

Examen para PSS04.

Intento 1.

Pregunta 1

Uno de los riesgos de los mayores riesgos de las aplicaciones es:

- a. Que no estén firmadas digitalmente.
- b. Instalarlas sin la autorización del usuario.
- c. Que se bajen de tiendas no oficiales.
- d. **Todas las anteriores.**

Pregunta 2

Los permisos especiales de iOS están firmados digitalmente. ¿Verdadero o Falso?
Seleccione una:

Verdadero

Falso

Pregunta 3

¿Qué significa CASB?:

- a. Cloud Advance Security Broker.
- b. Cloud Advanced Security Brokers.
- c. **Cloud Access Security Brokers.**
- d. Created Advanced Security Bureau.

Pregunta 4

¿Qué recibe el dispositivo móvil del entorno de CASB?:

- a. Apps a instalar.
- b. Usuarios permitidos.
- c. Sincronización agente.
- d. **Lista de políticas y configuraciones.**

Pregunta 5

Los sistemas de CASB tienen el objetivo de aportar visibilidad. ¿Verdadero o Falso?
Seleccione una:

Verdadero

Falso

Pregunta 6

¿Qué factor ha impulsado la tecnología CASB?:

- a. **Teletrabajo.**
- b. Transformación tecnológica.
- c. Número de vulnerabilidades.
- d. Machine learning.

Pregunta 7

Existe una única versión de la tecnología CASB y cada fabricante la implementa según considera. ¿Verdadero o falso?

Seleccione una:

Verdadero

Falso

Pregunta 8

Las aplicaciones piden autorización expresa para realizar compras. ¿Verdadero o Falso?

Seleccione una:

Verdadero

Falso

Pregunta 9

Los teléfonos móviles se han convertido en el objetivo de los cibercriminales. ¿Verdadero o Falso?

Seleccione una:

Verdadero

Falso

Pregunta 10

¿Qué usuario es el que está corriendo las apps de iOS?:

- a. Aleatorio basado en el UUID.
- b. Usuario raíz.
- c. Usuario original.
- d. mobile.

Intento 2.

Pregunta 1

No supone un problema que los empleados usen sus teléfonos personales para tareas corporativas. ¿Verdadero o falso?

Seleccione una:

Verdadero

Falso

Pregunta 2

No hay regulaciones especiales para el tratamiento de datos de carácter personal. ¿Verdadero o falso?

Seleccione una:

Verdadero

Falso

Pregunta 3

Cuál de las siguientes se considera una forma de limitar las capacidades de una aplicación en un dispositivo móvil:

- a. **Permisos.**
- b. Conectividad.
- c. Jailbreak.
- d. Chrooting.

Pregunta 4

Los desarrolladores deben de firmar sus aplicaciones. ¿Verdadero o Falso?
Seleccione una:

Verdadero
Falso

Pregunta 5

Las apps de Android funcionan todas con el mismo usuario. ¿Verdadero o falso?
Seleccione una:

Verdadero
Falso

Pregunta 6

¿Qué significa UEBA?:

- a. **User and Entity Behaviour Analytics.**
- b. User Endpoint Behaviour Analytics.
- c. User Endpoint Behaviour Analysis.
- d. User and Entity Behaviour Analysis.

Pregunta 7

Si bien son plataformas distintas tanto Android como iOS implementan mecanismos de seguridad. ¿Verdadero o Falso?
Seleccione una:

Verdadero
Falso

Pregunta 8

¿Las apps de iOS requieren permisos al usuario en la instalación?:

- a. Según se configure la app por el desarrollador.
- b. Si, siempre.
- c. Si, según la versión del sistema operativo.
- d. **No, solamente algunas funcionales especiales de privacidad pueden solicitar permiso del usuario.**

Pregunta 9

El dispositivo móvil contiene mucha información de carácter personal. ¿Verdadero o Falso?
Seleccione una:

Verdadero

Falso

Pregunta 10

La keystore es usada por los sistemas operativos iOS para gestionar contraseñas. ¿Verdadero o falso?

Seleccione una:

Verdadero

Falso

Intento 3.

Pregunta 1

Las apps de iOS tienen un directorio único donde se ejecutan e instalan sus ficheros.
¿Verdadero o falso?

Seleccione una:

Verdadero

Falso

Pregunta 2

¿Qué es una sandbox?

- a. Sistema nativo de aplicaciones.
- b. Entorno aislado y controlado.
- c. Imagen virtual de emulación de aplicaciones.
- d. Proceso de emulación de malware.

Pregunta 3

Las apps subidas a las tiendas oficiales deben cumplir bastantes requisitos. ¿Verdadero o falso?
Seleccione una:

Verdadero

Falso

Pregunta 4

¿Qué sistemas se usan para garantizar la seguridad del proceso de compra de las aplicaciones móviles?:

- a. Canales seguros de comunicación.
- b. HSTS.
- c. Software específico.
- d. Cambios en el aplicativo.

Pregunta 5

¿De qué manera podemos proteger los datos contenidos en los dispositivos móviles?:

- a. Mediante aplicaciones únicamente.
- b. Mediante el cifrado del terminal y los datos contenidos en él.
- c. Mediante SSL.
- d. Transfiriéndolos a la nube.

Pregunta 6

¿Cómo gestionan las claves las plataformas móviles?:

- a. Sistemas de nube.
- b. Mediante sistemas de gestión de claves.
- c. Mediante CASB.
- d. En memoria.

Pregunta 7

CASB aporta visibilidad sobre entornos de nube. ¿Verdadero o falso?

Verdadero

Falso

Pregunta 8

¿Cuándo una aplicación solicita permisos?

- a. Durante la descarga.
- b. Durante la instalación.
- c. Durante la ejecución.
- d. Durante la instalación y ejecución.

Pregunta 9

¿De qué manera suele funcionar la tecnología de CASB?:

- a. Modo nube.
- b. Mediante conexión síncrona.
- c. Agente instalado en el dispositivo.
- d. Mediante un dispositivo especial.

Pregunta 10

¿Es recomendable almacenar contraseñas y datos personales por parte de las aplicaciones móviles?

- a. Si, siempre.
- b. No.
- c. No deberían realizar este tipo de acción.
- d. Si, según el tipo de dato manejado por la aplicación.

Pregunta 11

Que es GDPR:

- a. Función especial de iOS.
- b. Tipo de protocolo.
- c. Reglamento General de Protección de Datos.
- d. Estándar de comunicación de los dispositivos móviles.

Pregunta 12

¿Qué se llave usa en algunos sistemas operativos de móviles para cifrar?:

- a. nombre de usuario.
- b. la llave se genera en tiempo real.
- c. fecha de nacimiento usuario.
- d. código desbloqueo o datos biométricos.