Ejemplo de Examen:	**Preguntas**
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 Especialista, 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 central del ISTQB® que consiste en el "**Syllabus Working Group**" y el "**Exam Working Group**".

Agradecimientos

Este documento fue producido por un equipo del ISTQB®: Dr. Frank Simon (chair), Alain Ribault, Gabriel Firmino Barjollo, Michael Pott, Beata Karpinska, Maria Kispal, Frans Dijkman.

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

Preguntas

Pregunta: 01

Puntos: 01	
¿Cuál de las siguientes opciones describe **MEJOR** el nivel de seguridad de los activos en cuanto a integridad?	
a) Solo los usuarios autenticados deben tener acceso para modificar archivos y aplicaciones b) Solo los propietarios de los archivos pueden tener acceso para modificar datos y establecer la integridad adecuada. c) El historial de registros de intentos no autorizados debe conservarse durante dos años. d) Establecer un proceso que permita a los usuarios acceder a datos sin cambios siempre que lo necesiten.	
Seleccionar **UNA** opción.	

Pregunta: 02

Puntos: 01	
¿Cuál de las siguientes opciones es una alternativa adecuada para describir cómo la prueba de seguridad puede confirmar que la confidencialidad de la información sensible cuenta con las salvaguardas adecuadas?	
a) Verifica que existen controles adecuados que impiden el acceso no autorizado a la información confidencial b) Verifica que existen controles adecuados que garantizan que solo se pueden realizar actualizaciones autorizadas y que todos los datos siguen siendo fiables c) Verifica mecanismos de recuperación rápida para restablecer los servicios rápidamente después de una incidencia d) Verifica que la respuesta de la organización a las incidencias sea efectiva, minimizando los daños y el tiempo de inactividad.	
Seleccionar **UNA** opción.	

Pregunta: 03

Puntos: 01	
¿Cuál de las siguientes opciones describe MEJOR una auditoría de seguridad?	
a) Una evaluación sistemática de la prueba de seguridad y la estrategia de seguridad general en toda la organización b) Una evaluación sistemática de la seguridad del sistema de información mediante la medición de su conformidad con un conjunto de criterios establecidos c) Una evaluación sistemática destinada a impedir que intrusos no autorizados accedan al sistema d) Una evaluación sistemática destinada a reducir los riesgos mediante la identificación de hardware y software sujetos a vulnerabilidad	
Seleccionar **UNA** opción.	

Pregunta: 04

Puntos: 01	
¿Cuál de las siguientes opciones describe la confianza cero?	
a) Cualquier usuario requiere una verificación continua de su identidad, independientemente de su ubicación. b) Por defecto, se confía en cualquier dispositivo y usuario con acceso al sistema. c) Solo los dispositivos dentro de la red de confianza obtienen acceso a los sistemas. d) A todos los usuarios se les concede el nivel de acceso que necesitan.	
Seleccionar **UNA** opción.	

Pregunta: 05

Puntos: 01	

¿Cuál de los siguientes puntos incluiría para verificar que el concepto de confianza cero se ha implementado correctamente?

a) Implementar controles que comprueben cada solicitud de acceso individual a cualquier recurso sensible.
b) Las solicitudes de acceso iniciadas por cuentas de servicio no humanas son siempre de confianza.
c) Verifique que los registros de acceso producidos por el sistema proporcionan un registro permanente y con fecha y hora de todas las actividades.
d) Implemente conjuntos de permisos estándar basados en los roles y responsabilidades de los usuarios.
e) Concentrarse en los controles de acceso a la red externa en lugar de en los controles de aplicaciones, recursos, datos y activos específicos.

Seleccionar **DOS** opciones.	

Pregunta: 06

Puntos: 01	

Términos utilizados en la pregunta

Español	**Inglés**
Open Web Application Security Project (OWASP)	Open Web Application Security Project (OWASP)
OWASP	Open Web Application Security Project (OWASP)

Nota:

- La traducción de “Open Web Application Security Project” es “Proyecto Abierto de Seguridad de Aplicaciones Web”. No se traduce debido a que es el nombre de una fundación
- Open Worldwide Application Security Project (OWASP) es una fundación sin ánimo de lucro que trabaja para mejorar la seguridad del software.

Al utilizar software de código abierto, ¿cuál de los siguientes **NO** es un factor crítico a tener en cuenta a la hora de abordar asuntos de interés relativos a la seguridad?

a) Alineación con OWASP y auditorías de seguridad activas por parte de los colaboradores.
b) Frecuencia y disponibilidad de parches y actualizaciones de seguridad.
c) La capacidad de su equipo para gestionar y personalizar la herramienta para su entorno.
d) Requisitos de licencia y conformidad con las directrices de seguridad del código abierto.

Seleccionar **UNA** opción.	

Pregunta: 07

Puntos: 01	

Información de Contexto

Un banco ha subcontratado el desarrollo de nuevas prestaciones para su portal de clientes, con el fin de mejorar su experiencia de usuario. El desarrollo de las prestaciones ha finalizado y se ha entregado al banco. El banco le llama para que planifique y realice pruebas de seguridad en un entorno de preproducción antes del despliegue.

¿Cuál de las siguientes opciones describe mejor cómo abordaría esta tarea?

a) Ejecutar una prueba de caja blanca para cubrir todo el código fuente y asegurarse de que no hay más defectos antes de la implantación.
b) Ejecutar un escaneo de vulnerabilidades de caja gris para estar seguro de que todas las vulnerabilidades conocidas en el alcance del proyecto, potencialmente explotables por un atacante, están o estarán identificadas.
c) Ejecutar una prueba de caja negra de inyección de defectos para encontrar posibles puntos de entrada vulnerables.
d) Verificar que se han aplicado las normas de codificación de seguridad utilizando una herramienta estática de prueba de la seguridad de la aplicación.
e) Comprobar si las vulnerabilidades detectadas mediante la prueba de caja blanca podrían ser aprovechables.

Seleccionar **DOS** opciones.

Pregunta: 08

Puntos: 01	

Información de Contexto

Como ingeniero de prueba de seguridad del proyecto, se le ha encomendado la tarea de definir las técnicas de prueba de seguridad que deben aplicarse como prueba estática de seguridad.

¿Cuál sería su enfoque?

a) Comprobar que los desarrolladores aplican las reglas de codificación de seguridad, verificar que el diseño ha seguido las buenas prácticas de «seguridad por diseño» y, a continuación, comprobar que los requisitos de seguridad están completos.
b) Comprobar que los desarrolladores aplican las normas de codificación y, a continuación, construir la aplicación y ejecutar algunas inyecciones SQL para comprobar que los campos de entrada están correctamente protegidos contra la inyección SQL.
c) Comprobar que los requisitos de seguridad están completos, comprobar que el diseño ha seguido las buenas prácticas de «seguridad por diseño» y, a continuación, comprobar que los desarrolladores aplican las reglas de codificación de seguridad.
d) Comprobar que el conjunto de requisitos de seguridad es pertinente y completo y, a continuación, ejecutar pruebas de valor frontera en la aplicación construida para comprobar que se evitan los desbordamientos de memoria intermedia mediante la aplicación de reglas de codificación de seguridad específicas.

Seleccionar **UNA** opción.

Pregunta: 09

Puntos: 01	

Información de Contexto

Se le ha dado el siguiente requisito para la prueba de seguridad:

Un usuario podrá solicitar que se restablezca su contraseña. Si realizan esta solicitud, deberán responder correctamente a dos de sus tres preguntas de seguridad. Si responden correctamente, se les enviará un enlace a su correo electrónico. El enlace les llevará a una página en la que podrán restablecer su contraseña. Una vez restablecida, podrán iniciar sesión con la nueva contraseña. Ese enlace dejará de ser válido una hora después de haber sido enviado o si el usuario envía otra solicitud de restablecimiento de contraseña. Si el usuario envía más de dos solicitudes de restablecimiento de contraseña sin completar el restablecimiento, el ID de usuario se bloqueará. Para desbloquear el ID, el usuario deberá ponerse en contacto con el servicio de asistencia.

¿Cuál de las siguientes es la lista mínima de condiciones de prueba para probar adecuadamente la seguridad funcional cubierta por este requisito?

a) Usuario no válido; usuario válido; 2 respuestas correctas; 2 respuestas incorrectas; restablecimiento completo de la contraseña; enlace válido; enlace caducado; dos solicitudes sin restablecimiento; 3 solicitudes sin restablecimiento.
b) Usuario válido; Usuario válido; 2 respuestas correctas; 3 respuestas correctas; restablecimiento completo de la contraseña; enlace válido; dos solicitudes sin restablecimiento.
c) Usuario no válido; Usuario no válido; 2 respuestas incorrectas; enlace caducado; 3 solicitudes sin restablecimiento; caracteres no válidos.
d) Usuario no válido; usuario válido; usuario no válido; usuario válido; 2 respuestas correctas; 2 respuestas incorrectas; desbordamiento de memoria intermedia en cada campo de entrada; inyecciones SQL.

Seleccionar **UNA** opción.	

Pregunta: 10

Puntos: 01	

Información de Contexto

En su organización, usted es responsable de la Gestión de Identificación y Acceso para gestionar y mantener las cuentas y los derechos de los usuarios. Durante los dos últimos meses, ha habido dos nuevas incorporaciones y una persona de la empresa ha cambiado de departamento. Sus perfiles han sido asignados a sus nuevos roles y derechos.

¿Qué técnicas de prueba de seguridad debería probar en función de su responsabilidad?

a) No es necesario probar nada porque se han gestionado las cuentas y los derechos.
b) Revisar los permisos de los roles de la persona que ha cambiado de departamento.
c) Probar los roles y privilegios asignados a los recién llegados para asegurar que están configurados correctamente.
d) No es necesario realizar pruebas porque los recién llegados tienen roles y privilegios básicos y la persona que ha cambiado de departamento tiene menos privilegios que antes.
e) Una vez aplicados los cambios, comprobar si funciona el acceso a las nuevas aplicaciones.

Seleccionar **DOS** opciones.

Pregunta: 11

Puntos: 01	

¿Cuál de las siguientes opciones describe **CORRECTAMENTE** las técnicas de prueba de seguridad para el mecanismo de autenticación?

a) Examinar si los usuarios pueden gestionar los recursos del sistema en función de sus roles.
b) Comprobar los detalles de registro de entrada de fábrica y evaluar los requisitos de seguridad de la contraseña.
c) Verificar los niveles de permiso de los usuarios mediante el análisis de perfiles.
d) Monitorizar los registros de actividad de los usuarios durante el proceso de inicio de sesión.

Seleccionar **UNA** opción.

Pregunta: 12

Puntos: 01	
¿Cuál de los siguientes enunciados describe **MEJOR** cómo probar los controles de protección de datos?	
a) La prueba debe evaluar las medidas de seguridad al comprobar la conformidad del cifrado, los controles de acceso y las prestaciones de enmascaramiento de datos. b) La prueba debe medir exclusivamente la rapidez y la eficiencia con que funcionan las medidas de protección en el sistema. c) La prueba debe examinar cómo interactúan los usuarios con las prestaciones de seguridad a través de elementos de pantalla y controles. d) La prueba debe analizar el rendimiento de los sistemas de almacenamiento de datos cuando las prestaciones de seguridad están activas.	
Seleccionar **UNA** opción.	

Pregunta: 13

Puntos: 01	
Información de Contexto Se le pide a usted que explique los procedimientos para evaluar la fortificación de sistema como ejemplo típico de tecnología de protección.	
¿Qué procedimiento podría seguir para asegurar que los mecanismos de fortificación implantados funcionan según lo esperado?	
a) Monitorizar de cerca diversos informes de rendimiento y métricas de seguridad para determinar si se ha alcanzado el nivel correcto de accesibilidad y autenticación, es decir, que no sea demasiado restrictivo ni demasiado amplio. b) Auditar con frecuencia la autenticación fuerte para asegurar que se mantiene en todo momento un alto nivel de protección contra intrusiones. c) Evaluar los componentes hardware que han sido fortificados y compararlos con otros componentes software fortificados para asegurar que se está alcanzando el equilibrio. d) Reclutar a un jáquer conocido para que lleve a cabo una evaluación independiente de la efectividad del fortificado.	
Seleccionar **UNA** opción.	

Pregunta: 14

Puntos: 01	
Información de Contexto Usted es responsable de todos los aspectos del proceso de prueba de seguridad, incluida la prueba. Para esta tarea en particular, debe utilizar pruebas de alto nivel como base para las pruebas manuales y ejecutarlas desde la perspectiva de un proveedor externo.	
¿Qué tarea de prueba de seguridad se puede realizar en paralelo con esto?	
a) Creación de condiciones y objetivos de prueba de seguridad b) Implementación de pruebas de seguridad c) Evaluación general y suministro de información de la prueba de seguridad d) Análisis y diseño de pruebas de seguridad	
Seleccionar **UNA** opción.	

Pregunta: 15

Puntos: 01	
¿Cuál de las siguientes es una característica principal de un entorno de pruebas de seguridad efectivo?	
a) Estar estrechamente vinculado a los sistemas de producción para mejorar la seguridad en todos los puntos b) Aislar diferentes versiones antiguas de los sistemas operativos para su uso en el entorno c) Imitar el entorno de producción en términos de derechos de acceso d) Incluir todos los complementos del entorno de producción, así como otros complementos que no estén en el entorno de producción, para garantizar la configuración más completa	
Seleccionar **UNA** opción.	

Pregunta: 16

Puntos: 01	
Durante la prueba de componente, ¿qué advertencia del compilador activaría en mayor medida el probador de seguridad?	
a) Las que indican problemas de seguridad que deben solucionarse b) Las que indican posibles dificultades que deben investigarse c) Las que indican problemas de código que causarán defectos de adecuación funcional d) Las que indican malas prácticas de programación que aumentarán la mantenibilidad	
Seleccionar **UNA** opción.	

Pregunta: 17

Puntos: 01	
Información de Contexto Dada la siguiente especificación de diseño: El componente A y el componente B se comunican a través de una **IPA** de **Transferencia de Estado Representativo** [en inglés, Representational State Transfer (**REST**)].	
¿Cuál de las siguientes opciones es un ejemplo de prueba de seguridad realizada a nivel de integración de componentes?	
a) Probar el cifrado de datos durante las llamadas de IPA entre el componente A y el componente B. b) Probar si el componente A puede llamar a la IPA del componente B. c) Probar si los componentes externos son de proveedores de confianza. d) Probar el tiempo de respuesta entre el componente A y el componente B.	
Seleccionar **UNA** opción.	

Pregunta: 18

Puntos: 01	

¿Cuál de las siguientes opciones describe **MEJOR** el procedimiento correcto para la implementación de una prueba de seguridad de extremo a extremo para probar el tratamiento de los intentos fallidos de inicio de sesión por parte del sistema?

a) Antes de la ejecución de la prueba, preparar un generador de contraseñas para cambiar la contraseña al iniciar sesión. Cerrar sesión y luego iniciar sesión con la contraseña recién creada. Tres intentos fallidos de inicio de sesión generarán un mensaje de bloqueo.

b) Después de varios intentos de iniciar sesión, se deberá haber recibido un mensaje de bloqueo, se llama al Servicio de Asistencia para obtener una contraseña temporal por correo. Iniciar sesión con la contraseña temporal, cerrar sesión, volver a iniciar sesión e introducir una nueva contraseña.

c) Después de intentar iniciar sesión varias veces sin éxito, pulsar el botón para obtener un enlace para cambiar la contraseña. Después de obtener el enlace, volver a utilizar la antigua contraseña. El sistema acepta la contraseña.

d) Después del primer intento de usar una contraseña no válida, se extrae una lista de contraseñas del bloc de notas del ordenador para asegurarse de que se está utilizando la contraseña correcta. Se prueba otra contraseña de la lista y funciona.

Seleccionar **UNA** opción.	

Pregunta: 19

Puntos: 01

Información de Contexto

Usted trabaja como gestor de prueba en un banco que está desarrollando una nueva aplicación de banca en línea. La aplicación gestionará datos confidenciales de clientes y transacciones financieras. Se le pide que realice la prueba de seguridad de esa nueva aplicación. No hay requisitos explícitos, por lo que selecciona sus propios casos de prueba a partir de normas y buenas prácticas.

¿Cuáles tres (3) de los siguientes enunciados le guiarán mejor para seleccionar los casos de prueba?

i. Las normas son entradas válidas, ya que están aprobadas por un organismo de conocimiento reconocido.
ii. Los estándares pueden clasificarse en estándares de la industria, estándares de facto y estándares específicos del fabricante. Los estándares de la industria y los estándares de facto son entradas válidas, los estándares del fabricante pueden no ajustarse a un contexto específico.
iii. Como los estándares son obligatorios, son entradas válidas, ya que deben aplicarse en todos los entornos.
iv. Las buenas prácticas no son una entrada válida, ya que suelen ser de muy alto nivel.
v. Los estándares de facto son una buena entrada, ya que a menudo tienen sus raíces en los estándares de la industria.

a) i, ii y v
b) i, ii y iii
c) ii, iii y v
d) iii, iv y v

Seleccionar **UNA** opción.

Pregunta: 20

Puntos: 1	

Términos utilizados en la pregunta

Español	Inglés
Enumeración y Clasificación de Patrones de Ataque Comunes	Common Attack Pattern Enumeration and Classification (CAPEC)
Vulnerabilidades y Exposiciones Comunes	Common Vulnerabilities and Exposures (CVE)
Sistema de Puntuación de Vulnerabilidades Comunes	Common Vulnerability Scoring System (CVSS)
Sistema de Puntuación de Debilidades Comunes	Common Weakness Scoring System (CWSS)
Enumeración de Debilidades Comunes	Common Weakness Enumeration (CWE)

Información de Contexto

Una empresa emergente del sector bancario ha desarrollado un nuevo sistema principal. Hasta ahora, el equipo de desarrollo se ha concentrado en una buena usabilidad y un rendimiento excelente. Antes de ponerlo en marcha, la junta directiva quiere obtener una opinión independiente sobre el nivel de seguridad. Le piden que, como probador de seguridad, realice una prueba de caja negra. La tarea consiste en probar las vulnerabilidades más críticas que podrían aprovecharse en la nueva aplicación bancaria.

Si quiere realizar este trabajo, ¿cómo puede aprovechar los estándares para su tarea?

a) Usted selecciona las debilidades relevantes dentro del estándar Enumeración de Debilidades Comunes y ejecuta los casos de prueba enumerados.
b) Usted selecciona las debilidades relevantes dentro de la Enumeración de Debilidades Comunes, elige los medios disponibles para aprovechar una oportunidad (para atacar la seguridad).
c) Usted selecciona las debilidades relevantes dentro de la Enumeración de Debilidades Comunes, prioriza las Enumeración de Debilidades Comunes seleccionadas basándose en el estándar Sistema de Puntuación de Debilidades Comunes y selecciona las Vulnerabilidades y Exposiciones Comunes relevantes que cubren las Enumeración de Debilidades Comunes priorizadas.
d) Usted selecciona las debilidades relevantes dentro de la Enumeración de Debilidades Comunes, prioriza las Enumeración de Debilidades Comunes seleccionadas basándose en el estándar Sistema de Puntuación de Vulnerabilidades Comunes y obtiene casos de prueba individuales relacionados con la Enumeración de Debilidades Comunes del Sistema de Puntuación de Vulnerabilidades Comunes.
e) Para cada CVE seleccionada, obtiene casos de prueba para la aplicación bancaria y los ejecuta.

Seleccionar **DOS** opciones.	

Pregunta: 21

Puntos: 01	
Cuando se utilizan oráculos de prueba para una aplicación a partir de estándares y buenas prácticas, ¿qué hay que tener en cuenta?	
a) Estos oráculos de prueba son válidos independientemente de cualquier parámetro de la aplicación. b) Estos oráculos de prueba sólo pueden utilizarse como pistas difusas para la prueba de seguridad. c) Estos oráculos de prueba no pueden utilizarse para pruebas de seguridad. d) Cuanto menos específica sea una aplicación y su contexto, más eficiente es la reutilización de dichas pruebas.	
Seleccionar UNA opción.	

Pregunta: 22

Puntos: 01	
Información de Contexto Las buenas prácticas y los estándares proporcionan muchos artefactos que pueden utilizarse eficazmente para la prueba de seguridad. 1. Nomenclatura consistente 2. Conocimiento experto 3. Comparativa 4. Visión holística de la seguridad que puede utilizarse para: A. facilitar la comunicación B. reutilizar los conocimientos de los expertos en seguridad para las pruebas de seguridad C. comprobar la completitud de las actividades de pruebas de seguridad D. demostrar fácilmente la efectividad de las actividades de prueba de seguridad aplicadas	
¿Qué combinaciones de artefacto y actividad se corresponden de forma adecuada?	
e) Opción	
Seleccionar **UNA** opción.	

Pregunta: 23

Puntos: 01	

Información de Contexto

Usted ha sido contratado como probador de seguridad por la dirección de una empresa de ingeniería de tamaño medio que produce diferentes piezas para automoción y que depende en gran medida de sus proveedores, ya que el precio de las materias primas afecta directamente a los beneficios. La empresa sólo tiene un sitio web público y un dominio de correo muy conocido, pero no ofrece más servicios web. Su tarea consiste en obtener acceso al entorno de producción interno compuesto por varias instalaciones industriales modernas y comprometer al menos un sistema.

¿Qué DOS opciones exponen mejor cómo podría aprovecharse del contexto organizativo?

a) Infiltrar uno de los proveedores más utilizados para acercarse a la empresa objetivo real.
b) Realizar un ataque de ingeniería social fingiendo ser un proveedor existente o un nuevo proveedor potencial y tratar de saber más sobre el objetivo, por ejemplo, visitándolo y solicitando una breve visita.
c) Identificar la dirección de correo del departamento de contabilidad y enviar facturas falsas con contenido malicioso, por ejemplo, para obtener acceso remoto a través de una consola inversa.
d) Dispersar memorias USB por el edificio de la empresa y esperar a que alguien recoja una y la conecte.
e) Ejercer una fuerza bruta contra el inicio de sesión SSH del servidor web.

Seleccionar **DOS** opciones.

Pregunta: 24

Puntos: 01	

Información de Contexto

Su empresa desarrolla diferentes productos para la industria aeronáutica. A principios de año se anunció un nuevo producto. Por primera vez, se tratará de un dispositivo de comunicación. Su trabajo consiste en realizar la prueba de seguridad del nuevo producto antes de lanzarlo al mercado.

¿Cuál de los siguientes aspectos describe **MEJOR** lo que debe tener en cuenta?

a) La industria aeronáutica es un sector regulado; por lo tanto, el nuevo producto y el proceso de desarrollo completo deben cumplir la normativa vigente.
b) Algunos países tienen sus propias normativas en materia de antenas de radio y estándares utilizados. El producto debe funcionar correctamente, aunque algunas frecuencias puedan interferir con las utilizadas por el producto.
c) La prueba de seguridad debe ejecutarse con gran rapidez, ya que el producto debe lanzarse al mercado lo antes posible.
d) Los empleados necesitan demostrar sus conocimientos sobre radiocomunicaciones mediante certificaciones personales

Seleccionar **UNA** opción.

Pregunta: 25

Puntos: 02	
Términos utilizados en la pregunta	
Español	**Inglés**
director de seguridad de la información (DSI)	chief information security officer (CISO)

Información de Contexto

Durante la prueba de seguridad de un sistema principal, usted encuentra varios archivos sospechosos que no han sido creados por usted ni por otros probadores durante la prueba, ni utilizados por las aplicaciones que se ejecutan en ese sistema.

Elija la opción que **MEJOR** describa cómo procedería

a) Continuar la prueba de seguridad e informar de sus hallazgos una vez que haya finalizado todas las actividades de prueba
b) Hacer una pausa en la prueba de seguridad y escribir un correo electrónico global informativo, como mínimo, a todos los colegas que tengan acceso al sistema. Continuar, si nadie se opone.
c) Detener la prueba de seguridad y apagar el sistema inmediatamente, porque se ha producido un acceso no autorizado y hay que evitar más daños potenciales.
d) Detener la prueba de seguridad y seguir los pasos definidos por la «política de seguridad» de la empresa para informar de una incidencia. Si no existe una política para el suministro de información sobre incidencias, informar a la persona responsable {por ejemplo, el director de seguridad de la información (DSI) [en inglés, chief information security officer (CISO)]}.
e) Detener la prueba de seguridad e iniciar la investigación y seguir los pasos definidos por la política de seguridad de la empresa para la investigación.

Seleccionar **UNA** opción.

Pregunta: 26

Puntos: 02	

Información de Contexto

Cada ataque es diferente. Sin embargo, ciertos pasos son comunes a casi todos los ataques. Estos pasos pueden definirse como:

¿Cuál de las siguientes opciones identifica **MEJOR** los pasos comunes a casi todos los ataques?

a) Paso de recopilación de información, seguido de explotación/obtención de accesibilidad y al final persistencia/mantenimiento del acceso.
b) Ingeniería social, seguida del ataque de fuerza bruta y al final persistencia/mantenimiento del acceso.
c) Explotación/obtención de acceso, seguida de ingeniería social para entender los resultados y al final limpieza de pistas
d) Recopilación de información, seguida de limpieza de pistas y al final ingeniería social para tener una mejor línea base.

Seleccionar **UNA** opción.

Pregunta: 27

Puntos: 01	
Términos utilizados en la pregunta	
Español	**Inglés**
prueba estática de seguridad de las aplicaciones (PESA)	static application security testing (SAST)
prueba dinámica de seguridad de las aplicaciones (PDSA)	dynamic application security testing (DAST)
¿Cuál de los siguientes enunciados describe MEJOR cómo se debería implementar la prueba de seguridad en el ciclo de vida de desarrollo?	
a) Cada actividad de desarrollo debería tener su correspondiente actividad de prueba de seguridad b) La mayoría de las vulnerabilidades se pueden encontrar realizando un análisis de amenazas y un diseño de seguridad adecuados c) La prueba dinámica de seguridad de las aplicaciones (PDSA) y la prueba estática de seguridad de las aplicaciones (PESA) deberían ejecutarse en todas las fases del ciclo de vida de desarrollo del software. d) La prueba de seguridad debe realizarse durante todas las fases del ciclo de vida de desarrollo del software para mantener la sincronización con la prueba funcional manual.	
Seleccionar **UNA** opción.	

Pregunta: 28

Puntos: 02	
¿Cuáles **DOS** de los siguientes enunciados describen **MEJOR** el impacto de un modelo de desarrollo de software en la prueba de seguridad?	
a) El equipo puede implicar a un equipo facilitador de la seguridad para realizar la prueba de seguridad en cada modelo. b) El modelo de cascada es el que mejor soporta la prueba de seguridad durante su ciclo de vida de desarrollo del software. c) DevOps puede dar un mejor soporte para que la prueba de seguridad se realice durante las operaciones. d) Es más fácil realizar la prueba de seguridad utilizando Kanban que utilizando Scrum. e) Se puede planificar mejor la prueba de seguridad utilizando los modelos de desarrollo ágil de software en comparación con el modelo en cascada.	
Seleccionar **DOS** opciones.	

Pregunta: 29

Puntos: 01	
¿Cuál de los siguientes cuatro enunciados es correcto para la prueba de seguridad en el contexto de la prueba de mantenimiento?	
a) Concentrarse en confirmar que se satisfacen todos los requisitos de seguridad tras el cambio b) Ejecutar el conjunto de regresión existente contra funciones individuales para comprobar que el cambio funciona c) Probar las nuevas vulnerabilidades que pueda haber introducido el cambio. d) Ejecutar pruebas de confirmación y de regresión de la seguridad después de realizar un cambio.	
Seleccionar **UNA** opción.	

Pregunta: 30

Puntos: 01	
¿Cuál de las siguientes opciones describe MEJOR por qué se deberían analizar los resultados de la prueba de seguridad?	
a) Para comprender mejor las amenazas y los riesgos de seguridad específicos basándose en evaluaciones de seguridad, auditorías y fuentes estándar de vulnerabilidades conocidas. b) Para traducir las pruebas conceptuales en pruebas que puedan ejecutarse manualmente o con herramientas c) Para definir un alcance adecuado de las pruebas que se corresponda con los riesgos de seguridad. d) Llevar las actividades de pruebas de seguridad a un punto de cierre para que las pruebas puedan mantenerse y realizarse de forma regular para respaldar cualquier nuevo requisito de seguridad y/o detectar nuevas amenazas.	
Seleccionar **UNA** opción.	

Pregunta: 31

Puntos: 01	

Términos utilizados en la pregunta

Español	Inglés
Open Web Application Security Project (OWASP)	Open Web Application Security Project (OWASP)

Información de Contexto

Usted es responsable de la seguridad del sistema. Alguien de su equipo está interesado en la prueba de seguridad y realiza una prueba de penetración en su sistema, que incluye las 10 vulnerabilidades más importantes de Open Web Application Security Project (OWASP). El informe de prueba correspondiente consta únicamente de los casos de prueba superados y fallidos que cubren estas vulnerabilidades.

¿Qué razonamiento para aceptar o rechazar el informe de prueba es correcto?

a) Aceptar, ya que la prueba de penetración fue realizada por un colaborador interno que conoce las guías de estilo de seguridad específicas.
b) Rechazar, ya que sus criterios de aceptación para la seguridad no fueron comunicados y no se tienen en cuenta en el informe de prueba. Por tanto, no está claro si se utilizaron las técnicas de prueba correspondientes y si los resultados de la prueba son relevantes para su comprobación anual de conformidad con las guías de estilo de seguridad.
c) Aceptar, ya que OWASP es una buena práctica y define una lista general de criterios de aceptación.
d) Rechazar, porque una guía de estilo de código de seguridad debe probarse mediante enfoques de prueba de caja blanca, no mediante una prueba de penetración dinámica de caja negra.
e) Aceptar, ya que OWASP refleja su guía de estilo de código de seguridad.

Seleccionar DOS opciones.	

Pregunta: 32

Puntos: 01	
Información de Contexto Texto	
Para aprovechar la prueba de seguridad al máximo nivel de eficiencia y efectividad debe: a) Estar integradas en un proceso global de seguridad, que intente minimizar el riesgo y asegurar la continuidad del negocio. b) Ser aplicada anualmente a todos los sistemas informáticos utilizados. c) Ser utilizada para limitar de forma proactiva el impacto de una brecha de seguridad. d) Tener en cuenta las vulnerabilidades comunicadas día a día. e) Estar garantizado, que todas las vulnerabilidades identificadas son remediadas dentro de un plazo apropiado menor 6 meses.	
Seleccionar **DOS** opciones.	

Pregunta: 33

Puntos: 01	

Información de Contexto

Las dimensiones típicas que un ingeniero de pruebas de seguridad puede utilizar para mejorar el alcance del sistema de gestión de seguridad de la información (SGSI) son:

1. Añadir objetos de prueba adicionales a su alcance de prueba.
2. Añadir técnicas de prueba adicionales a su diseño de prueba.
3. Mejorar la cobertura de la prueba ciñéndose a determinados objetos de prueba y enfoques de prueba.
4. Aumentar la automatización de la ejecución de pruebas de seguridad.

Que pueden utilizarse para:

A. aportar conocimientos adicionales sobre un sistema dado que puedan utilizarse para mejorar un SGSI existente.
B. identificar debilidades adicionales para componentes conocidos para mejorar un SGSI existente.
C. identificar debilidades adicionales para componentes que aún no forman parte del SGSI general.
D. hacer que el sistema informático existente sea más seguro.

¿Cuál de las siguientes alternativas presenta la combinación correcta de acciones y objetivos del ingeniero de pruebas de seguridad?

a) 1-C, 2-A, 3-B
b) 1-B, 2-D, 3-B
c) 1-C, 2-A, 4-B
d) 2-D, 2-C, 4-A

Seleccionar UNA opción.	

Pregunta: 34

Puntos: 10	

Términos utilizados en la pregunta

Español	Inglés
planificar-hacer-comprobar-actuar (PHCA)	plan-do-check-act (PDCA)
sistema de gestión de la seguridad de la información (SGSI)	Information Security Management System (ISMS)

Información de Contexto

Texto

¿Cómo se puede mejorar la mensurabilidad de la prueba de seguridad dentro de un SGSI?

a) Se puede utilizar la prueba de seguridad como un análisis objetivo dentro del paso Comprobar del ciclo PHCA para medir la efectividad de un ciclo PHCA.
b) Toda la prueba de seguridad genera conocimientos cuantificables sobre la seguridad de un sistema que pueden utilizarse para medir la efectividad del SGSI.
c) Cuantas más pruebas de seguridad pase un sistema sujeto a prueba, mejor y más eficaz será el SGSI.
d) La efectividad de un SGSI es mejor cuantas más técnicas de pruebas de seguridad se utilicen.

Seleccionar **UNA** opción.

Pregunta: 35

Puntos: 01	

Términos utilizados en la pregunta

Español	Inglés
vulnerabilidades y exposiciones comunes	Common Vulnerabilities and Exposures (CVE)

Información de Contexto

Los informes de la prueba de seguridad deben tratarse con un alto nivel de confidencialidad.

¿Qué tipo de datos forman parte de la mayoría de los informes de la prueba de seguridad motiva esta clasificación?

a) Nombre del probador de seguridad, plazo de ejecución de la prueba, resultados de prueba (casos de prueba pasados y fallados).
b) Entorno de prueba utilizado, precondiciones preestablecidas de las pruebas ejecutadas, datos de prueba utilizados, procedimiento de ejecución de prueba, comportamiento detectado.
c) Lista de vulnerabilidades y exposiciones comunes probadas, lista de desarrolladores designados, método de desarrollo de software identificado, herramientas de desarrollo de software identificadas.
d) Convenciones de codificación de seguridad utilizadas, cobertura de la prueba funcional identificada, escaneado de vulnerabilidades aplicado.

Seleccionar UNA opción.

Pregunta: 36

Puntos: 01	

Información de Contexto

Imagine que ejecuta algunos casos de prueba de seguridad como parte de una prueba de penetración para un sistema crítico para la empresa. Uno de ellos falló y parece que ha identificado una posible vulnerabilidad, que podría tener algún impacto dramático para el negocio.

¿Qué hacer antes de motivar directamente su mitigación?

a) Demarcación de la vulnerabilidad, es decir, ejecutar casos de prueba similares para identificar la demarcación de la vulnerabilidad identificada.
b) Estimación del esfuerzo para la acción de mitigación, es decir, hacer una estructura desglosada de la mitigación prevista.
c) Diseño de la mitigación, es decir, diseñar la solución que mitigue la vulnerabilidad identificada
d) Ajuste del riesgo, es decir, para volver a comprobar que la vulnerabilidad identificada puede explotarse en producción.
e) Comenzar a mitigar la vulnerabilidad identificada de forma inmediata.

Seleccionar **DOS** opciones.

Pregunta: 37

Puntos: 01	

Términos utilizados en la pregunta

Español	Inglés
autenticación multifactor (AMF)	multi-factor authentication (MFA)

Información de Contexto

Imagine que ha identificado una vulnerabilidad de nivel CVSS 9.8. Usted ha comprobado dos veces que esta vulnerabilidad puede incluso ser explotada en producción, y el negocio le ha confirmado que esta vulnerabilidad puede tener un impacto negativo muy fuerte. Por otro lado, la aplicación es crítica para el negocio, por lo que se decide mitigar el riesgo asociado a la vulnerabilidad identificada:

¿Cuál es su recomendación?

a) Si la vulnerabilidad afecta a un conjunto de prestaciones específico, se debería analizar si es posible desactivar la prestación concreta que contiene la vulnerabilidad.
b) En la mayoría de los casos es más fácil bloquear el tráfico específico en la capa de red, por lo que la tarea consiste en bloquear el tráfico vulnerable específico dentro del cortafuegos.
c) Si dispone de un cortafuegos de aplicaciones web moderno, las vulnerabilidades se identifican y mitigan automáticamente.
d) Si puede añadir un control de seguridad adicional a la lista de usuarios (por ejemplo, mediante el filtrado de IP o añadiendo AMF) puede tenerse en cuenta para reducir la probabilidad de riesgo mediante esta técnica.
e) En la mayoría de los casos, la acción de mitigación más rápida y barata es evitarlo por completo reparando la vulnerabilidad de los sistemas afectados.

Seleccionar **DOS** opciones.	

Pregunta: 38

Puntos: 01	

Términos utilizados en la pregunta

Español	Inglés
análisis de la composición del software (ACS)	Software Composition Analysis (SCA)
prueba estática de seguridad de las aplicaciones (PESA)	Static Application Security Testing (SAST)
prueba dinámica de seguridad de las aplicaciones (PDSA)	Dynamic Application Security Testing (DAST)
prueba interactiva de seguridad de aplicación (PISA)	Interactive Application Security Testing (IAST)

Información de Contexto

En un entorno de integración continua/entrega continua (IC/EC) se está creando una nueva canalización para el siguiente proyecto en el que está trabajando.

¿Cuál de los siguientes recomendaría que fuera el primer paso desencadenado como parte de la canalización?

a) ACS
b) PESA
c) PDSA
d) PISA

Seleccionar **UNA** opción.

Pregunta: 39

Puntos: 01	

Términos utilizados en la pregunta

Español	Inglés
análisis de la composición del software (ACS)	Software Composition Analysis (SCA)
prueba estática de seguridad de las aplicaciones (PESA)	Static Application Security Testing (SAST)
prueba dinámica de seguridad de las aplicaciones (PDSA)	Dynamic Application Security Testing (DAST)
prueba interactiva de seguridad de aplicación (PISA)	Interactive Application Security Testing (IAST)

Información de Contexto

Texto

¿Cuál de los siguientes escáneres y métodos de prueba escanea la aplicación bajo prueba en tiempo de ejecución?

a) PDSA
b) Análisis estático
c) ACS
d) PESA

Seleccionar **UNA** opción.

Pregunta: 40

Puntos: 01	

Términos utilizados en la pregunta

Español	Inglés
extremo de IPA	API endpoint
Interfaz De Programación De Aplicación (IPA)	Application Programming Interface (API)

¿Qué objetos de prueba se pueden escanear con herramientas de prueba estática?

a) Archivos de configuración
b) Diseño de seguridad
c) Extremos de IPA
d) Procesos en RAM

Seleccionar **UNA** opción.