**Preguntas Parcial Seguridad y Calidad**

**Unidad 3**

1. Dada la clave publica (p, y, n) y la clave privada (p, x, n). Indique a que logaritmo corresponden las siguientes definiciones de cifrado: **(Unidad 3)**

a = p^k (mod n)

b = y^k m (mod n)

1. **ElGamal**
2. AES
3. RSA
4. Ninguna de las opciones
5. ¿Qué mecanismo adiciona criptografía al proceso de hash con el fin de incorporar autenticación a la seguridad del mismo? **(Unidad 3)**
6. **MAC**
7. MD5
8. AES
9. Ninguna de las anteriores
10. ¿Cuál es el significado de SSL? **(Unidad 3)**
11. **Secure Sockets Layer**
12. Simple Socket Layer
13. Secure Socket Level
14. Standard Socket Layer
15. Indique cual es la definición correcta de j según la siguiente representación de un sistema criptográfico: Dj (Ej (m)) = m **(Unidad 3)**
16. Representa un conjunto de todos los mensajes sin cifrar
17. Representa el conjunto de transformaciones de cifrado
18. Representa el conjunto de todos los posibles mensajes cifrados
19. **Representa el conjunto de claves que se pueden emplear**
20. Indique a que corresponde la siguiente definición: “se define como una función o método para generar un valor que representa de manera casi univoca un dato” **(Unidad 3)**
21. Función de descifrado de datos
22. Función de firma digital
23. **Función de Hash**
24. Función de encriptación de datos
25. ¿Para qué se utiliza la firma digital? **(Unidad 3)**
26. Generar datos aleatorios
27. Garantizar la confidencialidad de datos
28. **Garantizar la autenticidad de datos**
29. Ninguna de las anteriores
30. ¿Cuál de los siguientes algoritmos es denominado AES? **(Unidad 3)**
31. Serpent
32. **Rijndael**
33. IDEA
34. DES
35. ¿Que condiciona el libre uso de los algoritmos? **(Unidad 3)**
36. Que sean públicos
37. **Que tengan patentes en vigencia**
38. Que sean privados
39. Ninguna de las anteriores
40. ¿Cuál de los siguientes elementos NO corresponde a una característica positiva de los sistemas criptográficos simétricos? **(Unidad 3)**
41. Robustez
42. Velocidad de Cifrado
43. **Longitud del mensaje limitada por la implementación**
44. Sencillez de implementación
45. ¿Cuál de los siguientes NO es un modo de cifrado de bloques? **(Unidad 3)**
46. CBC – Cipher Block Chaining
47. OFB – Output Feedback
48. CFB – Cipher Feedback
49. **Ninguna de las opciones**
50. ¿Cuál de las siguientes NO es una propiedad de la firma digital? **(Unidad 3)**
51. Va ligada indisolublemente al mensaje
52. **Se genera en base a la clave pública del destinatario**
53. Solo puede ser generada por su legítimo titular
54. Es públicamente verificable
55. Determine el mensaje original para el siguiente cifrado obtenido mediante el cifrado de XOR solamente: **(Unidad 3)**

Valor cifrado: 101110110010

Contraseña: 011100110110

1. 101010100011
2. **110010000100**
3. 001110110110
4. 111100111010
5. ¿A qué se denomina “Padding”? **(Unidad 3)**
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. ¿Cuál de los siguientes datos NO está contenido en los campos de un certificado X509? **(Unidad 3)**
11. Número de serie
12. Nombre del sujeto
13. **Clave privada del sujeto**
14. Clave publica del sujeto
15. Indique cual es la definición correcta de j según la siguiente representación de un sistema criptográfico: Dj (Ej (m)) = m **(Unidad 3)**

A. Representa un conjunto de todos los mensajes sin cifrar

B. Representa el conjunto de transformaciones de cifrado  
C. Representa el conjunto de todos los posibles mensajes cifrados  
**D.** **Representa el conjunto de claves que se pueden emplear**

1. ¿A qué tipo de algoritmo corresponde el cifrado del Cesar? **(Unidad 3)**
2. Cifrado por transposición de grupos
3. **Cifrado por sustitución**
4. Cifrado Asimétrico
5. Cifrado de simétrico de flujo
6. Indique a que corresponde la siguiente definición: “se define como una función o método para generar un valor que representa de manera casi univoca un dato” **(Unidad 3)**
7. Función de descifrado de datos
8. Función de firma digital
9. **Función de Hash**
10. Función de encriptación de datos
11. Marque la respuesta correcta según indica el siguiente mensaje generado mediante el cifrado del Cesar: “od uhvsxhvwd fruuhfwd frqwlhqh od sdodeud ixhjr” **(Unidad 3)**
12. Los fideos tienen salsa
13. Hay estrellas en el cielo
14. La torre es demasiado alta
15. **El fuego se apagará pronto**
16. ¿Qué mecanismo adiciona criptografía al proceso de hash con el fin de incorporar autenticación a la seguridad del mismo? **(Unidad 3)**
17. MD5
18. **MAC**
19. AES
20. Ninguna de las anteriores
21. ¿Cuál de los siguientes algoritmos se basa en la dificultad de factorizar grandes números? **(Unidad 3)**
22. **RSA**
23. AES
24. ElGamal
25. Ninguna de las anteriores
26. ¿Cuál es el puerto por defecto para transmisiones HTTPS? **(Unidad 3)**
28. ¿Cuál de las siguientes opciones no corresponde a un protocolo para interactuar con una aplicación sin contraseña? **(Unidad 3)**

**(¿Autenticación básica?) HTTP**

1. ¿Qué tipo de algoritmo es Salsa20? **(Unidad 3)**

**Cifrado simétrico de flujo**

1. ¿Cuál de los siguientes es una ventaja de los algoritmos asimétricos? **(Unidad 3)**

**Permite autentificar mensajes**

1. ¿Cuál de las siguientes es una desventaja de los algoritmos asimétricos? **(Unidad 3)**

**Se requieren claves de gran extensión**

1. ¿Cuál de las siguientes no es una propiedad de la firma digital? **(Unidad 3)**

**Se genera en base a la clave pública del destinatario**

1. Dada la clave publica (p,y,n) y la clave privada (p,x,n). Indique a que algoritmo corresponden las siguientes definiciones de cifrado ……. (mod n) **(Unidad 3)**

**ElGammal**

1. ¿Cuál es el significado de SSL? **(Unidad 3)**

**Secure Sockets Layer**

1. ¿A qué se denomina Padding? **(Unidad 3)**

**Al método para completar el final de un bloque de datos**

1. ¿Cuál de las siguientes es una desventaja de los algoritmos asimétricos? **(Unidad 3)**

**Tamaño del mensaje cifrado es mayor**

**Unidad 4**

1. ¿Qué estándar se ha definido para la seguridad especifica de Web Services? **(Unidad 4)**
2. WSDL
3. TLS
4. HTTPS
5. **WSS**
6. ¿Cuál de los siguientes puntos NO es un objetivo de la administración de usuarios y privilegios? **(Unidad 4)**
7. Los usuarios no pueden acceder o utilizar funcionalidades administrativas
8. Las funciones de nivel de administrador están segregadas apropiadamente de la actividad del usuario
9. **Los usuarios transmiten información de manera cifrada y confidencial**
10. Proveer la necesaria auditoria y trazabilidad de funcionalidad administrativa
11. Indique cual es el orden creciente en base al nivel de seguridad de las siguientes técnicas de autenticación de usuarios **(Unidad 4)**
12. Básica y segura, integrada, basada en formularios, basada en certificado, fuerte.
13. Basada en formularios, básica y segura, integrada, fuerte, basada en certificado
14. **Básica y segura, basada en formularios, integrada, basada en certificado, fuerte**
15. Basada en formularios, básica y segura, integrada, basada en certificado, fuerte
16. Básica y segura, basada en formularios, integrada, fuerte, basada en certificado
17. ¿Cuál de los siguientes puntos NO es un objetivo de la administración de usuarios y privilegios? **(Unidad 4)**
18. Los usuarios no pueden acceder o utilizar funcionalidades administrativas
19. Las funciones de nivel de administrador están segregadas apropiadamente de la actividad del usuario
20. **Los usuarios transmiten información de manera cifrada y confidencial**
21. Proveer la necesaria auditoria y trazabilidad de funcionalidad administrativa
22. ¿Sobre qué tecnología están desarrollados los Web Services? **(Unidad 4)**
23. **XML/SOAP**
24. HTTPS
25. AES
26. HTML
27. Indique cual es el orden creciente en base al nivel de seguridad de las siguientes técnicas de autenticación de usuarios **(Unidad 4)**
28. Básica y segura, integrada, basada en formularios, basada en certificado, fuerte.
29. Basada en formularios, básica y segura, integrada, fuerte, basada en certificado
30. **Básica y segura, basada en formularios, integrada, basada en certificado, fuerte**
31. Basada en formularios, básica y segura, integrada, basada en certificado, fuerte
32. Básica y segura, basada en formularios, integrada, fuerte, basada en certificado
33. Que modelo de autorización utiliza un sistema UNIX/Linux convencional para manejar sus archivos? **(Unidad 4)**
34. Mandatory Access Control (MAC)
35. **Discretionary Access Control (DAC)**
36. Role Based Access Control (RBAC)
37. Ninguna de las anteriores
38. ¿Cuál de los siguientes es un método de Autorización en donde se restringe el acceso a la información sobre la pertenencia a ciertos grupos? **(Unidad 4)**

**Discretionary Access Control (DAC)**

1. ¿Cuál de los siguientes es un método de Autorización en donde se asegura la información mediante la asignación de etiquetas de sensibilidad en la información y comparando esta con el nivel de sensibilidad de un usuario está operando? **(Unidad 4)**

**Mandatory Access Control (MAC)**

**Unidad 5**

1. ¿Cuál de los siguientes elementos NO se corresponde con una propiedad de la Calidad en Uso? **(Unidad 5)**
2. Seguridad
3. Productividad
4. Eficacia
5. Satisfacción
6. **Ninguna de las anteriores**
7. ¿Cuál de los siguientes elementos NO corresponde con una propiedad de la Calidad en Uso? **(Unidad 5)**
8. Productividad
9. Seguridad
10. Satisfacción
11. Eficacia
12. **Ninguna de las opciones**
13. Que característica de la calidad Interna/externa NO está contemplada en SQuaRE? **(Unidad 5)**
14. Portabilidad
15. Mantenibilidad
16. Fiabilidad
17. **Ninguna de las anteriores**
18. Según Deming ¿Cuál de los siguientes elementos no es una etapa del ciclo de calidad total? **(Unidad 5)**

**El que no es ni planificar, hacer, verificar, actuar**

1. ¿Dentro de calidad externa-interna cuál de las siguientes es una característica de usabilidad? **(Unidad 5)**

**Operabilidad**

1. ¿A que corresponde la siguiente definición “Propiedad o conjunto de propiedades inherentes a un objeto que permiten apreciarlo como mejor, igual o peor que otros objetos de su especie”? **(Unidad 5)**

**Definición de calidad de la RAE**

1. Concepto de calidad interna-externa… ¿Cuál de las siguientes es una característica de Capacidad de mantenimiento? **(Unidad 5)**

**Estabilidad**

1. Características de calidad externa-interna… ¿Cuál de las siguientes es una característica de Funcionalidad? **(Unidad 5)**

**Adecuación**

1. Características de calidad externa-interna… ¿Cuál de las siguientes es una característica de Portabilidad? **(Unidad 5)**

**Adaptabilidad**

**Unidad 6**

1. ¿Cuál de estos elementos no corresponde a la lista de requerimientos verificación de ASVS2014? **(Unidad 6 – vieja)**
2. Cryptography at Rest
3. Authentication
4. Communications
5. Data Protection
6. **Performance**
7. Mobile
8. ¿Cuál de los siguientes elementos NO corresponde a una función de negocio de SAMM? **(Unidad 6)**
9. Gobierno
10. Implementación
11. Verificación
12. Diseño
13. **Construcción**
14. ¿Qué significa el acrónimo CMM? **(Unidad 6)**
15. Capacity Model Metrics
16. **Capability Maturity Model**
17. Capability Model and Metrics
18. Capacity Measure Model
19. ¿Qué norma define la metodología de SCRUM? **(Unidad 6)**
20. ISO 25000
21. ISO/IEC 9126
22. ISO/IEC 14598
23. **Ninguna de las anteriores**
24. ¿Cuál de estos elementos NO corresponde a la lista de requerimientos verificación de ASVS 2014? **(Unidad 6 – vieja)**
25. Cryptography at Rest
26. Authentication
27. Communications
28. Data Protection
29. **Performance**
30. Mobile
31. ¿Que establece el marco legal para el uso de la Firma Digital en la República Argentina? **(Unidad 6)**
32. El Pacto de San José de Costa Rica
33. **La Ley 25.506**
34. La Ley 24.449
35. La Constitución Nacional
36. ¿Cuál de estos elementos corresponde la escala con que se representan los niveles de madurez de SAMM? **(Unidad 6)**
37. A, B, C
38. Bajo, Medio, Alto
39. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
40. **0, 1, 2, 3**
41. ¿Cuál de estos elementos corresponde a un nivel que no define requerimientos detallados de verificación en ASVS? **(Unidad 6)**
42. Advanced
43. **Cursory**
44. Opportunistic
45. Standard
46. ¿Qué cantidad de Pas están definidas para el SSE-CMM? **(Unidad 6)**
47. 24
48. 16
49. 18
50. **22**
51. ¿Cuál de los siguientes puntos corresponde al grupo de .. para “PROJECT AND ORGANIZATIONAL BASE PRACTICES”? **(Unidad 6)**

**Plan technical effort**