POF: PRUEBA OBJETIVA FINAL			
Denominación del curso	IFCT0109. Seguridad Informática	**Código curso:**	23-38/002065
Denominación del MF/ UF	MF0489_3 Sistemas seguros de acceso y transmisión de datos	**Fecha:**	22/10/2024
		Duración:	60 minutos
Nombre Docente Examinador	Benito Manuel González Rodríguez	**Firma Docente**	
Nombre y apellido del alumno/a **DNI**	Vicente López Chávez 45457006J	**Firma Alumno**	*Vicente López*
		Nota Obtenida	

INSTRUCCIONES:

- Lea detenidamente la prueba y conteste a los siguientes ítems.
- La prueba tiene una duración de 60 minutos.

PRUEBA OBJETIVA FINAL

Seguridad Informática.

MF0489_3 Sistemas seguros de acceso y transmisión de datos

Marca con una "x" en las casillas de "V" (verdadero) o "F" (falso) según sean las siguientes afirmaciones. Se recomienda en estos ítems que se contesten los que se sepan ya que los errores restan puntuación. El valor de cada pregunta correcta será de 1 punto.

1. **En la criptografía de CLAVE PÚBLICA los comunicantes deben disponer de la misma clave secreta para acceder al contenido del mensaje** V__ F__

2. **Cuando se realiza un seguimiento de todas las acciones de los usuarios del sistema, de modo que todos ellos sean responsables de sus acciones se habla de AUTENTICIDAD** V__ F__

3. **REVOCAR UN CERTIFICADO consiste en invalidarlo, consiguiendo que posteriores usos de la clave privada no se consideren legítimos** V__ F__

4. **DIFFIE Y HELLMAN propusieron un protocolo para establecer una clave compartida a través de un canal inseguro.** V__ F__

5. **Para obtener un certificado de clave pública NO es necesario identificarse en una Autoridad de Registro (AR), es opcional** V__ F__

6. **Las infraestructuras de gestión de privilegio (PMI), permiten administrar de manera eficaz los permisos o acciones que una determinada entidad está autorizada a realizar** V__ F__

7. **Las VPN permiten que equipos físicamente distantes se comporten como si estuvieran dentro del mismo dominio de seguridad, es decir, en la misma red** V__ F__

8. **El propósito de IPsec es facilitar la verificación en línea de los certificados evitando posibles fallos en el proceso de revocación** V__ F__

9. **SSL VPN es una forma de utilizar VPN en la que se utiliza el navegador web para establecer la conexión entre dos extremos** V__ F__

10. **La criptografía de CLAVE PÚBLICA hace uso de claves distintas para el cifrado y el descifrado de los mensajes, de modo que cada usuario tiene un par de claves: una pública y una privada.** V__ F__

A continuación, presentamos una serie de ítems de selección múltiple, para responder señala con una "X" la respuesta correcta. Recuerda que el error se penaliza. Si te equivocas, rodea con un círculo la "x" y vuelve a marcar con una "X". 1 punto.

11. **El protocolo en el que cada comunicante dispone de un par de claves, una conocida por todos (pública) y otra sólo conocida por el poseedor (privada) es la criptografía…**
    a) Simétrica
    b) PKI
    c) Enigma
    d) De clave pública

12. **La magnitud que permite medir esa incertidumbre y la cantidad de información de un determinado mensaje es la…**
    a) Asimetría
    b) Autenticación
    c) Entropía
    d) Certificación

13. **Cuando una determinada entidad no puede alegar que no ha realizado una acción, se habla de…**
    a) No repudio
    b) Autenticación
    c) Integridad
    d) Entropía

14. **Un documento electrónico que vincula a una entidad (persona, servidor, etc.) con un par de claves que pueden utilizarse tanto para firmar digitalmente como para cifrar es…**
    a) Un algoritmo de cifrado simétrico
    b) Un certificado digital
    c) Una infraestructura de clave pública
    d) Un protocolo de cifrado

15. La posibilidad de que una CA pueda emitir un certificado para otra CA que le permita a la segunda emitir certificados que sean válidos también para la primera es la Certificación…

a) Asíncrona
b) Revocada
c) Cruzada
d) De Diffie-Hellman

16. El prestador de servicios de certificación que asegura la autenticidad, validez e integridad de las transacciones más críticas, es la Autoridad de…

a) Registro
b) Validación
c) Certificación
d) Revocación

17. De las siguientes entidades, ¿Cuál no pertenece a una Infraestructura de clave pública (PKI)…

a) Autoridad de certificación
b) Autoridad de autentificación
c) Autoridad de registro
d) Autoridad de validación

18. El servicio que permite crear una red privada a partir de una red pública insegura se denomina…

a) Cifrado asimétrico
b) Autoridad de Certificación
c) Red privada virtual (VPN)
d) Infraestructura de clave pública (PKI)

19. Los certificados que vinculan a un individuo con una clave pública manteniéndose en secreto la clave privada asociada, se denominan certificados...

a) De atributos
b) SSL
c) De no repudio
d) Digitales

20. ¿Cuál de las siguientes no es una aplicación de las Infraestructuras de clave pública?

a) Autenticación
b) Cifrado
c) Funciones resumen
d) Firma electrónica

A continuación, presentamos una serie de ítems de completar. Para responder rellena la línea de puntos con la respuesta correcta. Puntuación: 1 punto.

21. La misión de una ……. es gestionar el ciclo de vida de los certificados de clave pública.

22. En criptografía, las funciones ……. Son aquellas que, dado un mensaje de cualquier tamaño, producen una salida de un tamaño fijo.

23. Los cifradores **…….** son adecuados cuando los datos que van a cifrarse son continuos y no se conoce su tamaño.

24. En los sistemas criptográficos ……. La clave de cifrado es la misma que la de descifrado

25. Las …… permiten que equipos físicamente distantes se comporten como si estuvieran dentro del mismo dominio de seguridad, es decir, en la misma red.

A continuación, presentamos una serie de ítems de respuesta breve. Para responder rellena la línea de puntos con la respuesta correcta. Puntuación: 1 punto.

26. Define y explica las diferencias entre Autoridad de Certificación, Autoridad de Registro y Autoridad de Validación:

27. ¿Cuáles son los cuatro elementos fundamentales del sistema de firma digital?

28. **Explica las diferencias entre cifradores de flujo y de bloque:**

A continuación, presentamos una serie de ítems de respuesta de correspondencia. Deber relacionar las premisas a la derecha con las respuestas a la derecha. Para responder traza una flecha de cada premisa a su respuesta o respuestas, Si te equivocas, marca la flecha con una x. También puedes poner la correspondencia entre las letras y números. Por ejemplo: B2, C6… Puntuación: 2 puntos.

29. Relaciona los conceptos de la izquierda con los nombres de la derecha.

A. PKI
B. VPN
C. RESUMEN

1) SSH
2) AUTORIDAD DE VALIDACIÓN (VA)
3) DIGEST
4) IPSEC
5) AUTORIDAD DE CERTIFICACIÓN (CA)
6) SSL
7) HASH

Solución: _____

30. Relaciona las capas del modelo OSI con sus nombres

1) CAPA 1	A. NIVEL DE ENLACE
2) CAPA 2	B. NIVEL DE SESION
3) CAPA 3	C. NIVEL FÍSICO
4) CAPA 4	D. NIVEL DE RED
5) CAPA 5	E. NIVEL DE PRESENTACIÓN
6) CAPA 6	F. NIVEL DE TRANSPORTE

Solución: _____

Fdo. _____

PLANTILLA DE CORRECCIÓN
IFCT0109. Seguridad Informática
MF0489_3 Sistemas seguros de acceso y transmisión de datos

Puntuación:

Ítems de verdadero/Falso
Puntuación=1 Punto
Fórmula P=A-E

Ítems de selección múltiple
Puntuación=1 Punto
Fórmula P=A-(E/3)

Ítems de texto incompleto
Puntuación=1 Punto
Fórmula P=A

Ítems de respuesta breve
Puntuación=1 Punto
Fórmula P=A

De correspondencia
Puntuación
2 puntos = 0 errores
1 punto =1 error
0 puntos > 1 errores