

Pruebas para la obtención del Título de Técnico en Sistemas Microinformáticos y Redes

Convocatoria correspondiente al curso académico 2023-2024

(Resolución de 29 de diciembre de 2023 de la Dirección General de Educación Secundaria, Formación Profesional y Régimen Especial)

DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	DNI NIE o Pasaporte:	Fecha: 23 – 05 - 2024	

Código del ciclo: IFCM01	Denominación completa del título: TÉCNICO EN SISTEMAS MICROINFORMÁTICOS Y REDES
Clave o código del módulo: 0226	Denominación completa del módulo profesional: SEGURIDAD INFORMÁTICA

INSTRUCCIONES GENERALES PARA LA REALIZACIÓN DE LA PRUEBA
<ul style="list-style-type: none">• Se entrega un examen con preguntas tipo test y una plantilla de respuestas.• Cada pregunta tiene una única respuesta correcta.• Solo se tendrán en cuenta las respuestas marcadas en la plantilla.• La respuesta se marcará en la plantilla rellenando el círculo.• Al finalizar el examen se entrega tanto la plantilla de respuestas como el examen.• No se podrá utilizar ninguna documentación a la hora de realizar el examen.
CRITERIOS DE CALIFICACIÓN Y VALORACIÓN
<ul style="list-style-type: none">• Cada pregunta tiene el valor de 1 pto.• La valoración máxima es de 60 ptos• En las preguntas de cuatro opciones cada respuesta correcta sumará 1 punto y cada respuesta errónea restará 1/3 puntos• El examen se aprueba con una calificación mayor o igual a 30 puntos

CALIFICACIÓN



DATOS DEL ASPIRANTE	FIRMA
DNI:	

1. Cuando firmamos un documento digitalmente...
 - a) Garantizamos la confidencialidad usando criptografía de clave privada y función hash.
 - b) Garantizamos la confidencialidad usando criptografía de clave pública y función hash.
 - c) Garantizamos la confidencialidad siempre.
 - d) Ninguna de las anteriores.
2. El certificado digital...
 - a) Se genera por seguridad pero no haría falta.
 - b) Se genera para luego poder generar la clave privada.
 - c) Se genera para garantizar la autenticación del propietario a través de su clave pública.
 - d) Ninguna de las anteriores.
3. La firma digital nos permite asegurar en una VPN:
 - a) Autenticación.
 - b) No integridad.
 - c) Fiabilidad.
 - d) Las dos primeras son correctas.
4. ¿Qué opción se utiliza para realizar un escaneo de puertos UDP del ssh y ftp?
 - a) nmap -sT -p 20,21,22
 - b) nmap -sU -p 20,21,22
 - c) nmap -sU -p 20,21,23
 - d) nmap -sT -p 20,21,23
5. ¿Qué técnica se utiliza para ocultar la dirección IP real de un dispositivo en la red?
 - a) VPN
 - b) Proxy
 - c) HoneyPot
 - d) IDS/IPS
6. ¿Qué es el filtrado de paquetes?
 - a) La revisión de los datos en los paquetes de red para identificar y eliminar las amenazas de malware
 - b) La ocultación de la dirección IP real de un dispositivo en la red
 - c) La eliminación de los paquetes de red no deseados para mejorar el rendimiento de la red
 - d) La inspección de los paquetes de red para permitir o denegar su paso a través de un firewall



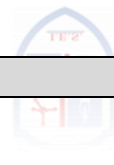
DATOS DEL ASPIRANTE	FIRMA
DNI:	

7. Las amenazas del software podemos englobarlas en los siguientes tipos
- a) Virus, gusanos y troyanos.
 - b) Código malicioso e ingeniería social.
 - c) Malware y phishing.
 - d) El total de las respuestas anteriores es correcta.
8. Cuando hablamos de una política de lista negra en un firewall nos referimos a:
- a) Se acepta todo menos lo que se deniega explícitamente.
 - b) Se deniega todo menos lo que se acepta explícitamente.
 - c) Es más segura que la de lista blanca
 - d) Ninguna respuesta es correcta.
9. ¿Cuál de los dispositivos se emplea en seguridad activa?
- a) ISD
 - b) IDPS
 - c) Extintor
 - d) Ninguna de las anteiores
10. La orden "`setfacl -d -m user:prueba:rw- ~/datos/archivos/`" dará permisos de:
- a) Lectura y escritura al usuario *prueba* sobre el fichero *archivos*.
 - b) Lectura y escritura al usuario *prueba* sobre los archivos del directorio *datos*.
 - c) Lectura y escritura al usuario *prueba* sobre los ficheros que se creen dentro de *archivos*.
 - d) Lectura y escritura al usuario *prueba* sobre los ficheros que se creen dentro de *datos*.
11. La orden "`setfacl -m -R user:prueba:rw- midirectorio`" dará permisos de:
- a) Lectura y escritura y ejecución al usuario *prueba* sobre el fichero *archivos*.
 - b) Lectura y escritura al usuario *prueba* sobre los archivos y directorios *midirectorio*.
 - c) Lectura y escritura al usuario *prueba* sobre los ficheros que se creen dentro de *midirectorio*.
 - d) No dará permisos porque la orden no es correcta.
12. Indica cuál de estas opciones no es una característica para llegar a cumplir las propiedades de un sistema informático seguro.
- a) Autenticación o confidencialidad.
 - b) No repudio en origen.
 - c) Encriptación.
 - d) Integridad.



DATOS DEL ASPIRANTE	FIRMA
DNI:	

13. La criptografía simétrica con respecto a la asimétrica
- a) Es rápida para cifrar y no tiene agujeros de seguridad.
 - b) Es lenta para cifrar y tiene agujeros de seguridad.
 - c) Es rápida para cifrar y tiene agujeros de seguridad.
 - d) Todas las anteriores son correctas.
14. Indica que sentencia es falsa
- a) La integridad permite asegurar que los datos ni se han falseado
 - b) Confidencialidad es desvela datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
 - c) Disponibilidad es que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.
 - d) Todas son verdaderas
15. Una de las siguientes medidas no pertenece a la seguridad lógica:
- a) Contraseñas
 - b) SAI
 - c) Copias de seguridad
 - d) Software antimalware
16. Un hacker:
- a) Siempre tiene una finalidad maliciosa
 - b) La mayoría de las veces tiene una finalidad maliciosa
 - c) A veces posee una finalidad maliciosa, entonces se denomina cracker
 - d) Es un curioso con una finalidad conocida
17. Las medidas de seguridad biométricas :
- a) Permiten el acceso a un sistema mediante contraseña asimétrica
 - b) Emplean la biología para medir parámetros de seguridad.
 - c) Emplean características biológicas para identificar usuarios.
 - d) Son el fundamento de la identificación mediante certificado digital.
18. En caso de tener una instalación CPD crítico con un suministro eléctrico muy fluctuante, el tipo e SAI a utilizar es:
- a) Online o doble conversión
 - b) Offline
 - c) Inline
 - d) Línea interactiva



DATOS DEL ASPIRANTE	FIRMA
DNI:	

19. El sistema biométrico más empleado por su relación fiabilidad/coste es:

- a) Reconocimiento de voz
- b) Huella dactilar
- c) Iris
- d) Escritura y firma

20. ¿Qué es la identificación?

- a) Momento en que el usuario se da a conocer en el sistema
- b) Verificación que realiza el sistema sobre el intento de login.
- c) Un número de intentos de login
- d) Un proceso de creación de contraseñas.

21. Las contraseñas de sistemas GNU/Linux se encuentran encriptadas en el archivo:

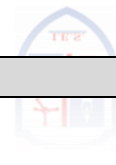
- a) /etc/groups
- b) /etc/passwd
- c) /etc/shadow
- d) /etc/sha-pass

22. ¿Cómo se denomina el dispositivo de red que controla el tráfico a través de un firewall que lleva instalado y que se coloca en la parte más externa de la red corporativa?

- a) Router perimetral.
- b) Router frontera.
- c) Bastion frontera.
- d) Router externo.

23. Los firewalls pueden implementarse mediante una solución:

- a) Hardware.
- b) Software.
- c) Hardware o Software, siendo estas últimas las más comunes.
- d) Todas las respuestas son correctas.



DATOS DEL ASPIRANTE	FIRMA
DNI:	

24. ¿Qué efecto tiene la siguiente orden # iptables -F en la línea de comandos siendo root el usuario?
- a) Ver las reglas introducidas para la tabla filter.
 - b) Eliminar todos los paquetes de la entrada.
 - c) Eliminar todos los paquetes de la salida.
 - d) Borrar todas las reglas de la tabla filter.
25. En la seguridad perimetral, los nodos bastión
- a) Son equipos seguros que sirven como punto de contacto entre la red local e Internet.
 - b) Son máquinas vulnerables por estar expuestas directamente a Internet.
 - c) Suelen ser máquinas UNIX/Linux en las que se han extremado las medidas de seguridad.
 - d) Todas las respuestas son correctas.
26. Un servidor cuyo objetivo es la centralización del tráfico entre Internet y una red local a nivel de capa de aplicación es un:
- a) Firewall
 - b) VPN
 - c) Proxy
 - d) ISD
27. Un sistema configurado con vulnerabilidades usado para recoger ataques y estudiar nuevas técnicas es un...:
- a) Firewall
 - b) HoneyPot
 - c) Proxy
 - d) ISD
28. ¿Qué opción se utiliza para escanear todos los puertos con NMAP?
- a) -p-
 - b) -p0-65535
 - c) -sS
 - d) -sT



DATOS DEL ASPIRANTE	FIRMA
DNI:	

29. ¿Qué es la seguridad perimetral?

- a) La protección de los datos en el interior de la red
- b) La protección de la red y los recursos de la organización contra amenazas externas
- c) La protección de los dispositivos personales de los empleados
- d) La protección de los edificios y las instalaciones físicas de la organización

30. Qué información se encuentra en un certificado digital X509?

- a) Nombre y dirección del propietario del certificado.
- b) Clave pública y firma digital del propietario del certificado.
- c) Número de serie y fecha de expiración del certificado.
- d) Todos los anteriores.

31. ¿Qué es el cifrado asimétrico?

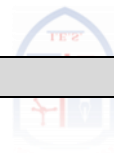
- a) Un método de cifrado que utiliza la misma clave para cifrar y descifrar la información.
- b) Un método de cifrado que utiliza una clave diferente para cifrar y descifrar la información.
- c) Un método de cifrado que utiliza una clave privada para cifrar y una clave pública para descifrar la información.
- d) Un método de cifrado que utiliza una clave pública para cifrar y una clave privada para descifrar la información.

32. Qué tipo de mecanismo de seguridad sería una contraseña?

- a) Física / Pasiva.
- b) Física / Activa.
- c) Lógica / Pasiva.
- d) Lógica / Activa.

33. ¿En un buen análisis de riesgos tendrías en cuenta...?

- a) Con los Activos y vulnerabilidades es más que suficiente.
- b) Las vulnerabilidades puesto que son las debilidades que tengo que cubrir.
- c) Los activos, vulnerabilidades, amenazas, riesgos, ataques e impactos.
- d) Vulnerabilidades, riesgos, amenazas y ataques.



DATOS DEL ASPIRANTE	FIRMA
DNI:	

34. Si una amenaza se materializa sobre un activo aprovechando una vulnerabilidad del mismo decimos que se ha producido...

- a) Un riesgo.
- b) Un impacto.
- c) Un ataque.
- d) Ninguna de las respuestas anteriores es correcta.

35. Las ACL permiten...

- a) Asignar permisos a usuarios concretos, pero no a grupos.
- b) Asignar permisos a usuarios o a grupos concretos.
- c) Asignar permisos a grupos concretos, pero no a usuarios.
- d) Ampliar permisos, pero no disminuirlos.

36. Los datos hay que protegerlos fundamentalmente por:

- a. Para que no sean modificados
- b. Para que la empresa pueda funcionar con normalidad
- c. Para que no sean atacados por virus
- d. Para que no sean visibles por otros usuarios.

37. Indica cuál de los siguientes elementos no corresponde a la seguridad física:

- a. Discos duros
- b. Servidores
- c. Aplicación de backup(copia de seguridad)
- d. CPD

38. Indica cuál de las siguientes amenazas no es lógica:

- a. Ataque a las aplicaciones de los servidores
- b. Pérdida de datos
- c. Fallos en el suministro
- d. Fallo en backup

39. Con respecto a la ubicación del CPD en los edificios siempre seleccionaremos:

- a. La planta baja
- b. Plantas subterráneas
- c. Primeras plantas
- d. Plantas superiores



DATOS DEL ASPIRANTE	FIRMA
DNI:	

40. De las siguientes amenazas, cual de ellas hace referencia a seguridad física
- Virus, Troyanos y Malware
 - Pérdida de datos
 - Fallos de suministro
 - Ataques a las aplicaciones de los servidores
41. El funcionamiento de un SAI en espera (Stand-by)
- Toma corriente de las baterías del SAI directamente, posteriormente después de un corte hemos de sustituir esas baterías.
 - Toma corriente del suministro principal y activa las baterías en caso de corte de suministro.
 - Toma corriente de las baterías del SAI directamente y en el caso de un corte, posteriormente vuelve a cargarlas una vez restaurado el suministro.
 - Toma corrientes del suministro principal, pero en caso de corte apaga el equipo.
42. Un SAI
- Protege todas las máquinas de la empresa
 - Protege solo los servidores
 - Protege las máquinas del CPD
 - Protege solo los servidores de los clientes.
43. El acceso a la sala del CPD
- Está permitido a cualquier empleado de la empresa
 - Está permitido a cualquier persona.
 - Está más restringido que cualquier otra sala de trabajo
 - Está restringido solo para mantenimientos de sistemas de refrigeración y limpieza.
44. Contraseñas de la BIOS
- Siempre hay que activarlas todas: usuario, supervisor, cifrado de disco, etc.
 - Como mínimo, activaremos la contraseña del supervisor para impedir modificaciones de la configuración.
 - Activaremos solo a nivel de cifrado de disco.
 - La BIOS no dispone de contraseñas.



DATOS DEL ASPIRANTE	FIRMA
DNI:	

45. El acceso mediante biometría
- Es más seguro si lo combinamos con la introducción de una contraseña (“algo que eres, algo que sabes”).
 - Es más seguro si la combinamos de una contraseña y la lectura de una tarjeta (“algo que eres, algo que sabes y algo que tienes”).
 - Es mas seguro si utilizamos únicamente biometría, pues la utilización de combinadas puede ser peligroso en el caso de que falle alguna de ellas.
 - Solo está disponible para servicios propios de banca.
46. La integridad de los datos
- Consiste en que éstos queden almacenados tal y como espera el usuario: que no sean alterados sin su consentimiento.
 - Consiste en que éstos estén disponibles en todo momento al usuario.
 - Consiste en que éstos sean únicamente utilizados por las personas autorizadas.
 - Consiste en que éstos estén debidamente ordenados por clave.
47. Si ponemos seis discos duros de 1TB en RAID1, el usuario ve:
- 6TB
 - 1TB
 - 3TB
 - 5TB
48. Si tenemos cuatro discos de 1 TB en RAID 0 y falla uno de ellos
- El usuario todavía puede acceder a 3 TB de ficheros.
 - El RAID se ha roto, pero reponiendo el disco podemos recuperarlo.
 - Hemos perdido todo.
 - El usuario puede acceder a la mitad de la información.
49. Si tenemos cuatro discos de 1TB en RAID 5 y falla uno de ellos
- El usuario todavía puede acceder a 3 TB de ficheros.
 - El usuario solo puede acceder a la mitad de los discos.
 - El usuario solo puede acceder a 1 TB de ficheros.
 - Hemos perdido todo.
50. De los siguientes sistemas, indica cual de ellos corresponde a un sistema de almacenamiento
- CISC
 - SAN
 - LIFO
 - CFS



DATOS DEL ASPIRANTE	FIRMA
DNI:	

51. Un sistema de almacenamiento NAS
- Es un armario de discos conectado a uno o varios servidores.
 - Es un equipo que ofrece disco a los equipos conectados a su misma red.
 - Es un conjunto de equipos conectado en red compartiendo información.
 - No es un sistema de almacenamiento.
52. En general, una copia incremental
- Ocupa más que la copia completa.
 - Ocupa más que la copia diferencial.
 - Ocupa menos que la copia diferencial.
 - Es la suma entre la completa y la diferencial.
53. Una copia diferencial
- Incluye solo los archivos cambiados desde la última copia incremental.
 - Incluye solo los archivos cambiados desde la última copia incremental.
 - Incluye todos los archivos.
 - Incluye solo los archivos cambiados desde la última copia.
54. Un backup consiste en...
- Copia de seguridad de aplicaciones y sistema operativo.
 - Copia de seguridad de datos de usuario o empresa.
 - Copia de seguridad de aplicaciones, sistema operativo y datos.
 - Copia de seguridad de aplicaciones.
55. Un Gusano...
- Intenta dejar inservible el ordenador infectado
 - Va acaparando todos los recursos del ordenador: disco, memoria,...
 - Suele habilitar puertas traseras en los equipos
 - Obtienen las posibles contraseñas almacenadas en cookies
56. Se desea realizar una copia de seguridad de un directorio(/tmp/original) a otro(/tmp/copia), ambos en la misma máquina. La copia de seguridad se debe realizar solo de aquellos ficheros nuevo o modificados. Indica cual es la instrucción correcta, teniendo en cuenta que trabajamos en un Ubuntu:
- cp /tmp/original/miFichero.txt /tmp/copia/miFichero.txt
 - rsync -av /tmp/original /tmp/copia
 - rsync -avvb /tmp/original /tmp/copia
 - cp /tmp/original/ /tmp/copia/



DATOS DEL ASPIRANTE	FIRMA
DNI:	

57. Una VLAN basada en grupos de puertos:
- Solo funciona dentro del mismo switch.
 - Podemos conectarla con otra VLAN de grupo de puertos en otro switch.
 - Esos equipos quedarán aislados del resto de la red.
 - No podemos conectarla a otra VLAN de grupo de puerto en el mismo switch.
58. En un Access Point...
- Podemos separar dos grupos de usuarios.
 - Podemos separar dos grupos de usuarios, pero en dos SSID distintos.
 - Solo podemos tener un grupo de usuarios.
 - En un Access Point no se permiten crear grupos de usuarios.
59. En la criptografía asimétrica utilizamos:
- Dos claves públicas.
 - Dos claves públicas y una privada.
 - Una clave pública y otra privada.
 - Dos claves privadas.
60. Se pretende firmar un documento en Ubuntu con gpg, con la intención de identificar a la persona que envía el documento, ¿Cuál es la instrucción correcta para firmar el documento?
- gpg - -verifiy mensaje.asc
 - gpg -a - -detach-sign mensaje
 - gpg -a - -clearsign mensaje
 - gpg - -decrypt mensaje.asc



DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	DNI NIE o Pasaporte:	Fecha:	

1	A	B	C	D
2	A	B	C	D
3	A	B	C	D
4	A	B	C	D
5	A	B	C	D
6	A	B	C	D
7	A	B	C	D
8	A	B	C	D
9	A	B	C	D
10	A	B	C	D
11	A	B	C	D
12	A	B	C	D
13	A	B	C	D
14	A	B	C	D
15	A	B	C	D
16	A	B	C	D
17	A	B	C	D
18	A	B	C	D
19	A	B	C	D
20	A	B	C	D
21	A	B	C	D
22	A	B	C	D
23	A	B	C	D
24	A	B	C	D
25	A	B	C	D
26	A	B	C	D
27	A	B	C	D
28	A	B	C	D
29	A	B	C	D
30	A	B	C	D
31	A	B	C	D
32	A	B	C	D
33	A	B	C	D
34	A	B	C	D
35	A	B	C	D
36	A	B	C	D

37	A	B	C	D
38	A	B	C	D
39	A	B	C	D
40	A	B	C	D
41	A	B	C	D
42	A	B	C	D
43	A	B	C	D
44	A	B	C	D
45	A	B	C	D
46	A	B	C	D
47	A	B	C	D
48	A	B	C	D
49	A	B	C	D
50	A	B	C	D