

Seguridad 2do parcial recuperatorio

1. ¿Cuál de las siguientes es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado lapso de tiempo?
 - A. Autoridad de registro
 - B. Autoridad de Certificación
 - C. Autoridad de Validación
 - D. Autoridad de sellado de tiempo
2. ¿Cuál de las siguientes es una ventaja de los algoritmos simétricos?
 - A. Permite autenticar mensajes
 - B. No requiere confidencialidad en la distribución de clave.
 - C. La misma clave puede ser utilizada por múltiples actores en la comunicación
 - D. Longitud del mensaje "ilimitado"
3. Indique a que elemento corresponde la siguiente definición: "[...] es un marco de trabajo abierto para ayudar a las organizaciones a formular e implementar una estrategia de seguridad para Software que sea adecuada a las necesidades específicas que esta enfrentando la organización"
 - A. WSS
 - B. SAMM
 - C. SCRUM
 - D. Square
4. Según Deming, ¿Cuál de los siguientes elementos NO es una etapa del Ciclo de Calidad Total?
 - A. Planificar
 - B. Actuar
 - C. Auditar
 - D. Hacer
5. ¿Cuál de los siguientes es un método de Autorización en donde las decisiones de acceso se basan en las funciones y responsabilidades de un individuo dentro de la organización?
 - A. Mandatory Access Control (MAC)
 - B. Discretionary Access Control (DAC)
 - C. Ninguna de las opciones
 - D. Role Based Access Control (RBAC)
6. ¿Cuál es el puerto por defecto para transmisiones HTTPS?
 - A. 843
 - B. 8080
 - C. 80
 - D. 443

7. ¿Cuál de los siguientes puntos NO es un objetivo de la administración de usuarios y privilegios?
- A. Las funciones de nivel de administrador están segregadas apropiadamente de la actividad del usuario
 - B. Los usuarios no pueden acceder o utilizar funcionalidades administrativas
 - C. Los usuarios transmiten información de manera cifrada y confidencial
 - D. Proveer la necesaria auditoria y trazabilidad de funcionalidad administrativa
8. ¿A que tipo de algoritmo corresponde el cifrado del Cesar?
- A. Cifrado de simétrico de flujo
 - B. Cifrado por trasposición de grupos
 - C. Cifrado por sustitución
 - D. Cifrado Asimétrico
9. ¿Cuál de estos elementos NO corresponde a la lista de verificación de requerimientos de seguridad de la ASVS.
- A. Protección de Datos
 - B. Desempeño
 - C. Comunicación
 - D. Autenticación
10. ¿Cuál de los siguientes algoritmos NO requiere confidencialidad de la distribución de clave?
- A. AES
 - B. El Gamal
 - C. Ninguna de estas opciones
 - D. DES
11. ¿Cuál de los siguientes algoritmos se basa en la dificultad para factorizar grandes números?
- A. RSA
 - B. Ninguna de estas opciones
 - C. El Gamal
 - D. AES
12. ¿Qué elemento debe ser excluido del log o bitácora de la aplicación?
- A. Autenticaciones exitosas y fallidas
 - B. Eventos legales
 - C. Valores de identificación de la sesión
 - D. Código de estado HTTP
13. ¿Qué estándar se ha definido para la seguridad específica de Web Services?
- A. WSS
 - B. WSOL
 - C. HTTPS
 - D. TLS

14. ¿Qué modelo de infraestructura de seguridad utiliza PGP?

- A. Anillo o Circulo de confianza
- B. PKI – Infraestructura de Clave Publica
- C. Ninguna opción es valida
- D. ISI – Identificación integral de seguridad

15. ¿Cuál de las siguientes es una ventaja de los algoritmos simétricos?

- A. No requiere confidencialidad en la distribución de clave
- B. La misma clave puede ser utilizada por múltiples actores en la comunicación
- C. Permite autenticar mensajes
- D. Sencillez de implementación