Examen Teórico

(Prueba Objetiva)

Denominación del curso	IFCT0109. Seguridad Informática	**Código**	23-38/000014
Denominación del módulo	MF0486_3: SEGURIDAD EN EQUIPOS INFORMÁTICOS	**Fecha**	05/03/2024
Formador/a	Benito Manuel González Rodríguez	**Nota Final**	
Nombre y Apellidos		**DNI/NIE**	

INSTRUCCIONES:

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

PRUEBA OBJETIVA FINAL

Seguridad Informática.

MF0486_3. Seguridad en equipos informáticos.

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. **Una amenaza es la probabilidad de que haya un fallo que dañe los sistemas** V__ F__

2. **El BIA es una herramienta para estudiar la continuidad del negocio** V__ F__

3. **Los elementos intervienen en un problema de seguridad son: amenaza, vulnerabilidad e incidente de seguridad.** V__ F__

4. **El análisis de riesgos es la selección e implantación de las salvaguardas para conocer, prevenir, impedir, reducir, o controlar los riesgos identificados.** V__ F__

5. **En ISO 27001, el grupo de controles antes, durante y después de emplear es el Control de Acceso.** V__ F__

6. **El CPD es el última área a proteger, ya que no está visible al público** V__ F__

7. **En la arquitectura TCP/IP, en la capa de Internet se usa la dirección MAC del adaptador de red que conecta el nodo al medio físico** V__ F__

8. **Los DPD para desempeñar sus funciones deben tener cualidades profesionales relacionadas con conocimientos en derecho y práctica en el ámbito de la protección de datos** V__ F__

9. **Siempre que sea posible, deben deshabilitarse los usuarios que el sistema incorpora por defecto** V__ F__

10. **El objetivo de un SGSI es asegurar la continuidad del negocio, minimizando los riesgos, y maximizando el retorno de la inversión en seguridad** 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. **Dentro de los parámetros empleados en seguridad informática para que una persona sea identificada, una tarjeta identificativa magnética es…**

a) Algo que se escucha
b) Algo que se tiene
c) Algo que se sabe
d) Algo que se es

12. **El derecho que permite a los interesados controlar el uso, conocer y obtener información sobre el tratamiento de sus datos personales es…**

a) Derecho de acceso
b) Derecho de rectificación
c) Derecho de supresión o derecho al olvido
d) Derecho a la limitación del tratamiento.

13. **El proceso por el que una persona dice quién es, es la…**

a) La autenticación
b) La identificación
c) La homologación
d) La autorización

14. **De los siguientes protocolos, ¿Cuál de ellos podemos definir como seguro?**

a) SMTP
b) FTP
c) HTTPS
d) POP3

15. **El código malicioso que actúa bajo una circunstancia programada, como puede ser una fecha, se denomina…**

a) Hoax
b) Spyware
c) Keylogger
d) Bomba lógica

16. **De los siguientes derechos digitales contemplados en la LOPDGDD, cual es un derecho en el ámbito laboral**

a) Derecho a la actualización de informaciones en medios de comunicación digitales
b) Derecho a la desconexión digital
c) Derecho a la neutralidad en internet
d) Derecho al testamento digital

17. **El principio de seguridad que indica que la información esté accesible cuando sea necesario es la…**

a) Autenticidad
b) Disponibilidad
c) Confidencialidad
d) Integridad

18. **El protocolo SFTP …**

a) Emplea SSH para la transferencia de ficheros
b) Es un protocolo para el envío seguro de correos
c) Es un comando solo utilizado en Linux
d) Es el protocolo HTTP al que se ha añadido SSH

19. **El método que se utiliza para que si un atacante obtiene acceso al tráfico durante la transmisión de información, no pueda ver correctamente la información se denomina…**

a) Correo electrónico
b) Autenticación
c) Cifrado
d) Autocorrección

20. **Las contramedidas que se realizan para regresar a donde se debe estar después un incidente de seguridad se denominan …**

a) Reactivas de emergencia
b) De detección
c) Preventivas
d) Reactivas de recuperación

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

21. El ……..….. de sistemas consiste en reducir su vulnerabilidad.

22. La …….. es el proceso por el que se comprueba si se puede llevar a cabo una acción sobre un recurso.

23. La Huella dactilar es un factor de autenticación de algo que se …,,,,,...

24. La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se conoce como ……

25. El riesgo …… es el riesgo que permanece después de se han hecho todos los esfuerzos para identificar y eliminar el riesgo.

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. Nombra y describe los tipos de contramedidas a aplicar para gestionar los riesgos de seguridad:

27. Enumera al menos 3 grupos de controles de ISO 27001:

28. Enumera y describe los 3 principios de la seguridad de la información

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 la función correspondiente de la derecha.

A. HERRAMIENTAS BÁSICAS DE RED

B. PROTOCOLO

C. CONTROL DE ACCESO LÓGICO

1) FTP
2) AUTENTICACIÓN
3) PING
4) HTTP
5) IDENTIFICACIÓN
6) SNMP
7) TRACEROUTE

Solución: _____

30. Relaciona los conceptos de la izquierda con los correspondientes de la derecha.

A) PRINCIPIOS DE SEGURIDAD

B) SGSI

C) SEGURIDAD FÍSICA

D) SEGURIDAD LÓGICA

1) SUMINISTRO ELÉCTRICO
2) AGR (ANÁLISIS Y GESTIÓN DE RIESGOS)
3) DISPONIBILIDAD
4) IDENTIFICACIÓN
5) CONFIDENCIALIDAD
6) DRP (PLAN DE RECUPERACIÓN DE DESATRES)
7) INTEGRIDAD
8) CLIMATIZACIÓN
9) AUTENTICACIÓN

Solución: _____

Fdo. _____

PLANTILLA DE CORRECCIÓN
IFCT0109. Seguridad Informática
MF490_3 – GESTION DE SERVICIOS EN EL SISTEMA INFORMATICO
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