resposta)
  - Nível K, objetivo de aprendizado e valor de pontos

- *As perguntas estão contidas em um documento separado*

Resposta

Número da questão (#)	Resposta correta	LO	Nível K	Pontos
1	A	STE 1.1.1	K2	1
2	A	STE 1.1.2	K2	1
3	B	STE 1.2.1	K2	1
4	A	STE-1.3.1	K2	1
5	A, C	STE-1.3.2	K3	1
6	C	STE 1.4.1	K2	1
7	B, C	STE-2.1.1	K2	1
8	C	STE-2.1.2	K2	1
9	A	STE-2.2.1	K3	1
10	B, C	STE-2.2.2	K2	1
11	B	STE-2.2.3	K2	1
12	A	STE-2.2.4	K2	1
13	A	STE-2.2.5	K2	1
14	B	STE-3.1.1	K2	1
15	C	STE-3.1.2	K2	1
16	B	STE-3.2.1	K2	1
17	A	STE-3.2.2	K2	1
18	A	STE-3.2.3	K3	1
19	A	STE-4.1.1	K3	1
20	C, E	STE-4.2.1	K3	1

Número da questão (#)	Resposta correta	LO	Nível K	Pontos
21	D	STE 4.3.1	K2	1
22	A	STE 4.3.2	K3	1
23	B, C	STE 5.1.1	K3	1
24	A	STE-5.2.1	K3	1
25	D	STE-5.3.1	K4	2
26	A	STE 5.3.1	K4	2
27	A	STE 6.1.1	K2	1
28	D, E	STE 6.1.2	K4	2
29	C	STE 6.2.1	K3	1
30	C	STE 6.2.2	K2	1
31	B, D	STE 7.1.1	K2	1
32	A, C	STE 7.2.1	K2	1
33	A	STE 7.3.1	K3	1
34	A	STE 7.3.2	K2	1
35	B	STE 8.1.1	K2	1
36	A, D	STE 8.2.1	K3	1
37	A, D	STE 8.3.1	K3	1
38	A	STE 9.1.1	K3	1
39	A	STE-9.2.1	K2	1
40	A	STE-9.2.2	K2	1

Legenda:

Q: Questão	**C**: Resposta correta	**LO**: Objetivo de aprendizagem	**K**: Nível Cognitivo	**P**: Pontuação da questão

Q	C	Explicação / Justificativa	LO	K	P
1	a	A) CORRETO: a integridade busca evitar que os dados sejam modificados ou excluídos por qualquer parte não autorizada e é medida pelo grau em que um ativo permite apenas acesso e modificação autorizados. B) INCORRETO: A permissão de modificação de dados não é reservada aos proprietários de dados, mas é concedida apenas a usuários autorizados. C) INCORRETO: a política de retenção de dados está sujeita à política da organização e aos requisitos da jurisdição. D) INCORRETO: o acesso do usuário precisa ser feito com base na autorização e não sempre que o usuário precisar.	STE-1.1.1	K2	1
2	a	A) CORRETO: A confidencialidade nos testes de segurança garante que os dados confidenciais sejam acessados somente por usuários autorizados. Os testes de segurança verificam se os mecanismos de controle de acesso são eficazes, evitando assim o acesso não autorizado a informações confidenciais. B) INCORRETO: trata-se de integridade. C) INCORRETO: trata-se de disponibilidade e mecanismos de recuperação rápida após um incidente. D) INCORRETO: trata-se da resposta da organização a incidentes	STE-1.1.2	K2	1
3	b	A) INCORRETO: Essa é uma descrição dos testes de segurança em geral. B) CORRETO: A auditoria de segurança avalia os processos e as infraestruturas de segurança de uma organização e é um tipo de técnica de teste estático C) INCORRETO: Embora o objetivo esteja correto, o foco da auditoria está nos processos e controles D) INCORRETO: As auditorias se concentram em processos e controles	STE-1.2.1	K2	1
4	a	A) CORRETO: todos os usuários são tratados como não confiáveis e precisam se autenticar e autorizar antes de poderem acessar qualquer recurso B) INCORRETO: Uma rede tradicional é aquela em que todos os dispositivos e usuários são confiáveis por padrão. C) INCORRETO: Uma arquitetura Zero Trust refere-se a um modelo de segurança que não confia inerentemente em nada dentro da rede. D) INCORRETO: Um sistema Zero Trust garante que ninguém possa acessar os dados a menos que tenha as credenciais adequadas.	STE-1.3.1	K2	1

Q	C	Explicação / Justificativa	LO	K	P
5	a, c	A) CORRETO: O Zero Trust verifica a identidade e os privilégios do usuário, bem como a identidade e a segurança do dispositivo para cada acesso. Os logins e as conexões são interrompidos periodicamente, forçando os usuários e os dispositivos a serem continuamente verificados novamente. B) INCORRETO: contas não humanas também devem ser monitoradas C) CORRETO: o acesso concedido aos recursos deve ser registrado permanentemente e com registro de data e hora. D) INCORRETO: a criptografia e a restrição de acesso aos ativos são baseadas em políticas organizacionais E) INCORRETO: Limitar os controles de acesso a aplicativos, recursos, dados e ativos específicos, e não à rede mais ampla.	STE-1.3.2	K3	1
6	c	A) INCORRETO: O alinhamento com a OWASP e as auditorias de segurança são essenciais para garantir a segurança do software. B) INCORRETO: Patches e atualizações regulares são essenciais para solucionar vulnerabilidades. C) CORRETO: A personalização da equipe é importante, mas não está diretamente ligada a questões de segurança. D) INCORRETO: A conformidade com o licenciamento garante o uso adequado, o que pode afetar a segurança indiretamente.	STE-1.4.1	K2	1
7	b, c	A) INCORRETO: porque o código-fonte não está disponível em um ambiente de pré-produção e não é possível descobrir todos os defeitos B) CORRETO: porque essa é uma prática recomendada para fazer a varredura de vulnerabilidades em caixa cinza antes da implementação C) CORRETO: porque essa é uma prática recomendada para verificar se todos os pontos de entrada não estão vulneráveis D) INCORRETO: porque o código-fonte não está disponível em um ambiente de pré-produção E) INCORRETO: porque o código-fonte não está disponível em um ambiente de pré-produção	STE 2.1.1	K2	1
8	c	A) INCORRETO: porque a verificação das regras de codificação de segurança deve ser feita após a conclusão do conjunto de regras de requisitos de segurança B) INCORRETO: porque os testes dinâmicos são executados C) CORRETO: porque há apenas verificações estáticas e elas são bem ordenadas D) INCORRETO: porque os testes dinâmicos são executados	STE-2.1.2	K2	1
9	a	A) CORRETO: porque abrange os principais cenários para a segurança funcional especificada no requisito B) INCORRETO: porque testa apenas testes válidos C) INCORRETO: porque testa apenas condições inválidas D) INCORRETO: porque se expande para o teste de penetração	STE-2.2.1	K3	1
10	b, c	A) INCORRETO: porque as modificações de funções e direitos devem ser revisadas B) CORRETO: porque os direitos e funções definidos ou modificados devem ser revisados	STE-2.2.2	K2	1

Q	C	Explicação / Justificativa	LO	K	P
		C) CORRETO: porque as modificações de funções e direitos devem ser verificadas (correção) e validadas (alinhadas com as necessidades da pessoa) D) INCORRETO: porque não sabemos quais modificações são aplicadas às diferentes contas. E) INCORRETO: porque também precisamos verificar a revogação do acesso ao aplicativo.			
11	b	A) INCORRETO: porque descreve o monitoramento de recursos do sistema, não o teste de autenticação. B) Está correto. Essas são técnicas válidas de teste de autenticação mencionadas no programa de estudos para verificar os mecanismos de autenticação. C) INCORRETO: porque isso descreve o teste de autorização, não o teste de autenticação. D) INCORRETO: porque isso descreve o teste de desempenho, não o teste de autenticação.	STE-2.2.3	K2	1
12	a	A) CORRETO: porque descreve a abordagem de teste completa para controles de proteção de dados. B) INCORRETO: porque, embora o desempenho do sistema seja uma consideração, o foco exclusivo na velocidade e na eficiência oferece uma visão incompleta dos testes de proteção de dados. C) INCORRETO: porque o teste das interações do usuário e dos elementos da tela aborda apenas o nível superficial dos recursos de segurança. D) INCORRETO: porque representa apenas uma pequena parte dos testes de proteção de dados.	STE-2.2.4	K2	1
13	a	A) CORRETO: porque há relatórios e métricas de desempenho de segurança disponíveis que podem ser usados para determinar se você atingiu o nível correto de proteção. B) INCORRETO: porque a autenticação forte é apenas um aspecto do endurecimento. C) INCORRETO: porque o equilíbrio não é necessário. As áreas mais críticas podem justificar um melhor endurecimento. D) INCORRETO: pois há o risco de o hacker não informar o que foi encontrado.	STE-2.2.5	K2	1
14	b	A) INCORRETO: porque isso já foi feito com a criação dos testes de alto nível. B) CORRETO: porque o uso dos testes de alto nível para criar os testes manuais e realizar a execução faz parte da implementação do teste de segurança C) INCORRETO: porque ocorrerá depois que os testes forem executados D) INCORRETO: porque isso já foi feito com a criação dos testes de alto nível.	STE-3.1.1	K2	1
15	c	A) INCORRETO: porque o sistema não precisa e provavelmente não deve ser conectado B) INCORRETO: porque pode ser útil, mas não é uma característica principal C) CORRETO: porque quanto mais o ambiente de teste imitar a produção, mais válido será o teste. Isso é particularmente verdadeiro quando se trata de direitos de acesso e configurações de delegação.	STE-3.1.2	K2	1

Q	C	Explicação / Justificativa	LO	K	P
		D) INCORRETO: porque inclui plug-ins que não estão em produção, o que pode resultar em falsos positivos e falsos negativos nos testes			
16	b	A) INCORRETO: porque os avisos não exigem necessariamente uma correção B) CORRETO: porque, do ponto de vista dos testes de segurança, os avisos do compilador indicam possíveis problemas que podem levar a uma vulnerabilidade de segurança C) INCORRETO: porque pode ser verdade, mas não está relacionado a testes de segurança D) INCORRETO: porque pode ser verdade, mas não está relacionado a testes de segurança	STE-3.2.1	K2	1
17	a	A) CORRETO: porque o projeto de teste de segurança no nível de integração de componentes deve incluir testes de segurança de APIs integradas e fluxos integrados configurados com foco na confidencialidade e na integridade entre os componentes. B) INCORRETO: porque esse é um teste de integração funcional que verifica apenas a conectividade da API. De acordo com o programa de estudos, os testes de segurança em nível de integração devem se concentrar em aspectos de segurança como autorização, confidencialidade e integridade dos fluxos integrados, e não apenas na capacidade de conexão. C) INCORRETO: porque, embora a confiabilidade do fornecedor seja importante, essa é uma atividade de auditoria. O programa de estudos exige especificamente o teste de segurança real dos componentes integrados para verificar se estão livres de vulnerabilidades, e não apenas a verificação das credenciais do fornecedor. D) INCORRETO: porque esse é um teste de desempenho em nível de integração, não um teste de segurança. De acordo com o programa de estudos, os testes de segurança devem se concentrar nas possíveis vulnerabilidades e nos vetores de ataque que surgem das interações dos componentes, e não em suas características de desempenho.	STE-3.2.2	K2	1
18	a	A) CORRETO: Essa é a melhor prática de segurança em comparação com as outras B) INCORRETO: porque o número de tentativas não é quantificado. C) INCORRETO: porque reutilizar uma senha antiga não é uma boa prática, pois pode comprometer sua segurança e privacidade on-line. D) INCORRETO: pois definitivamente não seria uma boa prática de segurança armazenar senhas não criptografadas no bloco de notas.	STE-3.2.3	K3	1
19	a	A) CORRETO: pois os padrões são aprovados por um órgão de conhecimento reconhecido B) INCORRETO: pois os padrões do setor e os padrões de fato não são obrigatórios C) INCORRETO: pois os padrões não são obrigatórios. D) INCORRETO: pois não há correlação entre o nível de detalhe e as práticas recomendadas, ou seja, existem práticas recomendadas muito detalhadas.	STE-4.1.1	K3	1

Q	C	Explicação / Justificativa	LO	K	P
20	c, e	A) INCORRETO: pois os CWEs não contêm nenhum caso de teste (a camada de abstração CVE está ausente) B) INCORRETO: pois os CWEs não contêm explorações (a camada de abstração CVE está ausente). C) CORRETO: pois o CWE agrupa diferentes tipos de ataque, o CWSS os prioriza e os CVSs são vulnerabilidades específicas para um determinado CWE. D) INCORRETO: pois os CWSSs não contêm casos de teste (a camada de abstração CVE está ausente) E) CORRETO: pois o CVE deixa para o testador de segurança a tarefa de derivar casos de teste específicos	STE-4.2.1	K3	1
21	d	A) INCORRETO: pois os parâmetros de contexto podem ter um impacto no comportamento do aplicativo B) INCORRETO: pois os oráculos de teste para aplicativos sem um contexto específico podem ser usados com eficiência para testes de segurança C) INCORRETO: pois os oráculos de teste para aplicativos sem um contexto específico podem ser usados com eficiência para testes de segurança D) CORRETO: se todos os parâmetros de um aplicativo forem padrão, os oráculos de teste poderão ser reutilizados diretamente para testes de segurança	STE-4.3.1	K2	1
22		A) CORRETO: pois uma nomenclatura consistente permite uma comunicação mais fácil (1a), o conhecimento especializado reutiliza o conhecimento especializado em segurança (2b), o benchmarking demonstra facilmente a eficácia das atividades de teste de segurança aplicadas (3d) e a visão geral holística da segurança por um grupo de especialistas experientes pode verificar novamente a integridade das atividades de teste de segurança. B) 3c INCORRETO: (o benchmarking não fornece necessariamente nenhuma evidência de integridade) 4d INCORRETO: (a visão geral holística da segurança não fornece nenhuma evidência de eficácia. C) 1d INCORRETO: (a nomenclatura não fornece nenhuma evidência de eficácia), 2a INCORRETO: (o conhecimento especializado não necessariamente limita a comunicação) 3b INCORRETO: (o benchmarking não permite necessariamente a reutilização do conhecimento especializado) D) 1b INCORRETO: (a nomenclatura não reutiliza o conhecimento especializado em segurança), 2d INCORRETO: (o conhecimento especializado não fornece necessariamente nenhuma evidência de eficácia), 3a INCORRETO: (a avaliação comparativa não permite uma comunicação mais fácil)	STE-4.3.2	K3	1
23	b, c	A) INCORRETO: Levar as atividades de teste de segurança a um ponto de encerramento para que os testes possam ser mantidos e realizados regularmente para dar suporte a quaisquer novos requisitos de segurança e/ou detectar novas ameaças. B) CORRETO: uma vez que a empresa é altamente dependente de seus fornecedores, há uma chance maior de obter sucesso falsificando a identificação de um fornecedor	STE-5.1.1	K3	1

Q	C	Explicação / Justificativa	LO	K	P
		C) CORRETO: uma vez que a empresa é altamente dependente de seus fornecedores, o faturamento de um fornecedor pode ser mais importante para a contabilidade do que o de outros D) INCORRETO: pois não aproveita o contexto organizacional. E) INCORRETO: pois não aproveita o contexto organizacional			
24	a	A) CORRETO: a aviação é fortemente regulamentada e deve ser considerada pelo testador de segurança B) INCORRETO: Embora isso tenha que ser testado, o teste visa mais a um requisito funcional e não é o escopo do teste de segurança. Se houver efeitos colaterais negativos, isso deve ser testado em vez de ser ignorado C) INCORRETO: pois o tempo/orçamento não é uma restrição em nenhum contexto regulamentado. D) INCORRETO: pois não aproveita o contexto organizacional e não fornece nenhuma orientação ao se concentrar nas atividades de teste	STE-5.2.1	K3	1
25	d	A) INCORRETO: pois as atividades de teste contínuas podem borrar os rastros de um incidente de segurança real. Além disso, relatar somente depois de concluir todas as atividades de teste pode ser tarde demais no caso de um incidente grave B) INCORRETO: pois um invasor também pode ser um insider. Veja também a) por que o teste contínuo não é uma solução válida C) INCORRETO: A interrupção de um sistema pode causar perda de rastros no caso de um incidente. Embora essa possa ser uma solução válida em alguns casos, um testador de segurança não tem autoridade para decidir isso por conta própria D) CORRETO: pois uma empresa deve ter Mecanismos de Resposta a Incidentes em funcionamento e, após a comunicação de um incidente, devem ser realizados processos para investigar o incidente comunicado	STE-5.3.1	K4	2
26	a	A) CORRETO: conforme mencionado no programa de estudos B) INCORRETO: Nem todos os ataques estão começando com engenharia social C) INCORRETO: A exploração/obtenção de acesso é feita após a coleta de informações (por exemplo, por meio de engenharia social) D) INCORRETO: A etapa de obtenção de acesso está ausente, portanto, nenhum ataque é realizado	STE-5.3.1	K4	2
27	a	A) CORRETO: conforme mencionado no programa de estudos B) INCORRETO: Somente as atividades de teste de segurança estática não conseguirão encontrar todas as vulnerabilidades C) INCORRETO: O SAST e o DAST podem ser realizados, mas devem ser complementados com D) INCORRETO: atividades e verificações adicionais de testes de segurança E) INCORRETO: Não há necessidade documentada de manter os testes de segurança em sincronia com os testes manuais	STE-6.1.	K2	1
28	d, e	A) CORRETO: como no programa de estudos	STE-6.1.2	K4	2

Q	C	Explicação / Justificativa	LO	K	P
		B) INCORRETO: as atividades do modelo em cascata precisam ser planejadas com antecedência, o que pode causar mudanças necessárias durante a execução C) INCORRETO: A maioria das organizações que usam DevOps tem uma equipe de segurança verificando a produção durante a operação. Não é certo que a equipe de DevOps esteja envolvida D) CORRETO: ambos os modelos de desenvolvimento de software permitem mudanças ad hoc nas tarefas e o uso de equipes capacitadas quando necessário E) CORRETO: O modelo de desenvolvimento Ágil permite mudanças ad hoc no plano quando necessário			
29	c	A) Incorreto de acordo com o glossário B) Incorreto, não há provas para essa afirmação C) CORRETO: conforme mencionado no programa de estudos D) INCORRETO	STE-6.2.1	K3	1
30	c	A) INCORRETO: de acordo com o glossário B) INCORRETO: não há provas para essa afirmação C) CORRETO: conforme mencionado no programa de estudos D) INCORRETO	STE-6.2.2	K2	1
31	b, d	A) INCORRETO: pois um relatório de teste deve conter todas as informações necessárias para entender os resultados. Ele não precisa de nenhum histórico sobre o testador específico. B) CORRETO: pois os critérios de aceitação específicos do projeto não fazem necessariamente parte do OWASP Top-10. C) INCORRETO: pois a OWASP lista as vulnerabilidades de práticas recomendadas, mas os critérios de aceitação dependem de um contexto comercial específico. D) CORRETO: pois um pentest tem uma visão de caixa preta desse sistema e não pode testar nenhum aspecto de caixa branca. E) INCORRETO: pois existem muitos guias de estilo de código de segurança específicos do contexto, que não podem ser refletidos por um OWASP genérico.	STE-7.1.1	K2	1
32	a, c	A) CORRETO: pois os testes de segurança sem nenhuma estrutura envolvente e iterações regulares não geram nenhum valor sistematicamente agregado. B) INCORRETO: pois uma frequência anual pode ser muito baixa para sistemas muito críticos e pode ser muito alta para uma ferramenta que é bom ter. C) CORRETO: pois os testes de segurança ajudam a identificar as vulnerabilidades o mais cedo possível D) INCORRETO: pois as vulnerabilidades comunicadas diariamente podem ser irrelevantes para um contexto específico (por exemplo, sem conexão com a Internet).	STE-7.2.1	K2	1

Q	C	Explicação / Justificativa	LO	K	P
		E) INCORRETO: pois podem existir vulnerabilidades identificadas que são irrelevantes para um contexto específico ou que não precisam de nenhuma correção, já que existem outros sistemas de atenuação (por exemplo, um firewall específico). Por outro lado, podem existir vulnerabilidades, para as quais o prazo de 6 meses pode ser muito longo para vulnerabilidades identificadas e exploráveis com gravidade alta ou crítica.			
33	a	A) CORRETO: pois a adição de objetos de teste adicionais a um plano de teste pode ser usada para identificar pontos fracos adicionais (1c), a adição de abordagens de teste adicionais pode ser usada para trazer insights adicionais sobre um determinado sistema (2a) e uma cobertura de teste aprimorada ao se ater a determinados objetos de teste e abordagens de teste pode ser usada para identificar pontos fracos adicionais B) INCORRETO: pois 1b INCORRETO: (objetos de teste adicionais não são conhecidos pelo ISMS) e 2d INCORRETO: (abordagens de teste adicionais não tornam nenhum sistema de TI mais seguro). C) INCORRETO: pois 4b está errado (o aumento da automação da execução de testes de segurança não aumenta o ISMS de forma alguma, nem identifica outros pontos fracos. D) INCORRETO: pois 1d está errado (objetos de teste adicionais não tornam nenhum sistema de TI mais seguro), 2c está errado (abordagens de teste adicionais não identificam novos componentes) e 4a está errado (o aumento da automação da execução de testes de segurança não aumenta o ISMS de forma alguma, nem gera novas percepções sobre um determinado sistema)	STE-7.3.1	K3	1
34	a	A) CORRETO: resposta correta é A (explicada no Syllabus) B) INCORRETO: Todos os testes de segurança geram percepções quantificáveis sobre a segurança de um sistema que podem ser usadas para medir a eficácia do ISMS. C) INCORRETO: O número de testes de segurança não se correlaciona com a qualidade da segurança. D) INCORRETO: A eficácia de um ISMS é maior quanto mais técnicas de teste de segurança forem usadas.	STE-7.3.2	K2	1
35	b	A) INCORRETO: pois o nome do testador de segurança e a estrutura do teste são irrelevantes B) CORRETO: pois o ambiente de teste, as pré-condições predefinidas dos testes executados, os dados de teste usados, o procedimento de execução do teste e o comportamento detectado podem representar dados confidenciais. C) INCORRETO: pois a lista de desenvolvedores nomeados, o método de desenvolvimento de software identificado e as ferramentas de desenvolvimento são irrelevantes. D) INCORRETO: pois as funções de codificação, bem como a cobertura do teste funcional, são irrelevantes.	STE 8.1.1	K2	1
36	a, d	A) CORRETO: pois as vulnerabilidades identificadas ainda podem perder algumas informações antes da mitigação. B) INCORRETO: pois não é tarefa do testador de segurança fazer uma estimativa de esforço para uma vulnerabilidade identificada.	STE 8.2.1	K3	1

Q	C	Explicação / Justificativa	LO	K	P
		C) INCORRETO: pois não é tarefa do testador de segurança criar um projeto sobre como atenuar uma vulnerabilidade identificada. D) CORRETO: pois é importante verificar novamente se a vulnerabilidade identificada pode ser explorada na produção E) INCORRETO: pois não é tarefa do engenheiro de segurança reparar imediatamente qualquer descoberta.			
37	a, d	A) CORRETO: pois o desligamento de um recurso específico pode atenuar um risco identificado. B) INCORRETO: pois depende do tipo de vulnerabilidade se essa técnica for bem-sucedida. C) INCORRETO: pois não se pode esperar que todas as vulnerabilidades sejam bloqueadas automaticamente em um Web Application Firewall. D) CORRETO: pois adicionar controles de segurança pode reduzir o risco E) INCORRETO: pois a exclusão de vulnerabilidades pode ser muito cara e demorada, portanto, outras oportunidades devem ser analisadas com antecedência para reduzir o risco muito antes.	STE 8.2.2	K3	1
38	a	A) CORRETO: O SCA é uma verificação muito rápida dos componentes em uso e deve ser executado antes de qualquer outra verificação. B) INCORRETO: Embora o SAST garanta que nenhuma vulnerabilidade de segurança permaneça desconhecida, ele se concentra no código do aplicativo C) INCORRETO: Isso requer que o aplicativo esteja em execução. D) INCORRETO: Isso exige que o desenvolvimento do aplicativo seja feito em um estágio posterior	STE 9.1.1	K3	1
39	a	A) CORRETO: O DAST é um scanner dinâmico B) INCORRETO: A SA não é dinâmica C) INCORRETO: O SCA é um método de teste estático D) INCORRETO:. SAST	STE 9.2.1	K2	1
40	a	A) CORRETO: pois o código pode ser analisado B) INCORRETO: Um projeto pode ser revisado manualmente C) INCORRETO: O código pode comprar o serviço não pode D) INCORRETO: Os processos podem ser monitorados, mas não analisados estaticamente	STE 9.2.2	K2	1