|  |
| --- |
| Tema 3 |
|  |
| Programación de servicios y procesos 2ºDAM  Rodrigo Tapiador Cano |

5.1. ¿Cómo se llama al par identificador-contraseña de un sistema de seguridad?

Respuesta: b) Credencial.

Justificación: Una credencial es un par compuesto por un identificador y una contraseña, utilizado para autenticar a un usuario en un sistema de seguridad.

Referencia: [**Credenciales | Cyberzaintza**](https://www.ciberseguridad.eus/ciberglosario/credenciales)

5.2. ¿Cuál de las siguientes características físicas no puede ser un control de acceso biométrico?

Respuesta: d) La altura.

Justificación: Los controles de acceso biométrico se basan en características físicas únicas, como la huella dactilar, la voz y el reconocimiento facial, pero la altura no es una característica única y fiable para este propósito. Referencia: [**Biometría - Wikipedia, la enciclopedia libre**](https://es.wikipedia.org/wiki/Biometr%C3%ADa)

5.3. ¿Por qué se deben almacenar los resúmenes de las contraseñas en lugar de estas?

Respuesta: b) Para impedir obtener la contraseña.

Justificación: Al almacenar los resúmenes (hashes) de las contraseñas, se dificulta la obtención de las contraseñas originales en caso de que la base de datos sea comprometida.

Referencia: [**¿Qué Es Un Hash Y Cómo Funciona? | Blog oficial de Kaspersky**](https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/)

5.4. ¿Qué parte de un sistema criptográfico debe ser secreto?

Respuesta: c) Las contraseñas.

Justificación: En un sistema criptográfico, las contraseñas deben mantenerse secretas para garantizar la seguridad. Los algoritmos criptográficos y la longitud de las contraseñas generalmente no son secretos.

Referencia: [**Criptografía - Wikipedia, la enciclopedia libre**](https://es.wikipedia.org/wiki/Criptograf%C3%ADa)

5.5. ¿Cuál de las siguientes características no es propia de un sistema criptográfico de clave simétrica?

Respuesta: b) La salida generada por el algoritmo tiene un tamaño constante.

Justificación: En un sistema criptográfico de clave simétrica, la salida puede variar en tamaño dependiendo de los datos de entrada.

Referencia: [**Criptografía simétrica - Wikipedia, la enciclopedia libre**](https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica)

5.6. ¿Cuál de los siguientes algoritmos no es un algoritmo HASH?

Respuesta: d) DES.

Justificación: DES es un algoritmo de cifrado, no un algoritmo de hash. Algoritmos como MD5, SHA-2 y SHA-3 son algoritmos de hash.

Referencia: [**¿Qué Es Un Hash Y Cómo Funciona? | Blog oficial de Kaspersky**](https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/)

5.7. ¿Cuál de los siguientes algoritmos es un algoritmo de clave pública?

Respuesta: d) RSA.

Justificación: RSA es un algoritmo comúnmente utilizado para realizar firmas digitales, proporcionando autenticidad e integridad de los datos.

Referencia: [**Criptografía asimétrica - Wikipedia, la enciclopedia libre**](https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica)

5.8. ¿Cuál de los siguientes algoritmos se utiliza para realizar la firma digital?

Respuesta: a) RSA.

Justificación: Un socket servidor necesita un puerto para escuchar las peticiones entrantes.

Referencia: <https://es.wikipedia.org/wiki/Socket_de_Internet>

5.9. ¿Cuál de los siguientes algoritmos se utiliza para almacenar información cifrada?

Respuesta: b) AES.

Justificación: AES es un algoritmo de cifrado simétrico ampliamente utilizado para almacenar información cifrada de manera segura.

Referencia: [**Firma digital - Wikipedia, la enciclopedia libre**](https://es.wikipedia.org/wiki/Firma_digital)

5.10. ¿Qué se garantiza con la firma digital?

Respuesta: a) La integridad del mensaje.

Justificación: La firma digital garantiza que el mensaje no ha sido alterado y confirma la identidad del remitente.

Referencia: [**Firma digital - Wikipedia, la enciclopedia libre**](https://es.wikipedia.org/wiki/Firma_digital)

5.11. ¿Cuál es el punto débil de utilizar un algoritmo de clave simétrica en transferencia de datos?

Respuesta: b) La distribución de las contraseñas.

Justificación: El principal desafío de los algoritmos de clave simétrica es la distribución segura de las contraseñas entre las partes comunicantes.

Referencia: [**Criptografía simétrica - Wikipedia, la enciclopedia libre**](https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica)