# Seguridad Final 12/2023

1. ¿Qué modelo de infraestructura de seguridad utiliza PGP?
2. Anillo o circulo de confianza
3. PKI – Infraestructura de Clave Publica
4. Ninguna opción es valida
5. ISI – Identificación integral de seguridad
6. 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:

1. UPDATE ítems SET Price = 50 WHERE itemname = ‘table
2. 1 = 1 AND itemname = Table
3. ‘; UPDATE ítems SET Price = 50 WHERE itemname = ‘table
4. ‘; UPDATE ítems SET Price = 50 WHERE itemname = ‘table’
5. ¿Cual es el significado de SSL?
6. Secure Socket Level
7. Simple Socket Layer
8. Secure Sockets Layer
9. Standard Socket Layer
10. ¿Cuál de los siguientes puntos corresponde a la seguridad física en dispositivos móviles?
11. Insertar software solo de fuentes confiables
12. Considerar el uso de software de seguimiento, borrado de datos y/o bloqueo remoto
13. Evitar o restringir la manipulación del dispositivo en zonas publicas
14. Evitar o restringir conexiones a redes públicas o no confiables
15. ¿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?
16. PCI DSS
17. ISO/IEC 21827:2008
18. A4609
19. ISO 25000
20. ¿Cuál es el significado del acrónimo DSA?
21. Ninguna de estas opciones
22. Data Signature Algorithm
23. Digital Signature Algorithm
24. Dynamic Signature Algorithm
25. ¿Cuál de los siguientes puntos corresponde al grupo de Pas para “PROJECT AND ORGANIZATION”
26. Specity Security Needs
27. Build Assurance Argument
28. Assess Security Risk
29. Plan Technical Elfort
30. ¿Cuál de los siguientes elementos NO forma parte de la pirámide ID?
31. Ninguno
32. Identificación
33. Confidencialidad
34. Disponibilidad
35. ¿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?
36. DIscretionary Access Control (DAC)
37. Role Based Access Control (RBAC)
38. Mandatory Access Control (MAC)
39. Ninguna de las opciones
40. ¿Segun Daming, cual de los siguientes elementos no es una etapa del ciclo de Calidad Total?
41. Auditar
42. Planificar
43. Actuar
44. La tecnología de TLS es un aporte para reducir la probabilidad de cual de los siguientes tipos de ataque?
45. Fallas Criptograficas
46. Almacenamiento criptografico inseguro
47. Inyección
48. KSS – Cross site reference
49. ¿A que elemento corresponde la definición “Es una lista de tipos de debilidades de software y hardware”?
50. NVD
51. CYSS
52. CWE
53. CVE
54. ¿Cuál de las siguientes características no están asociadas a los firewalls?
55. Balanceo de carga (BCFW)
56. Perdidas de contenido / Anti-spam
57. Alta disponibilidad (AD)
58. Almacenamiento de datos de negocio
59. ¿Cuál es el puerto por defecto para transacciones HTTPS?
60. 80
61. 433
62. 123
63. 8080
64. ¿Cuál de los siguientes elementos no corresponde a la lista de CWE?
65. Log Shell ACE
66. Out of bounds read
67. Cross site request forgery
68. Improper Input validation
69. ¿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

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

1. ¿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”
2. Anonimato
3. No repudio
4. Integridad
5. Confidencialidad
6. A que Capability Level corresponde los siguientes common features

* Objectively Managing Performance
* Estabish Measure Quality Goals

1. Capability Level 4
2. Capability Level 2
3. Capability Level 5
4. Capability Level 3
5. ¿Cuál de los siguientes puntos NO es un objetivo de la administración de usuario y privilegios?
6. Las funciones de nivel de administrador están segredadas apropiadamente de la actividad del usuario
7. Los usuarios no pueden acceder o utilizar funcionalidades administrativas
8. Los usuarios transmiten información de manera cifrada y confidencial
9. Proveer la necesidad auditoria y trazabilidad de funcionalidad administrativa
10. Indique a que termino se asocia la siguiente definición: “(…) es la propiedad que busca mantener los datos libres de modificaciones no autorizadas”
11. Integridad
12. Confidencialidad
13. Consistencia
14. Disponibilidad
15. ¿Cuál es el objetivo del ataque BackDoors?
16. Habilitar un acceso alternativo evitando los métodos de autentificación
17. Registrar las actividades de los dispositivos de entrada
18. Retener el control del equipo o cifrar información para que no pueda ser accedida
19. Acceder a la información almacenada para enviarla al atacante
20. ¿Cuál de las siguientes normas ha sido emitida por la Unión Europea?
21. CCPA
22. GDPR
23. HIPAA
24. A4609
25. Al hablar de daño…
26. Tenemos que calcular la probabilidad que ocurra
27. Todas las otras opciones
28. Necesitamos cuantificar el perjuicio
29. No hace faltar cuantificar el perjuicio
30. Marque la respuesta correcta según indica el siguiente mensaje generado mediante el cifrado del Cesar: “od uhbsahrwd fruuhfwd frqwlhqh od sdodeud vdovd”
31. Hay estrellas en el cielo
32. Los fideos tienen salsa
33. El fuego se apagará pronto
34. La torre es demasiada alta
35. ¿Cuál de las siguientes es una ventaja de los algoritmos Asimetricos?
36. Longitud del mensaje “ilimitada”
37. No requiere confidencialidad en la distribución de clave
38. Velocidad de cifrado
39. Robustez
40. ¿Cuál de las siguientes opciones NO es una buena practica para evitar vulnerabilidades de XSS?
41. Validacion de entrada positiva o de “Lista Blanca”
42. Ninguna de estas opciones
43. Codificar los datos no confiables basados en el contexto donde serán ubicadas
44. Utilizar APIs de auto-sanitizacion
45. 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”
46. Inyección
47. Referencia directa insegura a objetos
48. Falsificación de peticiones en sitios cruzados (CSRF)
49. Perdida de autentificación y gestión de sesión
50. ¿Para que tipo de ataque se podría utilizar la siguiente instrucción? : “ document.body.innnerHTML(“atacado(\*)”);”
51. XSS (Site defacement)
52. JS injection
53. CSRF
54. Injection
55. ¿Qué se utiliza cuando una clave publica pierde su validez y debe ser anulada?
56. La clave privada del certificado
57. Un Certificado de renovación
58. No se requiere acciones, simplemente se procede a crear un nuevo certificado
59. Un mail de cancelación firmado digitalmente