

Nombre Completo:

LU:

Parcial – Seguridad de la Información – DC - 13/6/2022

Elija la opción correcta (2 ptos):

1. ¿En qué principio está basado el modelo de Clark-Wilson?

- A. Integridad
- B. Disponibilidad
- C. Confidencialidad
- D. Auditabilidad

2. Ud. fue seleccionado para encontrar e implementar soluciones de multiple factor de autenticación. ¿Cuál de estas es realmente de múltiple factor?

- A. Usuario y contraseña
- B. Huella dactilar y contraseña
- C. Contraseña y PIN
- D. Huella dactilar y escaneo de retina

3. Compramos una compañía de nuestra línea de negocios. Detectamos que utilizan WEP para sus redes WIFI. WEP es considerado

- A. El mecanismo de cifrado preferido para redes wireless.
- B. Standard por defecto para routers wifi que se compran en la actualidad.
- C. Inseguro
- D. Seguro

4. Si estamos usando la propiedad simple de seguridad del modelo Bell-LaPadula, ¿Qué podemos hacer?

- A. Escribir hacia abajo
- B. Leer hacia arriba
- C. Escribir hacia arriba.
- D. Leer hacia abajo.

5. Tenemos 100 usuarios que necesitan comunicarse cada uno con el otro. Si usamos criptografía asimétrica, ¿cuántas claves serán necesarias?

- A. 2000
- B. 100
- C. 200
- D. 4950

6. ¿Qué es tu clave pública en un algoritmo de cifrado asimétrico?

- A. Compartida
- B. Secreta
- C. Usada por alguien más para descryptar mensajes dirigidos a vos.
- D. Usada por vos para descryptar mensajes enviados a vos.

Desarrolle (identifique todo lo que asume):

1. Una forma de clasificar las vulnerabilidades en el software es según se presenten en la etapa de diseño, implementación u operación. De un ejemplo de cada una. (1 pto)
2. Describa el concepto de forward secrecy. (1pto)
3. Discuta la siguiente afirmación: "Mi aplicación web es segura porque mantengo el servidor con los parches al día y sólo permito conexiones HTTPS". (1 pto)
4. Describa la idea de type-enforcement en SE-linux (1 pto)
5. ¿Cual es la característica principal de un firewall stateful? (1 pto)
6. La universidad quiere implementar un sistema para que los profesores puedan registrar las actas de finales. Al analizar el mecanismo de autenticación, deben elegir entre usar usuario y contraseña, o usar pares de claves públicas/privadas para cada usuario. Indique dos ventajas del 2do mecanismo. (1 pto)
7. Una licitación es el procedimiento administrativo para la adquisición de suministros, realización de servicios o ejecución de obras que celebran los organismos que forman parte del Sector Público. Consta de un anuncio de la licitación, un plazo para recepción de ofertas (que son secretas en sobre cerrado, e incluyen una propuesta económica, además del detalle de la propuesta de tareas a realizar/productos a entregar), un proceso de apertura de ofertas (en ese momento se hacen públicas para todos los oferentes) y un proceso de adjudicación. Defina consideraciones necesarias para digitalizar el circuito, impidiendo que tanto los oferentes como el organismo solicitante, puedan hacer trampa, es decir:
 - Que el oferente no pueda cambiar su propuesta, una vez realizada.
 - Que el oferente no pueda aducir que él no presentó la propuesta.
 - Que el organismo no pueda leer las propuestas recibidas, antes de que cierre el plazo de presentación de ofertas, para no poder pasar información a los competidores del oferente.
 - Que el oferente no pueda presentar una propuesta, una vez cerrado el plazo de presentación de ofertas.
 - Que el proceso de apertura puede ser auditado por todos los oferentes.(2 ptos)