

**Nombre y apellidos:**

**Grupo:**

**Fecha:**

Instrucciones generales para las preguntas cerradas:

- Marca solamente la respuesta más apropiada en cada caso, en la tabla de respuestas
- No se tendrán en cuenta anotaciones fuera de la tabla de respuestas
- Todas las preguntas tienen el mismo valor.
- Hay una, y sólo una, respuesta correcta en cada pregunta.
- Responde solamente las preguntas en las que estés seguro. Una respuesta incorrecta resta un tercio del valor de una respuesta acertada. Una pregunta sin responder no resta puntos.

Instrucciones generales para las preguntas abiertas:

- Es necesario responder a la pregunta y justificar dicha respuesta
- Todas las preguntas tienen el mismo valor.

Puntuación:

- La parte tipo test es un 60 % de la nota
- La parte de preguntas abiertas es un 40% de la nota

|    |  |    |  |    |  |    |  |    |  |
|----|--|----|--|----|--|----|--|----|--|
| 1  |  | 2  |  | 3  |  | 4  |  | 5  |  |
| 6  |  | 7  |  | 8  |  | 9  |  | 10 |  |
| 11 |  | 12 |  | 13 |  | 14 |  | 15 |  |
| 16 |  | 17 |  | 18 |  | 19 |  | 20 |  |
| 21 |  | 22 |  | 23 |  | 24 |  | 25 |  |
| 26 |  | 27 |  | 28 |  | 29 |  | 30 |  |
| 31 |  | 32 |  | 33 |  | 34 |  | 35 |  |
| 36 |  | 37 |  | 38 |  | 39 |  | 40 |  |
| 41 |  | 42 |  | 43 |  | 44 |  | 45 |  |
| 46 |  | 47 |  | 48 |  | 49 |  | 50 |  |
| 51 |  | 52 |  | 53 |  | 54 |  | 55 |  |
| 56 |  | 57 |  | 58 |  | 59 |  | 60 |  |
| 61 |  | 62 |  |    |  |    |  |    |  |

- 
1. ¿Un sistema informático de una empresa
- a) Es parte del sistema de información
  - b) No incluye a los equipos (hardware), sino a la información y los procesos (software) para tratarla.
  - c) Incluye al sistema de información
  - d) No incluye la información, sólo los equipos (hardware) y procesos (software) para tratarla.
- 
2. En la cadena de seguridad
- a) se mantiene la seguridad mientras no se rompa el primer eslabón (el más cercano al origen)
  - b) Se mantiene la seguridad mientras no se rompa el último eslabón (el más cercano al usuario)
  - c) Es necesario que no se rompa ningún eslabón de los extremos para garantizar la seguridad, pero pueden comprometerse eslabones intermedios
  - d) Es necesario que no se rompa ningún eslabón para garantizar la seguridad
- 
3. El personal de una empresa
- a) Forma parte de los riesgos
  - b) Forma parte de los impactos
  - c) Forma parte de los activos
  - d) No se tiene en cuenta en el plan de actuación
- 
4. Las medidas de seguridad activas
- a) Mitigan o corrigen el impacto que provoca un ataque
  - b) Eliminan vulnerabilidades de los activos
  - c) Evitan los ataques activos
  - d) Evitan las amenazas
- 
5. Las medidas de seguridad pasivas
- a) Mitigan o corrigen el impacto que provoca un ataque
  - b) Evitan que los activos tengan vulnerabilidades
  - c) Evitan que las amenazas lleguen a producir daños
  - d) Evitan los ataques activos

- 
6. La información
- a) Es un activo de los sistemas de información
  - b) Es un activo de los sistemas informáticos
  - c) Es el final de la cadena de seguridad
  - d) Es el principio de la cadena de seguridad
- 
7. Un ataque pasivo es
- a) Aquel que puede ser prevenido
  - b) Aquel que daña la confidencialidad del sistema
  - c) Aquel que no puede ser prevenido
  - d) Aquel que daña la integridad del sistema
- 
8. Un impacto
- a) Es la estimación (generalmente monetaria) de los daños provocados por un ataque
  - b) Son las características de seguridad que se pierden en un ataque (integridad,conficencialidad,...)
  - c) Son los activos afectados por un ataque
  - d) Es la vulnerabilidad explotada para realizar un ataque
- 
9. Son objetivos de la seguridad informática (propiedades que se desea que debe tener un sistema seguro)
- a) La encriptación y el no repudio
  - b) La integridad y la auditoría
  - c) La disponibilidad y la encriptación
  - d) La integridad y la disponibilidad
- 
10. La confidencialidad mejora con la siguiente medida
- a) Encriptación
  - b) Discos redundantes
  - c) Copias de seguridad
  - d) Firma digital

---

11. La disponibilidad no mejora con la siguiente medida

- a) Discos redundantes
- b) RAID
- c) Firma digital
- d) Cluster de servidores

---

12. Para evitar que las amenazas puedan crear problemas en un sistema es necesario eliminar

- a) Las posibles vulnerabilidades
- b) Los posibles riesgos
- c) Los puntos de acceso local y remoto
- d) Los puntos de acceso remoto

---

13. Las medidas de seguridad activa

- a) Aplican medidas paliativas cuando se producen problemas
- b) Eliminan vulnerabilidades
- c) Restringen accesos remotos
- d) Evitan amenazas

---

14. Las medidas de seguridad pasiva

- a) Evitan las vulnerabilidades
- b) Restringen los accesos remotos
- c) Evitan las amenazas
- d) Aplican medidas paliativas cuando se producen problemas

---

15. ¿Cuáles de estas medidas de seguridad son físicas?

- a) SAI y antivirus
- b) SAI y toma de tierra
- c) Encriptación y copias de seguridad
- d) Encriptación y puertas anti-incendios

---

16. ¿Cuáles de estas medidas de seguridad son lógicas?

- a) Encriptación y puertas anti-incendios
- b) SAI y toma de tierra
- c) SAI y antivirus
- d) Encriptación y copias de seguridad

---

17. En el marco de análisis de riesgos del sistema de información de una empresa, un activo es

- a) Cualquier elemento de la empresa que realice algún tipo de tarea en el sistema de información
- b) Cualquier elemento que sea de valor para una empresa,
- c) Cualquier elemento informático (datos, hardware, configuraciones, servicios,...)
- d) Cualquier elemento de la empresa que no puedan imitar otras empresas, siendo por tanto una ventaja

---

18. En caso de que un desastre afecte a los sistemas informáticos, es necesario poner en práctica

- a) Las medidas activas
- b) El plan de actuación
- c) El plan de contingencia
- d) Las medidas lógicas y físicas

---

19. Una auditoría de seguridad informática

- a) Verifica que se cumple una política de seguridad
- b) Verifica que no hay amenazas
- c) Verifica que los activos no tienen vulnerabilidades
- d) Se utiliza como paso intermedio en un análisis de riesgos

---

20. El plan de emergencia forma parte de

- a) El plan de contingencia
- b) El análisis de riesgos
- c) El plan de recuperación
- d) La auditoría de seguridad

---

21. Los SAIS (UPS) más caros suelen ser

- a) Los online
- b) Los offline, si no incluyen AVR
- c) No hay diferencia de precio entre online u offline
- d) Los offline

---

22. Las baterías más comunes en un SAI son

- a) Ión Litio
- b) De plomo y ácido

- c) Nanotubos  
d) Salinas
- 
23. Los SAIS que incluyen un inversor son
- a) Los online y los offline, indistintamente
  - b) Los offline, si no incluyen AVR
  - c) Los offline
  - d) Los online
- 
24. Se distingue entre los servidores y las estaciones de trabajo de una red
- a) Por la función que se les asigna
  - b) Por la potencia del procesador
  - c) Por la capacidad de memoria y disco duro
  - d) Por la versión de sistema operativo
- 
25. El frontal de un servidor de tipo "pizza box" mide (" significa pulgadas)
- a) 0.75" x 10"
  - b) 0.75" x 19"
  - c) 1.75" x 10"
  - d) 1.75" x 19"
- 
26. Un servidor tipo blade
- a) Incluye más de un ordenador, completamente independientes
  - b) Es un sólo ordenador, con un número muy grande de discos intercambiables
  - c) Incluye más de un ordenador, para los que centraliza servicios como comunicaciones y alimentación
  - d) Es un sólo ordenador, con un número muy grande de discos y memoria RAM intercambiable
- 
27. Para entrar a un CPD es necesario introducir un PIN en un teclado. El teclado sólo se muestra si previamente se ha acercado a la puerta una tarjeta RFID. Este sistema de autenticación se basa en
- a) Algo que se sabe y algo que se es
  - b) Una contraseña y un PIN
  - c) Algo que se sabe y algo que se posee
  - d) Un usuario y una contraseña
- 
28. La corriente eléctrica proporcionada a consumidores particulares en España es de
- a) 50Hz a 230V
  - b) 60Hz a 230V
  - c) 50Hz a 115V
  - d) 60Hz a 115V
- 
29. En una instalación informática tipo SOHO en la que se implementa un modelo de grupo de trabajo
- a) Ningún ordenador puede ser un servidor
  - b) Se mejora la característica segura de la confidencialidad
  - c) Se centralizan las vulnerabilidades del sistema
  - d) Puede existir más de un ordenador servidor
- 
30. Un interruptor magnetotérmico marcado con C24
- a) Permite el paso de corriente hasta los 24 Voltio-Amperios
  - b) Permite el paso de corriente hasta los 24 Amperios
  - c) Permite el paso de corriente, siempre que no supere los 240 Voltios
  - d) Permite el paso de corriente, siempre que supere los 240 Voltios
- 
31. Los colores de los cables de fase, neutro y tierra son, respectivamente
- a) rojo/marrón/negro, amarillo, azul
  - b) azul, amarillo, rojo/marrón/negro
  - c) rojo/marrón/negro, azul, amarillo
  - d) amarillo, rojo/marrón/negro, azul
- 
32. Un aparato electrónico puede prescindir de la toma de tierra si
- a) Utiliza menos de 10 Amperios
  - b) Utiliza menos de 2.5 Amperios
  - c) Está marcado con el símbolo de "doble aislamiento"
  - d) Utiliza un conector macho "schuko"
- 
33. Un SAI offline interactivo tiene como componentes
- a) Cargador, Inversor, Batería, y AVR

- 
- b) Cargador, Inversor, Batería y conmutador
- c) Cargador, Inversor, Batería, AVR y conmutador
- d) Inversor, Batería, AVR y conmutador
- 
34. ¿A la hora de crear copias de seguridad, es preferible copiar
- a) Los programas
- b) Todos los datos de todos los ordenadores de la empresa
- c) Aquellos datos con mayor impacto (según el plan de actuación)
- d) Aquellos programas y datos con mayor resultado (según el plan de contingencia)
- 
35. Las copias de seguridad mejoran
- a) La integridad
- b) La integridad y la confidencialidad
- c) La confidencialidad
- d) La integridad y la disponibilidad
- 
36. Las copias incrementales se distinguen de las diferenciales
- a) En UNIX/LINUX no hay diferencia, pero en Windows la incremental utiliza el atributo A de los ficheros
- b) Porque estadísticamente una copia incremental ocupa menos espacio que una diferencial
- c) En Windows no hay diferencia, pero en UNIX/LINUX la incremental utiliza el contenido de los ficheros
- d) Porque estadísticamente una copia diferencial ocupa menos espacio que una incremental
- 
37. El tipo de copia de seguridad que acaba utilizando el menor espacio en disco
- a) La estadística o la incremental, indistintamente
- b) La diferencial
- c) La estadística
- d) La incremental
- 
38. El tipo de copia que ofrece mayores garantías de integridad y disponibilidad es
- a) La completa o la estadística, indistintamente
- b) La estadística
- c) La completa
- d) La diferencial
- 
39. El tipo de copia de seguridad más simple de restaurar es
- a) La diferencial
- b) La completa
- c) La completa o la estadística, indistintamente
- d) La estadística
- 
40. Una empresa define una política de seguridad en la que un backup con todos los datos se transfiere semanalmente a GoogleDrive, y se mantiene allí dos meses. Es una copia
- a) Off-site y completa
- b) Off-line y diferencial
- c) On-line y diferencial
- d) On-line y completa
- 
41. El tipo de copia de seguridad que acaba utilizando el mayor espacio en disco es
- a) La incremental
- b) La estadística
- c) La diferencial
- d) La estadística o la incremental, indistintamente
- 
42. Se necesita una copia completa inicial para basar en ella
- a) Las copias incrementales
- b) Las copias estadísticas
- c) Las copias diferenciales
- d) Las copias incrementales y las diferenciales
- 
43. El medio soporte de datos con peor tiempo de acceso (para lectura y escritura) es
- a) Dvd
- b) Disco duro interno
- c) Disco duro externo

- d) Cinta
- 
44. Se puede restaurar sin una copia total
- a) Una copia incremental
  - b) Otra copia total
  - c) Una copia diferencial
  - d) Una serie de copias diferenciales
- 
45. Una copia de seguridad off-site es deseable porque
- a) Mejora la disponibilidad
  - b) Mejora comunicación dentro de la empresa
  - c) Mejora la confidencialidad
  - d) Mejora la rapidez con la que se realizan las copias
- 
46. Un grupo de discos en RAID 0
- a) Puede fallar uno de los discos, ya que la información puede extraerse del resto de discos
  - b) Presenta un tiempo medio de fallo menor que cada disco por separado
  - c) Necesita poder accederse desde la red (como los I-SCSI)
  - d) Necesitan ser todos del mismo tamaño
- 
47. Un grupo de discos de 1TB cada uno esta formando un RAID. El tiempo medio de escritura en el RAID sigue siendo el mismo que en cada disco individual. El RAID montado:
- a) Es un RAID 5
  - b) Es un RAID 0, con mas de 2 discos
  - c) Es un RAID 0, con exactamente dos discos
  - d) Es un RAID 1
- 
48. Un grupo de discos de 1TB cada uno esta formando un RAID. La capacidad total del RAID es de 4 TB. Se trata de
- a) Un RAID 0, con 5 discos
  - b) Un RAID 5, con 5 discos
  - c) Un RAID 1, con 4 discos
  - d) Un RAID 5, con 4 discos
- 
49. Se ha montado un sistema de discos RAID. Este sistema no mejora ninguno de los objetivos de la seguridad informática
- a) Es un RAID 4
  - b) Es un RAID 5, con solo dos discos
  - c) Es un RAID 1, con solo dos discos
  - d) Es un RAID 0
- 
50. Una empresa necesita mejorar el tiempo de escritura del disco de un servidor. Para ello
- a) Puede utilizar un RAID 0 o un RAID 5 en vez de un disco simple
  - b) Puede utilizar cualquier tipo de RAID (0,1,5,6), pues todos mejoran la velocidad de escritura de los discos
  - c) Puede utilizar un RAID 1 en vez de un disco simple
  - d) Ningún nivel de RAID mejora los tiempos de escritura de los discos
- 
51. Una empresa necesita mejorar el tiempo de lectura del disco de un servidor. Para ello
- a) Puede utilizar un RAID 0 o un RAID 5 en vez de un disco simple
  - b) Ningún nivel de RAID mejora los tiempos de lectura de los discos
  - c) Puede utilizar cualquier tipo de RAID (0,1,5,6), pues todos mejoran la velocidad de lectura de los discos
  - d) Puede utilizar un RAID 1 en vez de un disco simple
- 
52. Un spare disk en RAID es
- a) Un disco del que no hay paridad
  - b) Un disco no utilizado hasta el estado de emergencia del RAID
  - c) Un disco que solo tiene paridad
  - d) Un disco tradicional, que no forma parte de un RAID
- 
53. La diferencia entre un RAID 5 y un RAID 5e es
- a) El RAID 5 utiliza más espacio para la paridad de los datos
  - b) El RAID 5e utiliza más espacio para la paridad de los datos
  - c) El RAID 5e necesita un disco más que RAID 5, para almacenar el mismo volumen de datos

- d) El RAID 5e tiene mejores tiempos de escritura que el RAID 5
- 
54. La diferencia entre un RAID 6 y un RAID 6e es
- a) El RAID 6e tiene mejores tiempos de lectura
  - b) El RAID 6e tiene mejores tiempos de lectura y escritura
  - c) El RAID 6e comienza su estado de recuperación nada más iniciarse el estado de emergencia
  - d) El RAID 6e utiliza un sistema de paridad que ahorra espacio, por lo que puede almacenar más datos en los mismos discos
- 
55. La tecnología S.M.A.R.T. se puede utilizar
- a) Para predecir un fallo en un disco duro
  - b) Para detectar un fallo en un disco duro
  - c) Para realizar una copia de respaldo de un disco duro defectuoso
  - d) Para realizar una copia de respaldo de un disco que aún no es defectuoso
- 
56. En la tecnología S.M.A.R.T., un disco duro presenta una alta probabilidad de fallo cuando
- a) Alguno de sus niveles llega a 255
  - b) Alguno de sus niveles cae por debajo del umbral (threshold) definido por el fabricante del disco
  - c) Alguno de sus niveles llega a 0 (cero)
  - d) Alguno de sus niveles cae por debajo del umbral (threshold) definido por el administrador del sistema
- 
57. El estado de recuperación
- a) Es la parte del estado de emergencia hasta que hay un disco disponible para recuperar la normalidad
  - b) Es la parte inicial del estado de emergencia
  - c) Incluye al estado de emergencia
  - d) Es la parte del estado de emergencia que comienza cuando hay un nuevo disco disponible para recuperar la normalidad
- 
58. Un disco conectado por USB a un ordenador se considera
- a) SAN
  - b) DAS
  - c) NAS
  - d) No entra dentro de estas categorías
- 
59. Si un disco es accedido, desde el punto de vista del sistema operativo, mediante operaciones de lectura/escritura sobre sectores, es un disco
- a) NAS o SAN
  - b) DAS o SAN
  - c) NAS
  - d) DAS
- 
60. Un disco es utilizado a la vez por dos ordenadores. Los sistemas operativos de ambos acceden al disco mediante operaciones de lectura/escritura sobre sectores. Es un disco
- a) SAN
  - b) DAS
  - c) NAS
  - d) SAN o NAS
- 
61. En una instalación NAS (Network Attached Storage)
- a) Los discos duros no pueden tener una configuración RAID
  - b) Los accesos a los discos se realizan en base a sectores
  - c) Los accesos a los discos se realizan en base a ficheros
  - d) Los discos duros no pueden compartirse entre ordenadores
- 
62. iSCSI es un caso particular de
- a) SAN
  - b) RAID
  - c) NAS
  - d) DAS

- 
63. Una oficina utiliza un NAS, durante las 24 horas del día, y se está quedando sin espacio. Propón un procedimiento para aumentar el tamaño de dicho NAS, minimizando el tiempo en el que los usuarios no tendrán disponible dicho NAS

- 
64. Determina a cuál (o cuáles) de los objetivos de la seguridad informática (características seguras) ayuda cada una de estas medidas, especificando el por qué: Backups de datos, antivirus, autenticación mediante contraseñas, RAID 0, RAID 6e



---

65. Se ha montado un RAID 6e usando 5 discos. Dibuja su configuración indicando qué bloques se destinan a la paridad, y de qué bloques son paridad

---

66. Realiza un diagrama que indique la estructura de los siguientes documentos: Plan de actuación, análisis de riesgos, plan de contingencia, políticas de seguridad