Apellidos: _____

Nombre: _____

Fecha: _____ **Grupo:** _____

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							

Instrucciones generales para las preguntas cerradas:

- 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 solo a aquellas preguntas de las que estés seguro. Una respuesta incorrecta resta un tercio del valor de una respuesta acertada, pero una pregunta sin responder no resta puntos.
- Un aspa marca una respuesta. Se puede desmarcar una respuesta con un círculo sobre el aspa.

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.
- Se necesita un mínimo de 3,5 en cada parte del examen para que hagan media.

1. Un sistema informático de una empresa
   a) No incluye a los equipos (hardware), sino a la información y los procesos (software) para tratarla.
   b) Incluye al sistema de información
   c) No incluye la información, sólo los equipos (hardware) y procesos (software) para tratarla.
   d) Es parte del sistema de información

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 para garantizar la seguridad
   d) Es necesario que no se rompa ningún eslabón de los extremos para garantizar la seguridad, pero pueden comprometerse eslabones intermedios

3. El personal de una empresa
   a) Forma parte de los impactos
   b) Forma parte de los activos
   c) No se tiene en cuenta en el plan de actuación
   d) Forma parte de los riesgos

4. Las medidas de seguridad activas
   a) Mitigan o corrigen el impacto que provoca un ataque
   b) Evitan las amenazas
   c) Eliminan vulnerabilidades de los activos
   d) Evitan los ataques activos

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 el final de la cadena de seguridad
   b) Es el principio de la cadena de seguridad
   c) Es un activo de los sistemas de información
   d) Es un activo de los sistemas informáticos

7. Un ataque pasivo es
   a) Aquel que puede ser prevenido
   b) Aquel que daña la integridad del sistema
   c) Aquel que daña la confidencialidad del sistema
   d) Aquel que no puede ser prevenido

8. Un impacto
   a) Son los activos afectados por un ataque
   b) Es la vulnerabilidad explotada para realizar un ataque
   c) Son las características de seguridad que se pierden en un ataque (integridad,conficencialidad,...)
   d) Es la estimación (generalmente monetaria) de los daños provocados por 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 integridad y la disponibilidad
   d) La disponibilidad y la encriptación

10. La confidencialidad mejora con la siguiente medida
   a) Discos redundantes
   b) Encriptación
   c) Firma digital
   d) Copias de seguridad

11. La disponibilidad no mejora con la siguiente medida
   a) Firma digital
   b) Cluster de servidores
   c) Discos redundantes
   d) RAID

12. Para evitar que las amenazas puedan crear problemas en un sistema es necesario eliminar
   a) Los posibles riesgos
   b) Las posibles vulnerabilidades
   c) Los puntos de acceso local y remoto
   d) Los puntos de acceso remoto

13. Las medidas de seguridad activa
   a) Eliminan vulnerabilidades
   b) Restringen accesos remotos
   c) Evitan amenazas
   d) Aplican medidas paliativas cuando se producen problemas

14. Las medidas de seguridad pasiva
   a) Aplican medidas paliativas cuando se producen problemas
   b) Evitan las amenazas
   c) Restringen los accesos remotos
   d) Evitan las vulnerabilidades

15. ¿Cuáles de estas medidas de seguridad son físicas?
   a) SAI y toma de tierra
   b) Encriptación y copias de seguridad
   c) Encriptación y puertas anti-incendios
   d) SAI y antivirus

16. ¿Cuáles de estas medidas de seguridad son lógicas?
   a) SAI y antivirus
   b) Encriptación y copias de seguridad
   c) Encriptación y puertas anti-incendios
   d) SAI y toma de tierra

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

a) Cualquier elemento informático (datos, hardware, configuraciones, servicios,...)
b) Cualquier elemento de la empresa que realice algún tipo de tarea en el sistema de información
c) Cualquier elemento que sea de valor para una empresa,
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) El plan de contingencia
b) Las medidas activas
c) Las medidas lógicas y físicas
d) El plan de actuación

19. Una auditioría de seguridad informática

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

20. El plan de emergencia forma parte de

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

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
c) Los online
d) Los offline, si no incluyen AVR

24. Se distingue entre los servidores y las estaciones de trabajo de una red

a) Por la potencia del procesador
b) Por la capacidad de memoria y disco duro
c) Por la versión de sistema operativo
d) Por la función que se les asigna

25. El frontal de un servidor de tipo "pizza box" mide (" significa pulgadas)

a) 1.75" x 10"
b) 1.75" x 19"
c) 0.75" x 10"
d) 0.75" x 19"

26. Un servidor tipo blade

a) Es un sólo ordenador, con un número muy grande de discos intercambiables
b) Es un sólo ordenador, con un número muy grande de discos y memoria RAM intercambiable
c) Incluye más de un ordenador, para los que centraliza servicios como comunicaciones y alimentación
d) Incluye más de un ordenador, completamente independientes

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 autentificación se basa en

a) Algo que se sabe y algo que se es
b) Algo que se sabe y algo que se posee
c) Una contraseña y un PIN
d) Un usuario y una contraseña

28. La corriente eléctrica proporcionada a consumidores particulares en España es de

a) 50Hz a 115V
b) 60Hz a 230V
c) 50Hz a 230V
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) Puede existir más de un ordenador servidor
c) Se centralizan las vulnerabilidades del sistema
d) Se mejora la característica segura de la confidencialidad

30. Un interrupor magnetotérmico marcado con C24

a) Permite el paso de corriente, siempre que no supere los 240 Voltios
b) Permite el paso de corriente, siempre que supere los 240 Voltios
c) Permite el paso de corriente hasta los 24 Voltio-Amperios
d) Permite el paso de corriente hasta los 24 Amperios

31. Los colores de los cables de fase, neutro y tierra son, respectivamente

a) azul, amarillo, rojo/marrón/negro
b) rojo/marrón/negro, amarillo, azul
c) amarillo, rojo/marrón/negro, azul
d) rojo/marrón/negro, azul, amarillo

32. Un aparato electrónico puede prescindir de la toma de tierra si

a) Está marcado con el símbolo de "doble aislamiento"
b) Utiliza menos de 2.5 Amperios
c) Utiliza menos de 10 Amperios
d) Utiliza un conector macho "schuko"

33. Un SAI offline interactivo tiene como componentes

a) Cargador, Inversor, Batería y conmutador
b) Inversor, Batería, AVR y conmutador
c) Cargador, Inversor, Batería, AVR y conmutador
d) Cargador, Inversor, Batería, y AVR

34. A la hora de crear copias de seguridad, es preferible copiar

a) Todos los datos de todos los ordenadores de la empresa
b) Aquellos programas y datos con mayor resultado (según el plan de contingencia)
c) Los programas
d) Aquellos datos con mayor impacto (según el plan de actuación)

35. Las copias de seguridad mejoran

a) La confidencialidad
b) La integridad
c) La integridad y la confidencialidad
d) La integridad y la disponibilidad

36. Las copias incrementales se distinguen de las diferenciales

a) Porque estadísticamente una copia diferencial ocupa menos espacio que una incremental
b) Porque estadísticamente una copia incremental ocupa menos espacio que una diferencial
c) En UNIX/LINUX no hay diferencia, pero en Windows la incremental utiliza el atributo A de los ficheros
d) En Windows no hay diferencia, pero en UNIX/LINUX la incremental utiliza el contenido de los ficheros

37. El tipo de copia de seguridad que acaba utilizando el menor espacio en disco

a) La estadística
b) La diferencial
c) La incremental
d) La estadística o la incremental, indistintamente

38. El tipo de copia que ofrece mayores garantías de integridad y disponibilidad es

a) La estadística
b) La completa
c) La diferencial
d) La completa o la estadística, indistintamente

39. El tipo de copia de seguridad más simple de restaurar es

a) La estadística
b) La completa o la estadística, indistintamente
c) La diferencial
d) La completa

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) On-line y completa
b) Off-line y diferencial
c) On-line y diferencial
d) Off-site y completa

41. El tipo de copia de seguridad que acaba utilizando el mayor espacio en disco es

a) La estadística
b) La estadística o la incremental, indistintamente
c) La diferencial
d) La incremental

42. Se necesita una copia completa inicial para basar en ella

a) Las copias incrementales
b) Las copias diferenciales
c) Las copias estadísticas
d) Las copias incrementales y las diferenciales

43. El medio soporte de datos con peor tiempo de acceso (para lectura y escritura) es

a) Disco duro interno
b) Disco duro externo
c) Dvd
d) Cinta

44. Se puede restaurar sin una copia total

a) Una serie de copias diferenciales
b) Otra copia total
c) Una copia incremental
d) Una copia diferencial

45. Una copia de seguridad off-site es deseable porque

a) Mejora comunicación dentro de la empresa
b) Mejora la disponibilidad
c) Mejora la confidencialidad
d) Mejora la rapidez con la que se realizan las copias

46. Un grupo de discos en RAID 0

a) Necesita poder accederse desde la red (como los I-SCSI)
b) Presenta un tiempo medio de fallo menor que cada disco por separado
c) Puede fallar uno de los discos, ya que la información puede extraerse del resto de discos
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 0, con exactamente dos discos
b) Es un RAID 1
c) Es un RAID 0, con mas de 2 discos
d) Es un RAID 5

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 5, con 5 discos
b) Un RAID 5, con 4 discos
c) Un RAID 0, con 5 discos
d) Un RAID 1, 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 5, con solo dos discos
b) Es un RAID 1, con solo dos discos
c) Es un RAID 4
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 cualquier tipo de RAID (0,1,5,6), pues todos mejoran la velocidad de lectura de los discos
b) Ningún nivel de RAID mejora los tiempos de lectura de los discos
c) Puede utilizar un RAID 1 en vez de un disco simple
d) Puede utilizar un RAID 0 o un RAID 5 en vez de un disco simple

52. Un spare disk en RAID es

a) Un disco que solo tiene paridad
b) Un disco no utilizado hasta el estado de emergencia del RAID
c) Un disco tradicional, que no forma parte de un RAID
d) Un disco del que no hay paridad

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 utiliza un sistema de paridad que ahorra espacio, por lo que puede almacenar más datos en los mismos discos
d) El RAID 6e comienza su estado de recuperación nada más iniciarse el estado de emergencia

55. La tecnología S.M.A.R.T. se puede utilizar

a) Para realizar una copia de respaldo de un disco duro defectuoso
b) Para realizar una copia de respaldo de un disco que aún no es defectuoso
c) Para detectar un fallo en un disco duro
d) Para predecir un fallo en un disco duro

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 administrador del sistema
c) Alguno de sus niveles llega a 0 (cero)
d) Alguno de sus niveles cae por debajo del umbral (threshold) definido por el fabricante del disco

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) Es la parte del estado de emergencia que comienza cuando hay un nuevo disco disponible para recuperar la normalidad
d) Incluye al estado de emergencia

58. Un disco conectado por USB a un ordenador se considera

a) SAN
b) DAS
c) No entra dentro de estas categorías
d) NAS

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) DAS
b) NAS
c) NAS o SAN
d) DAS o SAN

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 o NAS
b) SAN
c) NAS
d) DAS

61. En una instalación NAS (Network Attached Storage)
   a) Los discos duros no pueden compartirse entre ordenadores
   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 tener una configuración RAID

62. iSCSI es un caso particular de
   a) RAID
   b) NAS
   c) SAN
   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, autentificación 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