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		63		64		65	
66		67		68		69		70	
71		72		73		74		75	
76		77		78		79		80	
81		82		83		84		85	
86		87		88		89		90	
91		92		93					

1. ¿En la cadena de seguridad

   a) Es necesario que no se rompa ningún eslabón para garantizar la seguridad
   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) se mantiene la seguridad mientras no se rompa el primer eslabón (el más cercano al origen)

2. El personal de una empresa

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

3. Las medidas de seguridad activas

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

4. Las medidas de seguridad pasivas

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

5. La información

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

6. Un ataque pasivo es

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

7. Un ataque activo es

   a) Aquel que no es provocado por una amenaza
   b) Aquel que es provocado por una amenaza
   c) Aquel que daña la integridad y/o la confidencialidad del sistema
   d) Aquel que daña la integridad del sistema, pero no la disponibilidad

8. 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 disponibilidad
   c) La disponibilidad y la encriptación
   d) La integridad y la auditoría

9. La confidencialidad mejora con la siguiente medida

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

10. La disponibilidad no mejora con la siguiente medida

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

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

    a) Los puntos de acceso local y remoto
    b) Los puntos de acceso remoto

c) Las posibles vulnerabilidades

d) Los posibles riesgos

12. Las medidas de seguridad pasiva

a) Evitan las amenazas

b) Evitan las vulnerabilidades

c) Aplican medidas paliativas cuando se producen problemas

d) Restringen los accesos remotos

13. ¿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

14. 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) El plan de actuación

d) Las medidas lógicas y físicas

15. Una auditioría de seguridad informática

a) Verifica que no hay amenazas

b) Verifica que se cumple una política de seguridad

c) Se utiliza como paso intermedio en un análisis de riesgos

d) Verifica que los activos no tienen vulnerabilidades

16. El plan de emergencia forma parte de

a) El plan de contingencia

b) La auditoría de seguridad

c) El plan de recuperación

d) El análisis de riesgos

17. En una comunicación HTTPS

a) No hay certificados con claves públicas, ya que se usa criptografía asimétrica

b) Solo puede haber un certificado, que es el que el servidor envía al cliente

c) El servidor podría requerir también un certificado del usuario, aunque no es común

d) No hay certificados con claves públicas, ya que se usa criptografía híbrida

18. En Linux, se puede encriptar

a) Particiones y discos completos, pero no las de inicio (para eso se crean "/" y "/home" en particiones separadas)

b) Particiones y discos completos, incluso las particiones de inicio

c) Particiones completas

d) Discos completos

19. Los SAIS (UPS) más caros suelen ser

a) Los offline, si no incluyen AVR

b) Los online

c) No hay diferencia de precio entre online u offline

d) Los offline

20. Las baterías más comunes en un SAI son

a) De plomo y ácido

b) Ión Litio

c) Nanotubos

d) Salinas

21. Los SAIS que incluyen un conmutador son

a) Los offline

b) Los online

c) Los online y los offline, indistintamente

d) Los offline, si no incluyen AVR

22. Los SAIS que incluyen un inversor son

a) Los offline, si no incluyen AVR

b) Los online y los offline, indistintamente

c) Los offline

d) Los online

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

a) Por la capacidad de memoria y disco duro

b) Por la versión de sistema operativo

c) Por la potencia del procesador

d) Por la función que se les asigna

24. Un rango adecuado para la temperatura de un datacenter, según lo visto en clase, es de

a) Menor de 20º

b) 20º a 25º

c) Menor de 10º

d) 20º a 35º

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

a) 1.75" x 19"

b) 0.75" x 19"

c) 1.75" x 10"

d) 0.75" x 10"

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

a) 60Hz a 115V

b) 50Hz a 115V

c) 60Hz a 230V

d) 50Hz a 230V

27. 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) Ningún ordenador puede ser un servidor

c) Se centralizan las vulnerabilidades del sistema

d) Se mejora la característica segura de la confidencialidad

28. Un extintor de polvo polivalente es válido para fuegos de tipo

a) A y B

b) A, B y C

c) A, C y D

d) B y C

29. Las señales de evacuación en caso de incendio son de color

a) Verde y/o rojo

b) No está normalizado el color, pero sí los símbolos que deben aparecer en ellas

c) Rojo

d) Verde

30. Un interrupor magnetotérmico marcado con C24

a) Permite el paso de corriente, siempre que supere los 240 Voltios

b) Permite el paso de corriente, siempre que no 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) rojo/marrón/negro, azul, amarillo

b) rojo/marrón/negro, amarillo, azul

c) amarillo, rojo/marrón/negro, azul

d) azul, amarillo, rojo/marrón/negro

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

a) Utiliza menos de 2.5 Amperios

b) Utiliza un conector macho "schuko"

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

d) Utiliza menos de 10 Amperios

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

a) Todos los datos de todos los ordenadores de la empresa

b) Aquellos datos con mayor impacto (según el plan de actuación)

c) Los programas

d) Aquellos programas y datos con mayor resultado (según el plan de contingencia)

34. Las copias de seguridad mejoran

a) La confidencialidad

b) La integridad y la disponibilidad

c) La integridad y la confidencialidad

d) La integridad

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

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

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

37. 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-site y completa
c) On-line y diferencial
d) Off-line y diferencial

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

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

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

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

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

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

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

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

42. 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 0, con mas de 2 discos
c) Es un RAID 5
d) Es un RAID 1

43. 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 1, con 4 discos
d) Un RAID 0, con 5 discos

44. 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 1, con solo dos discos
c) Es un RAID 5, con solo dos discos
d) Es un RAID 0

45. 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) Ningún nivel de RAID mejora los tiempos de escritura de los discos

d) Puede utilizar un RAID 1 en vez de un disco simple

46. 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) Puede utilizar un RAID 1 en vez de un disco simple

c) Puede utilizar cualquier tipo de RAID (0,1,5,6), pues todos mejoran la velocidad de lectura de los discos

d) Ningún nivel de RAID mejora los tiempos de lectura de los discos

47. 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

48. 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

c) El RAID 6e tiene mejores tiempos de lectura y escritura

d) El RAID 6e utiliza un sistema de paridad que ahorra espacio, por lo que puede almacenar más datos en los mismos discos

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

a) Para realizar una copia de respaldo de un disco duro defectuoso

b) Para detectar un fallo en un disco duro

c) Para realizar una copia de respaldo de un disco que aún no es defectuoso

d) Para predecir un fallo en un disco duro

50. La tecnología S.M.A.R.T. es una medida de seguridad

a) Activa

b) Remota

c) Pasiva

d) Distribuida

51. Se dice de un certificado que es raíz si

a) Es el certificado que se utilizó para instalar el sistema operativo

b) Es un certificado firmado por otro que tenga mayor nivel

c) Es un certificado considerado seguro, que puede firmar otros certificados

d) Es el certificado asociado a la raíz del DNS (.)

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

a) SAN

b) No entra dentro de estas categorías

c) DAS

d) NAS

53. 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 o SAN

c) DAS

d) NAS

54. 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) DAS

c) SAN o NAS

d) SAN

55. En una instalación NAS (Network Attached Storage)

a) Los accesos a los discos se realizan en base a ficheros

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

56. iSCSI es un caso particular de

a) DAS
b) SAN
c) NAS
d) RAID

57. Una persona que extrae y analiza los datos que se transmiten por una línea de comunicación es un

a) DoS
b) Phreaker
c) Sniffer
d) Hacker

58. Cuando un servicio informático (por ejemplo, una web) es imitado por otro para hacerse pasar por el servicio original, se esta utilizando

a) Spamming
b) Dos
c) Phishing
d) Spoofing

59. Un adware

a) Muestra mensajes al usuario
b) Es indetectable por el usuario
c) Es un virus, del tipo troyano
d) Es un virus, pero no un troyano

60. Es spyware

a) Todos los keyloggers
b) Todos los adware
c) Todos los spoofing
d) Todos los virus

61. Un malware que modifica otros ficheros ejecutables para que contengan copias del malware es un

a) Troyano
b) Adware
c) Virus
d) Hoax

62. Un malware que se propaga, pero sin modificar otros ficheros ejecutables, es un

a) Troyano
b) Virus
c) Gusano
d) Hoax

63. El payload

a) Es la función maliciosa de un malware
b) Es un sinónimo de adware
c) Es un sinónimo de spyware
d) Es el sistema de propagación de un malware

64. La llamada a casa de un malware

a) Puede evitarse instalando un firewall con NAT
b) Se usa para infectar a nuevos sistemas
c) Se usa para comunicar datos privados del usuario, o modificar el payload
d) Se usa para instalar un rootkit

65. Un troyano se caracteriza porque

a) El usuario colabora en su instalación en el sistema
b) Se instala a través de spam
c) Instala un keylogger
d) Roba contraseñas, especialmente de cuentas de banco

66. La ingeniería social

a) Encuentra formas de construir contraseñas que las personas puedan recordar fácilmente
b) Se utiliza para hacer sniffing
c) Se basa en el comportamiento social usual de las personas
d) Consiste en manipular sistemas biométricos de autentificación

67. Generalmente, se utiliza el email para enviar spam porque

a) Permite llegar a más gente, con menor inversión en dinero y tiempo
b) No es fácil conseguir otro tipo de direcciones de personas, por ejemplo, de Whatsapp
c) Es más fácil engañar a un antivirus con un email que, por ejemplo, con Whatsapp
d) Es el método tradicional

68. Las actualizaciones de software

a) Son importantes para la seguridad, ya que pueden arreglar vulnerabilidades
b) No son importantes para la seguridad, excepto la del antivirus
c) Deben retrasarse lo más posible, porque son una fuente de troyanos (excepto la actualización del antivirus)
d) No son importantes para la seguridad, pero sí para el usuario, ya que añaden nuevas funcionalidades

69. Las actividades del _____ se orientan a perjudicar al atacado, y a veces a obtener algún provecho de ello

a) Hacker
b) Nerd
c) Samurai
d) Cracker

70. Se llama poisoning, en ocasiones, al

a) Sniffing
b) Phishing
c) Spoofing
d) Fuerza bruta

71. La técnica de la inundación (flooding) suele utilizarse para realizar un ataque de

a) DNS hijacking
b) Sniffing
c) Denial of service
d) DNS spoofing

72. Para conseguir un ataque man-in-the-middle, suele ser necesario utilizar previamente

a) Fuerza bruta
b) Phishing
c) Denial of service
d) Spoofing

73. Desde el punto de vista del atacante, un ataque de diccionario es una alternativa a

a) Denial of service
b) Code injection
c) Fuerza bruta
d) Flooding

74. El malware más complicado de detectar es

a) Un rootkit
b) Un DOS
c) Un spam
d) Un gusano

75. Un exploit es

a) Un hacker de reconocido prestigio
b) Una vulnerabilidad ya conocida por el fabricante
c) Un software que automatiza los ataques
d) Una vulnerabilidad aun desconocida por el fabricante

76. Un 0-day (zero day) es

a) Una vulnerabilidad ya conocida por el fabricante
b) Un software que automatiza los ataques
c) Un hacker de reconocido prestigio
d) Una vulnerabilidad aun desconocida por el fabricante

77. Elige la política de contraseñas más segura (sin incluir la ñ)

a) Tres letras mayúsculas o minúsculas seguidas de tres números
b) Cinco letras mayúsculas o minúsculas
c) 8 números
d) Cuatro letras minúsculas seguidas de tres números

78. Los ataques de code injection se caracterizan por

a) Propagarse como un troyano
b) Provocar una denegación de servicio (DOS)
c) Aprovechar vulnerabilidades de los programas o servicios para que ejecuten un código elegido por el atacante
d) Propagarse como un gusano

79. El antivirus puede ejecutarse

a) A demanda
b) Al vuelo, a demanda y antes de la carga del sistema operativo
c) Al vuelo y a demanda
d) Al vuelo, a demanda, antes de la carga del sistema operativo y antes del arranque BIOS

80. Realizar sniffing es más fácil

a) Es igual de complicado en una red con un hub o un switch
b) En una red con un switch
c) En una red con un hub
d) El sniffing no puede realizarse en redes ethernet, sólo en redes inalámbricas

81. Un ataque de flooding es un tipo concreto de

a) Phishing
b) DOS
c) Man in the middle
d) Troyano

82. Al cifrar un texto en claro con una de las claves de un sistema asimétrico, el texto cifrado resultante

a) Se puede descifrar con la misma clave del sistema asimétrico
b) Tiene siempre la misma longitud (por ejemplo, 32 bytes para MD5)
c) Se puede descifrar con la otra clave del sistema asimétrica
d) Es igual al texto cifrado que se conseguiría con la otra clave asimétrica

83. ¿Para qué puede utilizar un "hidden volume" de TrueCrypt?

a) Todos los discos son "hidden", porque los datos están encriptados
b) El concepto de "hidden volume" no es de TrueCrypt, se aplica a los discos no montados en el fichero /etc/fstab
c) El concepto de "hidden volume" no es de TrueCrypt, se aplica a los discos externos en la BIOS para no arrancar desde ellos
d) Para poder presentar un conjunto de ficheros creible, pero falso

84. Para mejorar el objetivo de "no repudio" de los envíos de información

a) Basta con encriptar los ficheros
b) Hay que firmar y encriptar los ficheros
c) Hay que enviar el fichero encriptado y sin encriptar, para su comparación
d) Basta con firmar los ficheros

85. La criptografía híbrida

a) Mezcla métodos de sustitución y transposición
b) Mezcla encriptación y firma
c) Mezcla claves públicas y privadas
d) Mezcla métodos simétricos y asimétricos

86. Son funciones resumen

a) PKI, MD5
b) MD5, SHA1
c) SHA1, PKI
d) MD5, GPL

87. La desventaja de un sistema de clave asimétrica respecto de uno con clave simétrica es que

a) Es menos seguro, porque es una tecnología más antigua
b) Es menos seguro el intercambio de claves
c) Es más lento, por el tiempo de proceso
d) Es menos seguro, porque las claves son más cortas

88. La desventaja de un sistema de clave simétrica respecto de uno con clave asimétrica es que

a) Es menos seguro, porque las claves son más cortas
b) Es menos seguro el intercambio de claves
c) Es más difícil y caro realizar programas que lo implementen
d) Es más lento, por el tiempo de proceso

89. En una comunicación se comienza utilizando una clave asimétrica para intercambiar una clave simétrica. Esto se hace para

a) Ahorrar tiempo de proceso, ya que las claves asimétricas son más difíciles de computar
b) Ahorrar tiempo de proceso, ya que las claves simétricas son más difíciles de computar
c) Aumentar el objetivo de "no repudio"
d) Aumentar la confidencialidad

90. En un sistema de criptografía híbrida, como el estudiado en clase, hay

a) 2 claves (una pública y una privada)
b) 3 claves (una pública, una privada y una simétrica)
c) 3 claves (dos públicas y una privada)
d) 2 claves (dos públicas)

91. En un sistema de criptografía híbrida, como el estudiado en clase

a) Una de las partes inventa sobre la marcha una clave simétrica
b) Una de las partes inventa sobre la marcha una clave pública
c) Una de las partes inventa sobre la marcha un par de claves (pública y privada)
d) Una de las partes inventa sobre la marcha una clave privada

92. El "Cifrado del César" es

a) Criptografía simétrica, porque se usa la misma clave para cifrar y descifrar
b) Criptografía asimétrica, porque se usa distinto algoritmo para cifrar que para descifrar
c) Criptografía híbrida, porque mezcla métodos manuales y automáticos
d) Criptografía estadística, porque se necesitan probar varias posibilidades

93. La autenticación consiste en

a) firmar un documento
b) usar métodos biométricos
c) otorgar permisos a cierto usuario
d) verificar la identidad de un usuario

94. Determina si cada una de estas medidas que aumentan la seguridad informática son activas o pasivas, especificando el por qué de esa clasificación: Cuotas de disco, discos redundantes (RAID), antivirus, autentificación mediante contraseñas

95. Explica qué apartados debe incluir un plan de contingencias

96. Determina a cuál (o cuáles) de los objetivos de la seguridad informática (características seguras) ayuda cada una de estas medidas, especificando el por qué: Cuotas de disco, discos redundantes (RAID), antivirus, autentificación mediante contraseñas

97. Describe qué pasos realiza un navegador web para decidir que una conexión https es segura

a)