PARCIAL 1.1

1 - ¿A qué ataque del OWASP Top-Ten se refiere la siguiente definición: “El atacante puede ejecutar secuencias de comandos en el navegador de la víctima”?

A – Secuencia de Comandos en Sitios Cruzados (XSS)

B – Ausencia de Control de Acceso a Funciones

C – Falsificación de Peticiones en Sitios Cruzados (CSRF)

D – Referencia Directa Insegura a Objetos

2 - ¿Cuál de estas tecnologías es considerada generadora de riesgo por ser ejecutada en el cliente?

A – Java Applet

B – ActiveX

C – JavaScript

Shockwave

Portable Document Format (PDF) Flash

D – Todas las respuestas

3 - ¿Cuáles de los siguientes puntos NO corresponde a un tipo de vulnerabilidad?

Las 3 corresponden a los tipos de vulnerabilidad: Debidas al uso, Debidas al diseño, Debidas a la implementación.

A – Debidas al uso

B – Debidas al diseño

C – Debidas a la implementación

D – Ninguna de las anteriores

4 – ¿Cuáles de estas afirmaciones es verdadera en la relación a los Firewalls?

A – No protege de accesos no autorizados

B – No protege de ataques internos

C – Todas las anteriores

D – No protege de todos los ataques dañinos

5 - ¿Cuál de los siguientes puntos no es un atributo del protocolo TCP?

A – No es orientado a conexión

B – Corre sobre IP

C – Cada paquete tiene un numero de secuencia y un flag

D – Un paquete tiene un numero de origen y destino

6 - ¿Qué se entiende por tampering?

A – Es una técnica para redireccionar al usuario hacia otro servidor

B – Es un ataque de alteración de datos no autorizados

C – Ninguna respuesta es correcta

D – Es una vulnerabilidad que afecta al código JavaScript

7 - ¿Cuál de los siguientes factores no es evaluado por la OWASP para determinar los riesgos incluidos en el proyecto Top-Ten?



A – Vectores de Ataque

B – Detectabilidad de Debilidades

C – Impacto Técnico

D – Impacto en el Negocio

8 - ¿Qué es un bugtraq?

A – Ninguna de las opciones es correcta

B – Es una lista de notificación sobre vulnerabilidades encontradas en software y hardware

C – Es una variante de virus o troyano

D – Es un software diseñado para buscar vulnerabilidades

9 - ¿Cómo se denomina a la zona ubicada entre la red interna y la externa donde habitualmente se ubican a los servidores de la empresa (Web, DB, FTP, Etc.)?

A – DMZ

B – B2B

C – Router

D – LBA

10 - ¿Qué es un firewall?

A – Un dispositivo que permite bloquear o filtrar el acceso entre dos redes; usualmente una privada y otra externa

B – Un dispositivo de antivirus de red

C – Una librería de software que permite asegurar una aplicación web

D – Un dispositivo que permite la autenticación en aplicaciones

11 - ¿Cuál es la principal función de un comprobador de integridad?

A – Identificar archivos que han sido alterados en el sistema de archivos

B – Notificar vía email sobre cambios en el sistema de archivos

C – Identificar los cambios realizados en los archivos del sistema

D – Identificar al usuario que ha introducido cambios en el sistema de archivos

12 - ¿Qué se entiende por tampering?

A – Es un ataque de alteración de datos no autorizados

B – Es una vulnerabilidad que afecta al código JavaScript

C – Ninguna respuesta es correcta

D – Es una técnica para redireccionar al usuario hacia otro servidor

13 - ¿A qué tipo de equipo se está refiriendo la siguiente definición?

“Analiza el tráfico de la red para tratar de detectar patrones sospechosos que indiquen ataques o intenciones de ataques contra algún recurso. Una vez identificados, puede tomar ciertas medidas contra ese tipo de tráfico, como generar alertas o inclusive bloquear o descartar el tráfico que viene de ese origen.”

A – Statefulls

B – HoneyNets

C – IDS

D – HoneyPots

14 - ¿Cuál de los siguientes elementos corresponde a una Modalidad de Acceso a la información en Seguridad Lógica?

A – Escritura

B – Ejecución

C – Borrado

D – Lectura

E – Todas las opciones

15 - ¿Cuál de las siguientes opciones corresponde al modelo de funcionamiento general de un IDS?

A – Filtrado – Identificación – Acción

B – Recolección – Análisis – Respuesta

C – Ninguna de los anteriores

D – Recolección – Identificación – Clasificación

16 – A qué tipo de equipo se está refiriendo la siguiente definición?

“Divide la LAN en varios segmentos limitando el tráfico a uno o más segmentos en vez de permitir la difusión de paquetes por todos los puertos”

A – Switch

B – Router

C – Bridge

D – Hub

17 - ¿Cuál de los siguientes elementos no compone la lista de técnicas de OWASP Top-Ten Proactive Controls?

A – Implement Appropiate Access Controls

B – Validate All Inputs

C – Parameterize Queries

D – Use Virtual Keyboard in the Login

E – Encode Data

18 – Indique el tipo de ataque correspondiente a la siguiente definición: “[…] ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada.”

A – Falsificación de peticiones en sitios cruzados (CSRF)

B – Inyección

C – Referencia directa insegura a objetos

D – XSS-Cross Site Scripting

19 – Indique el tipo de ataque correspondiente a la siguiente definición: “ocurre cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder a datos no autorizados.”

A – Referencia directa insegura a objetos

B – Inyección

C – Falsificación de peticiones en sitios cruzados (CSRF)

D – Perdida de autenticación y gestión de sesiones

20 - ¿Cuál de los siguientes tipos no corresponde a la lista OWASP de 10 ataques más frecuentes?

A – Inyección

B – Control de accesos sin contraseñas seguras

C – Perdida de autenticación y gestión de sesiones

D – Falsificación de peticiones en sitios cruzados (CSRF)

21 - ¿A qué ataque del OWASP Top-Ten se refiere la siguiente definición: “El atacante puede ejecutar secuencias de comandos en el navegador de la víctima…”?

A – Referencia Directa Insegura a Objetos

B – Ausencia de Control de Acceso a Funciones

C – Falsificación de Peticiones en Sitios Cruzados (CSRF)

D – Secuencia de Comandos en Sitios Cruzados (XSS)

22 - ¿Cuál de las siguientes características no están asociadas a los firewalls?

A – Alta disponibilidad (AD)

B – Balanceo de carga (BCFW)

C – Filtrados de contenidos / Anti-spam

D – Almacenamiento de datos de negocio

PARCIAL 1.2

1 – ¿Cuáles de los siguientes elementos no forma parte del OWASP Top-Ten?

A – Referencia Directa Insegura a Objetos

B – Redirecciones y reenvíos no validos

C – Configuración de Seguridad Incorrecta

D – Denegación de Servicio

2 – 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 – Disponibilidad

C – Consistencia

D – Confidencialidad

3 - ¿Qué es un firewall?

A – Un dispositivo que permite bloquear o filtrar el acceso entre dos redes; usualmente una privada y otra externa.

B – Un dispositivo de antivirus de red

C – Un dispositivo que permite la autenticación en aplicaciones

D – Una librería de software que permite asegurar una aplicación web

4 - ¿En qué zona ubica al ataque de Exposición de datos sensibles?

A – Área de Cliente

B – Área de Red

C – Área de Servidor

D – Área de Red y Área de Servidor

5 - ¿Cuál de estas tecnologías es considerada generadora de riesgo por ser ejecutada en el cliente?

A – Java Applet

B – ActiveX

C – JavaScript

D – Todas las respuestas

6 - ¿A que se denomina “Learning Mode” en el contexto de la implementación de un WAF?

A – Al modo de operación donde la herramienta registra la actividad normal de la aplicación para que posteriormente pueda ser utilizada a fin de generar reglas

B – Al modo de operación donde se permite que el usuario acceda a la aplicación para generar los ataques que posteriormente serán bloqueados

C – A la capacitación del personal que llevara adelante la configuración de la herramienta

D – Ninguna de las opciones

7– SYN Flood corresponde a una técnica utilizada para realizar un ataque de …

A – Inyección

B – Denegación de Servicio

C – Control remoto de un servidor

D – Secuencia de Comandos en Sitios Cruzados (XSS)

8 - ¿Cuál de las siguientes tecnologías no puede ser utilizada en un ataque de Inyección?

A – SQL

B - Ninguna

C – LDAP

D – X-Path

9 – ¿Cuáles de estas afirmaciones es verdadera en la relación a los Firewalls?

A – Todas las anteriores

B – No protege de accesos no autorizados

C – No protege de todos los ataques dañinos

D – No protege de ataques internos

10 - ¿Qué protocolo soporta la implementación de VPNs?

A – Ninguna de las opciones

B – IPSec

C – Secure TCP

D – ICMP

11 - ¿Qué es un bugtraq?

A – Es una lista de notificación sobre vulnerabilidades encontradas en software y hardware

B – Es un software diseñado para buscar vulnerabilidades

C – Es una variante de virus o troyano

D – Ninguna de las opciones es correcta

PARCIAL 1.3

1 - ¿A qué tipo de equipo se está refiriendo la siguiente definición?

“Analiza el tráfico de la red para tratar de detectar patrones sospechosos que indiquen ataques o intenciones de ataques contra algún recurso. Una vez identificados, puede tomar ciertas medidas contra ese tipo de tráfico, como generar alertas o inclusive bloquear o descartar el tráfico que viene de ese origen.”

A – Statefulls

B – HoneyPots

C – HoneyNets

D – IDS

2 - ¿A qué ataque del OWASP Top-Ten se refiere la siguiente definición: “El atacante puede ejecutar secuencias de comandos en el navegador de la víctima…”?

A – Secuencia de Comandos en Sitios Cruzados (XSS)

B – Falsificación de Peticiones en Sitios Cruzados (CSRF)

C – Ausencia de Control de Acceso a Funciones

D – Referencia Directa Insegura a Objetos

3 – Indique el tipo de ataque correspondiente a la siguiente definición: “ocurre cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder a datos no autorizados.”

A – Perdida de autenticación y gestión de sesiones

B – Falsificación de peticiones en sitios cruzados (CSRF)

C – Referencia directa insegura a objetos

D – Inyección

4 – Seleccione el tipo de ataque correspondiente a la siguiente definición: “es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.”

A – Inyección

B – Perdida de autenticación

C – Tampering

D – Denegación de Servicio

5 - ¿Cuál de los siguientes factores no es evaluado por la OWASP para determinar los riesgos incluidos en el proyecto Top-Ten?

A – Impacto en el Negocio

B – Impacto Técnico

C – Vectores de Ataque

D – Detectabilidad de Debilidades

6 - ¿Cuál de las siguientes tecnologías no puede ser utilizada en un ataque de Inyección?

A – SQL

B – LDAP

C - Ninguna

D – X-Path

7 - ¿Cuál es la principal función de un comprobador de integridad?

A – Identificar los cambios realizados en los archivos de sistema

B – Notificar vía email sobre cambios en el sistema de archivos

C – Identificar al usuario que ha introducido cambios en el sistema de archivos

D – Identificar archivos que han sido alterados en el sistema de archivos

8 - ¿Cuál de los siguientes elementos corresponde a una Modalidad de Acceso a la información en Seguridad Lógica?

A – Todas las opciones

B – Borrado

C – Escritura

D – Lectura

E – Ejecución

9 - ¿Cuál de estos elementos corresponde a la siguiente definición?:

“Se trata de un dispositivo que analiza el trafico web (entre el servidor web y la WAN), los datos recibidos por parte del usuario y protege de diferentes ataques”

A – Firewall Personal

B – WAF

C – Layer 3 Firewall

D – IDS

10 - ¿Cuál de los siguientes elementos NO forma parte de la pirámide ID?

A – Identificación

B – Ninguno

C – Confidencialidad

D – Disponibilidad

11 - Explique el ataque por Inyección comparándolo y asociándolo con el de XSS.

Adicionalmente indique que medidas se recomiendan para proteger a una aplicación de este ataque

12 – Desarrolle la definición y función de un IDS, explique sus diferencias con un IPS y un Firewall.

11 - ¿Cuál de los siguientes elementos NO está catalogado como una Acción Hostil en Seguridad Física?

A – Sabotaje

B – Fraude

C – Inundación

D – Robo

12 - ¿Cuál de los siguientes elementos NO forma parte de la pirámide ID?

A – Confidencialidad

B – Identificación

C – Disponibilidad

D – Ninguno

13 - ¿Cuál de los siguientes elementos NO se encuentra dentro de los Controles de Acceso Interno de la seguridad lógica?

A – Ninguno

B – Contraseñas

C – Etiquetas de seguridad

D – Listas de control de accesos

14 – Seleccione la opción según la definición de amenaza: “Entendemos por amenaza aquella situación de daño cuyo …”

A – Riesgo de producirse es significativo

B – Impacto genera una detención total del sistema

C – Origen se encuentra en el código de la aplicación

D – Impacto no afecta a la funcionalidad del sistema

15 - ¿Cuál de los siguientes puntos no es un atributo del protocolo TCP?

A – No es orientado a conexión

B – Un paquete tiene un numero de puerto origen y destino

C – Corre sobre IP

D – Cada paquete tiene un numero de secuencia y un flag

16 - ¿Cuál de los siguientes elementos se utiliza con el fin de capturar tramas de red?

A – Sniffer

B – Ninguno de los anteriores

C – IDS

D – Firewall Personal

17 - ¿Cómo se denomina a la zona ubicada entre la red interna y la externa donde habitualmente se ubican a los servidores de la empresa (Web, DB, FTP, Etc.)?

A – B2B

B – DMZ

C – Router

D – LBA

18 - ¿En qué zona ubica al ataque de Inyección?

A – Área de Servidor

B – Área de Red

C – Área de Cliente

D – Ninguna

Parcial 2 – Modelo

1. ¿Para qué se utiliza la firma digital?
2. Generar datos aleatorios
3. Garantizar la confidencialidad de los datos
4. Garantizar la autenticidad de los datos
5. Ninguna de las anteriores

*Una firma digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).*

1. ¿Cuál de los siguientes algoritmos es denominado AES?
2. Serpent
3. Rijndael
4. IDEA
5. DES

Advanced Encryption Standard (AES), también conocido como Rijndael (pronunciado “Rain Doll” en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.

1. ¿Qué condiciona el libre uso de los algoritmos?
2. Ninguna de estas opciones
3. Que sean públicos
4. Que tengan patentes en vigencia
5. Que sean privados
6. ¿Cuál de los siguientes elementos no corresponde a una función de negocio SAMM?
7. Gobierno
8. Implementación
9. Verificación
10. Diseño
11. Construcción

*Elementos que si corresponden:*

*Gobernabilidad: Está centrada en la definición de la estrategia, en los procesos y políticas relacionadas a cómo una organización debe gestionar el SDLC (Software Development Life Cycle).*

*Construcción: Se refiere a los procesos y actividades que la organización debe seguir para el desarrollo de la aplicación, lo cual incluye la administración del producto, recolección de requerimientos, especificaciones de la arquitectura a alto nivel, definición del diseño detallado e implementación de la aplicación.*

*Verificación: Se enfoca a los procesos relacionados a la revisión y pruebas de los artefactos producidos durante el desarrollo del software; incluye aseguramiento de calidad y diferentes tipos de pruebas.*

*Implementación: Se refiere a las actividades relacionadas a la liberación de la aplicación.*

1. ¿Cuál de los siguientes elementos no corresponde a una característica positiva de los sistemas criptográficos simétricos?
2. Robustez
3. Velocidad de cifrado
4. Longitud del mensaje limitada por la implementación
5. Sencillez de implementación

*La criptografía de clave simétrica (en inglés symmetric key cryptography), también llamada criptografía de clave secreta, es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.*

1. ¿Cuál de los siguientes NO es un modo de cifrado de bloques?
2. CBC - Cipher Block Chaining
3. OFB - Output feedback
4. CFB - Cipher Feedback
5. Ninguna de las anteriores

Cifrados de Bloque: cifran el mensaje dividiendo el flujo en bloques de k bits. Cada bloque se corresponde con otro diferente. Por ejemplo, un bloque con k=3 “010” se podría corresponder con “110”. Un ejemplo de cifrado de bloque es el algoritmo AES.

1. ¿Cuál de las siguientes NO es una propiedad de la firma digital?
2. Va ligada indisolublemente al mensaje
3. Se genera en base a la clave pública del destinatario
4. Solo puede ser generada por su legítimo titular
5. Es públicamente verificable
6. ¿Qué significa el acrónimo CMM?
7. Capacity Model Metrics
8. Capability Maturity Model
9. Capability Model and Metrics
10. Capacity Measure Model

El Modelo de Madurez de Capacidades o CMM (Capability Maturity Model), es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon para el Software Engineering Institute (SEI).

El SEI es un centro de investigación y desarrollo patrocinado por el Departamento de Defensa de los Estados Unidos de América y gestionado por la Universidad Carnegie-Mellon. “CMM” es una marca registrada del SEI.

1. ¿Qué norma define la metodología SCRUM?
2. Ninguna de las anteriores
3. ISO 25000
4. ISO/IEC 9126
5. ISO/IEC 14598
6. Determine el mensaje original para el siguiente cifrado obtenido mediante el cifrado de XOR solamente.

Valor cifrado: 101110110010

Contraseña: 011100110110

Se conoce la existencia de los siguientes valores binarios 100111000011 y 110011110011

1. 101010100011
2. 110010000100
3. 001110110110
4. 111100111010
5. ¿A que se denomina Padding?
6. Al método para autenticar mensajes con algoritmos asimétricos
7. Al método para completar el inicio de un bloque de datos
8. Al método que permite generar una distorsión entre los distintos bloques
9. Al método para completar el final de un bloque de datos
10. ¿Sobre qué tecnología están desarrollados los Web Services?
11. XML/SOAP
12. HTTPS
13. AES
14. HTML
15. Identifique a que corresponde la siguiente definición:

Se define como una función o método para generar un valor que represente de manera casi unívoca a un dato".

1. Función de encriptación de datos
2. Función de descifrado de datos
3. Función hash
4. Función de firma digital
5. Indique cual es el orden creciente en base al nivel de seguridad de las siguientes técnicas de autenticación de usuarios.
6. Básica y segura, Basada en formas, Integrada, Fuerte, Basada en certificado.
7. Basada en formas, Básica y segura, Integrada, Fuerte, Basada en certificado.
8. Básica y segura, Integrada, Basada en formas, Basada en certificado, Fuerte
9. Básica y segura, Basada en formas, Integrada, Basada en certificado, Fuerte
10. Basada en formas, Básica y segura, Integrada, Basada en certificado, Fuerte
11. ¿Cuál de estos elementos corresponde a un nivel que no define requerimientos detallados de verificación en ASVS?
12. Advanced
13. Cursory
14. Opportunistic
15. Standart

ASVS: Normaliza el rango de cobertura y el nivel de rigurosidad disponible en el mercado cuando se realiza la verif de seguridad de aplicaciones web.

1. ¿Qué cantidad de PAs están definidos para el SSE-CMM?
2. 24
3. 16
4. 18
5. 22
6. ¿Qué modelo de autorización utiliza un sistema UNIX/Linux convencional para manejar sus archivos?
7. Mandatory Access Control (MAC)
8. Discretionary Access Control (DAC)
9. Role Based Access Control (RBAC)
10. Ninguna de las anteriores.
11. Marque la respuesta correcta segun indica el siguiente mensaje generado mediante el cifrado del Cesar:

"od uhvsxhvwd fruuhfwd frqwlhqh od sdodeud ixhjr"

a b c d e f g h i j k l m n o p q r s t u v w x y z

la respuesta correcta contiene la palabra fuego

1. Los fideos tienen salsa
2. Hay estrellas en el cielo
3. La torre es demasiado alta
4. El fuego se apagará pronto
5. ¿Qué mecanismo adiciona criptografía al proceso de hash con el fin de incorporar autenticación a la seguridad del mismo?
6. MD5
7. MAC
8. AES
9. Ninguna de las anteriores
10. ¿Cuál de los siguientes algoritmos se basa en la dificultad para factorizar grandes números?
11. Ninguna de estas opciones
12. RSA
13. AES
14. Elgamal
15. ¿Cuáles de los siguientes puntos NO es un objetivo de la administración de usuarios y (…)?
16. Los usuarios no pueden acceder o utilizar funcionalidades administrativas.
17. Las funciones de nivel de administrador están segregadas apropiadamente de la actividad de usuario.
18. Los usuarios transmiten información de manera cifrada y confidencial
19. Proveer la necesaria auditoria y trazabilidad de funcionalidades administrativas.
20. Dada la clave pública (p,y,n) y la clave privada (p,x,n) Indique a que algoritmo corresponden las siguientes definiciones de cifrado

a = p^n (mod n)

b = y^k m (mod n)

1. ElGamal
2. AES
3. RSA
4. Ninguna de estas opciones
5. ¿Qué mecanismo adiciona criptografía al proceso de hash con el fin de incorporar autenticación a la seguridad del mismo?
6. MAC
7. Ninguna
8. MD5
9. AES
10. ¿Cuál es el significado de SSL?
11. Secure Sockets Layer
12. Simple Socket layer
13. Secure socket level
14. Standart Socket layer
15. ¿Cuál de los siguientes elementos NO se corresponde con una propiedad de la calidad de uso?
16. Seguridad
17. Ninguna de las opciones
18. Productividad
19. Eficacia
20. Satisfacción
21. Indique cual es la definición correcta de j segun la siguiente representación de un sistema criptográfico Dj (Ej (m)) = m
22. Representa el conjunto de todos los mensajes sin cifrar
23. Representa el conjunto de transformaciones de cifrado
24. Representa el conjunto de todos los posibles mensajes cifrados
25. Representa el conjunto de claves que se pueden emplear
26. Indique a que corresponde la siguiente definición:

“Se define como una función o método para generar un valor que representa de manera casi univoca a un dato.”

1. Función de descifrado de datos
2. Función de firma digital
3. Función hash
4. Función de encriptación de datos
5. ¿Cuál de los siguientes datos NO está contenido en los campos de un certificado X500?
6. Número de serie
7. Nombre del sujeto
8. Clave privada del sujeto
9. Clave pública del sujeto

En criptografía, X.509 es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI).1​ X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. Su sintaxis, se define empleando el lenguaje ASN.1 (Abstract Syntax Notation One), y los formatos de codificación más comunes son DER (Distinguish Encoding Rules) o PEM (Privacy Enhanced Mail).

1. ¿Cuál de los siguientes puntos no es de interés para el manejo de sesiones de estado?
2. Seguridad de transporte
3. Ataques de autenticación de sesión
4. Paginas y credenciales en formularios
5. Entropía de credencial de sesión
6. ¿Cuál de estos elementos no corresponde a la lista de requerimientos de verificación de ASVS2014?
7. Cryptography at Rest
8. Authentication
9. Data protection
10. Communication
11. Mobile
12. Performance
13. ¿Cuál de los siguientes elementos NO se corresponde con una propiedad de la calidad en uso?
14. Productividad
15. Seguridad
16. Satisfacción
17. Eficacia
18. Ninguna de las anteriores

Productividad, seguridad, eficacia y satisfacción

1. ¿Que establece el marco legal para el uso de la Firma Digital en la república Argentina?
2. El pacto de San Jose de Costa Rica
3. La ley 25.506
4. La ley 24.449
5. La constitución nacional
6. ¿Qué característica de calidad interna/externa NO está contemplada de SQuaRE?
7. Portabilidad
8. Mantenibilidad
9. Ninguna de las anteriores
10. Fiabilidad

*Funcionalidad, confiabilidad, usabilidad, eficiencia, mantenibilidad, portabilidad.*

1. ¿A qué tipo de algoritmo corresponde el cifrado del Cesar?
2. Cifrado por transposición de grupos
3. Cifrado por sustitución
4. Cifrado Asimétrico
5. Cifrado de simétrico de flujo
6. ¿Cuál de estos elementos corresponde a la escala que se representa los niveles de madurez de SAMM?
7. A,B,C
8. Bajo, Medio, Alto
9. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
10. 0, 1, 2, 3