



DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	D.N.I. N.I.E.	Fecha:	

Pruebas para la obtención de títulos de Técnico y Técnico Superior

Convocatoria correspondiente al curso académico 2025-2026

Código del ciclo:	ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED
Clave o código del módulo:	SEGURIDAD Y ALTA DISPONIBILIDAD

INSTRUCCIONES GENERALES PARA LA REALIZACIÓN DE LA PRUEBA

- Material necesario: Bolígrafo azul o negro
- Duración: una hora y treinta minutos (1:30)
- Todos los aspirantes deben cumplimentar sus datos antes del examen y firmar en todas las hojas que se entreguen.
- Todos los aspirantes deben tener el **DNI encima la mesa y el móvil apagado**.
- **Las respuestas se deben indicar en las última hoja (RESPUESTA DE TEST)**
- Si se ha de rectificar una respuesta, tachar con una línea horizontal e indica al lado cual es el valor correcto. No utilizar líquido corrector (Tippex).
- Utilizar solamente el papel facilitado por el centro examinador.

CRITERIOS DE CALIFICACIÓN Y VALORACIÓN

- La prueba consta de 60 preguntas, las respuestas correctas se calificarán con un punto (1), las erróneas descontarán 0,33 (1/3) puntos,
- Para superar el examen se deberá obtener una calificación igual o superior a 30 puntos.
- La nota de la prueba se calculará dividiendo entre seis la total de puntos obtenidos.

Ejemplo: 30 puntos totales / 6 → Calificación 5

Respuestas Acertadas (1)	Respuestas erróneas (-0.33)	Puntos Totales	Calificación



DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	D.N.I. N.I.E.	Fecha:	

1. ¿Cómo se define una 'vulnerabilidad' en un sistema informático?

- A) Una debilidad que puede ser aprovechada para un ataque
- B) La probabilidad de que ocurra un desastre natural
- C) El daño causado tras un ataque exitoso
- D) Un programa diseñado para atacar el sistema

2. En el análisis de riesgos, ¿qué representa la 'probabilidad'?

- A) El coste económico de reponer los equipos
- B) La frecuencia con la que puede ocurrir una amenaza
- C) La cantidad de datos perdidos respecto al total
- D) La eficacia de los antivirus instalados frente al número de ataque

3. El principio de 'No repudio' garantiza que:

- A) Los datos no sean modificados por terceras personas
- B) El sistema esté siempre disponible ante peticiones
- C) Un emisor no pueda negar haber enviado un mensaje
- D) Solo las personas autorizadas lean la información

4. ¿En qué consiste un ataque de "día cero" (Zero-day attack)?

- A) Un ataque que se programa para ejecutarse exactamente a en un día concreto
- B) Un ataque que solo tiene éxito si se realiza en las primeras 24 horas desde la instalación del sistema operativo.
- C) Un ataque de denegación de servicio que dura menos de un día completo.
- D) Un ataque que aprovecha una vulnerabilidad para la cual aún no existe todavía un parche de seguridad.

5. En un análisis forense, ¿qué es la 'cadena de custodia'?

- A) El registro que garantiza que la evidencia no ha sido alterada
- B) Un tipo de cifrado para discos duros que se
- C) El proceso de identificación y detención de un delincuente
- D) La copia de seguridad de todos los registros de log

6. ¿Cuál es el primer paso en la metodología de gestión de riesgos?

- A) Implementar cortafuegos seguro
- B) Tener actualizados el sistema de antivirus
- C) Identificar los activos
- D) Contratar un seguro

7. ¿Qué figura es obligatoria en organismos públicos para supervisar el cumplimiento de la protección de datos?

- A) Administrador de sistemas
- B) Director de Seguridad
- C) Delegado de Protección de Datos
- D) Auditor externo

8. El derecho de 'Supresión' también es conocido comúnmente como:

- A) Derecho al olvido
- B) Derecho de acceso
- C) Derecho de rectificación
- D) Derecho a la portabilidad



DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	D.N.I. N.I.E.	Fecha:	

9. En el contexto de la LOPDGDD (Ley de protección de datos, ¿qué se considera un "dato de categoría especial"?

- A) El número de teléfono profesional
- B) La dirección de correo electrónico
- C) Datos sanitarios
- D) El nombre y apellidos del interesado

10. ¿Cuál es una característica fundamental de las funciones Hash?

- A) Son reversibles
- B) Son de un solo sentido (irreversibles)
- C) Requieren una clave pública
- D) Generan un resultado de longitud variable

11. ¿Qué algoritmo de cifrado simétrico es el estándar actual más utilizado?

- A) RSA
- B) DES
- C) AES
- D) Diffie-Hellman

12. La autenticación de doble factor (2FA) combina:

- A) Dos contraseñas diferentes
- B) Algo que sabes y algo que tienes
- C) Dos sistemas biométricos
- D) Nombre de usuario y contraseña

13. ¿Qué problema resuelve el algoritmo de Diffie-Hellman?

- A) El almacenamiento seguro de logs
- B) El intercambio seguro de claves sobre un canal inseguro
- C) La detección de virus en archivos comprimidos
- D) La velocidad de los discos SSD

14. ¿Qué técnica se utiliza en los CPD para optimizar la refrigeración de los servidores?

- A) Humidificación extrema
- B) Pasillos fríos y pasillos calientes
- C) Ventiladores de techo industriales
- D) Apagar los equipos por la noche

15. ¿Qué tipo de malware se caracteriza por ocultar su presencia y la de otros procesos al sistema operativo?

- A) Gusano
- B) Spyware
- C) Adware
- D) Rootkit

16. La función 'Secure Boot' en sistemas UEFI sirve para:

- A) Aumentar la velocidad de arranque cuando hay varios sistemas
- B) Asegurar que solo se cargue software firmado por el fabricante
- C) Evitar que el usuario cambie la contraseña de la BIOS
- D) Restaurar un backup automático del sistema en caso de fallo

17. ¿Para qué se utiliza un 'Honeypot'?

- A) Para detectar virus que intenten cambiar la configuración
- B) Para controlar el acceso a bases de datos
- C) Como servidor de archivos principal
- D) Como señuelo para detectar ataques



DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	D.N.I. N.I.E.	Fecha:	

18. ¿Qué herramienta se especializa en el análisis de vulnerabilidades y escaneo de puertos?

- A) Nmap
- B) Wireshark
- C) Putty
- D) VLC

19. ¿Qué es un 'exploit'?

- A) Un tipo de cortafuegos hardware
- B) Una técnica que aprovecha una vulnerabilidad específica
- C) Una copia de seguridad incremental completa
- D) Un usuario no autorizado que consigue escalar de privilegios

20. ¿Qué puerto utiliza habitualmente el protocolo SSH?

- A) 21
- B) 22
- C) 443
- D) 80

21. ¿Qué nivel de RAID ofrece tolerancia a fallos mediante la división de datos y doble paridad, permitiendo el fallo de hasta 2 discos?

- A) RAID 0
- B) RAID 1
- C) RAID 5
- D) RAID 6

22. En una copia de seguridad 'Diferencial':

- A) Se copian todos los datos del sistema cada vez
- B) Se copian los datos modificados desde la última copia total
- C) Se copian los datos modificados desde la última copia diferencial
- D) Se borran los datos modificados desde la última copia incremental

23. ¿Qué tecnología permite conectar servidores a cabinas de almacenamiento mediante una red de alta velocidad, normalmente de fibra?

- A) NFS
- B) SAN
- C) DAS
- D) SMB

24. Un 'Snapshot' de una máquina virtual se utiliza para:

- A) Sustituir a la copia de seguridad total
- B) Volver rápidamente a un estado anterior tras un cambio fallido
- C) Aumentar la capacidad del disco duro
- D) Encriptar el tráfico de red

25. RAID 10 es una combinación de:

- A) Espejo (Mirror) y División (Striping)
- B) División y Paridad
- C) Dos sistemas RAID 5
- D) Un disco de datos y uno de paridad

26. ¿Qué zona de la red se utiliza para ubicar servidores que deben ser accesibles desde Internet?

- A) LAN interna
- B) DMZ
- C) Red de gestión
- D) Intranet



DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	D.N.I. N.I.E.	Fecha:	

27. ¿Qué tipo de ataque DoS inunda al objetivo con paquetes de inicio de conexión TCP llegar a establecerla totalmente?

- A) ICMP Flood
B) UDP Flood
C) Smurf Attack
D) SYN Flood

28. ¿Qué puerto utiliza el protocolo HTTPS?

- A) 443
B) 80
C) 8080
D) 2525

29. ¿Qué tipo de Proxy permite filtrar el tráfico web sin necesidad de configurar nada en el navegador del cliente?

- A) Proxy Inverso
B) Proxy Transparente
C) Proxy de Aplicación
D) Proxy SOCKS

30. Un Proxy Inverso se utiliza habitualmente para:

- A) Proteger y balancear la carga de los servidores web internos
B) Ocultar la identidad de los clientes que navegan por internet
C) Acelerar la descarga desde redes inversas
D) Evitar que los usuarios usen clientes web anónimos

31. ¿Qué servicio proporciona autenticación centralizada, autorización y contabilidad (AAA)?

- A) DNS
B) WHOIS
C) RADIUS
D) DHCP

32. En un cluster 'Activo-Pasivo', el nodo pasivo:

- A) También procesa peticiones simultáneamente
B) Solo se usa para hacer backups
C) Permanece en espera hasta que el nodo activo falla
D) Está apagado físicamente a la espera del arranque remoto

33. En alta disponibilidad, ¿qué es un 'SPOF' (Single Point of Failure)?

- A) Un servidor que realiza las tareas más relevantes
B) Un componente cuyo fallo provoca la caída de todo el sistema
C) Un servidor de discos con un sector dañado.
D) Un protocolo de enrutamiento capaz de definir rutas alternativas

34. ¿En qué tabla de iptables se deben configurar las reglas destinadas a permitir o denegar el paso de paquetes (filtrado) por defecto?

- A) nat
B) mangle
C) filter
D) raw

35. ¿Qué diferencia fundamental existe entre un IDS y un IPS?

- A) El IDS es dispositivo hardware y el IPS una aplicación software
B) El IDS solo funciona en redes locales y el IPS en redes externas
C) El IDS protege contra virus y el IPS contra ataques de red y spam
D) El IDS solo alerta, mientras que el IPS toma medidas frene el ataque



DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	D.N.I. N.I.E.	Fecha:	

36. ¿Qué tipo de malware se caracteriza por cifrar los archivos del usuario y exigir un pago para recuperarlos?

- A) Adware
B) Spyware
C) Ransomware
D) Rootkit

37. En la redes WIFI. ¿qué sistemas de cifrado es más seguro?

- A) WEP
B) WPA3- PSK
C) WPA3- Radius
D) WIFI-Sec

38. ¿Cuál es la función principal de una técnica de "hashing" en seguridad?

- A) Cifrar archivos para que nadie los lea
B) Garantizar la integridad de los datos detectando alteraciones
C) Comprimir el tamaño de los archivos para el envío por red
D) Generar claves públicas a partir de claves privadas

39. ¿Cuál es el objetivo principal de realizar un análisis forense digital tras un incidente?

- A) Borrar los rastros del atacante para que el evento no vuelva a repetir
B) Actualizar el sistema antivirus y el contrafirewalls en todos los equipos de la red
C) Detectar y sancionar a los usuarios responsables del fallo del sistema
D) Identificar, preservar y analizar evidencias digitales para determinar lo ocurrido

40. ¿En qué consiste el ataque conocido como "Man-in-the-Middle"?

- A) Un ataque de fuerza bruta para adivinar una contraseña cifrada
B) Un ataque intercepta y puede llegar altera la comunicación entre dos partes
C) El envío masivo de correos electrónicos basura entre los sistemas abiertos
D) La suplantación de la identidad de un servidor de correo para enviar spam

41. ¿Cuál es uno de los principales inconveniente del cifrado simétrico?

- A) Suele ser más lento comparado con el cifrado asimétrico
B) La dificultad de distribuir la clave secreta de forma segura
C) No permite cifrar archivos de gran tamaño de un forma segura
D) No se puede usar en sistemas operativos Windows o Mac

42. ¿Qué protocolo se utiliza en el nivel de red para crear túneles VPN seguros e interoperables entre dos redes privada independientes?

- A) SSH
B) IPsec
C) HTTPS
D) TSL

43. ¿Qué tipo de ataque de inyección busca obtener datos o manipular una base de datos mediante formularios web?

- A) XSS (Cross Site Scripting)
B) Buffer Overflow
C) SQL Injection
D) OS Command Injection



DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	D.N.I. N.I.E.	Fecha:	

44. ¿Qué técnica criptográfica se utiliza para asegurar que un mensaje no ha sido modificado durante su envío?

- A) Encriptación
B) Firma Digital
C) Fragmentación
D) Encapsulación

45. En el contexto de valoración de riesgos, ¿qué se entiende por "impacto"?

- A) Número de vulnerabilidades existentes
B Consecuencias de un incidente
C) Probabilidad de ocurrencia
D) Coste de las copias de seguridad

46. ¿Qué elemento NO forma parte de un plan de seguridad física?

- A) Control de accesos
B) Configuración de Firewall de red
C) Protección contra incendios
D) Ubicación de servidores

47. En una infraestructura de clave pública PKI, ¿cuál es la función principal de una Autoridad de Certificación (CA)?

- A) Generar claves simétricas seguras
B) Emitir y revocar certificados digitales
C) Comprobar la validez de los certificados digitales.
D) Encriptar archivos de forma segura

48. ¿Cuáles son los cuatro tipos de amenazas en seguridad informática?

- A) Interrupción, interceptación, duplicación y fabricación
B) Diseño, fabricación, distribución y comercialización.
C) Interrupción, Interceptación, fabricación y modificación
C) Modificación, Interrupción, fabricación y denegación

49 ¿Qué tipo de ataque aprovecha vulnerabilidades en inserción de código javascript en páginas web para ejecutar código malicioso en el navegador del usuario?

- A) SQL Injection
B) Cross-Site Scripting (XSS)
C) Man-in-the-Middle
D) DoS

50. ¿Cuál de las siguientes opciones es una amenaza física para un sistema informático?

- A) Un virus informático.
B) Una inundación
C) Un ataque de denegación de servicio (DoS).
D) Un ataque de phishing.

51. Si quiero enviar un mensaje a un destinatario que incluya mi firma digital del mensaje, ¿qué clave utilizamos para crearla?

- A) Mi clave privada.
B) La clave privada del destinatario
C) La clave pública del destinatario
D) Una clave elegida al azar compleja

52. Un emisor me ha enviado un mensaje cifrado utilizando mi clave pública que previamente le indiqué, ¿con qué clave descifraré el mensaje que me ha enviado?

- A) Con mi clave pública
B) Con la clave pública del emisor
C) Con mi clave privada.
D) Con la clave privada del emisor



DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	D.N.I. N.I.E.	Fecha:	

53. ¿Qué tecnología crea una conexión segura y cifrada a través de una red pública como Internet?

- a) NAT
b) IDS
c) VPN
d) QoS

54. ¿Qué efecto tiene esta regla?:

`iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT`

- A) Bloquea todas las conexiones nuevas que no se haya establecido
B) Permite solo conexiones iniciadas desde el exterior
C) Permite el tráfico de conexiones ya establecidas o relacionadas
D) Cierra todos los puertos no usados por servicios inseguros

55. Si queremos permitir que desde el exterior se puedan conectar a un servidor web interno con IP 10.0.0.200 ¿Qué regla incluiremos en nuestro cortafuegos de red?

- A) `iptables -A FORWARD -d 10.0.0.200 -p tcp --dport 80 -j ACCEPT`
B) `iptables -A FORWARD -s 10.0.0.200 -p tcp --dport 80 -j ACCEPT`
C) `iptables -A OUTPUT -s html -ip 10.0.0.200 -j ACCEPT`
D) `iptables -A INPUT -o 10.0.0.200 -d 80:8080 -j ACCEPT`

56. ¿Qué tecnología de virtualización permite ejecutar aplicaciones aisladas en el espacio de usuario de un sistema operativo anfitrión, compartiendo el mismo kernel?

- A) Virtualización completa
B) Paravirtualización
C) Virtualización mediante contenedores
D) Virtualización de hardware asistida.

57. Según la LOPDGDD, ¿cuál es la edad mínima para que un menor pueda dar su consentimiento para el tratamiento de sus datos personales en el ámbito de los servicios de la sociedad de la información?

- A) 12 años.
B) 14 años.
C) 16 años.
D) 18 años.

58. ¿Cuál es la norma ISO que trata sobre la seguridad informática?:

- A) ISO 140001
B) ASO 803.2
C) ISO 27001
D) ISO 9000.

59. ¿Cuál de los siguientes servicios no es un proveedor de servicios de computación en la nube?

- A) Microsoft Azure
B) Amazon WS
C) Oracle VM Virtualbox
D) Google Cloud

60. ¿Cual es el sistema más habitual de manejo de contenedores?

- A) Dockers
B) Emulación hardware
C) Virtual Machine Enterprise
D) Hot virtualización



DATOS DEL ASPIRANTE			FIRMA
APELLIDOS:			
Nombre:	D.N.I. N.I.E.	Fecha:	

HOJA DE RESPUESTAS (Sólo se calificarán las respuestas indicadas en esta hoja)

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

Página 5	Pregunta	Respuesta
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
Página 6	Pregunta	Respuesta
	44	
	45	
	46	
	47	
	48	
	49	
	50	
	51	
	52	
Página 7	Pregunta	Respuesta
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	