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

2. En la cadena de seguridad

   a) Es necesario que no se rompa ningún eslabón para garantizar la seguridad
   b) Es necesario que no se rompa ningún eslabón de los extremos para garantizar la seguridad, pero pueden comprometerse eslabones intermedios
   c) se mantiene la seguridad mientras no se rompa el primer eslabón (el más cercano al origen)
   d) Se mantiene la seguridad mientras no se rompa el último eslabón (el más cercano al usuario)

3. El personal de una empresa

   a) No se tiene en cuenta en el plan de actuación
   b) Forma parte de los activos
   c) Forma parte de los impactos
   d) Forma parte de los riesgos

4. Las medidas de seguridad activas

   a) Evitan las amenazas
   b) Eliminan vulnerabilidades de los activos
   c) Mitigan o corrigen el impacto que provoca un ataque
   d) Evitan los ataques activos

5. Las medidas de seguridad pasivas

   a) Evitan que las amenazas lleguen a producir daños
   b) Evitan los ataques activos
   c) Mitigan o corrigen el impacto que provoca un ataque
   d) Evitan que los activos tengan vulnerabilidades

6. La información

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

7. Un ataque pasivo es

   a) Aquel que daña la integridad del sistema
   b) Aquel que daña la confidencialidad del sistema
   c) Aquel que puede ser prevenido
   d) Aquel que no puede ser prevenido

8. Un impacto

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

9. Son objetivos de la seguridad informática (propiedades que se desea que debe tener un sistema seguro)

   a) La disponibilidad y la encriptación
   b) La integridad y la auditoría
   c) La encriptación y el no repudio
   d) La integridad y la disponibilidad

10. La confidencialidad mejora con la siguiente medida

    a) Discos redundantes
    b) Copias de seguridad
    c) Encriptación
    d) Firma digital

11. La disponibilidad no mejora con la siguiente medida

a) Firma digital
b) RAID
c) Discos redundantes
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) Eliminan vulnerabilidades
b) Restringen accesos remotos
c) Evitan amenazas
d) Aplican medidas paliativas cuando se producen problemas

14. Las medidas de seguridad pasiva

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

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

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

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

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

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 no puedan imitar otras empresas, siendo por tanto una ventaja
c) Cualquier elemento que sea de valor para una empresa,
d) Cualquier elemento de la empresa que realice algún tipo de tarea en el sistema de información

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

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

19. Una auditioría de seguridad informática

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

20. El plan de emergencia forma parte de

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

21. Los SAIS (UPS) más caros suelen ser

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

22. Las baterías más comunes en un SAI son

a) De plomo y ácido
b) Ión Litio

c) Salinas

d) Nanotubos

23. Los SAIS que incluyen un inversor son

a) Los online

b) Los online y los offline, indistintamente

c) Los offline

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 versión de sistema operativo

c) Por la función que se les asigna

d) Por la capacidad de memoria y disco duro

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 19"

d) 1.75" x 10"

26. Un servidor tipo blade

a) Es un sólo ordenador, con un número muy grande de discos y memoria RAM intercambiable

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) 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 230V

b) 50Hz a 115V

c) 60Hz a 115V

d) 60Hz a 230V

29. En una instalación informática tipo SOHO en la que se implementa un modelo de grupo de trabajo

a) Puede existir más de un ordenador servidor

b) Se centralizan las vulnerabilidades del sistema

c) Se mejora la característica segura de la confidencialidad

d) Ningún ordenador puede ser un servidor

30. Un interrupor magnetotérmico marcado con C24

a) Permite el paso de corriente hasta los 24 Amperios

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, siempre que no 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 2.5 Amperios

b) Está marcado con el símbolo de "doble aislamiento"

c) Utiliza menos de 10 Amperios

d) Utiliza un conector macho "schuko"

33. Un SAI offline interactivo tiene como componentes

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

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

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

36. Las copias incrementales se distinguen de las diferenciales

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

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

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

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

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

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

a) La estadística
b) La diferencial
c) La completa o la estadística, indistintamente
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) Off-line y diferencial
b) On-line y completa
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 diferencial
b) La incremental
c) La estadística o la incremental, indistintamente
d) La estadística

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

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

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

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

d) Dvd

44. Se puede restaurar sin una copia total

a) Otra copia total
b) Una serie de copias diferenciales
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 rapidez con la que se realizan las copias
c) Mejora la disponibilidad
d) Mejora la confidencialidad

46. Un grupo de discos en RAID 0

a) Necesitan ser todos del mismo tamaño
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) Necesita poder accederse desde la red (como los I-SCSI)

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 mas de 2 discos
b) Es un RAID 0, con exactamente dos discos
c) Es un RAID 1
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 0, 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 0
b) Es un RAID 4
c) Es un RAID 5, con solo dos discos
d) Es un RAID 1, con solo dos discos

50. Una empresa necesita mejorar el tiempo de escritura del disco de un servidor. Para ello

a) Puede utilizar cualquier tipo de RAID (0,1,5,6), pues todos mejoran la velocidad de escritura de los discos
b) Puede utilizar un RAID 0 o un RAID 5 en vez de un disco simple
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) Ningún nivel de RAID mejora los tiempos de lectura de los discos
b) Puede utilizar cualquier tipo de RAID (0,1,5,6), pues todos mejoran la velocidad de lectura de los discos
c) Puede utilizar un RAID 0 o un RAID 5 en vez de un disco simple
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 que solo tiene paridad
c) Un disco no utilizado hasta el estado de emergencia del RAID
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 5e tiene mejores tiempos de escritura que el RAID 5
b) El RAID 5 utiliza más espacio para la paridad de los datos
c) El RAID 5e utiliza más espacio para la paridad de los datos

d) El RAID 5e necesita un disco más que RAID 5, para almacenar el mismo volumen de datos

54. La diferencia entre un RAID 6 y un RAID 6e es

a) El RAID 6e comienza su estado de recuperación nada más iniciarse el estado de emergencia
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 tiene mejores tiempos de lectura

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 cae por debajo del umbral (threshold) definido por el administrador del sistema
b) Alguno de sus niveles llega a 255
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 inicial del estado de emergencia
b) Es la parte del estado de emergencia hasta que hay un disco disponible para recuperar la normalidad
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) No entra dentro de estas categorías
c) NAS
d) DAS

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

61. En una instalación NAS (Network Attached Storage)

a) Los discos duros no pueden tener una configuración RAID
b) Los discos duros no pueden compartirse entre ordenadores
c) Los accesos a los discos se realizan en base a ficheros
d) Los accesos a los discos se realizan en base a sectores

62. iSCSI es un caso particular de

a) SAN
b) NAS
c) RAID
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