**Preguntas Parcial Seguridad y Calidad**

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. 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. ¿Cuál de los siguientes elementos NO se corresponde con una propiedad de la Calidad en Uso? **(Unidad 5)**
16. Seguridad
17. Productividad
18. Eficacia
19. Satisfacción
20. **Ninguna de las anteriores**
21. Indique cual es la definición correcta de j según la siguiente representación de un sistema criptográfico: Dj (Ej (m)) = m **(Unidad 3)**
22. Representa un 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 un dato” **(Unidad 3)**
27. Función de descifrado de datos
28. Función de firma digital
29. **Función de Hash**
30. Función de encriptación de datos
31. ¿Cuál de estos elementos no corresponde a la lista de requerimientos verificación de ASVS2014? **(Unidad 6 – vieja)**
32. Cryptography at Rest
33. Authentication
34. Communications
35. Data Protection
36. **Performance**
37. Mobile
38. ¿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
39. Enumere, defina y relacione las etapas del proceso de gestión de la Calidad Total y su vinculo con el modelo SCRUM.

Parcial 2

1. ¿Para qué se utiliza la firma digital? **(Unidad 3)**
2. Generar datos aleatorios
3. Garantizar la confidencialidad de datos
4. **Garantizar la autenticidad de datos**
5. Ninguna de las anteriores
6. ¿Cuál de los siguientes algoritmos es denominado AES? **(Unidad 3)**
7. Serpent
8. **Rijndael**
9. IDEA
10. DES
11. ¿Que condiciona el libre uso de los algoritmos? **(Unidad 3)**
12. Que sean públicos
13. Que tengan patentes en vigencia
14. **Que sean privados**
15. Ninguna de las anteriores
16. ¿Cuál de los siguientes elementos NO corresponde a una función de negocio de SAMM? **(Unidad 6)**
17. Gobierno
18. Implementación
19. Verificación
20. Diseño
21. **Construcción**
22. ¿Cuál de los siguientes elementos NO corresponde a una característica positiva de los sistemas criptográficos simétricos? **(Unidad 3)**
23. Robustez
24. Velocidad de Cifrado
25. **Longitud del mensaje limitada por la implementación**
26. Sencillez de implementación
27. ¿Cuál de los siguientes NO es un modo de cifrado de bloques? **(Unidad 3)**
28. CBC – Cipher Block Chaining
29. OFB – Output Feedback
30. CFB – Cipher Feedback
31. **Ninguna de las opciones**
32. ¿Cuál de las siguientes NO es una propiedad de la firma digital? **(Unidad 3)**
33. Va ligada indisolublemente al mensaje
34. **Se genera en base a la clave pública del destinatario**
35. Solo puede ser generada por su legítimo titular
36. Es públicamente verificable
37. ¿Qué significa el acrónimo CMM? **(Unidad 6)**
38. Capacity Model Metrics
39. **Capability Maturity Model**
40. Capability Model and Metrics
41. Capacity Measure Model
42. ¿Qué norma define la metodología de SCRUM? **(Unidad 6)**
43. ISO 25000
44. ISO/IEC 9126
45. ISO/IEC 14598
46. **Ninguna de las anteriores**
47. 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. ¿Cuál de los siguientes puntos NO es de interés para el manejo de sesiones de estado? **(No esta)**
16. Seguridad de transporte
17. Ataques de autenticación de sesión
18. Paginas y credenciales en formularios
19. Entropía de credencial de sesión
20. ¿Cuál de estos elementos NO corresponde a la lista de requerimientos verificación de ASVS 2014? **(Unidad 6 – vieja)**
21. Cryptography at Rest
22. Authentication
23. Communications
24. Data Protection
25. **Performance**
26. Mobile
27. Indique cual es la definición correcta de j según la siguiente representación de un sistema criptográfico: Dj (Ej (m)) = m **(Unidad 3)**
28. Representa un conjunto de todos los mensajes sin cifrar
29. Representa el conjunto de transformaciones de cifrado
30. Representa el conjunto de todos los posibles mensajes cifrados
31. **Representa el conjunto de claves que se pueden emplear**
32. ¿Cuál de los siguientes elementos NO corresponde con una propiedad de la Calidad en Uso? **(Unidad 5)**
33. Productividad
34. Seguridad
35. Satisfacción
36. Eficacia
37. **Ninguna de las opciones**
38. ¿Que establece el marco legal para el uso de la Firma Digital en la República Argentina? **(Unidad 6)**
39. El Pacto de San Jose de Costa Rica
40. **La Ley 25.506**
41. La Ley 24.449
42. La Constitución Nacional
43. Que característica de la calidad Interna/externa NO está contemplada en SQuaRE? **(Unidad 5)**
44. Portabilidad
45. Mantenibilidad
46. Fiabilidad
47. **Ninguna de las anteriores**
48. ¿A qué tipo de algoritmo corresponde el cifrado del Cesar? **(Unidad 3)**
49. Cifrado por transposición de grupos
50. **Cifrado por sustitución**
51. Cifrado Asimétrico
52. Cifrado de simétrico de flujo
53. ¿Cuál de los siguientes puntos NO es un objetivo de la administración de usuarios y privilegios? **(Unidad 4)**
54. Los usuarios no pueden acceder o utilizar funcionalidades administrativas
55. Las funciones de nivel de administrador están segregadas apropiadamente de la actividad del usuario
56. **Los usuarios transmiten información de manera cifrada y confidencial**
57. Proveer la necesaria auditoria y trazabilidad de funcionalidad administrativa
58. ¿Cuál de estos elementos corresponde la escala con que se representan los niveles de madurez de SAMM? **(Unidad 6)**
59. A, B, C
60. Bajo, Medio, Alto
61. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
62. **0, 1, 2, 3**
63. ¿Sobre qué tecnología están desarrollados los Web Services? **(Unidad 4)**
64. **XML/SOAP**
65. HTTPS
66. AES
67. HTML
68. 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)**
69. Función de descifrado de datos
70. Función de firma digital
71. **Función de Hash**
72. Función de encriptación de datos
73. Indique cual es el orden creciente en base al nivel de seguridad de las siguientes técnicas de autenticación de usuarios **(Unidad 4)**
74. Básica y segura, integrada, basada en formularios, basada en certificado, fuerte.
75. Basada en formularios, básica y segura, integrada, fuerte, basada en certificado
76. **Básica y segura, basada en formularios, integrada, basada en certificado, fuerte**
77. Basada en formularios, básica y segura, integrada, basada en certificado, fuerte
78. Básica y segura, basada en formularios, integrada, fuerte, basada en certificado
79. ¿Cuál de estos elementos corresponde a un nivel que no define requerimientos detallados de verificación en ASVS? **(Unidad 6)**
80. Advanced
81. **Cursory**
82. Opportunistic
83. Standard
84. ¿Qué cantidad de Pas están definidas para el SSE-CMM? **(Unidad 6)**
85. 24
86. 16
87. 18
88. **22**
89. Que modelo de autorización utiliza un sistema UNIX/Linux convencional para manejar sus archivos? **(Unidad 4)**
90. Mandatory Access Control (MAC)
91. **Discretionary Access Control (DAC)**
92. Role Based Access Control (RBAC)
93. Ninguna de las anteriores
94. Marque la respuesta correcta según indica el siguiente mensaje generado mediante el cifrado del Cesar: “od uhvsxhvwd fruuhfwd frqwlhqh od sdodeud ixhjr” **(Unidad 3)**
95. Los fideos tienen salsa
96. Hay estrellas en el cielo
97. La torre es demasiado alta
98. **El fuego se apagará pronto**
99. ¿Qué mecanismo adiciona criptografía al proceso de hash con el fin de incorporar autenticación a la seguridad del mismo? **(Unidad 3)**
100. MD5
101. **MAC**
102. AES
103. Ninguna de las anteriores
104. ¿Cuál de los siguientes algoritmos se basa en la dificultad de factorizar grandes números? **(Unidad 3)**
105. **RSA**
106. AES
107. ElGamal
108. Ninguna de las anteriores

**Parcial 3**

1. ¿Cuál es el puerto por defecto para transmisiones HTTPS? **(Unidad 3)**
3. ¿Cuál de las siguientes opciones no corresponde a un protocolo para interactuar con una aplicación sin contraseña? **(Unidad 3)**

**(¿Autenticación básica?) HTTP**

1. 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. ¿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 verifica la relación de los certificados y la identidad de sus titulares?

**Autoridad de registro**

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

**Cifrado simétrico de flujo**

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)**

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 los siguientes puntos corresponde al grupo de .. para “PROJECT AND ORGANIZATIONAL BASE PRACTICES”? **(Unidad 6)**

**Plan technical effort**

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

**Estabilidad**

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

**Tamaño del mensaje cifrado es mayor**

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**