



1. Según la ley orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, constituye acoso por razón de sexo: (artículo 7)
 - a. Cualquier comportamiento verbal o físico, de naturaleza sexual que tenga el propósito o produzca el efecto de atentar contra la dignidad de una persona, en particular cuando se crea entorno intimidatorio, degradante u ofensivo.
 - b. Cualquier comportamiento realizado en función del sexo de una persona, con el propósito de crear un entorno intimidatorio, degradante u ofensivo.
 - c. A y B son correctas.
 - d. Ninguna es correcta.

2. Según establece el III Convenio colectivo de Puertos del Estado y Autoridades Portuarias, ¿Cuántos días le corresponden a un/a trabajador/a por traslado de domicilio? (artículo 25)
 - a. Tres días naturales en la misma provincia o isla y cuatro días naturales en distinta provincia o isla.
 - b. Cuatro días naturales en la misma provincia o isla y seis días naturales en distinta provincia o isla.
 - c. Dos días naturales en la misma provincia o isla y cuatro días naturales en distinta provincia o isla.
 - d. Ocho días naturales en la misma provincia o isla y diez días naturales en distinta provincia o isla.

3. ¿Cuál es el límite máximo de trienios que establece el III Convenio Colectivo de Puertos del estado y Autoridades Portuarias como derecho a percibir por el personal sujeto al mismo? (artículo 61)
 - a. No existe límite.
 - b. Doce trienios.
 - c. Diez trienios.
 - d. Nueve trienios.

4. Según establece el III Convenio colectivo de Puertos del Estado y Autoridades Portuarias, la jornada de trabajo general será:
 - a. Como máximo de 40 horas semanales.
 - b. Como máximo de treinta y seis horas semanales.
 - c. Como máximo de treinta y siete horas y media semanales.
 - d. Como máximo de treinta y cinco horas semanales.

5. Según establece el III Convenio colectivo de Puertos del Estado y Autoridades Portuarias, el periodo vacacional queda establecido, con carácter general entre los meses de:
 - a. Enero y septiembre (ambos inclusive)
 - b. Mayo y septiembre (ambos inclusive)
 - c. Junio y septiembre (ambos inclusive)
 - d. Junio y agosto (ambos inclusive)

6. Un SIEM típicamente se alimenta de:
 - a. Tráfico de backup
 - b. Logs de sistemas, dispositivos de red y aplicaciones
 - c. Solo registros de bases de datos
 - d. Solo tráfico de web

7. En criptografía asimétrica, ¿qué clave se utiliza para verificar una firma digital?
 - a. La clave simétrica compartida
 - b. La clave privada del emisor
 - c. La clave pública del emisor
 - d. Ninguna de las anteriores

8. En un proyecto de integración de sistemas mediante APIs REST, la utilización de tokens JWT suele emplearse para:
 - a. Comprimir mensajes
 - b. Autenticar y autorizar peticiones de forma segura
 - c. Cifrar los mensajes
 - d. Validar los mensajes

9. En una arquitectura Java/JEE típica de 3 capas para un sistema portuario, ¿qué corresponde a la capa de presentación?
 - a. EJBs de negocio
 - b. Base de datos relacional
 - c. JSP/JSF/Servlets o front web que interactúa con el usuario
 - d. Servicios SOAP/REST externos

10. ISO 27001 está relacionada con:
 - a. Calidad del software
 - b. Gestión de seguridad de la información
 - c. Gestión medioambiental
 - d. Continuidad de negocio exclusivamente

11. Un sistema NAS configurado en RAID5 se utiliza para:
 - a. Procesar transacciones de base de datos
 - b. Monitorizar sistemas
 - c. Gestionar identidades
 - d. Almacenamiento de ficheros a través de la red

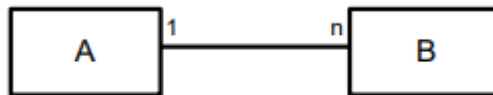
12. Un sistema EDI sirve para:
 - a. Intercambiar documentos electrónicos estructurados entre organizaciones
 - b. Compartir documentación interna en PDF
 - c. Hibridar redes WIFI
 - d. Monitorizar bases de datos

13. Un IPS, a diferencia de un IDS, se caracteriza por:
- No necesitar firmas
 - Actuar de forma preventiva bloqueando tráfico malicioso
 - No requerir configuración
 - No generar falsos positivos
14. En una estrategia de backup 3-2-1 se recomienda:
- 3 copias, en 2 soportes distintos, 1 de ellas fuera de la ubicación principal
 - 3 copias diarias, 2 semanales, 1 mensual
 - 3 cintas, 2 discos, 1 nube
 - 3 usuarios, 2 administradores, 1 auditor
15. En un ataque de colisión sobre una función hash, el atacante:
- Intenta encontrar un mensaje dado a partir de su hash
 - Busca dos mensajes distintos que produzcan el mismo hash
 - Intenta obtener la clave secreta de cifrado
 - Intenta invertir la función hash de forma exacta
16. Al diseñar una red de una Autoridad Portuaria con múltiples VLAN (administración, explotación, cámaras, IoT, invitados...), ¿qué componente es clave para inter-VLAN routing y control de tráfico?
- Hub de concentración
 - Switch de capa 2
 - Switch de capa 3
 - Router de capa 4
17. En una topología WAN con conexión redundante a Internet de dos operadores, ¿qué protocolo se utiliza típicamente para anunciar prefijos propios y gestionar rutas con los ISP?
- OSPF
 - RIP
 - BGP
 - STP
18. En el ámbito de la disponibilidad de la información ¿qué es el RPO?
- Es la cantidad máxima de información que puede perderse cuando el servicio es restaurado tras una interrupción del sistema.
 - Es la cantidad máxima de tiempo tolerable necesario para que todos los sistemas críticos vuelvan a estar en línea.
 - Es la cantidad máxima de tiempo tolerable que se necesita para verificar el sistema y/o la integridad de datos.
 - Es la cantidad total de tiempo que un proceso de negocio puede interrumpirse sin causar consecuencias inaceptables.

19. En un análisis forense de un incidente de seguridad en un sistema portuario, ¿qué orden es más apropiado para la adquisición de evidencias volátiles?
- Disco duro, RAM, conexiones de red, procesos
 - Procesos, RAM, conexiones de red, disco duro
 - RAM, procesos, conexiones de red, disco duro
 - Cualquier orden es equivalente
20. En un análisis de red corporativa, se observan estos puertos abiertos:
- 3306/TCP
 - 5432/TCP
 - 1521/TCP
- ¿Cuál es la interpretación correcta?
- Son puertos de servidores web alternativos (HTTP).
 - Indican la presencia de servicios de bases de datos: MySQL/MariaDB, PostgreSQL y Oracle DB respectivamente.
 - Indican servicios LDAP avanzados.
 - Son usados por servicios de backup y restauración SAN.
21. ¿Cuál de las siguientes asociaciones es completamente correcta respecto a puertos TCP/UDP y los protocolos que habitualmente los utilizan?
- 21/TCP → FTP Control, 20/TCP → FTP Datos, 22/UDP → SSH
 - 80/TCP → HTTP, 443/TCP → HTTPS, 53/UDP → DNS consultas estándar
 - 25/UDP → SMTP, 110/TCP → POP3, 35/UDP → DNS consultas estándar
 - Ninguna de las anteriores.
22. ¿Cuál es una causa habitual de deadlocks en sistemas transaccionales?
- Índices compuestos en exceso.
 - Replicación síncrona.
 - Tablas sin normalizar.
 - Acceso a recursos en distinto orden entre transacciones
23. En una base de datos Oracle, ¿cuál es la finalidad principal del modo ARCHIVELOG?
- Impedir que se sobrescriban los datafiles
 - Permitir recuperar la base de datos hasta cualquier punto en el tiempo
 - Desactivar el uso de los redo logs online
 - Optimizar el rendimiento de consultas
24. ¿Cuál es la diferencia más relevante entre SNMPv2 y SNMPv3?
- v3 incorpora autenticación y cifrado robusto.
 - v3 usa siempre TCP.
 - v2 permite streaming continuo.
 - v3 elimina MIBs.

25. En una VPN IPsec entre la Autoridad Portuaria y un proveedor, la opción más robusta en 2025 a nivel criptográfico es:
- IPsec con claves precompartidas
 - IPsec con AES-GCM y ECDH
 - IPsec con 3DES y MD5
 - PPTP con MS-CHAPv2
26. En el ENS, ¿cuál de las siguientes combinaciones de roles es INCORRECTA según la lógica de segregación de funciones?
- Responsable de la Información y Responsable del Servicio pueden ser la misma persona si coincide la unidad orgánica
 - Responsable de la Seguridad debe estar separado funcionalmente de los responsables de explotación de sistemas
 - Responsable del Sistema y Responsable del Servicio siempre deben ser personas diferentes
 - El Delegado de Protección de Datos (DPD) no sustituye a ningún rol ENS, sino que se coordina con ellos
27. Señale la opción correcta sobre el hash:
- La longitud del hash varía en función del tamaño del mensaje
 - Para su implementación se considera más seguro emplear MD5 frente a SHA-2
 - La función hash no es reversible, sino unidireccional
 - Dos mensajes diferentes podrían producir la misma firma
28. En el contexto de la metodología de trabajo Scrum, ¿cuál de las siguientes es una reunión oficial de Scrum?
- Sprint Planning
 - Sprint Review
 - Daily Scrum
 - Todas son correctas.

29. Dado el siguiente diagrama E-R:



Y las siguientes instancias y relaciones:

A	B	Relaciones
a1	b1	a1 - b1
a2	b2	a1 - b2
a3	b3	a2 - b1
a4	b4	a2 - b4
		a3 - b3

¿Qué relación(es) sería necesario eliminar para que los datos concordaran con el modelo?

- a. La tercera, a2-b1
 - b. La cuarta, a2-b4
 - c. La segunda y la cuarta, a1-b2 y a2-b4
 - d. La quinta, a3-b3
30. En un clúster activo-activo:
- a. La carga de trabajo la asume uno de los nodos y, en caso de caída, se traspasa al otro nodo
 - b. Las cargas de trabajo se distribuyen entre todos los nodos del clúster
 - c. Los clientes se conectan al nodo activo designado como primario y los procesos con menor prioridad se ejecutan en el resto de nodos
 - d. Ninguna de las anteriores.
31. El ENS clasifica sus medidas en tres tipos: organizativas, operacionales y medidas de protección. ¿Cuál de las siguientes afirmaciones es correcta?
- a. Las medidas organizativas solo aplican a sistemas de categoría Alta.
 - b. Las medidas de protección se aplican únicamente a los elementos hardware.
 - c. Las medidas operacionales son las relacionadas con la explotación y operación diaria del sistema.
 - d. Las medidas organizativas solo las debe cumplir el Responsable de Seguridad.
32. En un entorno de Integración Continua (CI), ¿cuál de las siguientes herramientas se utiliza específicamente para orquestar pipelines de build, test y despliegue de forma automatizada?
- a. Jenkins
 - b. Terraform
 - c. SonarQube
 - d. Nexus Repository Manager

33. En un Sistema Operativo Ubuntu, ¿qué muestra el siguiente comando?

```
df -h
```

- a. Uso de CPU en formato legible
- b. Uso del disco en formato legible (GB/MB)
- c. Archivos abiertos por procesos
- d. Uso de memoria RAM actual

34. ¿Cuál es el orden correcto de aplicación de las directivas de grupo en un entorno AD?

- a. Sitio → Dominio → OU → Local
- b. OU → Dominio → Sitio → Local
- c. Dominio → Sitio → OU → Local
- d. Local → Sitio → Dominio → OU

35. En una organización con Directorio Activo, donde se quiere que los usuarios utilicen sus mismas credenciales de dominio para acceder a distintas aplicaciones internas (intranet, portal de incidencias, herramientas web, etc.), ¿qué mecanismo es el más adecuado para centralizar la autenticación?

- a. Configurar cada aplicación para autenticarse directamente contra el controlador de dominio mediante LDAP simple
- b. Implementar un servicio de Federación de Identidad basado en SAML u OpenID Connect integrando Active Directory
- c. Usar scripts que sincronicen contraseñas del dominio hacia las aplicaciones
- d. Crear cuentas locales espejo en cada aplicación y mantener sus contraseñas alineadas con políticas de dominio

36. ¿Qué política implementan estas reglas sobre el acceso SSH al servidor?

```
iptables -A INPUT -s 192.168.10.0/24 -p tcp --dport 22 -j ACCEPT  
iptables -A INPUT -s 10.0.0.0/8 -p tcp --dport 22 -j ACCEPT  
iptables -A INPUT -p tcp --dport 22 -j DROP
```

- a. Permiten SSH desde cualquier origen interno y externo, luego lo registran
- b. Bloquean todo el tráfico SSH, incluyendo el de redes internas
- c. Permiten SSH solo desde Internet y lo bloquean desde redes internas
- d. Permiten SSH solo desde 192.168.10.0/24 y 10.0.0.0/8 y bloquean el resto

37. Dadas las siguientes tablas de una base de datos Oracle

BUQUES		
id_buque	nombre	tipo
1	AURORA	CARGA
2	SURESTE	PASAJES
3	MARBELA	CARGA
4	LEVANTE	CARGA

ESCALAS					
id_escalas	id_buque	puerto	fecha	tasa	atracado
10	1	VALENCIA	2025-01-01	300	1
11	1	VALENCIA	2025-02-01	0	0
12	1	ALGECIRAS	2025-02-10	150	1
13	2	VALENCIA	2025-02-05	200	1
14	2	VALENCIA	2025-03-01	200	1
15	3	CADIZ	2025-02-15	100	0
16	3	CADIZ	2025-02-20	250	1
17	4	VALENCIA	2025-01-15	400	1

Y dado el siguiente resultado:

NOMBRE	FECHA
AURORA	2025-01-01
AURORA	2025-02-01

¿Qué query produce el anterior resultado?

- a)
- ```
SELECT b.nombre, e.fecha
FROM buques b
JOIN escalas e ON b.id_buque = e.id_buque
WHERE e.fecha < DATE '2025-02-02'
ORDER BY e.fecha;
```
- b)
- ```
SELECT nombre, fecha
FROM buques
WHERE fecha <= DATE '2025-02-01';
```
- c)
- ```
SELECT b.nombre, e.fecha
FROM buques b
JOIN escalas e ON b.id_buque = e.id_buque
WHERE b.tipo = 'CARGA';
```
- d)
- ```
SELECT b.nombre, e.fecha
FROM escalas e
JOIN buques b ON e.id_buque = b.id_buque
WHERE e.puerto = 'ALGECIRAS';
```

38. Con las tablas del ejercicio anterior, queremos exponer un servicio REST que devuelva las escalas de un buque determinado entre dos fechas.

¿Cuál de las siguientes definiciones de servicio sería la más adecuada siguiendo buenas prácticas REST?

- a)
- Método: **GET**
 - URL: /api/v1/buques/{id_buque}/escalas
 - Parámetros: fecha_inicio y fecha_fin como query string
 - Ejemplo:
/api/v1/buques/3/escalas?fecha_inicio=2025-02-01&fecha_fin=2025-02-28
 - Body: ninguno

- b)
- Método: **PUT**
 - URL: /api/v1/buques/escalas
 - Body (JSON):

```
{
  "id_buque": 3,
  "fecha_inicio": "2025-02-01",
  "fecha_fin": "2025-02-28"
}
```

- c)
- Método: **GET**
 - URL: /api/v1/buques/escalas
 - Body (JSON):

```
{
  "id_buque": 3,
  "fecha_inicio": "2025-02-01",
  "fecha_fin": "2025-02-28"
}
```

- d)
- Método: **POST**
 - URL: /api/v1/buques/{id_buque}/escalas
 - Body (JSON):

```
{
  "fecha_inicio": "2025-02-01",
  "fecha_fin": "2025-02-28"
}
```

39. Dado el siguiente código Java (cliente):

```
URL wsdlURL = new URL("http://puerto.es/ws/BuquesService?wsdl");

QName SERVICE_NAME = new QName(
    "http://puerto.es/servicios/buques", // namespace
    "BuquesService"                       // service name
);

QName PORT_NAME = new QName(
    "http://puerto.es/servicios/buques", // namespace
    "BuquesPort"                          // port name
);

Service service = Service.create(wsdlURL, SERVICE_NAME);
BuquesPortType port = service.getPort(PORT_NAME, BuquesPortType.class);

RegistrarEscalaResponse resp = port.registrarEscala(
    "1234567", "ALGECIRAS", "VALENCIA"
);
```

¿Cuál de los siguientes fragmentos WSDL es el que mejor se ajusta al código Java mostrado? (Solo se muestra la parte de <service> y <port> para simplificar)

a)

```
<wsdl:definitions
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:tns="http://puerto.es/servicios/buques"
  targetNamespace="http://puerto.es/servicios/buques">

  <wsdl:service name="BuquesService">
    <wsdl:port name="BuquesPortTLS" binding="tns:BuquesSoapBindingTLS">
      <soap:address location="https://puerto.es/ws/BuquesService"/>
    </wsdl:port>
  </wsdl:service>

</wsdl:definitions>
```

b)

```
<wsdl:definitions
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:tns="http://puerto.es/ws/BuquesService"
  targetNamespace="http://puerto.es/ws/BuquesService">

  <wsdl:service name="BuquesService">
    <wsdl:port name="BuquesPort" binding="tns:BuquesSoapBinding">
      <soap:address location="http://puerto.es/servicios/buques"/>
    </wsdl:port>
  </wsdl:service>

</wsdl:definitions>
```

c)

```
<wsdl:definitions
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:tns="http://puerto.es/servicios/buques"
  targetNamespace="http://puerto.es/servicios/buques">

  <wsdl:service name="BuquesPortType">
    <wsdl:port name="BuquesService" binding="tns:BuquesSoapBinding">
      <soap:address location="http://puerto.es/ws/BuquesService"/>
    </wsdl:port>
  </wsdl:service>

</wsdl:definitions>
```

d)

```
<wsdl:definitions
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:tns="http://puerto.es/servicios/buques"
  targetNamespace="http://puerto.es/servicios/buques">

  <wsdl:service name="BuquesService">
    <wsdl:port name="BuquesPort" binding="tns:BuquesSoapBinding">
      <soap:address location="http://puerto.es/ws/BuquesService"/>
    </wsdl:port>
  </wsdl:service>

</wsdl:definitions>
```

40. En la Autoridad Portuaria se crea una nueva VLAN para dispositivos IoT (VLAN 40). Los dispositivos deben comunicarse con un servidor en VLAN 20 (192.168.20.50), pero no tienen conectividad IP, aunque:

- ✓ Pueden hacer ping a su gateway 192.168.40.1
- ✓ No pueden hacer ping a 192.168.20.50
- ✓ El switch L3 muestra esta tabla de rutas:

```
VLAN 20 → 192.168.20.0/24 (interface Vlan20)
VLAN 40 → 192.168.40.0/24 (interface Vlan40)
```

- ✓ Y esta ACL aplicada a la SVI de VLAN 40:

```
ip access-list extended VLAN40_OUT
 permit ip 192.168.40.0 0.0.0.255 any
```

¿Cuál es el problema más probable?

- a. Falta una ruta estática entre VLAN 40 y VLAN 20
- b. La ACL VLAN40_OUT bloquea tráfico hacia 192.168.20.0/24
- c. Falta aplicar una ACL de retorno en VLAN 50
- d. La ACL en VLAN 40 permite tráfico hacia “any”, pero no permite tráfico de retorno, que puede estar siendo filtrado por ACLs en VLAN 20 o por política de seguridad del L3

41. Durante un análisis de tráfico con openssl s_client, obtienes:

```
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-SHA
Server public key is 2048 bit
SSL-Session:
 Protocol : TLSv1.2
 Cipher   : ECDHE-RSA-AES256-SHA
 Verify return code: 0 (ok)
```

Un auditor comenta que la comunicación es “segura pero mejorable según ENS”. ¿Qué recomendación práctica harías?

- a. Deshabilitar TLS 1.2 y forzar solo TLS 1.1
- b. Cambiar a AES 256 CBC para obtener mayor seguridad
- c. Deshabilitar SHA based suites y priorizar AES GCM, que es más robusto
- d. Aumentar la clave pública RSA a 8192 bits para obtener mayor rendimiento

42. En un repositorio git, tienes una rama feature/A creada desde develop. Otro compañero ha hecho cambios en develop que afectan a los mismos ficheros. Quieres actualizar tu rama y mantener un historial limpio, evitando un merge commit. ¿Cuál es la estrategia correcta?

- a. git merge feature/A desde develop
- b. git push develop desde feature/A
- c. git rebase develop desde feature/A
- d. git pull feature/A desde develop

43. La dirección IP de un equipo es la 192.168.96.113/27. ¿Cuál es la dirección IP de la red a la que pertenece?

- a. 192.168.96.96
- b. 192.168.96.127
- c. 192.168.96.64
- d. 192.168.96.0

44. Un firewall registra estos eventos en un intervalo de 15 segundos:

```
Dec 11 10:05:21 DENY TCP src=192.168.10.50 dst=10.0.0.5 sport=54321 dport=22 flags=S
Dec 11 10:05:21 DENY TCP src=192.168.10.50 dst=10.0.0.5 sport=54322 dport=22 flags=S
Dec 11 10:05:21 DENY TCP src=192.168.10.50 dst=10.0.0.5 sport=54323 dport=22 flags=S
Dec 11 10:05:22 DENY TCP src=192.168.10.50 dst=10.0.0.5 sport=54324 dport=22 flags=S
Dec 11 10:05:27 DENY TCP src=192.168.10.51 dst=10.0.0.5 sport=40000 dport=22 flags=S
Dec 11 10:05:27 DENY TCP src=192.168.10.52 dst=10.0.0.5 sport=48000 dport=22 flags=S
```

¿Qué tipo de ataque describe mejor este patrón?

- a. Port scanning horizontal hacia múltiples servicios.
- b. SYN flood distribuido (DDoS) hacia el servidor SSH.
- c. Intento de SSH brute force desde una única IP.
- d. Conexiones legítimas fallidas por password incorrecto.

45. Un firewall corporativo tiene la siguiente política:

Nº	Acción	Protocolo	Origen	Destino	Puerto destino
1	DENY	TCP	10.0.0.0/24	10.10.10.10	22
2	ALLOW	TCP	10.0.0.50	10.10.10.10	22
3	ALLOW	TCP	10.0.0.0/24	10.10.10.0/24	443
4	DENY	ANY	ANY	ANY	ANY

Un administrador dice que desde el equipo 10.0.0.50 no puede acceder por SSH (puerto 22) al servidor 10.10.10.10, aunque teóricamente debería poder.

¿Cuál es la causa más probable del problema?

- La regla 2 debería estar antes que la regla 1, porque las ACL se evalúan en orden estricto.
- La regla 2 no funciona porque el firewall no permite excepciones a subredes completas.
- La regla 3 interfiere porque también incluye tráfico TCP.
- La regla 4 tiene prioridad sobre todas las demás.

PREGUNTAS DE RESERVA

1. ¿Cuál de los siguientes elementos es obligatorio en un mensaje SOAP válido?
 - a. <soap:Header>
 - b. <soap:Fault>
 - c. <soap:Envelope>
 - d. <soap:Attachment>

2. Un pentest donde el auditor solo conoce la URL o dirección IP del sistema, pero no credenciales ni arquitectura, se denomina:
 - a. White Box
 - b. Grey Box
 - c. Black Box
 - d. Red Team

3. ¿Cuál es el objetivo principal del proceso de Gestión de Incidentes en ITIL?
 - a. Identificar la causa raíz de un problema
 - b. Restaurar el servicio lo antes posible
 - c. Investigar cambios no autorizados
 - d. Ninguna de las anteriores

4. En un modelado de amenazas, ¿qué tipo de control es más adecuado para mitigar amenazas de Spoofing?
 - a. Autenticación fuerte
 - b. Cifrado en tránsito
 - c. Auditoría y logging
 - d. Limitar el número de solicitudes

5. En un documento HTML estándar, ¿cuál debe ser la primera etiqueta del archivo?
 - a. <body>
 - b. <head>
 - c. <html>
 - d. <web>