Tarea 6: Seguridad

1. ¿Cuáles son las dos **facetas** que tiene la **seguridad**?
2. Mencione tres **causas comunes** de **perdida de datos**.
3. ¿Cuáles son las dos **clases de intrusos** (descríbalos brevemente)?
4. ¿Cuáles son algunas categorías comunes de **intrusos activos**?
5. Describa tres **fallas de seguridad famosas** en los sistemas operativos.
6. ¿Qué es un **caballo de Troya** y una bomba lógica?
7. Mencione cuatro **aspectos sobre la seguridad** que todo diseñador de sistemas debe de tomar en cuenta.
8. ¿Qué es un **virus**?
9. ¿Cómo funciona un **programa virus**?
10. Describa los seis principios generales que pueden servir como guía para **diseñar sistemas seguros**
11. ¿Qué es la verificación de **autenticidad de usuarios**?
12. ¿Cómo funciona y que problemas existen al emplear una **contraseña** como medida de seguridad?
13. En que consiste la **identificación física** para seguridad.
14. Mencione algunas **medidas preventivas** para seguridad.
15. Describa en que consisten los **dominios de protección** para seguridad.
16. Muestre un ejemplo de los **dominios de protección** como objetos.
17. ¿Qué son las listas de **control de acceso** ?
18. ¿Qué es una **lista de capacidades**?
19. En que consisten los **canales encubiertos**.
20. ¿Cuáles son las cuatro áreas en las que se pueden dividir los **problemas de la seguridad en redes**?
21. ¿Qué es la **confidencialidad**?
22. ¿Qué es la **autentificación**?
23. ¿Qué es el **no repudio**?
24. ¿Qué es el **control de integridad**?
25. ¿En la pila de protocolos, como podemos protegernos en la **capa física**?
26. ¿En la pila de protocolos, como podemos protegernos en la **capa de enlace de datos**?
27. ¿En la pila de protocolos, como podemos protegernos en la **capa red**?
28. ¿En la pila de protocolos, como podemos protegernos en la **capa de transporte**?
29. ¿En la pila de protocolos, como podemos protegernos en la **capa de aplicación**?
30. ¿Qué es la **criptografía**?
31. ¿Qué es un **cifrado**?

32. Muestre el **modelo de encriptación** para el cifrado de llave simétrica.

33. ¿Qué es un **código**?

34. ¿Qué es el **texto plano**?

35. ¿Cuál es el **texto cifrado**?

36. Describa el modelo de encriptación para un cifrado con **clave simétrica**.

37. Mencione, una regla fundamental de la **criptografía**.

38. ¿Qué es una **clave**?

39. ¿Qué dice el **principio de Kerckhoff**?

40. Describa el **cifrado por sustitución**. Explique con un ejemplo.

41. En qué consiste el **cifrado César**.

42. ¿Cómo se descifra un **cifrado monoalfabético**?

43. ¿Qué es un **cifrado por transposición**? Muestre como cifrar "por favor transfiere un millón de pesos a mi cuenta en México", con la clave `MEGABUCK`.

44. ¿Cómo se descifra un **cifrado por transposición**?

45. En que consiste el **relleno de una sola vez**, y que lo hace inviolable. Muestre un ejemplo.

46. En que se basa la **criptografía cuántica**

47. ¿Cómo funciona la **criptografía cuántica**?

48. ¿Diga cuál es la característica principal de un **algoritmo de clave simétrica**?

49. Describa la operación del **E**stándar de **E**ncriptación de **D**atos (**DES**).

50. ¿En que consiste triple **DES** (**E**stándar de **E**ncriptación de **D**atos)?

51. Describa la operación del **E**stándar de **E**ncriptación **A**vanzada (**AES**).

52. ¿Cuál es el **estándar de encriptación** para el gobierno de los Estados Unidos?

53. ¿Qué requisitos propusieron **Deffie** y **Hellman** para los **algoritmos de clave pública**?

54. Describa el **algoritmo RSA** (**R**ivest, **S**hamir y **A**dleman).

55. Cifre el su **nombre** con el **algoritmo RSA** con **p = 3** y **q=11**.

56. Describa el **algoritmo mochila**.

57. En que consiste el cifrado por **curvas elipticas**.

58. ¿Cuál fue el propósito con el que se **diseño Kerberos**?

59. ¿Cuáles son los tres **elementos** que involucra **Kerberos**?

60. ¿Qué **sistemas operativos** se encuentran **Kerberizados**?