| | |
|---|---|
| Ejemplo de Examen: | **Respuestas** |
| Versión: | **ES - V01.00** |
| Versión de Ejemplo de Examen original: | **1.0.1** |
| Modelo: | **A** |
| Correspondiente al programa de estudio: | **Probador Certificado de ISTQB®, Nivel Avanzado, Ingeniero de Prueba de Seguridad** |

Traducción realizada por

**Spanish Software Testing Qualifications Board**

---

## International Software Testing Qualifications Board

## ISTQB®

---


# Nota sobre Derechos de Propiedad Intelectual



# Responsabilidad del Documento

"**Examination Working Group**" de ISTQB®" es responsable de este documento.

Este documento es mantenido por un equipo de ISTQB® que consiste en el "**Syllabus Working Group**" y el "**Exam Working Group**".

# Agradecimientos

Este documento fue producido por un equipo del ISTQB®.

El equipo agradece al equipo de revisión de "**Examination Working Group**", al "**Syllabus Working Group**" y a "**Exam Working Group**" y a las Comités Miembro por sus sugerencias y entradas.

# Notas de la Versión en Idioma Español

Este Ejemplo de Examen ha sido traducido por Spanish Software Testing Qualifications Board (SSTQB).

**Responsable de la traducción:** Gustavo Márquez Sosa (España)

En una siguiente versión se podrán incorporar aquellas aportaciones que se reciban a partir de la publicación del presente documento. El SSTQB considera conveniente mantener abierta la posibilidad de realizar cambios en los distintos contenidos que publica.

Madrid, 04 de marzo de 2025

# Historial de Revisiones

| Versión | Fecha | Observaciones |
|---|---|---|
| 1.0 | 10/09/2024 | Versión final para aprobación GA |
| 1.0.1 | 31/01/2025 | Versión final después de revisión EWG |

# Tabla de Contenidos

# 1. Introducción

## Propósito de este documento

Las preguntas y respuestas de ejemplo y las justificaciones asociadas en este ejemplo de examen han sido creadas por un equipo de expertos en la materia y redactores de preguntas experimentados con el objetivo de:

- Ayudar a los comités miembro y a los comités de examen de ISTQB® en la redacción de preguntas.
- Proporcionar ejemplos de preguntas de examen a los proveedores de formación y a los candidatos a los exámenes.

Estas preguntas no pueden utilizarse tal cual en ningún examen oficial.

Se debe tener en cuenta que los exámenes reales pueden incluir una amplia variedad de preguntas, y este ejemplo de examen no pretende incluir ejemplos de todos los tipos, estilos o longitudes de preguntas posibles; además, este ejemplo de examen puede ser más difícil o menos difícil que cualquier examen oficial.

## Instrucciones

En este documento encontrará:

- Tabla de respuestas correctas, que incluye para cada respuesta correcta:
  - Nivel K, objetivo de aprendizaje y valor en puntos.
- Conjuntos de respuestas, que incluyen para todas las preguntas:
  - Respuesta correcta.
  - Justificación para cada opción de respuesta.
  - Nivel K, objetivo de aprendizaje y valor en puntos.
- Conjuntos de respuestas adicionales, que incluyen para todas las preguntas [no se aplica a todos los ejemplos de examen]:
  - Respuesta correcta.
  - Justificación para cada opción de respuesta.
  - Nivel K, objetivo de aprendizaje y valor en puntos Las preguntas se encuentran en un documento separado.
  - Nivel K, objetivo de aprendizaje y valor en puntos.
- Las preguntas se encuentran en un documento aparte.

## 2. Guía de Respuestas

| Número de Pregunta (N.º) | Respuesta Correcta | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|
| 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 |
| 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 |

| Número de Pregunta (N.º) | Respuesta Correcta | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|
| 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 |

# 3. Respuestas

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **1** | a | a) Es correcto: la integridad trata de impedir que los datos sean modificados o borrados por cualquier parte no autorizada y se mide por el grado en que un activo sólo permite el acceso y la modificación autorizados.<br>b) No es correcto: El permiso de modificación de los datos no está reservado a los propietarios de los datos, sino que sólo se concede a los usuarios autorizados.<br>c) No es correcto: La política de conservación de datos está sujeta a la política de la organización y a los requisitos de la jurisdicción.<br>d) No es correcto: el acceso de los usuarios debe basarse en la autorización y no en cualquier momento en que un usuario necesite el mismo. | STE-1.1.1 | K2 | 1 |
| **2** | a | a) Es correcto: La confidencialidad en la prueba de seguridad asegura que sólo acceden a los datos sensibles los usuarios autorizados. La prueba de seguridad verifica que los mecanismos de control de acceso son eficaces, impidiendo así el acceso no autorizado a la información confidencial.<br>b) No es correcto: se trata de la integridad.<br>c) No es correcto: se trata de la disponibilidad y de los mecanismos de recuperación rápida tras una incidencia.<br>d) No es correcto: se trata de la respuesta de la organización a las incidencias. | STE-1.1.2 | K2 | 1 |
| **3** | b | a) No es correcto. Se trata de una descripción de la prueba de seguridad en general.<br>b) Es correcta. La auditoría de seguridad evalúa los procesos y las infraestructuras de seguridad de una organización y es un tipo de técnica de prueba estática.<br>c) No es correcta. Aunque el objetivo está bien, la auditoría se concentra en los procesos y controles<br>d) No es correcto. Las auditorías se concentran en los procesos y los controles | STE-1.2.1 | K2 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **4** | a | a) Es correcto: todos los usuarios son tratados como no fiables y se les exige autenticación y autorización antes de que puedan acceder a cualquier recurso.<br>b) No es correcto: Una red tradicional es aquella en la que todos los dispositivos y usuarios son de confianza por defecto.<br>c) No es correcto: Una arquitectura de confianza cero se refiere a un modelo de seguridad que no confía intrínsecamente en nada dentro de la red.<br>d) No es correcto: Un sistema de Confianza Cero asegura que nadie pueda acceder a los datos a menos que disponga de las credenciales adecuadas. | STE-1.3.1 | K2 | 1 |
| **5** | a, c | a) Es correcto: Confianza Cero verifica la identidad del usuario, sus privilegios, así como la identidad del dispositivo y la seguridad de cada acceso. Los inicios de sesión y las conexiones se interrumpen periódicamente, lo que obliga a volver a verificar continuamente a los usuarios y los dispositivos.<br>b) No es correcto: Las cuentas no humanas también deben ser monitorizadas.<br>c) Es correcta: el acceso concedido a los recursos debe registrarse de forma permanente y con una marca de tiempo.<br>d) No es correcto: El cifrado y la restricción de accesos a los activos se basan en políticas organizativas.<br>e) No es correcto: Limitar los controles de acceso a aplicaciones, recursos, datos y activos específicos, en lugar de a la red en general. | STE-1.3.2 | K3 | 1 |
| **6** | c | a) No es correcto. La alineación con OWASP y las auditorías de seguridad son esenciales para asegurar la seguridad del software.<br>b) No es correcto. Los parches y las actualizaciones periódicas son fundamentales para hacer frente a las vulnerabilidades.<br>c) Es correcto. La personalización del equipo es importante pero no está directamente ligada a asuntos de interés relativos a la | STE-1.4.1 | K2 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| | | seguridad.<br>d) No es correcta. La conformidad de las licencias asegura un uso adecuado, lo que puede afectar indirectamente a la seguridad. | | | |
| **7** | b, c | a) Es incorrecto porque el código fuente no está disponible en un entorno de preproducción y no es posible descubrir todos los defectos<br>b) Es correcta porque se trata de una buena práctica realizar un escaneado de vulnerabilidades de caja gris antes del despliegue<br>c) Es correcta porque se trata de una buena práctica para comprobar que todos los puntos de entrada no son vulnerables<br>d) No es correcto porque el código fuente no está disponible en un entorno de preproducción<br>e) No es correcto porque el código fuente no está disponible en un entorno de preproducción | STE 2.1.1 | K2 | 1 |
| **8** | c | a) No es correcto porque la comprobación de las reglas de codificación de seguridad debe realizarse una vez completado el conjunto de reglas de requisitos de seguridad.<br>b) No es correcto porque las pruebas dinámicas se ejecutan<br>c) Es correcta porque sólo hay comprobaciones estáticas y están bien ordenadas<br>d) No es correcto porque se ejecutan pruebas dinámicas | STE-2.1.2 | K2 | 1 |
| **9** | a | a) Es correcta porque cubre los principales escenarios para la seguridad funcional especificados en el requisito<br>b) No es correcta porque sólo prueba las pruebas válidas<br>c) No es correcta porque sólo prueba condiciones no válidas<br>d) No es correcto porque se amplía a pruebas de penetración | STE-2.2.1 | K3 | 1 |
| | | | | | |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **10** | b, c | a) No es correcto porque las modificaciones de roles y derechos deben ser revisadas<br>b) Es correcto porque deben revisarse los derechos y roles establecidos o modificados<br>c) Es correcto porque las modificaciones de roles y derechos deben ser verificadas (corrección) y validadas (alineadas con las necesidades de la persona)<br>d) No es correcto porque no sabemos qué modificaciones se aplican a las diferentes cuentas.<br>e) No es correcto porque tenemos que comprobar también la revocación del acceso a la aplicación. | STE-2.2.2 | K2 | 1 |
| **11** | b | a) No es correcto porque describe la monitorización de los recursos del sistema, no la prueba de autenticación.<br>b) Es correcto se trata de técnicas de prueba de autenticación válidas mencionadas en el programa de estudio para verificar los mecanismos de autenticación.<br>c) No es correcto porque describe la prueba de autorización, no la prueba de autenticación.<br>d) No es correcto porque describe la prueba de rendimiento, no la prueba de autenticación. | STE-2.2.3 | K2 | 1 |
| **12** | a | a) Es correcto porque describe el enfoque de prueba completo para los controles de protección de datos.<br>b) No es correcto porque, aunque el rendimiento del sistema es una consideración, concentrarse exclusivamente en la velocidad y la eficiencia proporciona una visión incompleta de las pruebas de protección de datos.<br>c) No es correcto porque probar las interacciones del usuario y los elementos de la pantalla sólo aborda el nivel superficial de las prestaciones de seguridad.<br>d) No es correcto porque representa sólo una pequeña parte de las pruebas de protección de datos. | STE-2.2.4 | K2 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **13** | a | a) Es correcto porque existen informes y métricas sobre el rendimiento de la seguridad que pueden utilizarse para determinar si se ha alcanzado el nivel adecuado de fortificación.<br>b) No es correcto porque la autenticación fuerte es sólo un aspecto del fortificado.<br>c) No es correcto porque el equilibrio no es necesario. Las áreas más críticas pueden justificar un mejor fortificado.<br>d) No es correcto porque existe el peligro de que el jáquer no le diga lo que se ha encontrado. | STE-2.2.5 | K2 | 1 |
| **14** | b | a) No es correcto porque esto ya se ha hecho con la creación de las pruebas de alto nivel.<br>b) Es correcto porque el uso de las pruebas de alto nivel para crear las pruebas manuales y realizar la ejecución forma parte de la implementación de pruebas de seguridad.<br>c) No es correcto porque esto ocurrirá después de que se hayan ejecutado las pruebas<br>d) No es correcto porque esto ya se ha hecho con la creación de las pruebas de alto nivel. | STE-3.1.1 | K2 | 1 |
| **15** | c | a) No es correcto porque el sistema no necesita estar conectado y probablemente no debería estarlo<br>b) No es correcto porque puede ser útil, pero no es una característica principal<br>c) Es correcto porque cuanto más se asemeje el entorno de prueba a la producción, más válidas serán las pruebas. Esto es especialmente cierto cuando se trata de los derechos de acceso y la configuración de la delegación.<br>d) No es correcto porque incluye complementos que no están en producción, lo que podría dar lugar tanto a falsos positivos como a falsos negativos de las pruebas | STE-3.1.2 | K2 | 1 |
| | | | | | |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **16** | b | a) No es correcto porque las advertencias no requieren necesariamente una corrección<br>b) Es correcto porque, desde el punto de vista de la prueba de seguridad, las advertencias del compilador indican posibles dificultades que podrían dar lugar a una vulnerabilidad de seguridad<br>c) No es correcto porque puede ser cierto, pero no está relacionado con la prueba de seguridad Prueba<br>d) No es correcto porque puede ser cierto, pero no está relacionado con la prueba de seguridad | STE-3.2.1 | K2 | 1 |
| **17** | a | a) Es correcto porque el diseño de pruebas de seguridad a nivel de integración de componentes debe incluir pruebas de seguridad de API integradas y flujos integrados configurados que se concentren en la confidencialidad y la integridad entre componentes.<br>b) No es correcto porque se trata de una prueba de integración funcional que sólo verifica la conectividad de la API. Según el programa de estudio, las pruebas de seguridad a nivel de integración deben concentrarse en aspectos de seguridad como la autorización, la confidencialidad y la integridad de los flujos integrados, no sólo en la capacidad de conexión.<br>c) No es correcto porque, aunque la fiabilidad del proveedor es importante, se trata de una actividad de auditoría. El programa de estudio exige específicamente una prueba de seguridad real de los componentes integrados para verificar que están libres de vulnerabilidades, no sólo comprobar las credenciales del proveedor.<br>d) No es correcto porque se trata de una prueba de rendimiento a nivel de integración, no de una prueba de seguridad. Según el programa de estudio, las pruebas de seguridad deben concentrarse en las vulnerabilidades potenciales y los vectores de ataque que surgen de las interacciones de los componentes, no | STE-3.2.2 | K2 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| | | en sus características de rendimiento. | | | |
| **18** | a | a) Es correcto. Es la mejor práctica de seguridad en comparación con las demás.<br>b) No es correcto porque no se cuantifica el número de intentos.<br>c) No es correcto porque la reutilización de una contraseña antigua no es una buena práctica, ya que puede comprometer su seguridad en línea y su privacidad.<br>d) No es correcto porque definitivamente no sería una buena práctica de seguridad almacenar contraseñas no cifradas en el bloc de notas. | STE-3.2.3 | K3 | 1 |
| **19** | a | a) Es correcto, porque los estándares están aprobados por un cuerpo de conocimiento reconocido<br>b) No es correcto, porque los estándares industriales y de-facto-estándares no son obligatorios<br>c) No es correcto, porque los estándares no son obligatorios.<br>d) No es correcto, ya que no existe correlación entre el nivel de detalle y las buenas prácticas, es decir, existen buenas prácticas muy detalladas. | STE-4.1.1 | K3 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **20** | c, e | a) No es correcto ya que las enumeraciones de debilidades comunes no contienen ningún caso de prueba (falta la capa de abstracción vulnerabilidades y exposiciones comunes).<br>b) No es correcto ya que las enumeraciones de debilidades comunes no contienen no contienen explotables (falta la capa de abstracción vulnerabilidades y exposiciones comunes).<br>c) Es correcto ya que la enumeración de debilidades comunes agrupa diferentes tipos de ataques, el sistema de puntuación de debilidades comunes los prioriza y los cvs son vulnerabilidades específicas para una enumeración de debilidades comunes determinada.<br>d) no es correcto ya que los sistemas de puntuación de debilidades comunes no contienen casos de prueba (falta la capa de abstracción vulnerabilidades y exposiciones comunes).<br>e) Es correcto, ya que las Vulnerabilidades y Exposiciones Comunes dejan en manos del probador de seguridad la obtención de casos de prueba específicos. | STE-4.2.1 | K3 | 1 |
| **21** | d | a) No es correcto, ya que los parámetros de contexto podrían tener un impacto en el comportamiento de la app<br>b) No es correcto, ya que los oráculos de prueba para aplicaciones sin un contexto específico pueden utilizarse eficazmente para pruebas de seguridad.<br>c) No es correcto, ya que los oráculos de prueba para aplicaciones sin un contexto específico pueden utilizarse eficazmente para las pruebas de seguridad.<br>d) Es correcto: si todos los parámetros de una aplicación son estándar, los oráculos de prueba pueden reutilizarse directamente para las pruebas de seguridad. | STE-4.3.1 | K2 | 1 |
| | | | | | |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **22** | a | a) Es correcta, ya que una nomenclatura consistente facilita la comunicación (1a), el conocimiento experto reutiliza el conocimiento experto en seguridad (2b), la evaluación comparativa demuestra fácilmente la efectividad de las actividades de pruebas de seguridad aplicadas (3d) y la visión holística de la seguridad por parte de un grupo de expertos experimentados puede volver a comprobar la compleción de las actividades de pruebas de seguridad.<br>b) 3c no es correcta (la evaluación comparativa no aporta necesariamente ninguna prueba de completitud) 4d no es correcta (la visión global de la seguridad no aporta ninguna prueba de efectividad.<br>c) 1d no es correcta (la nomenclatura no aporta necesariamente ninguna prueba de efectividad), 2a no es correcta (el conocimiento experto no se limita necesariamente a la comunicación) 3b no es correcta (la evaluación comparativa no permite necesariamente la reutilización del conocimiento experto)<br>d) 1b no es correcta (la nomenclatura no reutiliza los conocimientos de los expertos en seguridad), 2d no es correcta (los conocimientos de los expertos no aportan necesariamente ninguna prueba de efectividad), 3a no es correcta (la evaluación comparativa no permite simplemente comunicar) | STE-4.3.2 | K3 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **23** | b, c | a) No es correcto: Llevar las actividades de prueba de seguridad a un punto de cierre para que las pruebas puedan mantenerse y realizarse de forma regular para apoyar cualquier nuevo requisito de seguridad y/o detectar nuevas amenazas.<br>b) Es correcto, ya que la empresa depende en gran medida de sus proveedores, hay más posibilidades de tener éxito falsificando la identidad de un proveedor<br>c) Es correcta, puesto que la empresa depende en gran medida de sus proveedores, la facturación de un proveedor podría ser más importante para la contabilidad que la de otros<br>d) No es correcta, porque no aprovecha el contexto organizativo.<br>e) No es correcta, porque no aprovecha el contexto organizativo | STE-5.1.1 | K3 | 1 |
| **24** | a | a) Es correcto, la aviación está fuertemente regulada lo que tiene que ser tenido en cuenta por el probador de seguridad<br>b) No es correcto. Aunque haya que probarlo, la prueba apunta más a un requisito funcional y no es alcance de las pruebas de seguridad. Si puede haber efectos secundarios negativos, hay que probarlo en lugar de ignorarlo.<br>c) No es correcto, ya que el tiempo/presupuesto no es una restricción en ningún contexto regulado.<br>d) No es correcta, porque no aprovecha el contexto organizativo y no da ninguna orientación a la hora de concentrarse en las actividades de prueba. | STE-5.2.1 | K3 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **25** | d | a) No es correcto, ya que las actividades de prueba continuas pueden difuminar los rastros de una incidencia de seguridad real. También informar sólo después de terminar todas las actividades de prueba podría ser demasiado tarde en caso de una incidencia grave.<br>b) No es correcto, ya que un atacante también podría ser un infiltrado. Véase también a) por qué las pruebas continuas no son una solución válida.<br>c) No es correcto, detener un sistema podría causar la pérdida de trazas en caso de incidencia. Aunque podría ser una solución válida en algunos casos, un probador de seguridad no tiene autoridad para decidir esto por sí mismo.<br>d) Es correcta, ya que una empresa debe contar con mecanismos de respuesta a incidentes que funcionen y, tras informar de un incidente, deben llevarse a cabo procesos para investigar el incidente del que se ha informado. | STE-5.3.1 | K4 | 2 |
| **26** | a | a) Como se menciona en el programa de estudio<br>b) No todos los ataques parten de la ingeniería social<br>c) La explotación/obtención de acceso se realiza tras la recopilación de información (por ejemplo, mediante ingeniería social)<br>d) Falta el STEP de obtención de accesibilidad, por lo que no se realiza ningún ataque | STE-5.3.1 | K4 | 2 |
| **27** | a | a) Correcto como se menciona en el programa de estudio.<br>b) Sólo las actividades de prueba estática de seguridad no podrán encontrar todas las vulnerabilidades<br>c) Pueden realizarse la prueba dinámica de seguridad de las aplicaciones (PDSA) y la prueba estática de seguridad de las aplicaciones (PESA) pero deben complementarse con actividades de pruebas de seguridad adicionales y verificaciones<br>d) No existe una necesidad documentada de sincronizar las pruebas de seguridad con las pruebas manuales | STE-6.1.1 | K2 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **28** | d, e | a) Es correcto como en el programa de estudio.<br>b) No es correcto: las actividades del modelo de cascada tienen que planificarse por adelantado, lo que puede provocar cambios necesarios durante la ejecución.<br>c) No es correcto: La mayoría de las organizaciones que utilizan DevOps cuentan con un equipo de seguridad que verifica en producción durante la operación. No se da el caso de que el equipo DevOps esté implicado.<br>d) Es correcto: Ambos modelos de desarrollo de software habilitan para cambios ad hoc en las tareas y el uso para equipos facilitadores cuando se necesitan.<br>e) Es correcto: El modelo de desarrollo ágil permite cambios de planes ad hoc cuando se necesitan. | STE-6.1.2 | K4 | 2 |
| **29** | c | a) Incorrecto según el glosario.<br>b) Incorrecto, no hay pruebas para tal enunciado.<br>c) Correcto, como se menciona en el programa de estudio.<br>d) Incorrecto. | STE-6.2.1 | K3 | 1 |
| **30** | c | a) No es correcto según el glosario.<br>b) No es correcto, no hay demostración para el tipo de enunciado.<br>c) Es correcta, tal y como se menciona en el programa de estudio.<br>d) No es correcta. | STE-6.2.2 | K2 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **31** | b, d | a) No es correcto ya que un informe de prueba debe contener toda la información necesaria para comprender los resultados. No necesita ningún antecedente sobre el probador específico.<br>b) b) Es correcta ya que los criterios de aceptación específicos de un proyecto no forman parte necesariamente del Top-10 de OWASP.<br>c) No es correcta, ya que OWASP enumera las vulnerabilidades de las buenas prácticas, pero los criterios de aceptación dependen de un contexto empresarial específico.<br>d) Es correcta, ya que un pentest tiene una visión de caja negra sobre ese sistema y no puede probar ningún aspecto de caja blanca.<br>e) No es correcta, ya que existen muchas guías de estilo de código de seguridad específicas para cada contexto, que no pueden reflejarse en una OWASP genérica. | STE-7.1.1 | K2 | 1 |
| **32** | a, c | a) Es correcta, ya que la prueba de seguridad sin ningún marco de trabajo circundante e iteraciones regulares no genera ningún valor añadido sistemático.<br>b) No es correcta ya que una frecuencia anual puede ser demasiado baja para sistemas muy críticos y puede ser demasiado alta para una herramienta «nice-to-have».<br>c) Es correcta, ya que la prueba de seguridad ayuda a identificar las vulnerabilidades lo antes posible.<br>d) d) No es correcta, ya que las vulnerabilidades comunicadas a diario pueden ser irrelevantes para un contexto específico (por ejemplo, sin conexión a Internet).<br>e) No es correcta, ya que pueden existir vulnerabilidades identificadas que sean irrelevantes para un contexto específico o que no necesiten nunca ningún tipo de remedio al existir otros sistemas mitigadores (por ejemplo, un cortafuegos específico). Por otro lado, podrían existir vulnerabilidades para las que el plazo de 6 meses podría ser demasiado largo para | STE-7.2.1 | K2 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| | | vulnerabilidades identificadas y explotables con una severidad alta o crítica. | | | |
| **33** | a | a) Es correcto, ya que añadir objetos de prueba adicionales a un plan de prueba puede servir para identificar debilidades adicionales (1c), añadir enfoques de prueba adicionales puede servir para aportar información adicional sobre un sistema determinado (2a) y mejorar la cobertura de la prueba mientras se mantienen determinados objetos de prueba y enfoques de prueba puede servir para identificar debilidades adicionales.<br>b) No es correcta, ya que 1b no es correcta (los objetos de prueba adicionales no son conocidos por el SGSI) y 2d no es correcta (los enfoques de prueba adicionales no hacen que ningún sistema informático sea más seguro.<br>c) No es correcta, ya que 4b es incorrecta (el aumento de la automatización de la ejecución de pruebas de seguridad no incrementa en nada un SGSI, ni identifica ninguna debilidad adicional.<br>d) No es correcta, ya que 1d es incorrecta (los objetos de prueba adicionales no hacen que ningún sistema de TI sea más seguro), 2c es incorrecta (los enfoques de prueba adicionales no identifican nuevos componentes) y 4a es incorrecta (el aumento de la automatización de la ejecución de la prueba de seguridad no aumenta un SGSI de ninguna manera, ni genera nuevos conocimientos sobre un sistema determinado). | STE-7.3.1 | K3 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **34** | a | a) La respuesta correcta es la A (explicada en el programa de estudio)<br>b) Todas las pruebas de seguridad generan conocimientos cuantificables sobre la seguridad de un sistema que pueden utilizarse para medir la efectividad del SGSI.<br>c) El número de pruebas de seguridad no se correlaciona con la calidad de la seguridad.<br>d) La efectividad de un SGSI es mayor cuantas más técnicas de pruebas de seguridad se utilicen. | STE-7.3.2 | K2 | 1 |
| **35** | b | a) La respuesta correcta es la A (explicada en el programa de estudio)<br>b) Todas las pruebas de seguridad generan conocimientos cuantificables sobre la seguridad de un sistema que pueden utilizarse para medir la efectividad del SGSI.<br>c) El número de pruebas de seguridad no se correlaciona con la calidad de la seguridad.<br>d) La efectividad de un SGSI es mayor cuantas más técnicas de pruebas de seguridad se utilicen. | STE 8.1.1 | K2 | 1 |
| **36** | a, d | a) Es correcta ya que una vulnerabilidad identificada aún podría omitir alguna información antes de su mitigación.<br>b) b) No es correcta ya que no es tarea del probador de seguridad hacer una estimación del esfuerzo para una vulnerabilidad identificada.<br>c) No es correcta ya que no es tarea del probador de seguridad crear un diseño sobre cómo mitigar una vulnerabilidad identificada.<br>d) Es correcta ya que es importante volver a comprobar que la vulnerabilidad identificada puede explotarse en producción.<br>e) No es correcta ya que no es tarea del ingeniero de seguridad reparar inmediatamente cualquier hallazgo. | STE 8.2.1 | K3 | 1 |
| | | | | | |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **37** | a, d | a) Es correcta ya que desactivar una prestación específica puede mitigar un riesgo identificado.<br>b) No es correcta ya que depende del tipo de vulnerabilidad que esta técnica tenga éxito.<br>c) No es correcta ya que no se puede esperar que todas las vulnerabilidades se bloqueen automáticamente en un cortafuegos de aplicaciones web.<br>d) Es correcta ya que añadir controles de seguridad puede reducir el riesgo.<br>e) eo es correcta ya que eliminar vulnerabilidades puede ser muy caro y llevar mucho tiempo, por lo que deberían analizarse otras oportunidades con antelación para mitigar el riesgo mucho antes. | STE 8.2.2 | K3 | 1 |
| **38** | a | a) Es correcto. El análisis de la composición del software (ACS) [en inglés, Software Composition Analysis (SCA)] es una comprobación muy rápida de los componentes en uso y debería ejecutarse antes que cualquier otra comprobación.<br>b) No es correcto. Aunque la prueba estática de seguridad de las aplicaciones (PESA) [en inglés,static application security testing (SAST)] asegura que no quedan vulnerabilidades de seguridad desconocidas, se concentra en el código de la aplicación.<br>c) No es correcto. Esto requiere que la aplicación esté en ejecución.<br>d) No es correcto. Esto requiere que el desarrollo de la aplicación se encuentre en una fase posterior. | STE 9.1.1 | K3 | 1 |
| **39** | a | a) Es correcto. PDSA es una prueba dinámica de seguridad de las aplicaciones (PDSA) [en inglés, dynamic application security testing (DAST)].<br>b) No es correcto. SA no es dinámico<br>c) No es correcto. SCA es un método de prueba estático [en inglés, Software Composition Analysis (SCA)<br>d) No es correcto. prueba estática de seguridad de las aplicaciones (PESA) [EN inglés, static application security testing (SAST) | STE 9.2.1 | K2 | 1 |

| Número de Pregunta (N.º) | Respuesta Correcta | Justificación/Explicación | Objetivo de Aprendizaje (OA) | Nivel K | Cantidad de Puntos |
|---|---|---|---|---|---|
| **40** | a | a) a) Es correcto ya que el código puede ser analizado<br>b) b) No es correcto. Un diseño puede revisarse manualmente<br>c) c) No es correcto. El código puede bu el servicio no puede<br>d) a) No es correcto. Los procesos pueden monitorizarse pero no analizarse estáticamente | STE 9.2.2 | K2 | 1 |