# Qosa Chaery

IES ROSA CHACEL c/ Abizanda, 70 28033 Madrid C.C.: 28037028

#### Comunidad de Madrid

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

#### Convocatoria correspondiente al curso académico 2022-2023

(Orden 3299/2020, de 15 de diciembre, de la Consejería de Educación y Juventud)

DATO	S DEL ASPIRANTE		FIRMA
APELLIDOS:			
Nombre:	DNI NIE o Pasaporte:	Fecha:	
		17 – 05 - 2023	

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

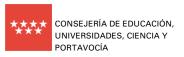
### INSTRUCCIONES GENERALES PARA LA REALIZACIÓN DE LA PRUEBA

- Se entrega un examen con preguntas tipo test y una plantilla de respuestas.
- Cada pregunta tiene una única respuesta correcta.
- Las respuestas sólo se marcarán en la plantilla, el examen con las preguntas no debe ser marcado.
- La respuesta se marcará en la plantilla con un círculo. Si se quiere rectificar, se tachará con una X.
- 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

- Cada pregunta tiene el valor de 1 punto.
- La valoración máxima es de 50 puntos.
- 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 25 puntos.

CALIFICACIÓN			





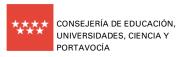
DATOS DEL ASPIRANTE	FIRMA
DNI:	710
	7.5

- 1. 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
- 2. 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
- 3. 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
- 4. 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
- 5. De las siguientes amenazas, cuál de ellas hace referencia a seguridad física
- a) Virus, Troyanos y Malware
- b) Pérdida de datos
- c) Fallos de suministro
- d) Ataques a las aplicaciones de los servidores
- 6. El funcionamiento de un SAI en espera (Stand-by)
- a) Toma corriente de las baterías del SAI directamente, posteriormente después de un corte hemos de sustituir esas baterías.
- b) Toma corriente del suministro principal y activa las baterías en caso de corte de suministro.
- c) Toma corriente de las baterías del SAI directamente y en el caso de un corte, posteriormente vuelve a cargarlas una vez restaurado el suministro.
- d) Toma corrientes del suministro principal, pero en caso de corte apaga el equipo.



DATOS DEL ASPIRANTE	FIRMA
DNI:	7-10

- 7. Un SAI
- a) Protege todas las máquinas de la empresa
- b) Protege solo los servidores
- c) Protege las máquinas del CPD
- d) Protege solo los servidores de los clientes.
- 8. El acceso a la sala del CPD
- a) Está permitido a cualquier empleado de la empresa
- b) Está permitido a cualquier persona.
- c) Está más restringido que cualquier otra sala de trabajo
- d) Está restringido solo para mantenimientos de sistemas de refrigeración y limpieza.
- 9. Contraseñas de la BIOS
- a) Siempre hay que activarlas todas: usuario, supervisor, cifrado de disco, etc.
- b) Como mínimo, activaremos la contraseña del supervisor para impedir modificaciones de la configuración.
- c) Activaremos solo a nivel de cifrado de disco.
- d) La BIOS no dispone de contraseñas.
- 10. El acceso mediante biometría
- a) Es más seguro si lo combinamos con la introducción de una contraseña ("algo que eres, algo que sabes").
- b) 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).
- c) Es más seguro si utilizamos únicamente biometría, pues la utilización de combinadas puede ser peligroso en el caso de que falle alguna de ellas.
- d) Solo está disponible para servicios propios de banca.
- 11. La integridad de los datos
- a) Consiste en que éstos queden almacenados tal y como espera el usuario: que no sean alterados sin su consentimiento.
- b) Consiste en que éstos estén disponibles en todo momento al usuario.
- c) Consiste en que éstos sean únicamente utilizados por las personas autorizadas.
- d) Consiste en que éstos estén debidamente ordenados por clave.
- 12. Si ponemos seis discos duros de 1TB en RAID1, el usuario ve:
- a) 6TB
- b) 1TB
- c) 3TB
- d) 5TB
- 13. Si tenemos cuatro discos de 1 TB en RAID 0 y falla uno de ellos
- a) El usuario todavía puede acceder a 3 TB de ficheros.
- b) El RAID se ha roto, pero reponiendo el disco podemos recuperarlo.
- c) Hemos perdido todo.
- d) El usuario puede acceder a la mitad de la información.





DATOS DEL ASPIRANTE	FIRMA
DNI:	710

- 14. Si tenemos cuatro discos de 1TB en RAID 5 y falla uno de ellos
- a) El usuario todavía puede acceder a 3 TB de ficheros.
- b) El usuario solo puede acceder a la mitad de los discos.
- c) El usuario solo puede acceder a 1 TB de ficheros.
- d) Hemos perdido todo.
- 15. De los siguientes sistemas, indica cuál de ellos corresponde a un sistema de almacenamiento
- a) CISC
- b) SAN
- c) LIFO
- d) CFS
- 16. Un sistema de almacenamiento NAS
- a) Es un armario de discos conectado a uno o varios servidores.
- b) Es un equipo que ofrece disco a los equipos conectados a su misma red.
- c) Es un conjunto de equipos conectado en red compartiendo información.
- d) No es un sistema de almacenamiento.
- 17. En general, una copia incremental
- a) Ocupa más que la copia completa.
- b) Ocupa más que la copia diferencial.
- c) Ocupa menos que la copia diferencial.
- d) Es la suma entre la completa y la diferencial.
- 18. Una copia diferencial
- a) Incluye solo los archivos cambiados desde la última copia incremental.
- b) Incluye solo los archivos cambiados desde la primera copia incremental.
- c) Incluye todos los archivos.
- d) Incluye solo los archivos cambiados desde la última copia.
- 19. Un backup consiste en...
- a) Copia de seguridad de aplicaciones y sistema operativo.
- b) Copia de seguridad de datos de usuario o empresa.
- c) Copia de seguridad de aplicaciones, sistema operativo y datos.
- d) Copia de seguridad de aplicaciones.
- 20. Un Gusano...
- a) Intenta dejar inservible el ordenador infectado
- b) Va acaparando todos los recursos del ordenador: disco, memoria, ...
- c) Suele habilitar puertas traseras en los equipos
- d) Obtienen las posibles contraseñas almacenadas en cookies



DATOS DEL ASPIRANTE	FIRMA
DNI:	7-10

- 21. 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:
- a) cp /tmp/original/miFichero.txt /tmp/copia/miFichero.txt
- b) rsync -av /tmp/original /tmp/copia
- c) rsync -avvb /tmp/original /tmp/copia
- d) cp /tmp/original/ /tmp/copia/
- 22. Una VLAN basada en grupos de puertos:
- a) Solo funciona dentro del mismo switch.
- b) Podemos conectarla con otra VLAN de grupo de puertos en otro switch.
- c) Esos equipos quedarán aislados del resto de la red.
- d) No podemos conectarla a otra VLAN de grupo de puerto en el mismo switch.
- 23. En un Access Point...
- a) Podemos separar dos grupos de usuarios.
- b) Podemos separar dos grupos de usuarios, pero en dos SSID distintos.
- c) Solo podemos tener un grupo de usuarios.
- d) En un Access Point no se permiten crear grupos de usuarios.
- 24. En la criptografía asimétrica utilizamos:
- a) Dos claves públicas.
- b) Dos claves públicas y una privada.
- c) Una clave pública y otra privada.
- d) Dos claves privadas.
- 25. 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?
- a) gpg -verifiy mensaje.asc
- b) gpg -a -detach-sign mensaje
- c) gpg -a -clearsign mensaje
- d) gpg -decrypt mensaje.asc
- 26. ¿Qué ley versa sobre la protección de datos de carácter personal?
- a) LPI
- b) LDCP
- c) LOPD
- d) RGPD





DATOS DEL ASPIRANTE	FIRMA
DNI:	717

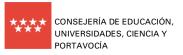
- 27. Para el tratamiento de datos de carácter personal de las personas físicas, se establecen tres niveles en funciones de la sensibilidad de los datos tratados. (Bajo, Medio y Alto). Indica que medida no corresponde al nivel medio de tratamiento de daos de carácter personal:
- a) Llevar un registro de incidencias acontecidas en el fichero
- b) Debe existir un control de acceso físico a los medios de almacenamiento de los datos.
- c) Cifrado de las comunicaciones.
- d) Realizar copia de seguridad como mínimo semanalmente.
- 28. Los derechos de autor en los entornos digitales, establece un canon sobre los distintos dispositivos de almacenamiento para compensar a los autores:
- a) Por las copias legales compradas por los usuarios en tiendas físicas.
- b) Por las copias legales compradas por los usuarios en tiendas online.
- c) Por las copias no controladas.
- d) Por las copias originales adquiridas de cualquier forma.
- 29. La Ley de Servicios de la Sociedad de la Información y Comercio Electrónico intenta cubrir el hueco legal con:
- a) Las empresas que prestan servicios.
- b) Los usuarios que reciben servicios.
- c) Sistemas de Información.
- d) Las comunicaciones de compra online.
- 30. El firewall es un software especializado que:
- a) Se interpone entre las aplicaciones de red.
- b) Se interpone entre las aplicaciones de una misma VPN.
- c) Se interpone entre el Sistema Operativo y las aplicaciones.
- d) Se interpone entre las aplicaciones y el software de red.
- 31. Con el comando netstat
- a) Comprobamos las estadísticas de red
- b) Comprobamos las conexiones anteriores.
- c) Comprobamos las conexiones establecidas en este momento
- d) Comprobamos el tráfico de nuestra red en este momento.
- 32. La autenticación en el puerto de un switch
- a) Consiste en utilizar siempre el mismo cable.
- b) Solo funciona con tarjetas del mismo fabricante.
- c) El switch identifica a ese equipo que se quiere conectar por ese puerto.
- d) Consiste en introducir la password previamente dada de alta en el switch.





DATOS DEL ASPIRANTE	FIRMA
DNI:	717

- 33. Para proteger el Access Point
- a) Lo guardamos en un armario bajo llave, como hacemos con los switch.
- b) Modificamos la contraseña de acceso a la configuración.
- c) Dejamos la contraseña por defecto de fábrica, pues es la más segura.
- d) El Access Point no implica ningún riesgo como para ser protegido.
- 34. Una tarjeta de red en modo promiscuo
- a) Nos permite ahorrar energía porque utiliza menos recursos.
- b) Procesa todos los paquetes de datos, no únicamente los dirigidos a su MAC.
- c) En este modo podemos unirnos con otra tarjeta para tener mucho más ancho de banda.
- d) Proceso todos los paquetes de datos, pero solo los dirigidos a su MAC.
- 35. Los protocolos TCP/IP son inseguros porque
- a) En su diseño se pensó más en la fiabilidad que en seguridad.
- b) En los años setenta no había hackers.
- c) Todos los protocolos son muy seguros: por eso se siguen utilizando.
- d) La sincronización entre equipos es de forma asíncrona.
- 36. Contra un ataque por envenenamiento ARP
- a) Podríamos bloquear el tráfico ARP en todos los routers de la red.
- b) Podríamos utilizar tablas ARP estáticas.
- c) Lo ideal es introducir un servidor NIPS que identifique este comportamiento anómalo.
- d) Podríamos utilizar tablas ARP dinámicas.
- 37. Para que funcione el ataque por envenenamiento ARP
- a) Basta con enviar una vez los paquetes adulterados, porque las víctimas lo dejan apuntado en su tabla.
- b) Hay que repetirlo continuamente, porque las tablas ARP caducan.
- c) Debemos de introducir un troyano en las víctimas, para que desinstalen el protocolo ARP.
- d) Debemos de introducir un gusano en las víctimas, para que saturen las tablas de enrutamiento
- 38. El ataque a una clave WEP utilizando aircrack-ng:
- a) Lo puede lanzar cualquier usuario, pues el software se descarga de internet
- b) Se puede lanzar desde cualquier punto de internet, siempre que sea un router wifi.
- c) Siempre se debe lanzar desde un equipo conectado con un cable de red.
- d) Lo debe lanzar un usuario privilegiado, porque había que poner la tarjeta en modo monitor.
- 39. Los ataques proxy en una red de empresa
- a) Debemos combatirlos mediante formación de los usuarios y análisis estadístico del tráfico.
- b) A veces son beneficiosos, porque optimizan la ocupación de la conexión a internet.
- c) Como son inevitables, deberíamos eliminar todas las restricciones de página deportivas, juegos, etc.
- d) Debemos combatirlos instalando un spyware





DATOS DEL ASPIRANTE	FIRMA
DNI:	7-10

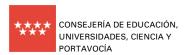
- 40. Cuando un usuario instala un proxy en su máquina
- a) No pasa nada: el firewall de red evitará que salga al exterior.
- b) Es una infracción grave, porque ha instalado software no autorizado
- c) Es recomendado para mejorar el tráfico entre los equipos de la red
- d) Solo se puede instalar Utrasurf, que es el recomendado por las revistas especializadas.
- 41. Las contramedidas, para evitar un ataque a las redes inalámbricas son:
- a) Utilizar un proxy, un firewall y un sniffer.
- b) Utilizar protocolos mejorados WPA2, reducir potencia de emisión y crear listas MAC autorizadas.
- c) Utilizar protocolos UDP, WPA2 y proxy.
- d) Utilizar un firewall, protocolo WEP-SK y varias SSID.
- 42. En una operación de firma con cifrado asimétrico
- a) Necesitamos la clave pública y privada del receptor de mensaje.
- b) Necesitamos la clave pública y privada del emisor del mensaje.
- c) Necesitamos la clave pública del emisor y la clave privada del receptor del mensaje.
- d) Necesitamos la clave pública del receptor y la clave privada del emisor del mensaje.
- 43. En una comunicación, ¿podemos utilizar algoritmos simétricos y asimétricos?
- a) Si. El simétrico para cifrar y el asimétrico para intercambiar la clave.
- b) Si. El asimétrico para cifrar y el simétrico para intercambiar las claves públicas y privadas.
- c) Si. El simétrico para cifrar y el asimétrico para firmar el documento.
- d) Nunca. Son incompatibles.
- 44. La confidencialidad dispone de tres mecanismos
- a) Autorización, Autenticación y Protección.
- b) Autenticación, Protección y Cifrado.
- c) Protección, Autorización y Cifrado.
- d) Autorización, Autenticación y Cifrado.
- 45. No repudio...
- a) se refiere a que, ante una relación entre dos partes, intentemos evitar que cualquiera de ellas pueda negar que participara en esa relación.
- b) se refiere a que cuando una persona intente acceder a un edificio, ésta no sea autorizada por el personal de seguridad.
- c) se refiere a que cuando una persona intente acceder a un ordenador, él ordenador no le permita acceder con su usuario y contraseña.
- d) se refiere a que, ante una relación entre dos partes, que cualquiera de ellas pueda negar que participara en esa relación





DATOS DEL ASPIRANTE	FIRMA
DNI:	7 0

- 46. Uno de los elementos fundamentales para proteger las comunicaciones, es el uso de:
- a) Envío de datos mediante soportes portátiles.
- b) Utilización del correo de la empresa para el envío de información.
- c) Canales cifrados.
- d) Envío de información solo en la intranet.
- 47. Indica cual es la regla de la cadena INPUT que nos permite acceder a nuestro servidor ftp (puerto 20):
- a) iptables -A INPUT -p tcp - dport 20 -j DROP
- b) iptables -A INPUT -p tcp - port 20 -j REJECT
- c) iptables -A INPUT -p tcp -port 20 -j ACCEPT
- d) iptables -A INPUT -p tcp - dport 20 -j ACCEPT
- 48. Son expertos en protocolos de comunicaciones capaces de procesar una captura de tráfico de red para localizar la información interesante
- a) Sniffers
- b) Ciberterrorista
- c) Script kiddie
- d) Protocol Hacker
- 49. Indica que regla de la cadena INPUT que rechaza todos los paquetes que se originan de la dirección 192.168.0.155 y envía un mensaje de error icmp:
- a) iptables -A INPUT -p tcp -o 192.168.0.155 -j REJECT
- b) iptables -A INPUT -s 192.168.0.155 -j DROP
- c) iptables -A INPUT -s 192.168.0.155 -j REJECT
- d) iptables -A INPUT -o 192.168.0.155 -j REJECT
- 50. Que actos realiza un hacker...
- a) Ataca la defensa informática de un sistema para hacer daño, es decir: desactivar servicios, alterar información...
- b) Ataca la defensa informática de un sistema por el reto que supone hacerlo.
- c) Ataca la defensa informática para practicar y generar nuevo software como antivirus.
- d) Ataca únicamente la defensa informática por motivos empresariales





DATOS DEL ASPIRANTE		FIRMA	
APELLIDOS:			7 0
Nombre:	DNI NIE o Pasaporte:	Fecha:	

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

37	Α	В	С	D
38	Α	В	С	D
39	Α	В	С	D
40	Α	В	С	D
41	Α	В	С	D
42	Α	В	С	D
43	Α	В	С	D
44	Α	В	С	D
45	Α	В	С	D
46	Α	В	С	D
47	Α	В	С	D
48	Α	В	С	D
49	Α	В	С	D
50	А	В	С	D