

## Capítulo 1. Principios de la Seguridad Informática

**Instrucciones: Contesta las siguientes preguntas de manera correcta y con ayuda del libro.**

1. ¿Cómo se define la Seguridad Informática?
  - Preservación de su confidencialidad, integridad y disponibilidad
2. ¿Cuáles son los 4 planos de actuación en la Seguridad Informática?
  - Plano humano, plano técnico, organización y legislación
3. Servicio o función de seguridad de la información mediante el cual se garantiza que cada mensaje solo podrá ser leído por su legítimo destinatario:
  - Confidencialidad
4. Servicio o función de seguridad de la información que garantiza que el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje:
  - Autenticación
5. Servicio o función de seguridad de la información que trata de impedir la realización de "ataques de repetición" por parte de usuarios maliciosos:
  - Protección a la replica

## **Seguridad de la Información y Criptografía**

6. Se han convertido en estos últimos años en uno de los mayores problemas de seguridad a escala global en el ámbito de la informática:

- Delitos informáticos

7. ¿En qué consiste el Principio de "Defensa en Profundidad"?

- En el diseño e implementación de varios niveles de seguridad dentro del sistema informático de la organización

8. ¿Qué son las Políticas de Gestión de la Seguridad de la Información?

- Están constituidas por el conjunto de normas reguladoras, procedimientos, reglas y buenas practicas que determinan el modo en que todos los activos y recursos incluyendo la información, son gestionados, protegidos y distribuidos dentro de una organización

9. Nombra los 4 niveles de madurez en la Gestión de la Seguridad de la Información en una organización:

- Implantación de medidas básicas de seguridad por sentido común
- Adaptación a los requisitos del marco legal y de las exigencias de los clientes
- Gestión integral de la Seguridad de la información
- Certificación de la Gestión de la Seguridad de la Información

## **Seguridad de la Información y Criptografía**

10. Es cualquier evento accidental o intencionado que puede ocasionar algún daño en el sistema informático, provocando pérdidas a la organización:

- Amenaza

11. ¿Cuáles son los tres tipos de amenazas dependiendo de la causa?

- Naturales, agentes externos y agentes internos

12. ¿Qué es la vulnerabilidad?

- Es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas en la organización

13. ¿Qué es una medida de seguridad activa y una pasiva?

- Defensas, salvaguardas o medidas de seguridad

14. ¿Con qué otro nombre se les conoce a las medidas de seguridad pasiva?

- Medidas de corrección

15. ¿Cuáles son las defensas físicas?

- Son medidas que implican el control de acceso físico a los recursos y de las condiciones ambientales que tiene que ser utilizadas