Seguridad Final 12/2023

1. ¿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

2. Dada la siguiente definición en el código de la aplicación:
   >String query = " SELECT * FROM ítems WHERE itemname = ' " + itemName + " ´ ";
   Indique cual de las opciones puede generar un ataque de inyección exitoso:
   A. UPDATE ítems SET Price = 50 WHERE itemname = 'table
   B. 1 = 1 AND itemname = Table
   C. '; UPDATE ítems SET Price = 50 WHERE itemname = 'table
   D. '; UPDATE ítems SET Price = 50 WHERE itemname = 'table'

3. ¿Cual es el significado de SSL?
   A. Secure Socket Level
   B. Simple Socket Layer
   C. Secure Sockets Layer
   D. Standard Socket Layer

4. ¿Cuál de los siguientes puntos corresponde a la seguridad física en dispositivos móviles?
   A. Insertar software solo de fuentes confiables
   B. Considerar el uso de software de seguimiento, borrado de datos y/o bloqueo remoto
   C. Evitar o restringir la manipulación del dispositivo en zonas publicas
   D. Evitar o restringir conexiones a redes públicas o no confiables

5. ¿Cuál de las siguientes opciones corresponde a un modelo enfocado en la madurez de las siguientes características esenciales de los procesos que deben existir en una organización para asegurar un sistema?
   A. PCI DSS
   B. ISO/IEC 21827:2008
   C. A4609
   D. ISO 25000

6. ¿Cuál es el significado del acrónimo DSA?
   A. Ninguna de estas opciones
   B. Data Signature Algorithm
   C. Digital Signature Algorithm
   D. Dynamic Signature Algorithm

7. ¿Cuál de los siguientes puntos corresponde al grupo de Pas para “PROJECT AND ORGANIZATION”
   A. Specity Security Needs
   B. Build Assurance Argument
   C. Assess Security Risk
   D. Plan Technical Elfort

8. ¿Cuál de los siguientes elementos NO forma parte de la pirámide ID?
   A. Ninguno
   B. Identificación
   C. Confidencialidad
   D. Disponibilidad

9. ¿Cuál de los siguientes es un método de Autorizacion en donde se asegura la información mediante etiquetas de sensibilidad en la información y comparando esto con el nivel de sensibilidad de un usuario?
   A. DIscretionary Access Control (DAC)
   B. Role Based Access Control (RBAC)
   C. Mandatory Access Control (MAC)
   D. Ninguna de las opciones

10. ¿Segun Daming, cual de los siguientes elementos no es una etapa del ciclo de Calidad Total?
   A. Auditar
   B. Planificar
   C. Actual

11. La tecnología de TLS es un aporte para reducir la probabilidad de cual de los siguientes tipos de ataque?
   A. Fallas Criptograficas
   B. Almacenamiento criptografico inseguro
   C. Inyección
   D. KSS – Cross site reference

12. ¿A que elemento corresponde la definición “Es una lista de tipos de debilidades de software y hardware”?
   A. NVD
   B. CYSS
   C. CWE
   D. CVE

13. ¿Cuál de las siguientes características no están asociadas a los firewalls?
   A. Balanceo de carga (BCFW)
   B. Perdidas de contenido / Anti-spam
   C. Alta disponibilidad (AD)
   D. Almacenamiento de datos de negocio

14. ¿Cuál es el puerto por defecto para transacciones HTTPS?
    A. 80
    B. 433
    C. 123
    D. 8080

15. ¿Cuál de los siguientes elementos no corresponde a la lista de CWE?
    A. Log Shell ACE
    B. Out of bounds read
    C. Cross site request forgery
    D. Improper Input validation

16. ¿Para que se utiliza la firma digital?
    A. Generar datos aleatorios
    B. Garantizar la confidencialidad de datos
    C. Garantizar la autenticidad de datos
    D. Ninguna de estas opciones

17. ¿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

18. ¿A que termino esta asociada la siguiente definición: “Cuando se recibe un mensaje no solo es necesario poder identificar de forma univoca al remitente, sino que este asuma todas las responsabilidades derivadas de la información que haya podido enviar”
    A. Anonimato
    B. No repudio
    C. Integridad
    D. Confidencialidad

19. A que Capability Level corresponde los siguientes common features
    - Objectively Managing Performance
    - Estabish Measure Quality Goals
        A. Capability Level 4
        B. Capability Level 2
        C. Capability Level 5
        D. Capability Level 3

20. ¿Cuál de los siguientes puntos NO es un objetivo de la administración de usuario y privilegios?
    A. Las funciones de nivel de administrador están segredadas 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 necesidad auditoria y trazabilidad de funcionalidad administrativa

21. Indique a que termino se asocia la siguiente definición: "(...) es la propiedad que busca mantener los datos libres de modificaciones no autorizadas"
    A. Integridad
    B. Confidencialidad
    C. Consistencia
    D. Disponibilidad

22. ¿Cuál es el objetivo del ataque BackDoors?
    A. Habilitar un acceso alternativo evitando los métodos de autentificación
    B. Registrar las actividades de los dispositivos de entrada
    C. Retener el control del equipo o cifrar información para que no pueda ser accedida
    D. Acceder a la información almacenada para enviarla al atacante

23. ¿Cuál de las siguientes normas ha sido emitida por la Unión Europea?
    A. CCPA
    B. GDPR
    C. HIPAA
    D. A4609

24. Al hablar de daño...
    A. Tenemos que calcular la probabilidad que ocurra
    B. Todas las otras opciones
    C. Necesitamos cuantificar el perjuicio
    D. No hace faltar cuantificar el perjuicio

25. Marque la respuesta correcta según indica el siguiente mensaje generado mediante el cifrado del Cesar: "od uhbsahrwd fruuhfwd frqwlhqh od sdodeud vdovd"
    A. Hay estrellas en el cielo
    B. Los fideos tienen salsa
    C. El fuego se apagará pronto
    D. La torre es demasiada alta

26. ¿Cuál de las siguientes es una ventaja de los algoritmos Asimetricos?
    A. Longitud del mensaje "ilimitada"
    B. No requiere confidencialidad en la distribución de clave
    C. Velocidad de cifrado
    D. Robustez

27. ¿Cuál de las siguientes opciones NO es una buena practica para evitar vulnerabilidades de XSS?
    A. Validacion de entrada positiva o de “Lista Blanca”
    B. Ninguna de estas opciones
    C. Codificar los datos no confiables basados en el contexto donde serán ubicadas
    D. Utilizar APIs de auto-sanitizacion

28. Indique el tipo de ataque correspondiente a la siguiente definición: “[...] obliga al navegador de una victima autenticada a enviar una peticion HTTP falsificada incluyendo la sesión del usuario y cualquier otra información de modificaciones incluida automaticamente a una aplicación web vulnerable”
    A. Inyección
    B. Referencia directa insegura a objetos
    C. Falsificación de peticiones en sitios cruzados (CSRF)
    D. Perdida de autentificación y gestión de sesión

29. ¿Para que tipo de ataque se podría utilizar la siguiente instrucción? : “ document.body.innnerHTML(“atacado(*)”);”
    A. XSS (Site defacement)
    B. JS injection
    C. CSRF
    D. Injection

30. ¿Qué se utiliza cuando una clave publica pierde su validez y debe ser anulada?
    A. La clave privada del certificado
    B. Un Certificado de renovación
    C. No se requiere acciones, simplemente se procede a crear un nuevo certificado
    D. Un mail de cancelación firmado digitalmente