A rellenar por el profesor: 1

A:_____ **B**:_____ **Calif.**:_____

Seguridad en Tecnologías de la Información

10 de febrero de 2012. Examen

Apellidos y Nombre: _____ D.N.I.: _____

A. Indique si cada uno de los siguientes enunciados es verdadero o falso, colocando una V o una F en la casilla correspondiente. Tenga en cuenta que las respuestas erróneas restan la mitad del valor de una respuesta correcta (5.0 puntos).

1. Las copias de seguridad no deben estar físicamente en el mismo lugar que el sistema. [ ]
2. Un sistema se considera seguro si la probabilidad de que se produzca un robo de datos, una manipulación, o una interrupción del servicio, está por debajo de un límite tolerable. [ ]
3. En Criptografía, hay que suponer que un atacante lo sabe todo sobre nuestro sistema, excepto los valores concretos de las claves que emplea. [ ]
4. El control de acceso por contraseñas es un método que deposita la responsabilidad en el usuario. [ ]
5. Una *Honeynet* captura habitualmente poca información, pero de mucho valor. [ ]
6. Lo más razonable es tener una copia de seguridad, que se irá sobreescribiendo cada vez que se genere otra. [ ]
7. Una *condición de carrera* se produce cuando dos recursos de red compiten por acceder a un mismo proceso. [ ]
8. El elemento más característico de una *honeynet* de segunda generación (GenII) es el *honeywall*. [ ]
9. Existen programas *maliciosos* diseñados expresamente para eliminar vulnerabilidades de los sistemas. [ ]
10. Un *bugtraq* es una lista de correo electrónico sobre vulnerabilidades y temas de seguridad. [ ]
11. Es inadmisible que Internet sea una red insegura; deberían prohibirla mientras puedan cometerse en ella crímenes tales como descargar discos de Chenoa, Ramoncín o Jarabe de Palo. [ ]
12. AES (Rijndael) es uno de los algoritmos criptográficos más modernos, y está considerado como muy seguro. [ ]
13. Es conveniente tener la misma contraseña para los servicios esenciales, ya que así será más fácil de memorizar. [ ]
14. Una *asociación de seguridad* en IPSec es una relación unidireccional entre un emisor y un receptor que ofrece servicios de seguridad al tráfico que transporta. [ ]
15. Las *vulnerabilidades* de un sistema pueden ser debidas al diseño, al uso o a la implementación. [ ]
16. Podemos considerar que todos los sistemas informáticos tienen vulnerabilidades. [ ]
17. Un sistema de archivos emplea el control de accesos para garantizar la confidencialidad y la disponibilidad de los datos. [ ]
18. La *ingeniería social* consiste en aprovechar vulnerabilidades en redes como *Facebook* o *Tuenti*. [ ]
19. El algoritmo de Diffie-Hellman es un refinamiento sobre el algoritmo RSA. [ ]
20. La inversión en seguridad en una empresa debe ser la necesaria para hacerla totalmente segura. [ ]
21. Las expectativas de seguridad representan el funcionamiento ideal de un sistema. [ ]

22. El algoritmo DES no se considera seguro porque puede romperse por la fuerza bruta. [ ]
23. Los cifrados monoalfabéticos son aquellos en los que una letra del texto claro se convierte siempre en la misma letra en el texto cifrado. [ ]
24. El algoritmo RC4 emplea 256 S–Cajas. [ ]
25. Una *auditoría de seguridad* es el proceso de generar, almacenar y revisar eventos de un sistema de forma cronológica. [ ]
26. La criptografía asimétrica permite resolver el problema de la distribución de claves. [ ]
27. Los distintos usuarios de un sistema operativo poseen *cuentas*, con una serie de privilegios asociados. [ ]
28. Los ataques a un sistema informático sólo pueden ser llevados a cabo por personas con muchos conocimientos y gran motivación. [ ]
29. Se dice que un Sistema de Detección de Intrusiones da respuestas activas cuando está programado para contraatacar a los intrusos que detecte. [ ]
30. Las copias de seguridad o *backups* deben realizarse con frecuencia. [ ]

B. Conteste brevemente **cinco** de las siguientes preguntas (5.0 puntos).

1. Enumere y explique los tres tipos de autentificación de un usuario frente a un sistema informático.
2. Enumere y explique brevemente al menos dos estrategias de prevención de alteraciones en sistemas de ficheros.
3. Defina el concepto de Criptoanálisis. ¿Qué entendemos por *ataque*?
4. Enumere y explique brevemente los tres elementos básicos de la arquitectura de seguridad OSI.
5. ¿Cuáles son las características principales de un *sistema trampa*?
6. Explique brevemente tres tipos de programas *maliciosos*.