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 2021-2022

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 azúl 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 de 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 ¿Cuáles son tres principales objetivos en seguridad informática?
a) Conectividad, Privacidad y Encriptación
b) Conectividad, Integridad y Excentricidad
c) Confidencialidad, Disponibilidad y Regularidad
d) Confidencialidad, Integridad y Disponibilidad

2 Un ataque que provoca un DoS (Denegación de servicio) afecta ¿a qué objetivo básico en seguridad?.
a) No repudio
b) Integridad
c) Confidencialidad
d) Disponibilidad

3 ¿Cuáles de las siguientes afirmaciones no es un objetivo planteado por la seguridad lógica de un sistema?
a) Restringir el acceso a los programas y archivos.
b) Garantizar que los datos enviados a un destinatario solo puedan ser interpretados por el auténtico destinatario y no por otros.
c) La información emitida por el emisor debe ser idéntica a la recibida por el receptor.
d) Impedir el acceso a la instalación mediante técnicas biométricas.

4 ¿Cuál de las siguientes vulnerabilidades queda reflejada en el nivel de enlace de la capa OSI?
a) Ataque sobre las líneas de cableado
b) Escucha de tramas con un sniffer
c) Suplantación de una dirección IP
d) Publicación de puertos sobre los que se ofrecen servicios

5 ¿Cuál es la mejor estrategia para evitar los ataques basados en la ingeniería social?
a) La encriptación de los datos más importantes
b) La formación de los usuarios del sistema
c) El uso de cortafuegos y sistemas IDS
d) El cambio frecuente de contraseña de los usuarios

6 Sobre políticas de contraseñas ¿qué medida ES aconsejable?
a) Definir contraseñas de menos de 6 caracteres
b) Definir contraseñas difíciles de memorizar
c) Definir una única contraseña segura para varios usos
d) Cambiar las contraseñas periódicamente

7 ¿Qué sistema biométrico se considera el más seguro?
a) Reconocimiento de la cara
b) Reconocimiento del iris
c) Reconocimiento de la huella dactilar
d) Reconocimiento del olor corporal

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

8 ¿Cuál de los siguientes métodos criptográficos se puede clasificar como de transposición?
a) Escílata
b) Vigenère
c) Polybios
d) Cesar

9 ¿Cuál es uno de los problemas de la criptográfica simétrica?
a) El tamaño reducido de las claves
b) La lentitud en el cifrado y descifrado.
c) La distribución de la claves
d) La dificultad en memorizar las claves

10 Para realizar la firma digital, ¿cuáles son los algoritmos de hash más utilizados?
a) Checksum, y AdmSig
b) RSA y DES.
c) HSEC y RunRun
d) MD5 y SHA

11 ¿Cuál es el orden cronológico correcto de las fases de un análisis forense digital?
a) Documentación del incidente, Análisis de la evidencia, Preservación de la incidencia, Identificación del incidente.
b) Identificación del incidente, Análisis de la evidencia, Preservación de la incidencia, Documentación del incidente
c) Identificación del incidente, Preservación de la incidencia, Análisis de la evidencia, Documentación del incidente
d) Preservación de la incidencia, Identificación del incidente, Análisis de la evidencia, Documentación del incidente

12 ¿Cuáles son los cuatro tipos de amenazas en seguridad informática?
a) Interrupción, intercepción, duplicación y fabricación
b) Diseño, fabricación, distribución y comercialización.
c) Interrupción, Intercepción, fabricación y modificación
d) Modificación, Interrupción, fabricación y denegación

13 ¿Para qué sirve la instalación de un honeypot en una red?
a) Para la detección temprana de intrusos o hacker
b) Para evitar la descarga de virus o troyanos
c) Para ofrecer un servicio de alta disponibilidad
d) Para evitar ataques DoS (Denegación de Servicio)

14 ¿Cómo podemos protegernos del ARP spoofing?
a) Definiendo reglas adecuadas en el cortafuegos
b) Asignado de forma estática las direcciones MAC
c) Bloqueando el protocolo ICMP
d) Cambiando la IP mediante la orden ipconfig -hardware addr

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

15 Los rootkits se caracterizan por:
a) Auto-enviarse por correo electrónico
b) Implementar técnicas para permanecer ocultos
c) Infectar a otros ejecutables
d) Presentar publicidad no deseada

16 ¿Cuáles de estas medidas o salvaguardias NO forman parte de la seguridad activa?
a) Cortafuegos
b) Discos espejos
c) Encriptación de datos
d) Uso de contraseñas seguras

17 ¿Para qué se puede utilizar la herramienta nmap?
a) Para explorar los servicios o puertos abiertos
b) Para detectar posibles bombas lógica en el sistema
c) Para cerrar o abrir puertos de comunicaciones TCP o UDP
d) Para ver la posición geográfica de una dirección IP

18 Si quiero enviar un mensaje a un destinatario que incluya mi firma digital del mensaje, ¿qué clave utilizamos para crearla?
a) La clave pública del destinatario
b) La clave privada del destinatario
c) Una clave elegida al azar compleja
d) Mi clave privada.

19 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 mi clave privada.
c) Con la clave pública del emisor
d) Con la clave privada del emisor

20 ¿Cuál de los siguientes mecanismos de seguridad de redes Wi-Fi está desaconsejado?
a) Filtrado por dirección MAC
b) Reducir la intensidad y alcance de la señal
c) Ocultación del nombre de la red Wi-Fi
d) Sistema de detección de intrusos inalámbrico (WIDS)

21 ¿Qué tipo de dispositivo convierte a un host apantallado en una subred apantallada?
a) Un router de frontera.
b) Un router situado entre la red perimetral y la red externa.
c) Un router situado entre dos segmentos de la red interna.
d) Un router situado entre la red perimetral y la red interna.

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

22 Un hacker ha penetrado en una red tomando el control de uno de los bastiones de la misma. Desde allí iniciará su actividad de búsqueda y ataque de nuevos objetivos en la red interna. ¿Qué dispositivos habría que configurar en la red interna y qué actividades habría que iniciar para averiguar las intenciones del atacante?

a) Instalar una UTM que gestione el riesgo.
b) Configurar el cortafuegos para impedir las conexiones desde el exterior.
c) Instalar un honey-pot.
d) Modificar las rutas del router de frontera para desviar el ataque.

23 ¿Cuál de las siguientes afirmaciones sobre segmento DMZ de aplicación ES CIERTA?

a) Se instalan en esta zona los equipos menos seguros de la red local
b) Se instalan en esta zona los equipos que ofrecen servicios a Internet
c) Se instalan en esta zona los equipos con menores velocidades
d) Se instalan en esta zona los equipos dinámicos de la red

24 ¿Qué característica técnica se asocia al modo túnel IPsec?

a) El cifrado se realiza de extremo a extremo
b) El datagrama IP no es encapsulado completamente
c) El cifrado se realiza entre los dos routers/firewalls entre sedes, pero no de extremo a extremo
d) Solo encapsula los datos del datagrama IP conservando la cabecera IP original del datagrama

25 De las siguientes afirmaciones relativas a las tecnologías PPP y PPTP, ¿cuál ES FALSA?

a) Se encapsula una PDU PPP dentro de un datagrama IP.
b) PPP puede encapsular segmentos TCP o UDP.
c) Se encapsula un datagrama IP dentro de una PDU PPP.
d) PPTP requiere una cabecera de protocolo GRE para confeccionar sus túneles.

26 ¿Cuál de los siguientes protocolos NO se utiliza en para implementar una VPN?

a) IPsec
b) SSL
c) L2TP
d) SMTP

27 En los túneles IP intervienen varias direcciones IP tanto en origen como en destino. Según esto, ¿cuáles de las siguientes afirmaciones ES FALSA?

a) En un túnel entre sedes solo se cifra entre los dos servidores VPN.

b) En un túnel entre sedes intervienen exclusivamente las dos IP públicas de los servidores VPN.

c) En un túnel Road-warrior se cifra desde el cliente hasta el servidor VPN de destino, pero no hasta el cliente de destino final.

d) En un túnel Road-warrior interviene la IP del cliente y la IP del servidor VPN exclusivamente.

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

28 ¿Qué afirmaciones siguientes relativas al encapsulamiento en túnel ES FALSA?
a) Un túnel válido a través de Internet podría construirse encapsulando IP dentro de NetBIOS.
b) Un túnel válido a través de Internet podría construirse encapsulando NetBIOS dentro de IP.
c) Cualquier túnel evita un ataque Man-In-The-Middle.
d) Los túneles se utilizan en conexiones punto a punto cifradas.

29 Un router/firewall publica en su red externa una batería de servidores web localizados en la red interna. ¿Cuál de las siguientes informaciones puede ser VERDADERA?
a) El router abre un único puerto (el 80) en la red externa, que conectará a cada servidor web.
b) El router debe abrir un puerto distinto por cada servidor web interno.
c) El router debe abrir un puerto distinto por cada cliente en la red externa que se conecte a cualquier servidor web.
d) El router abre un puerto por cada servidor web publicado y otro por cada cliente conectado

30 ¿Qué característica no es apropiada para un servidor RADIUS?
a) RADIUS es un servidor extensible y, por tanto, no cerrado.
b) La autenticación RADIUS utiliza el puerto TCP-1813.
c) Gestiona la autenticación y autorización de usuarios y servicios.
d) Utiliza el puerto UDP-1812.

31 ¿Cuál de las siguientes afirmaciones sobre cortafuegos de red ES ERRÓNEA?
a) Permite analizar los mensajes para detectar virus o troyanos
b) Define reglas en funciones de la cabecera del paquete IP
c) Filtra tanto paquetes de entrada como de salida de la red
d) Controla el acceso a determinados puertos y protocolos

32 ¿Cuáles de las siguientes características son específicas de un Web Application Firewall?
a) Filtra por direcciones IP.
b) Filtra por puertos.
c) Filtra por direcciones MAC.
d) Protege de ataques de inyección de código.

33 ¿Qué característica tecnológica es falsa para el caso del cortafuegos personal de Windows?
a) Permite el control de puertos e IP de origen de los paquetes entrantes.
b) Permite el control de IP de origen en los paquetes salientes.
c) Puede seleccionar las aplicaciones instaladas que accederán a la red externa.
d) Permite restringir el acceso por tipo de protocolo en cualquiera de las direcciones.

34 ¿Qué tipo de cortafuegos opera en el nivel de red de la arquitectura TCP/IP?
a) Red privada virtual común
b) Cortafuegos basado en proxy
c) Cortafuegos con inspección de estado
d) Cortafuegos de filtrado de paquetes

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

35 En una instalación se desea que los usuarios internos puedan navegar libremente por Internet y se abren en el cortafuegos corporativo las salidas hacia el puerto 80 mediante TCP para conexiones HTTP, así como el puerto TCP-443 para conexiones HTTPS. ¿Cómo NO podría conseguirse esto?
a) Filtrado dinámico de conexiones de navegación.
b) Filtrado con inspección de estado con reglas de navegación.
c) Filtrado estático de paquetes de salida únicamente.
d) Filtrado estático de paquetes de salida y de entrada relacionados.

36 Si queremos BLOQUEAR la entrada a todos los paquetes en nuestro equipo, ejecutaríamos:
a) iptables -A INPUT -j DROP
b) iptables -j INPUT -A DROP
c) iptables -A INPUT -j ACCEPT
d) iptables -A OUTPUT -j DROP

37 Si queremos permitir la conexión por ssh desde la IP 80.32.23.78 a nuestro equipo ¿qué regla debemos introducir?
a) iptables -A FORWARD -p udp -d 80.32.23.78 --sport 80 -j ACCEPT
b) iptables -A INPUT -s 80.32.23.78 -p tcp --dport 22 -j ACCEPT
c) iptables -A OUTPUT -s ssh -ip 80.32.23.78 -ja -ja ACCEPT
d) iptables -A INPUT -d 80.32.23.78 -p tcp --dport 20:21 -j ACCEPT

38 Si queremos permitir que desde el exterior se puedan conectar a un servidor web interno con IP 192.168.100.100 ¿Qué regla incluiremos en nuestro cortafuegos de red?
a) iptables -A FORWARD -d 192.168.100.100 -p tcp --dport 80 -j ACCEPT
b) iptables -A FORWARD -s 192.168.100.100 -p tcp --dport 80 -j ACCEPT
c) iptables -A OUTPUT -s html -ip 192.168.100.100 -j ACCEPT
d) iptables -A INPUT -o 192.168.100.100 -d 80:8080 -j ACCEPT

39 ¿Cuántas y cuáles son las conexiones que se realizan en un cortafuegos basado en proxy en el nivel de aplicación?
a) Una conexión: proxy-servidor.
b) Dos conexiones: cliente-proxy y proxy-servidor.
c) Dos conexiones: cliente-servidor y cliente-proxy.
d) Dos conexiones: cliente-proxy y proxy-cliente.

40 Un sistema tiene configurado iptables correctamente, sin embargo, los paquetes no son capaces de enrutarse desde un interfaz de red a otro. ¿Qué debe hacer el administrador del sistema?
a) Crear una ruta entre los dos interfaces de red.
b) Instalar netfilter.
c) Cambiar las reglas a la tabla FORWARD.
d) Editar el fichero */etc/sysctl.conf* y añadir el parámetro *net.ipv4.ip_forward=1*

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

41 ¿Qué característica de las siguientes se corresponde con un proxy anónimo?
a Se oculta su IP como servidor proxy y oculta la IP del cliente
b) Se identifica a sí mismo como proxy y falsea la IP del cliente
c) Se identifica a sí mismo como proxy y no oculta la IP del cliente
d) Se identifica a sí mismo como proxy, pero oculta la IP del cliente

42 ¿Cuáles de las siguientes afirmaciones sobre la arquitectura y ubicación de un servidor proxy es correcta?
a) Un proxy web puede tener un único adaptador de red.
b) Un servidor proxy tiene al menos dos adaptadores de red.
c) Un servidor proxy siempre realiza dos conexiones: una interna y otra externa.
d) Un proxy debe situarse siempre en el perímetro de la red.

43 ¿Para qué utiliza el protocolo ICP (Internet Caché Protocol) un proxy?
a) Para controlar la hora de acceso de las páginas web
b) Para comprimir la información a almacenar en la caché
c) Para enviar caché-test a los usuarios no autorizados
d) Para comunicarse con otros proxy padres o hermanos

44 Un administrador desea instalar un sistema de filtrado de contenidos con autenticación de usuarios utilizando software libre como Squid y DansGuardian. ¿Qué configuración debe diseñar para conseguir su objetivo?
a) Cliente-Squid-DansGuardian-Servidor.
b) Cliente-DansGuardian-Squid-DansGuardian-Servidor.
c) Cliente-Dan sGuardian-S quid-Servidor.
d) Cliente-Squid-DansGuardian-Squid-Servidor.

45 ¿Cuáles de las siguientes afirmaciones relativas a los proxies transparentes es FALSA?
a) Actúan como puerta por defecto del servicio al que sirven.
b) En el cliente hay que configurar el puerto de escucha del proxy.
c) Presentan problemas con la autenticación de los usuarios.
d) La petición se envía al proxy mediante una ruta creada en el cliente.

46 ¿Cuáles son los valores de la cabecera HTTP más relevantes para un proxy?
a) Server y Date
b) Content-type y Date
c) Expires y Last-Modified
d) html y body

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

47 ¿Con qué instrucciones impediríamos el acceso al portal chuletas.es mediante squid?
a) acl portal01 dstdomain chuletas.es
http_access deny portal01
b) acl chuletas deny portal01 domain
http_access drop chuletas
c) acl chuletas.es deny all domains
http_no_access to chuletas
d) acl portal01 srcdomain chuletas.es
http_access allow portal01

48 ¿Que implicarían las instrucciones?
acl cosa1 time 08:00-14:00
acl cosa2 urlpath_regex \.zip$;
http_access allow cosa1 !cosa2
a) Impide el acceso de ocho a dos, salvo si descargamos zip
b) Impide el acceso de ocho a dos, para descargar zip
c) Permite el acceso de ocho a dos, pero no descargar zip
d) Permite el acceso de ocho a dos, y la descarga de zip

49 La instalación de una red dispone de un servidor web interno (intranet) en la dirección 192.168.1.5 y de equipos que tienen configurado un DNS interno en la dirección 192.168.1.1. Este servidor DNS interno dirige las peticiones que no es capaz de resolver hacia otro DNS en Internet, en concreto al DNS de Google: 8.8.8.8. Se configura un servidor proxy Squid en la dirección 192.168.1.2 que tiene, entre otras, las siguientes directivas en su fichero de configuración:

http port 3128
visible_hostname proxy.miempresa.com
dns nameservers 8.8.8.8 192.168.1.1
cache_mgr proxy@miempresa.com
cache_mem 32 MB

Desde alguno de los clientes se hace una petición web desde un navegador que apunta su proxy a Squid por el puerto 3128 y navega perfectamente. Sin embargo, no puede navegar por las páginas del servidor web de la intranet. ¿Qué podemos hacer para solucionar el problema?
a) añadir una nueva directiva *dns_nameservers*.
b) Añadir una excepción al navegador para el servidor de intranet.
c) Instalar un proxy para la red interna y otro para la red externa.
d) Cambiar el DNS del sistema cliente para que apunte a 8.8.8.8.

50 Un sistema de alta disponibilidad tolerante a fallos por replicación:
a) Tiene varias instancias idénticas del servicio y las peticiones se hacen a todas ellas en paralelo
b) Tiene varias instancias idénticas del servicio y las peticiones se hacen sólo a uno de ellos
c) Tiene varias instancias idénticas del servicio y las peticiones se hacen indistintamente a uno de ellos
d) Tiene varias instancias idénticas del servicio y las peticiones se hacen por orden cada vez a uno de ellos

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

51 Un modelo de virtualización de escritorio ¿con qué característica tecnológica de las siguientes se corresponde?
a) Abstrae un recurso individual, pero nunca un sistema completo
b) Abstrae el perfil de un usuario
c) Encapsula una utilidad
d) Abstrae un sistema completo

52 ¿Qué técnica de virtualización utiliza una traducción binaria por software para simular plataformas completas para conseguir su objetivo?
a) Virtualización nativa
b) Virtualización a nivel de sistema operativo
c) Para-virtualización
d) Virtualización completa AxH

53 ¿Qué escenario técnico de los que se describen a continuación es el menos propio para ser gestionado mediante balanceo de carga?
a) Un firewall se replica sobre otro, pero cada uno es atendido por seguridad por un proveedor de Internet distinto.
b) Una granja de servidores proporciona comercio electrónico a una tienda virtual visitada por abundantes potenciales compradores.
c) Un firewall es replicado en otro para atender las peticiones de los usuarios como reparto de carga, siendo que cada firewall utiliza como salida un proveedor de Internet distinto.
d) Un servidor de correo electrónico no es capaz de soportar tantos buzones como se requiren y se crea un cluster para aliviarle.

54 En sistemas Windows un volumen reflejado corresponde a qué nivel RAID.
a) RAID 0
b) RAID 6
c) RAID 1
d) RAID 5

55 ¿Cuáles de estas características NO supone una ventaja en los sistemas cluster?
a) Alta disponibilidad
b) Fácil backup
c) Fácil Escalabilidad.
d) Alto rendimiento

56 La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española, el cual dice textualmente:
a) La ley limitará el uso de la información para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
b) La ley limitará el uso de la informática para garantizar el honor y la privacidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
c) La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
d) La ley limitará el uso de la información para garantizar el honor y la privacidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

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

57 ¿Que plataforma podemos utilizar para gestionar y automatizar el manejo de contenedores docker?
a) Vmware workstation
b) VirtualBox
c) Kubernetes
d) Oracle docker file

58 La Ley Orgánica de protección de datos (LOPD) afecta a ficheros en soporte:
a) Solo Electrónico.
b) Cualquier soporte.
c) Papel.
d) De audio.

59 ¿Cuál es la norma ISO que trata sobre la seguridad informática?:
a) ISO 140001
b) IEEE 803.2
c) ISO 27002
d) ISO 9000.

60 ¿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