**BLOQUE II: PROTECCIÓN Y GARANTIA DE LA INFORMACIÓN**

1. Desde la perspectiva de la seguridad, una organización es responsable de proteger a sus clientes...
2. la infraestructura y la plataforma de ejecución.
3. y a los servicios.
4. la infraestructura y a los proveedores de *peering services*.
5. la infraestructura y la confidencialidad de la infraestructura y la plataforma de ejecución formación.
6. Un sistema de seguridad que protege a los clientes del sistema, mantiene la confidencialidad e integridad de su información, pero además...
7. incluye funciones de búsqueda y compartición de interfaces.
8. les permite utilizar cualquier tipo de acción necesaria para conseguir los fines de los clientes.
9. protege a unos de las acciones indebidas de otros clientes.
10. mantiene la disponibilidad del servicio de confidencialidad.
11. En nuestra disciplina, interpretamos la confianza (trust) como cierta medida de...
12. la integridad de los sujetos del sistema.
13. las cualidades recomendables del algún objeto del sistema.
14. la seguridad con la que afirmamos algo.
15. la verosimilitud de la afirmación de la integridad de alguien o algo.
16. Cuando decimos que un sujeto confía (trust) en otro interpretamos que...
17. sus acciones son confiadas por ese otro sujeto.
18. depende de él sin reservas para ejecutar un conjunto de acciones.
19. depende de ese otro para ejecutar un conjunto de acciones.
20. ese otro realiza ciertas acciones sin haber hecho reserva previa.
21. En un dominio de confianza, dependemos sin reservas...
22. de la existencia de una autoridad de seguridad.
23. de un conjunto de relaciones y actividades entre sujetos y objetos.
24. de la existencia de una política de seguridad.
25. del respeto de las entidades a la política de seguridad del sistema.
26. ¿Es cierto que un sujeto que pertenece a un dominio de seguridad puede confiar en otro?
27. Sí, en general.
28. Sí, si éste pertenece al mismo dominio de seguridad.
29. No, pues entonces habría una cadena de dependencias.
30. No, pues entonces generaría otro dominio de seguridad distinto.
31. La característica básica que define de pertenencia de una entidad a un dominio de confianza es...
32. que respeta las reglas de seguridad del dominio de seguridad.
33. que presenta relaciones con objetos y sujetos del dominio de confianza.
34. que respeta a la autoridad del dominio de seguridad.
35. que confía en las reglas de seguridad.
36. Pongamos que Luis pertenece al dominio de confianza de Carlos cuando va pilotando su vehículo en un rally oficial. ¿Es posible que Luis, pueda darle instrucciones incorrectas a su piloto?
37. Sí, y eso le excluye automáticamente del dominio de confianza de Carlos.
38. No, pues un sujeto del dominio de confianza siempre realiza acciones correctas.
39. Sí, aunque posiblemente tenga repercusiones en su futura pertenencia al dominio de confianza de Carlos.
40. Sí, siempre que el canal de comunicación no sea seguro.
41. Usuarios desconfiados los hay en todas partes, pero en un ámbito de seguridad extrema, si decidimos incluir en nuestro dominio de confianza cierto software crítico, además de confiar en el código del programa debemos...
42. compilar/interpretar la aplicación en nuestra propia plataforma.
43. comprobar el hash del paquete que instalamos.
44. lanzar la aplicación a mano.
45. construir nosotros mismos el código.
46. Una definición moderna de servicios de seguridad incluye el siguiente catálogo:
47. Autenticación, Integridad, Disponibilidad, Autorización, y Contabilidad.
48. Autenticación, Confidencialidad, Autorización, Contabilidad y Disponibilidad.
49. Monitorización, Contabilidad, Disponibilidad, Autorización y Autenticación.
50. Autorización, Contabilidad, Disponibilidad, Autenticación y Monitorización.
51. La definición de servicios básicos de seguridad indicada en la norma ISO 7498 (también conocida como ITU X .800) se centra, como ya sabemos, en el entorno de las comunicaciones, y especifica como servicios básicos...
52. Autenticación, Integridad de Datos, No Repudio, Confidencialidad y Control de Acceso.
53. Autorización, Autenticación, No Repudio, Confidencialidad y Control de Acceso.
54. Integridad de Datos, Contabilidad, Confidencialidad, No Repudio y Control de Acceso.
55. No Repudio, Control de Acceso, Contabilidad, Confidencialidad y Autenticación.
56. Para garantizar la "integridad de la información" proporcionada por el Servicio de Integridad, debe obedecerse...
57. la separación de deberes y la utilización de transacciones bien formadas.
58. la integridad de datos y la separación de deberes.
59. la disponibilidad de la información y la integridad de datos.
60. la separación de derechos y la disponibilidad de la información.
61. El servicio de seguridad encargado de la disponibilidad (availability) consigue su cometido apoyado por los servicios de "prevención de la denegación de acceso al servicio", "restauración/continuidad de los servicios e información" y...
62. "contabilidad".
63. "integridad de tiempo de acceso".
64. “prevención de fallo del servicio".
65. "accesibilidad transparente a errores".
66. El servicio de autenticación proporciona autenticación a los sujetos y fuentes de datos. En concreto, el servicio de autenticación de la identidad de los sujetos que se comunican lo denominamos autenticación…
67. de origen de datos
68. de par-entidad.
69. de usuario.
70. de acceso.
71. Cuando hablamos de criptosistemas que implican intercambios de mensajes entre principales para proporcionar servicios de seguridad, nos referimos concretamente a...
72. los protocolos criptográficos.
73. transformación criptográfica.
74. mecanismo criptográfico, en general.
75. función criptográfica.
76. Un mecanismo criptográfico como OFB soportado por IDEA lo calificamos de la forma más específica posible como...
77. una función criptográfica.
78. un protocolo criptográfico.
79. un criptosistema.
80. una transformación criptográfica.
81. Una transformación criptográfica irreversible es, por ejemplo,...
82. RSA
83. 3DES
84. MD5
85. CDC con DES
86. Cierto criptoanalista ha encontrado una debilidad en un criptosistema de obtención de hash donde resulta fácil encontrar un documento que produzca el mismo valor de dispersión que otro de partida. Decimos que esta función de hash carece de la…
87. propiedad de irreversibilidad.
88. propiedad de dificultad de cómputo.
89. propiedad fuerte de resistencia a la colisión.
90. propiedad débil de resistencia a la colisión.
91. Un algoritmo que no presenta muy buenos resultados desde el punto de v ista de resistencia a la colisión hash es...
92. MD5
93. SHA-2
94. RIPEMD-160
95. SHA-1
96. La utilización de una función hash, sin más añadidos, resulta útil para obtener el servicio de...
97. integridad y autenticación.
98. confidencialidad.
99. autenticación.
100. integridad de datos.
101. Una transformación criptográfica hash compaginada con el uso de un secreto de emisor nos permite crear un servicio de...
102. autenticación de origen de datos, y protección de acceso.
103. integridad y autenticación de origen de datos.
104. integridad de usuario y autenticación de datos.
105. confidencialidad y autenticación de usuario.
106. El algoritmo ROT-13 o de encriptación "de César" es un mecanismo criptográfico...
107. de encriptación irreversible.
108. de encriptación simétrica.
109. esteganográfico.
110. de encriptación asimétrica.
111. Usualmente, el mecanismo criptográfico OTP suele emplearse con...
112. fragmentos de texto aleatorios.
113. claves criptográficas seudoaleatorias.
114. canales de comunicación sin pérdida.
115. claves criptográficas totalmente aleatorias.
116. El modo de operación de encriptación más apropiado para la encriptación de caracteres aislados parece ser...
117. ECB
118. CBC
119. OFB
120. CFB
121. Si estamos en EE.UU. y trabajamos para una organización del gobierno, tenemos que utilizar para el servicio de confidencialidad...
122. RC4, o mejor RC5.
123. DES
124. IDEA
125. AES
126. El ataque criptográfico donde el criptoanalista tiene acceso a textos en claro y criptogramas pero donde puede elegir los textos, se denomina ataque...
127. con texto en claro conocido.
128. con texto en claro escogido.
129. con criptograma escogido.
130. con clave escogida.
131. Una de las ventajas importantes de la criptografía asimétrica de clave pública actual es...
132. que facilita la solución del problema de distribución de claves.
133. que la desencriptación es menos costosa computacionalmente que los algoritmos de clave simétrica al uso.
134. las claves son sensiblemente más cortas que en la criptografía simétrica, con mejor grado de protección.
135. que la encriptación es menos costosa computacionalmente que los algoritmos de clave simétrica al uso.
136. En la mayoría de los protocolos criptográficos complejos intervienen diversos algoritmos y longitudes de claves de funciones de encriptación. A un conjunto completo de ellos que resuelve una situación concreta de comunicación lo llamamos...
137. criptosistema.
138. clave de cifra.
139. mecanismo criptográfico.
140. suite de cifrado.