

Anexo 2

Pruebas para la obtención de títulos de Técnico y Técnico Superior

Convocatoria correspondiente al curso académico 2025-2026

(Resolución de 12 de diciembre de 2025 de la Dirección General de Educación Secundaria, Formación Profesional y Régimen Especial)

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

Código del ciclo:	Denominación completa del título:
IFCS03	Técnico Superior en Desarrollo de Aplicaciones Web
Clave o código del módulo:	Denominación completa del módulo profesional:
09	Despliegue Aplicaciones Web

INSTRUCCIONES GENERALES PARA LA REALIZACIÓN DE LA PRUEBA
- El examen tendrá una duración de 1h y 30m. - La prueba consta de un examen tipo test con cuatro opciones de las cuales solamente una es correcta. - Cada pregunta se responderá en el espacio dejado al efecto, en la hoja de respuestas, la hoja 2. Se usarán X en los recuadros para señalar la respuesta seleccionada. - Si se quiere rectificar una respuesta contestada, se rellenará toda la casilla de la respuesta incorrecta, tal y como se puede apreciar aquí: a ☐ b ☒ c ☐ d ☒ - Se dispondrá de una hoja para borrador (o de varias si se requieren), que será proporcionada por el centro. Esa hoja se entregará obligatoriamente al final junto con el examen, si bien nada de lo escrito en la hoja de borrador se valorará en la corrección. - Sólo se utilizará bolígrafo negro o azul, no permitiéndose usar bolígrafo rojo, lapicero, Tipp-Ex, etc. - Por supuesto, tampoco se podrá emplear ningún dispositivo electrónico. - Cualquier tachadura o borrón en una respuesta podrá invalidar toda la puntuación de esta.

CRITERIOS DE CALIFICACIÓN Y VALORACIÓN
- El test se calificará sobre 10 puntos. Todas las preguntas se calificarán equitativamente con la misma cantidad de puntos. En cada pregunta se plantearán varias respuestas, y se deberá señalar la única que se considere correcta, según el caso. Cada respuesta correcta que se marque se valorará con 0,25 puntos, y si se marca alguna incorrecta, se valorará con una cantidad negativa equivalente a 1/3 de cada respuesta correcta. Es decir, se descontarán 0,08 puntos. Si no se está seguro de si una respuesta es correcta o no, y no se marca, no sumará ni restará puntos. - Calificación final del módulo profesional: - El alumno obtendrá en el módulo profesional una calificación entera entre 1 y 10. Dicha calificación se calculará redondeando la conseguida en la prueba. Si los decimales son inferiores a 0,5 la calificación se redondeará al entero más bajo; si son superiores o iguales a 0,5 al entero más alto. Esta regla tiene una excepción: las notas de examen inferiores a 1 se redondearán a 1.

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

CALIFICACIÓN

RESPUESTAS TEST

1 a ☐ b ☐ c ☐ d ☐	11 a ☐ b ☐ c ☐ d ☐	21 a ☐ b ☐ c ☐ d ☐	31 a ☐ b ☐ c ☐ d ☐
2 a ☐ b ☐ c ☐ d ☐	12 a ☐ b ☐ c ☐ d ☐	22 a ☐ b ☐ c ☐ d ☐	32 a ☐ b ☐ c ☐ d ☐
3 a ☐ b ☐ c ☐ d ☐	13 a ☐ b ☐ c ☐ d ☐	23 a ☐ b ☐ c ☐ d ☐	33 a ☐ b ☐ c ☐ d ☐
4 a ☐ b ☐ c ☐ d ☐	14 a ☐ b ☐ c ☐ d ☐	24 a ☐ b ☐ c ☐ d ☐	34 a ☐ b ☐ c ☐ d ☐
5 a ☐ b ☐ c ☐ d ☐	15 a ☐ b ☐ c ☐ d ☐	25 a ☐ b ☐ c ☐ d ☐	35 a ☐ b ☐ c ☐ d ☐
6 a ☐ b ☐ c ☐ d ☐	16 a ☐ b ☐ c ☐ d ☐	26 a ☐ b ☐ c ☐ d ☐	36 a ☐ b ☐ c ☐ d ☐
7 a ☐ b ☐ c ☐ d ☐	17 a ☐ b ☐ c ☐ d ☐	27 a ☐ b ☐ c ☐ d ☐	37 a ☐ b ☐ c ☐ d ☐
8 a ☐ b ☐ c ☐ d ☐	18 a ☐ b ☐ c ☐ d ☐	28 a ☐ b ☐ c ☐ d ☐	38 a ☐ b ☐ c ☐ d ☐
9 a ☐ b ☐ c ☐ d ☐	19 a ☐ b ☐ c ☐ d ☐	29 a ☐ b ☐ c ☐ d ☐	39 a ☐ b ☐ c ☐ d ☐
10 a ☐ b ☐ c ☐ d ☐	20 a ☐ b ☐ c ☐ d ☐	30 a ☐ b ☐ c ☐ d ☐	40 a ☐ b ☐ c ☐ d ☐

Correctas _____ Incorrectas _____ No Puntuadas/Sin Contestar _____

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

CONTENIDO DE LA PRUEBA:

- 1.- ¿Qué componente de Apache Tomcat se encarga de transformar los archivos JSP en código Java ejecutable (Servlets)?
 - a) Catalina
 - b) Jasper
 - c) Coyote
 - d) Apache
- 2.- ¿Qué es un "server block" en Nginx?
 - a) Una sección del archivo de configuración de Nginx que define el comportamiento para un grupo de servidores.
 - b) Una directiva que define el nombre del servidor web.
 - c) Un archivo de configuración que define el comportamiento del servidor web para un solo sitio web.
 - d) Un tipo de proxy que se utiliza para la seguridad web.
- 3.- ¿Cuál de las siguientes afirmaciones sobre el protocolo HTTP/2 es FALSA?
 - a) Requiere el uso de TLS para establecer una conexión segura.
 - b) Utiliza una única conexión TCP para realizar múltiples peticiones.
 - c) Mejora la latencia.
 - d) Implementa la compresión de cabeceras para optimizar el rendimiento.
- 4.- En el contexto de las cabeceras HTTP para mitigar ataques, ¿qué cabecera se utiliza para indicar al navegador que solo debe comunicarse con el servidor a través de HTTPS?
 - a) Access-Control-Allow-Origin
 - b) X-Frame-Options
 - c) Strict-Transport-Security (HSTS)
 - d) Ninguna de las anteriores
- 5.- ¿Qué cabecera de respuesta HTTP permite a un servidor indicar qué dominios externos pueden acceder a sus recursos?
 - a) Content-Security-Policy
 - b) Access-Control-Allow-Origin
 - c) Strict-Transport-Security
 - d) X-Content-Type-Options

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

- 6.- ¿Cuál es la diferencia entre el protocolo SFTP y el protocolo FTPS?
- SFTP dispone de comandos similares a FTP, pero está implementado sobre SSH.
 - El protocolo SFTP no existe.
 - SFTP es la versión sin autenticar de FTP, también conocido como TFTP.
 - Son lo mismo, uno nombrado en español y otro en inglés.
- 7.- En el sistema de nombres de dominio (DNS), ¿cuál de las siguientes afirmaciones describe correctamente a un servidor DNS secundario en relación a un servidor DNS maestro/primario?
- Mantiene una copia de lectura/escritura de los archivos de zona del servidor maestro y es autoritativo para esa zona.
 - Mantiene una copia de solo lectura de los archivos de la zona del servidor maestro, pero no es autoritativo para esa zona.
 - Mantiene una copia de solo lectura de los archivos del servidor maestro y es autoritativo para esa zona.
 - Mantiene una copia de lectura/escritura de los archivos de zona del servidor maestro, pero no es autoritativo para esa zona.
- 8.- Queremos obtener un certificado autofirmado y ejecutamos el comando:
`openssl x509 -req days 365 -in cert.csr -signkey key.pem -out cert.crt.`
 ¿Qué representa el parámetro key.pem?
- La clave pública del solicitante.
 - La clave pública de la CA.
 - La clave privada de la CA.
 - La clave privada del solicitante.
- 9.- ¿Cuál de las siguientes afirmaciones es un requisito para utilizar Virtual Hosting basado en IP?
- Direcciones IP separadas para cada virtual host.
 - Ficheros de configuración separados para cada virtual host.
 - Dispositivos independientes, cada uno de ellos con su propia dirección.
 - Directivas Alias separadas para cada virtual host.
- 10.- ¿Cómo se define la capacidad de un sistema para manejar el incremento de carga añadiendo más instancias de servidores?
- Escalabilidad vertical.
 - Escalabilidad horizontal.
 - Cualquier servidor que trabaje 24/7.
 - Configurar máquinas de manera que cada una ofrezca un servicio diferente.

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

11.- ¿Qué incluye un certificado digital?

- a) La clave privada de una entidad, firmada con la clave privada de la CA que certifica.
- b) La clave pública de una entidad, firmada con la clave privada de la CA que certifica.
- c) La clave privada de una entidad, firmada con la clave pública de la CA que certifica.
- d) La clave pública de una entidad, firmada con la clave pública de la CA que certifica.

12.- ¿Cuál es el propósito del atributo SameSite en una cookie?

- a) Evitar que la cookie sea manipulada por scripts del lado del cliente.
- b) Proteger la cookie de ataques de intermediarios (Man-in-the-Middle).
- c) Controlar si la cookie se envía con solicitudes de otros sitios.
- d) Definir el tiempo de vida de la cookie.

13.- ¿En qué se diferencia un csr (solicitud de certificado) de un crt (certificado)?

- a) El crt incluye la clave pública del propietario y el csr no.
- b) El crt está firmado por un CA y el csr está firmado por nosotros mismos.
- c) El crt incluye la clave privada del CA que lo firma y el csr no.
- d) El crt está firmado por el CA y el csr no.

14.- Durante el handshake TLS, ¿cuál es la primera información que envía un servidor a un cliente la primera vez que se conecta a él?

- a) La clave simétrica de sesión que deberá usarse durante toda la comunicación.
- b) Un certificado del servidor donde el cliente podrá poner su password y devolver al servidor.
- c) El resumen del password (en SHA256 o MD5) que es modificado con el password del cliente.
- d) Un certificado del servidor con la clave pública del servidor.

15.- En la cabecera HTTP, el campo If-None-Match se relaciona con:

- a) Etag (string/Hash MD5) que resume el contenido de la página para gestionar la caché.
- b) Solicitar al servidor que mantenga la conexión viva.
- c) Un formato especial de fecha para indicar la versión en caché.
- d) Ninguna de las anteriores.

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

- 16.- Para particularizar el código de error 403 en Apache 2.4 (GNU/Linux) con el archivo /etc/msg/error500.html, ¿cuál es la opción correcta?
- ErrorDocument 403 /etc/msg/error500.html
 - ErrorDocument 403 /root/msg/error500.html
 - ErrorDocument 403 /<directorio documentroot>/etc/msg/error500.html
 - ErrorDocument 403 /error500.html
- 17.- ¿Cómo puede un servidor web saber qué navegador está utilizando un cliente?
- Mediante la petición Request-Agent realizada por el servidor.
 - Mediante la cabecera User-agent incluida por defecto en la petición HTTP.
 - Mediante una configuración en el propio navegador.
 - Solo se puede realizar desde ciertos lenguajes de programación como PHP.
- 18.- ¿Cuál de las siguientes afirmaciones describe mejor una característica esencial de las funciones hash?
- RSA es un ejemplo de función hash comúnmente utilizada.
 - Es una función que permite recuperar la entrada original a partir del hash generado.
 - Es una función unidireccional, donde es computacionalmente inviable obtener la entrada original.
 - Todas las anteriores son correctas.
- 19.- En Apache 2.4 y Nginx, ¿en qué directorio se guardan los archivos de configuración correspondientes a los sitios virtuales activos?
- sites-active
 - sites-available
 - 000-default.conf
 - sites-enabled
- 20.- Una vez establecida la conexión HTTPS y tras el intercambio inicial, la información posterior entre cliente y servidor:
- Estará cifrada con una clave simétrica de sesión que conocen ambos.
 - Estará cifrada con la clave privada del cliente.
 - Estará cifrada con la clave pública del servidor.
 - Estará cifrada con la clave pública del cliente.

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

```
DocumentRoot /var/www

SetEnvIf User-Agent ^Mozilla/5.0 firefox

<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>

<Directory /var/www/>
    DirectoryIndex despliegue.html
    Options FollowSymLinks MultiViews
    AllowOverride None
    Order Allow,Deny
    Deny from daw.org
    Allow from 170.30.40.0/24
    Allow from env=firefox
</Directory>

<Directory /var/www/ciclos>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order deny,allow
    deny from 170.30.40.0/24
    allow from daw.org
</Directory>
```

Figura 1

- 21.- Según la Figura 1, si alguien se conecta desde una IP 170.30.50.0/24 (fuera de daw.org) usando Chrome a <http://192.168.2.13/ciclos>, ¿qué ocurre si el fichero despliegue.html existe en el directorio /var/www/ciclos?
- Se muestra un listado de ficheros.
 - Se muestra el contenido del fichero despliegue.html.
 - Se muestra el mensaje "Forbidden".
 - Se muestra el mensaje "Not Found".
- 22.- Según la Figura 1, si alguien se conecta desde una IP 170.30.60.0/24 (fuera de daw.org) usando Chrome a <http://192.168.2.13>, ¿qué ocurre si el fichero despliegue.html existe en /var/www?
- Se muestra el contenido del fichero despliegue.html.
 - Se muestra el mensaje "Not Found".
 - Se muestra el mensaje "Forbidden".
 - Se muestra un listado de ficheros.

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

23.- ¿Cuántas claves públicas contiene un certificado SSL?

- a) Una, la del solicitante.
- b) Dos, la del solicitante y la de la CA.
- c) Ninguna, solo contiene claves simétricas.
- d) Puede contener infinitas.

24.- Para obtener un certificado de la CA Digicert, el orden correcto es:

- a) 1º Enviamos el fichero .crt a Digicert, 2º nos devuelven un .csr, 3º configuramos SSLCertificateFile.
- b) 1º Enviamos el fichero .crt a Digicert, 2º nos devuelven un .csr, 3º incluimos SSLCertificateFile /etc/ssl/certs/cert.csr.
- c) 1º Enviamos el fichero .csr a Digicert, 2º nos devuelven un .crt, 3º incluimos SSLCertificateFile /etc/ssl/certs/cert.csr.
- d) 1º Enviamos el fichero .csr a Digicert, 2º nos devuelven un .crt, 3º incluimos SSLCertificateFile /etc/ssl/certs/cert.crt.

25.- Un certificado de nivel 1 está firmado por un CA de nivel 2, que a su vez está firmado por un CA Raíz de nivel 3. ¿Quién firma el certificado de nivel 3?

- a) Está firmado por el Cuerpo Nacional de Policía.
- b) Está certificado por el mismo (autofirmado).
- c) Al ser Raíz, no lo firma nadie.
- d) Está firmado por Aut-nivel1 y Aut-nivel2 (red de confianza).

26.- ¿Qué tipo de escalabilidad emplean los balanceadores de carga?

- a) Vertical.
- b) Depende de si es software o hardware.
- c) Horizontal.
- d) Ninguna de las anteriores.

27.- Hemos inyectado nuestra clave pública en un servidor SSH, pero al ejecutar `ssh pepe@172.22.200.203` nos sigue pidiendo el password. ¿Cuál es la causa más probable?

- a) Todas las anteriores son verdaderas.
- b) Hemos inyectado la clave con otro nombre de usuario.
- c) Hemos inyectado una clave distinta a la clave por defecto.
- d) Hemos almacenado la clave en un directorio distinto del actual.

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

- 28.- En el fichero known_hosts de una máquina que actúa como cliente SSH se almacenan:
- Las claves públicas del propio servidor ssh de la máquina.
 - Las claves privadas del servidor ssh.
 - Las claves públicas de los clientes que se han conectado.
 - Las claves públicas de los servidores a los que se ha conectado.
- 29.- En Apache 2.4, los comandos a2dissite y a2ensite sirven para:
- Activar y desactivar módulos de Apache.
 - Habilitar y deshabilitar sitios definidos en virtualhosts.
 - Habilitar la función proxy.
 - Ninguna de las anteriores.
- 30.- En Apache 2.4, para aceptar solo conexiones en el puerto 443 de la interfaz 192.168.200.250:
- Port 443
 - Listen *:443
 - Listen 192.168.200.250:443
 - Port 192.168.200.250: 443
- 31.- ¿Qué valor de la directiva MaxKeepAliveRequests permite solicitudes ilimitadas por conexión?
- 100
 - 300
 - 0
 - 1
- 32.- ¿Qué directiva de Apache se usa para activar el protocolo HTTPS en un Virtualhost?
- SSLEngine On
 - SSLEnable On
 - SSLEngine yes
 - SSLEnable yes
- 33.- El formato CLF (Common Log Format) se emplea para:
- Copias de seguridad en formato ext3.
 - Establecimiento de comunicaciones cifradas.
 - Establecer variables de entorno.
 - Estandarizar el formato de los logs para herramientas externas.

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

34.- ¿Cuál es el principal beneficio de seguridad del atributo HttpOnly en una cookie?

- a) Forzar el envío solo por HTTPS.
- b) Mitigar el robo de cookies mediante ataques XSS.
- c) Restringir el envío a solicitudes del mismo sitio.
- d) Establecer la fecha de expiración.

35.- Para ejecutar PHP de forma aislada y eficiente en Apache, se recomienda:

- a) Instalar Tomcat.
- b) Instalar una solución propietaria de Windows.
- c) Cargar un módulo como libapache2-mod-php7.3 o php7.3-fpm.
- d) Utilizar WildFly.

36.- Técnicamente, Apache Tomcat se clasifica como:

- a) Un contenedor de Servlets y JSPs.
- b) Un contenedor de EJB's.
- c) Un contenedor de solo JSP.
- d) Un servidor de archivos estáticos exclusivamente.

37.- Indique cuál de las siguientes afirmaciones es INCORRECTA:

- a) El lenguaje Java puede trabajar en el lado cliente y en el servidor.
- b) La tecnología ASP se ejecuta en el lado del cliente.
- c) El lenguaje PHP se ejecuta en el lado del servidor.
- d) El lenguaje JavaScript se ejecuta en el lado cliente.

38.- En Apache, las directivas SSLCertificateFile y SSLCertificateKeyFile definen:

- a) La ruta a la clave pública y privada del navegador.
- b) La ruta al certificado digital del servidor y a su clave privada, respectivamente.
- c) La ruta a la clave privada del servidor y al certificado digital del servidor.
- d) Ninguna de las anteriores.

39.- He perdido mi clave de acceso a un servicio web y solicito el reenvío. ¿Cuál es el procedimiento más seguro que debe seguir la empresa?

- a) Enviarme mi password actual, ya que solo se envía al correo registrado.
- b) Pedirme que firme la petición usando mi clave pública.
- c) Resetear la cuenta para introducir un password nuevo, ya que solo deben guardar el hash.
- d) Enviarme la clave cifrada con mi clave privada.

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

40.- En Apache 2.4, dada la siguiente configuración:

```
<Directory /var/www/privado>  
  <RequireAll>  
    Require all granted  
    Require not group restrictedadmin  
    Require not host bad.host.com  
  </RequireAll>  
</Directory>
```

¿Podrá acceder el usuario useraccounts?

- a) Sí, siempre que no pertenezca al grupo restrictedadmin y su hostname no sea bad.host.com.
- b) Sí, por estar incluido en el RequireAll, independientemente de lo demás.
- c) No, porque nunca podrá cumplir todas las condiciones.
- d) No tenemos suficientes datos para contestar.