1) ¿Para que se utiliza la firma digital ?
Generar datos aleatorios
Garantizar la confidencialidad de los datos
Gatantizar la autenticidad de datos
Ninguna de estas opciones
2) ¿Cual de los siguientes algoritsmos es denominado AES ?
Serpent
Rijndael
IDEA
DES
3) ¿Que condiciona el libre uso de los algoritmos ?
Ninguna de estas opciones
Que sean publicos
Que tengan patentes en vigencia
que sean privados
4) ¿Cual de los siguientes elementos NO corresponde a una funcion de negocio de SAMM ?
Gobierno
Implementacion
Verificacion
Diseño
Construccion
5) ¿Cual de los siguientes elementos NO coresponde a una caracteristica positiva de los sistemas criptograficos simetricos
Robustez
Velocidad de cifrado
Longitud del mensaje limitada por la implementacion
Sencillez de implementacion
6) ¿Cual de los siguientes no es un modo de cifrado de bloques ?
CBC - Cipher Block Chaining
OFB - Output Feedback
CFB - Cipher Feedback
Ninguna de las opciones
7) ¿Cual de las sigueintes NO es una propiedad de la firma digital ?
Va ligada indisolublemente al mensaje
Se genera en base a la clave publica del destinatario
solo puede ser generada por su legitimo titular
es publicacmente verificable
8) ¿Que significa el acronimo CMM ?
Capacity Model Metrics
Capability Maturity Model
Capability Model and Metrics
Capacity Measure Model
9) ¿Que norma define la metodologia SCRUM ?
Ninguna de estas opciones
ISO 25000
ISO /IEC 9126
ISO/IEC14598
10) Determina el mensaje original para el siguiente cifrado obteniendo mediante el cifrado de XOR solamente.(aca practiquen muchacho)

110010000100
11) ¿A que se denomina "Padding"?
Al metodo para autenticar mensajes con algoritmos asimetricos
Al metodo para completar el inicio de un bloque de datos
Al metodo que permite generar una distorsion entre los distintos bloques
Al metodo para completar el final de un bloque de datos
12) ¿Cual de los siguientes datos no esta contenido en los campos de un certificado X509 ?
Numero de serie
Nombre de sujeto
Clave privada del sujeto
clave publica del sujeto
13) ¿Cual de los siguientes puntos no es de interes para el manejo de sesiones de estado ?
Seguridad de transporte
Ataques de autenticacion de sesion
Paginas y credenciales en formularios
Entropia de credencial de sesion
14) ¿Cual de estos elementos no corresponde a la lista de requerimientos verificacion de ASVS2014?
Cryptography at Rest
Authentication
Data Protection
Communications
Mobile
Performance
15) Indique cual es la definicion correcta de j según la siguiente representacion de un sistema criptografico Dj(Ej (m))=m
Representa el conjunto de transformaciones de cifrado
Representa el conjunto de claves que se pueden emplear
Representa el conjunto de todos los mensajes sin cifrar
Representa el conjunto de todos los posibles mensajes cifrados
16) ¿Cual de los siguientes elementos NO se corresponde con una propiedad de la Calidad en uso ?
Productividad
Seguridad
Satisfaccion
Eficacia
Ninguna de las opciones
17) ¿Que establece el marco legal para el uso de la Firma Digital en la Republica Argentina ?
El pacto de San Jose de Costa Rica
La ley 25506
La ley 24449
La constitucion nacional
18) ¿Que caracteristica de calidad interna/externa no esta contemplada en SquaRE?
Portabilidad
Mantenibilidad
Ninguna de estas opciones
Fiabilidad
19) ¿A que tipo de algoritmo corresponde el cifrado del Cesar ?
Cifrado por transposicion de grupos
Cifrado por sustitucion

Cifrado Asimetrico
Cifrado de simetrico de flujo

20) ¿Cual de los siguientes puntos No es un objetivo de la administracion de usuarios y privilegios ?
Los usuarios no pueden acceder o utilizar funcionalidades administrativas
Las funciones de nivel de administrardor estan segregadas apropiadamente de la actividad del usuario
Los usuarios transmiten informacion de manera cifradad y confidencial
Proveer la necesaria auditoria y trazabilidad de funcionalidad administrativa

21) ¿Cual de ests elementos corresponde a la escala con que se representan los niveles de madures de SAMM ?
A, B, C
Bajo, Medio,Alto
1, 2, 3, 4, 5, 6, 7, 8, 9, 10
0, 1, 2, 3

22) ¿Sobre que tecnologia estan desarrollados los Web Services ?
XML/SOAP
HTTPS
AES
HTML

23) Indique a que corresponde la siguiente definicion: Se define como una funicon o metodo para generar un valor que represente de manera casi univoca a un dato
Funcion de encriptacion de datos
Funcion de descifrado de datos
Funcion hash
Funcion de firma digital

24) Indique cual es el orden creciente en base al nivel de seguridad de las siguientes tecnicas de autenticacion de
Basica y segura, Basada en formas, Integrada, Fuerte, Basada en certificado
Basada en formas, Basica y segura, Integrada, Fuerte, Basada en certificado
Basica y segura, Integrada, Basada en formas, Basada en certificado, Fuerte
Basica y segura, Basada en formas, Integrada, Basada en certificado, Fuerte
Basada en formas, Basica y segura, Integrada Basada en certificado, Fuerte

25) ¿Cual de estos elementos corresponde a un nivel que no define requerimientos detallados de verificacion ASVS ?
Advanced
Cursory
Opportunistic
Standard

26) ¿Que cantidad de Pas estan definidos para el SSE-CMM ?
24,
16,
18,
22,

27) ¿Que modelo de autorizacion utiliza un sistema UNIX/Linux convencional para mejorar sus archivos ?
Mandatory Access Control (MAC)
Discretionary Access Control (DAC)
Roole Based Access Control (RBAC)
Ninguna de estas opciones

28) Marque la respuesta correcta según indica el siguiente mensaje generado mediante el cifrado Cesar " no voy a tipear todos los caracteres, ixhjr= fuego y vdovd = salsa " (practica)
El fuego se apagará pronto.

29) ¿Que mecanismo adiciona criptografia al proceso de hash con el fin de incorporar autenticacion a la seguridad del mismo ?
MD5
MAC
AES
Ninguna de estas opciones
30) ¿Cual de los siguientes algoritmos se basa en la dificultad para factorizar grandes numeros?
Ninguna de estas opciones
RSA
AES
ElGamal
1) ¿Que estandar se ha definido para la seguridad especifica de Web Services ?
WSDL
TLS
HTTPS
WSS
2) Dada la clave publica (p. y. n) y la clave privada (p,x,n). Indique a que algoritmo corresponden las siguientes definiciones de cifrado : a = p ´ k (mod n) y b = y ´ ´ k m (mod n)
ElGamal
AES
RSA
Ninguna de estas opciones
3) ¿Cual es el significado SSL ?
Secure Sockets Layer
SimpleSocket Layer
Secure Socket Level
Standard Socket Layer
3) ¿Cual de estos elementos no corresponde a la lista de verificacion de requerimientos...
Proteccion de Datos
Desempeño
Communications
Autenticacion
4) ¿Cual de los siguientes algoritmos NO requiere confidencialidad en la distribucion de la clave
AES
ELGamal
Ninguna de estas opciones
DES
5) ¿Que modelo de infraestructura de seguridad utiliza PGP ?
Anillo o Circulo de confianza
PKI - Infraestructura de Clave Publica
Ninguna opcion es valida
ISI - Identificacion integrada de seguridad
6) ¿Cual de las siguientes es una ventaja de los algoritmos SIMETRICOS?
No requiere confidencialidad en la distribucion de clave
La misma clave puede ser utilizada por multiples actores en la comunicación
Permite autentificar mensajes
Sencillez de implementacion

7) ¿Cual de las siguientes opciones corresponde a un modelo enfocado en la madurez de las... las caracteristicas esenciales de los procesos que deben existir en una organización para asegurar... sistemas ?
PCI DSS
ISO/IEC 21827:2008
A4609
ISO 25000
8) ¿Cual es el significado del acronimo DSA ?
Ninguna de estas opciones
Data Signature Algorithm
Digital Signature Algorithm
Dynamic Signature Algorithm
9) ¿Cual de los siguientes puntos corresponde al grupo PAs para "PROJECT AND ORGANIZATIONAL BASE PRACTICES"?
Specity Security Needs
Build Assurance Argument
Assess Security Risk
Plan Technical Effort
10) ¿Cual de los siguientes es un metodo de autorizacion en dode se asegura la informacion mediante etiquetas de sencibilidad en la informacion y comparando esto con el nivel de sensibilidad de un usuario?
Dicretionary Access Control (DAC)
Role Based Access Control (RBAC)
Mandatory Access Control (MAC)
Ninguna de las opciones
11) Según Derning, ¿cual de los siguientes elementos no es una etapa del ciclo de calidad total ?
Auditar
Planificar
Actuar
Hacer
12) La tecnologia TLS es un aporte para reducir la probabilidad de cual de los siguientes tipos de ataque ?
Fallas Criptograficas
Almacenamiento criptografico inseguro
Inyeccion
XSS - Cross site reference
13) Cual de los siguientes es la encargada de firmar documentos con la finalidad de probar que existian antes de un determinado instante de tiempo ?
Autoridad de Certificacion
Autoridad de Registro
Autoridad de Validadcion
Autoridad de Sellado de Tiempo
14) ¿A que Capability Level correpnden los siguientes common features : Objetively Managing Perfomance y Establish Measure Quality Goals
Capability level 4
Capability level 2
Capability level 5
Capability level 3
15) ¿Cual de las siguientes normas ha sido emitida por la Union Europea ?
CCPA
GDPR
HPAA

A4609

16) ¿Cual de los siguientes es una ventaja de los algoritmos Asimetricos ?

Logitud del mensaje "Ilimitada"

No requiere confidencialidad en la distribucion de clave

Velocidad de cifrado

Robustez

17) ¿Cual de las siguientes opciones NO es una buena practica para evitar vulnerabilidades de XSS ?

Validacion de entrada positiva o de "Lista blanca"

Ninguna de estas opciones

Codificar los datos no confiables basados en el contexto donde seran ubicados

Utilizar Apis de auto-sanitizacion

18) ¿Que se utiliza cuando una clave publica pierde su validez y debe ser anulada ?

La clave privada del certificado

Un certificado de revocacion

No se requieren acciones, simplemente se procede a crear un nuevo certificado

Un mail de cancelacion firmado digitalmente

19) Indique a que elemento corresponde la siguiente definicion: es un marco de trabajo abierto para ayudar a las organizaciones formular e implementar una estrategia de seguridad para software que sea adecuada a las necesidades

WSS

SAMM

SCRUM

Square

20) ¿Cual de los siguentes es un metodo de autorizacion en donde las desiciones de accesos se basan en las funciones de un individuo dentro de la organización ?

Mandatory Access Control (MAC)

Discretionary Access Control (DAC)

Ninguna de las opciones

Role Based Access Control (RBAC)

21) ¿Cual es el puerto por defecto para transmisiones HTTPS ?

843

8080,

80,

443,

22) ¿Cual de las siguientes opciones no corresponde a un protocolo para interactuar con una aplicacion sin contraseña?

HTTP

XML

Opción 2

HTTPS

23) ¿Cual de los siguientes es un metodo de autorizacion en donde se restringe el acceso a la informacion sobre la pertenencia a ciertos grupos?

DAC

MAC

DAB

POM

24) Cual de los siguientes verifica la relacion de los certificados y la identidad de sus titulares?

Autoridad de registro

Autoridad por contraseña

Implementacion de metodos asincronicos

Implementacion de metodos sincronicos

25) ¿Que tipo de algoritmo es Salsa20?

Cifrado simetrico de flujo

Cifrado por remplazo

RSA

Cifrado Vigenere

26) Cual de las siguientes es una VENTAJA de los algoritmos ASIMETRICOS?

Permite autentificar mensajes

Permite autenticar a los usuarios

Es de facil implementacion

Todas las anteriores

27) Cual de las siguientes es una DESVENTAJA de los algoritmos ASIMETRICOS?

Se requieren claves de gran extension

No es tan segura como la simetrica

Se requieren mas de 5 llaves

Ninguna de las anteriores.

28) Dentro de calidad externa-interna cual de las siguientes es una caracteristica de usabilidad?

Operabilidad

Performance

Adaptabilidad

Adecuacion

29) ¿A que corresponde la siguiente definicion? Propiedad o conjunto de propiedades inherentes a un objeto que permiten apreciarlo como mejor, igual o peor que otros objetos de su especie?

Definicion de CALIDAD de la RAE

Definicion de ADECUACION de la RAE

Definicion de USABILIDAD de la RAE

Ninguna de las anteriores es valida

30) Concepto de calidad externa-interna--- cual de las siguientes es una caracteristica de FUNCIONALIDAD?

Adecuación

Adaptabilidad

Usabilidad

Todas las anteriores

31) Concepto de calidad externa-interna... cual de las siguientes es una caracteristica de PORTABILIDAD?

Adaptabilidad

Usabilidad

Adecuacion

Todas las anteriores

32) Cual de estas tecnologias no se utiliza para la implementacion de Web Services?

A) JSON

B) SOAP

C) XML

D) WSDL

33) Cual de los siguientes elementos no corresponde a un modo de operacion por bloques para algoritmos simetricos?

A) CBC

B) ECB

C) MDQ

D) GCM

34) ¿Cual de los siguientes elementos NO se vincula al area de Portabilidad?

A) Adaptabilidad
B) Coexistencia
C) Utilizacion de recursos
D) Intercambiabilidad

35) ¿Cual es la utilidad de OWASP ASVS?
A) Normalizar el nivel de rigurosidad disponible en una verificacion de seguridad
B) Normalizar el rango de cobertura en una verificacion de seguridad
C) Todas son correctas
D) Establecer un estandar tanto para consumidores como para proveedores de servicio o herramienta.

36) ¿Cual de los siguientes algoritmos corresponde a un cifrador simetrico de flujo?
A) MARS
B) Salsa20
C) AES
D) Serpent

37) ¿Cual de los siguientes elementos no forma parte de las funciones de negocio del modelo SAMM?
A) Implementacion
B) Gobierno
C) Constitucion
D) Verificacion

38) Los cifradores de sustitucion utilizan la tecnica de
A) Permutacion de cada caracter de texto claro por otro correspondiente al texto cifrado
B) Ninguna
C) Modificacion de cada caracter de texto claro por otro correspondiente al texto cifrado
D) Calculo de hash de los caracteres del texto claro para reemplazar el texto cifrado

39) Que NO se debe registrar en un log?
A) Ids de sesion
B) Eventos legales
C) Fallos de autenticacion
D) Fallos de validacion

40) Cual de los siguientes algoritmos corresponde a un cifrador asimetrico?
A) 3DEs
B) RSA
C) AES
D) Twofish

41) Cual de las siguientes no es una buena practica para la autenticacion?
A) Utilizar sistemas de autenticacion de factor multiple
B) El uso de case sensitive para los user IDs
C) Solicitar re-autenticacion
D) Almacenar contraseñas de forma segura

¿Cómo opera el modo ECB (Electronic Codebook)?
Divide el mensaje en partes y cifra cada parte de manera independiente.
Realiza un XOR con el bloque previo antes de cifrar cada parte.
Utiliza un vector de inicialización para cifrar el mensaje.
Opera de manera similar a CFB pero con bloques de salida.

¿Cuáles son las dos ramas principales de la criptografía mencionadas en el resumen?
Clásica y Moderna
Simétrica y Asimétrica
Transposición y Sustitución

ECB y CBC

11) ¿Cuál es la diferencia entre SSE-CMM y ASVS? Desarrolle los detalles y casos de aplicación de cada uno de estos elementos en su respuesta.

12) Enumere, defina y relacione las etapas del proceso de gestión de la "Calidad Total" y su vínculo con el modelo SCRUM.