JUNTA DE ANDALUCIA

INSTITUTO ANDALUZ DE ADMINISTRACIÓN PÚBLICA

(O.E.P. 2016)

CUERPO DE TÉCNICOS DE GRADO MEDIO, OPCIÓN INFORMÁTICA (A2.2012)

SEGUNDO EJERCICIO, ACCESO LIBRE

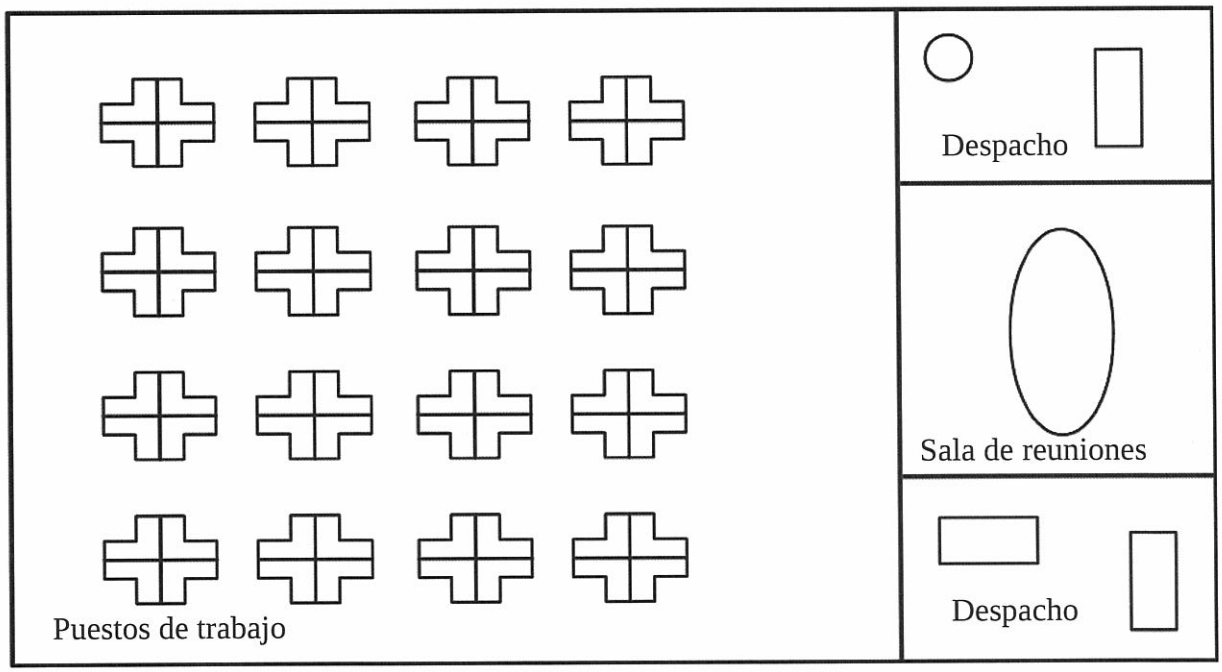
ADVERTENCIAS:

1. No abra este cuestionario hasta que se le indique.
2. El presente ejercicio, de carácter eliminatorio, consistirá en la resolución de un caso de carácter práctico, mediante el análisis de un supuesto o la preparación de un informe, referido al contenido del temario, a elegir entre las dos propuestas incluidas en este cuestionario.
3. Si observa alguna anomalía en la impresión del cuestionario, solicite su sustitución.
4. El tiempo máximo para la realización de este ejercicio es de 120 minutos.
5. Este ejercicio se calificará de 0 a 30 puntos. Para superar la prueba será necesario obtener una calificación mínima de 15 puntos.
6. Se valorará, globalmente, el rigor analítico, la claridad expositiva, los conocimientos generales y específicos, aplicados, la capacidad de relacionar, el enfoque coyuntural adaptado al contexto desde el punto de vista socio-económico, así como el grado de iniciativa y la capacidad de decisión.
7. Si necesita alguna aclaración, por favor, pídalo en voz baja al personal del aula, de tal forma que se evite molestar al resto del aula.
8. El personal del aula no le podrá dar información acerca del contenido del examen.

1 Primer Supuesto

Una vez incorporado a la Junta de Andalucía, entra usted ocupando una plaza de titulado de grado medio, opción Informática, en una Delegación Territorial. Su responsable directo nada más llegar le informa que la Delegación se va a trasladar parcialmente a un nuevo edificio, y le comunica que sus tareas serán todas las necesarias (desde el punto de vista de las TIC) para que los usuarios puedan mudarse al nuevo edificio en el plazo de 3 meses, disfrutando de los mismos servicios TIC que poseen actualmente. El nuevo edificio se convertirá en la sede principal de la Delegación, quedando el antiguo como sede auxiliar. Los edificios se conectarán entre ellos a través de la Red Corporativa de la Junta de Andalucía (y no mediante conexión directa).

En el edificio nuevo se ocuparán dos plantas bastante diáfanas de 500 m² cada una, con la planimetría orientativa que se muestra a continuación:



Se aprovechará la puesta en marcha de la nueva sede para montar nueva electrónica de red, nuevos servidores departamentales y una cabina de almacenamiento (todo el equipamiento ya existente se quedará en el edificio "antiguo"). Entre las dos plantas se estima una ocupación de aproximadamente 150 usuarios, con previsión de que se llegue al menos a 200 en un futuro cercano. El personal de informática (6 personas) se trasladará al nuevo edificio en la planta inferior. El edificio no tiene ascensor.

Notas: Se recomienda la lectura de todo el supuesto antes de empezar, ya que la redacción de algunas preguntas puede contener algunas "pistas" para responder de la forma más correcta posible a otras.

1.1 Primer supuesto - preguntas

1. Dibuje un diagrama de arquitectura de red lógico en el que se muestren los elementos que formarán parte de la red local y las conexiones entre ellos, con tanto detalle como considere. Aproveche el diagrama para incluir la segmentación de redes a nivel IPv4 que realizaría para poder atender a las necesidades actuales y futuras (suponga que puede hacer uso de hasta tres clases C en caso de que lo considere necesario, la 10.0.1.0, 10.0.2.0 y 10.0.3.0). No olvide incluir en el diagrama algunas características mínimas de los diferentes elementos. Por ejemplo: número de switches para dar conectividad a todos los usuarios (asuma que pueden ser de 24 o 48 puertos), número de dispositivos de electrónica de red de cada tipo que incluiría (tenga en cuenta que la disponibilidad de la red en horario laboral, o al menos del "core", es importante), tipo de cableado que usaría para comunicar los diferentes elementos entre ellos (cobre de diferentes velocidades y calidades, fibra, etc), etc. Sería interesante que a las diferentes redes o subredes les asigne un nombre, podría facilitarle responder a posteriores preguntas. Tenga en cuenta la normativa de la Junta de Andalucía de cableado de red para el dimensionamiento de la red (e indique el número de tomas de usuario y auxiliares que considere necesarias, indicando cuantas pondría en cada sala). Puede añadir las aclaraciones o explicaciones textuales que considere al diagrama. (hasta 5 puntos)

2. Su responsable le pide que no olvide que hay que añadir reglas al cortafuegos de la sede, de tal forma que se garantice que los usuarios pueden trabajar con normalidad manteniendo un mínimo de seguridad. Para ello, le da cierta directrices para que las tenga en cuenta: (hasta 4 puntos)

1. Los usuarios del nuevo edificio podrán hacer uso de carpetas de red situadas en los servidores del edificio antiguo, y viceversa. Las impresoras sin embargo no hay necesidad de ser compartidas entre edificios.
2. Los usuarios podrán acceder a Internet (pero solo a servicios web en los puertos estándar 80 y 443, salvo los informáticos que no tendrán restricciones al respecto)
3. Sólo los informáticos tienen que tener la capacidad de conectarse a cualquier PC o servidor por escritorio remoto (protocolo RDP).
4. Sólo los informáticos tienen que tener la capacidad de conectarse a cualquier servidor o elemento de electrónica de red por SSH.
5. Sólo los informáticos tienen que poder acceder a la configuración de las impresoras, que disponen de un pequeño servidor web de configuración en el puerto 8443.
6. El antivirus de los PC's recibe las actualizaciones desde el servidor antivirus de la sede a través del puerto 12345.
7. Los servidores no deberían tener salida directa a Internet, puesto que no lo necesitan, salvo el servidor antivirus y el servidor de parches para la descarga de patrones y parches desde los servidores del fabricante del antivirus y del sistema operativo.
8. Algunos usuarios disponen de VPN de la Red Corporativa, y trabajan habitualmente conectándose por escritorio remoto a sus PCs de la oficina. Las VPN de la Junta tienen direccionamiento 10.247.0.0/23.

Indique las reglas que incluiría en el cortafuegos para cumplir con los requisitos anteriores, numerándolas en orden de prelación (la regla 1 se ejecuta en primer lugar), y si es necesario para mantener la seguridad de la red puede añadir alguna más que considere imprescindible. En el

origen y destino puede usar los nombres de las redes que haya definido en la pregunta 1, o direccionamiento IP (como prefiera). Se recomienda responder creando una tabla con este formato:

NUM REGLA	INTERFAZ/VLAN ORIGEN	INTERFAZ/VLAN DESTINO	PUERTO	ACCIÓN
1	RED_DE_EJEMPLO_1	RED_DE_EJEMPLO_2	22	PERMITIR/DENEGAR

Puede hacer uso si lo considera necesario en las columnas de origen y destino de los valores "TODAS LAS REDES"o "LAS REDES X, Y, Z, ...", y en la de puertos "TODOS LOS PUERTOS" o "PUERTOS X, Y, Z, ..."

3. Su responsable le pide que configure el escáner de las impresoras multifunción de tal forma que los documentos que se digitalicen al menos tengan el mínimo de resolución que recomiendan las normas técnicas del Esquema Nacional de Interoperatibilidad. ¿Cual sería la configuración mínima de escaneado que aplicaría? (hasta 1 punto)

4. Su responsable le indica que es extremadamente importante que todos los equipos Windows se mantengan actualizados, y le pide que defina una política de despliegue de parches que de ciertas garantías de que los equipos reciben e instalan los parches con regularidad desde el servidor de parches (que tendrá instalado WSUS), pero sin correr riesgos innecesarios (y le cuenta una historia de aquella vez que aplicó un parche en producción al día siguiente de su publicación por el fabricante del S.O. que provocó que los servidores dieran un "pantallazo azul" y hubo que reinstalarlos). Haga una propuesta de política para que su responsable pueda revisarla. (hasta 3 puntos)

5. De entre todos los dispositivos que serán necesarios (servidores, electrónica de red, etc), los únicos que tendrá que adquirir la Delegación con su presupuesto son los cortafuegos, ya que el resto será proporcionado por los Servicios Centrales. El precio de un cortafuegos con las características mínimas necesarias es de 8.500€ + IVA. Teniendo en cuenta la Ley de Contratos vigente en el momento de hacer este supuesto práctico, ¿que tipo de contrato usaría para adquirir estos dispositivos? ¿A que Organismo de la Junta de Andalucía tendría que solicitar un informe favorable? (hasta 2 puntos)

6. Una vez resueltos todos los problemas relacionados con la red local, es necesario empezar a montar la infraestructura de servidores. Desde servicios centrales les envían 5 servidores enracables con sistema operativo Windows, todos con las mismas características hardware, para que desplieguen en ellos los servicios de directorio activo, dhcp, servidor de ficheros, impresión, antivirus y wsus. ¿Cual cree que sería una distribución razonable de servicios en los diferentes servidores? (hasta 3 puntos)

7. Un viernes a media mañana recibe un correo de los servicios centrales indicando que el siguiente lunes ponen en marcha un nuevo proxy para controlar el acceso a Internet, por lo que tiene usted poco mas de 4 horas para buscar una solución que permita a los usuarios seguir navegando el lunes sin problemas, al menos con el navegador oficial que es Internet Explorer. A partir de ese día la navegación directa a Internet no será posible, siempre habrá que pasar por el proxy (un servidor Squid que responde en 10.10.0.17:3128) ¿Cuál cree que es la solución más sencilla para evitar esta problemática sin que haya que ir puesto por puesto configurando cada equipo manualmente, y sobre que elementos habría que actuar? (hasta 2 puntos)

8. Su responsable directo está haciendo una pequeña aplicación para ciertos usuarios. La aplicación se está desarrollando en Java y como base de datos Oracle Database Express Edition 11g. Está teniendo problemas con la conexión al LDAP corporativo para la autenticación de usuarios, y eso que ha usado una pieza de código que ha sacado de MADEJA. ¿Podría indicar donde está el problema en el siguiente código? (asuma que las cadenas de texto son correctas, y que todas las clases y funciones que se usan son parte estándar de Java): (1 punto)

```
Hashtable env = new Hashtable()
env.put(DirContext.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.ldap.LdapCtxFactory");
env.put(DirContext.PROVIDER_URL, "ldap://mihost:389/dc=company,dc=com");


DirContext dirContext = null;
try {
      dirContext = InitialDirContext(env);
      dirContext.addToEnvironment("java.naming.referral","follow");
}
catch(NamingException ne) {
      //TODO: controlar excepciones
}
```

9. Continuando con la aplicación, su responsable le pide ayuda con una sentencia SQL. Está intentando recuperar un listado de los 10 usuarios que más veces acceden a la aplicación. Su responsable viene del mundo SQL Server, donde ese tipo de consultas se resolvían con la cláusula TOP, pero no tiene mucha idea de como hacer lo mismo en Oracle. ¿Podría adaptar la siguiente consulta para que funcione en Oracle?: SELECT TOP 10 * FROM USUARIOS_QUE_MAS_ACCEDEN (hasta 1 punto)

10. También está teniendo problemas en acceder a la tabla USUARIOS usando como usuario de conexión a la base de datos el usuario USR_APP. Para empezar, ni siquiera puede conectarse a la base de datos. Y tampoco está muy seguro de que una vez consiga conectar pueda leer y escribir datos en dicha tabla. ¿Podría escribir la/las sentencia/s Oracle que permitirían a dicho usuario conectarse a la base de datos, así como leer, escribir y borrar datos en dicha tabla? (hasta 2 puntos)

11. Existe un sistema de información en la Delegación que se ha identificado de criticidad alta según el Esquema Nacional de Seguridad. ¿Qué mecanismos de autenticación estarían permitidos y cuáles no (o desaconsejados) teniendo en cuenta que la nueva aplicación tendrá una categoría MEDIA según el ENS? (hasta 2 puntos).

12. Como medida de seguridad para la salvaguarda de los datos de la Delegación debe implantar un sistema de copias de seguridad que siga la política "abuelo-padre-hijo". Describa brevemente en qué consiste esta política y cómo la implantaría en la instalación con indicación de la política de retención que aplicaría. (hasta 2 puntos)

13. Su responsable le pide que configure una cabina de discos que acaba de llegar. La cabina viene con cuatro discos duros de 4 TB, y tiene que elegir entre montar un RAID 0+1 o un RAID 5 con dichos discos. Comente brevemente en qué consisten cada una de estas configuraciones RAID, indicando en cada caso cómo se distribuirían los datos entre los cuatro discos disponibles y cuál sería la capacidad máxima teórica de almacenamiento útil. (hasta 2 puntos)

2 Segundo Supuesto

Se incorpora usted como funcionario del cuerpo de Técnicos de Grado Medio opción Informática de la Junta de Andalucía y su destino es una plaza en los Servicios Centrales de una Consejería, en concreto en el departamento de seguridad informática que está adscrito al área de sistemas del Servicio de Informática. Existe otra área relacionada con la temática pero independiente, que orgánicamente no depende del Servicio de Informática, sino de la Secretaría General Técnica. Se trata del Servicio de Seguridad de la Información.

Su trabajo consistirá en atender cualquier incidente de seguridad informática que pudiera surgir: desde una epidemia por virus hasta el cambio de la configuración del cortafuegos, pasando por la realización de análisis de vulnerabilidades en aplicaciones web. También participará, junto con el área de Seguridad de la Información, en la definición de políticas, normas, procedimientos e instrucciones técnicas de seguridad, así como en la implantación de nuevas medidas de seguridad informática. Otro punto importante de su trabajo será la participación en las auditorías de seguridad a las que periódicamente son realizadas en su Consejería.

2.1 Segundo supuesto - preguntas

1. Explique cuál es la diferencia entre "seguridad de la información" y "seguridad informática". ¿Por qué cree que se ha optado porque dichas áreas estén separadas y no dependan las dos del Servicio de Informática? (Hasta 2 puntos).

2. En este ámbito de trabajo son de aplicación varias normas de referencia. En particular en su Consejería se tienen en cuenta principalmente tres: el Esquema Nacional de Seguridad, la norma ISO 27001 y la norma ISO 27002. Indique cual es el alcance/objetivo de cada una, y a quienes son de aplicación (suponiendo que alguna de ellas sea de aplicación obligatoria para alguien). ¿Son incompatibles entre sí o complementarias (razone el por qué)? (hasta 3 puntos)

3. Enumere al menos 3 de las principales diferencias entre la norma ISO 27002 y el Esquema Nacional de Seguridad (hasta 3 puntos).

4. Entre sus funciones también está la de asesorar a otros compañeros y compañeras en materia de seguridad. Uno de ellos se acerca y le pide que le aclare cuales son las diferencias entre rasomware, troyano, spyware, y gusanos informáticos. Describa cada uno de los términos indicados resaltando las diferencias existentes entre ellos (hasta 3 puntos)

5. Hace falta dar de alta un nuevo fichero en la Agencia Española de Protección de Datos, y una de sus compañeras del Servicio le pregunta cómo proceder porque no conoce muy bien cuales son los pasos a realizar. ¿Cuáles serían estos pasos a fecha de hoy?¿Cuáles deberían ser estos pasos a partir del 25 de mayo de 2018? ¿Qué ocurre en esta fecha? (hasta 2 puntos)

6. Un compañero del área de desarrollo le pide que le asesore a la hora de establecer los mecanismos de autenticación para una nueva aplicación cuyo desarrollo está dirigiendo. ¿Qué mecanismos de autenticación estarían permitidos y cuáles no (o desaconsejados) teniendo en cuenta que la nueva aplicación tendrá una categoría MEDIA según el ENS? (hasta 2 puntos).

7. Un buen día la Consejería empieza a sufrir grandes problemas de conectividad. Un análisis por su parte le lleva a determinar que el organismo está sufriendo un ataque DDOS. El responsable de su área no sabe muy bien que es un ataque DDOS y le pide que se lo explique. Describa en qué consiste este tipo de ataque (hasta 1 punto)

8. Otro día, haciendo una auditoría de seguridad de una aplicación web, encuentra usted que la aplicación es vulnerable a ataques de SQL Injection, XSS y CSRF. Informa al responsable del desarrollo de la aplicación, pero este le pide que le ayude explicándole en qué consisten dichos ataques y que podría hacer para eliminar dichas vulnerabilidades. Describa pormenorizadamente los tipos de ataques a los que se ha hecho referencia y las medidas a implantar para evitar dichas vulnerabilidades. (hasta 3 puntos).

9. Una de las aplicaciones que hay en producción tiene un webservice que no está securizado mediante usuario y contraseña, por lo que cualquier usuario malintencionado podría hacer uso del mismo sin restricciones simplemente conociendo la URL. Le piden consejo sobre cómo podrían restringir el acceso al mismo, y le explican que dicho webservice solo debería ser consumido desde otro servidor (B) que está en la misma VLAN que el que aloja el webservice (servidor A). ¿Qué solución adoptaría para que únicamente se pudiera acceder al webservice del servidor A desde el servidor B? (hasta 2 puntos)

10. Como los técnicos del área de seguridad al final acaban sabiendo un poco de todo (ya que para poder hacer bien su trabajo tienen que conocer múltiples tecnologías), los compañeros y compañeras del Servicio con frecuencia se acercan a pedirles ayuda sobre múltiples temas. Uno de ellos le pide que le ayude a identificar los métodos que proporciona un WebService del que solo tiene su definición WSDL. ¿Sería capaz de construir a partir del WSDL las clases y métodos que conforman el webservice, indicando los parámetros de entrada y salida y tipos de datos? (hasta 3 puntos).

```
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:tm="http://microsoft.com/wsdl/mime/textMatching/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:tns="http://tempuri.org/"
xmlns:s="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:http="http://schemas.xmlsoap.org/wsdl/http/" targetNamespace="http://tempuri.org/"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
 <wsdl:types>
  <s:schema elementFormDefault="qualified" targetNamespace="http://tempuri.org/">
   <s:element name="ConnectToBD">
    <s:complexType>
     <s:sequence>
      <s:element minOccurs="0" maxOccurs="1" name="bbdd" type="s:string" />
      <s:element minOccurs="0" maxOccurs="1" name="usuario" type="s:string" />
      <s:element minOccurs="0" maxOccurs="1" name="password" type="s:string" />
      <s:element minOccurs="1" maxOccurs="1" name="timeout" type="s:int" />
     </s:sequence>
    </s:complexType>
   </s:element>
   <s:element name="ConnectToBDResponse">
    <s:complexType>
     <s:sequence>
```

```
      <s:element minOccurs="0" maxOccurs="1" name="ConnectToBDResult" type="tns:Cnx" />
    </s:sequence>
   </s:complexType>
  </s:element>
  <s:complexType name="Cnx">
   <s:sequence>
    <s:element minOccurs="0" maxOccurs="1" name="token" type="tns:ArrayOfString" />
    <s:element minOccurs="1" maxOccurs="1" name="max_users" type="s:int" />
   </s:sequence>
  </s:complexType>
  <s:complexType name="ArrayOfString">
   <s:sequence>
    <s:element minOccurs="0" maxOccurs="unbounded" name="string" nillable="true" type="s:string" />
   </s:sequence>
  </s:complexType>
  <s:element name="GetPrice">
   <s:complexType>
    <s:sequence>
     <s:element minOccurs="0" maxOccurs="1" name="codproducto" type="s:string" />
    </s:sequence>
   </s:complexType>
  </s:element>
  <s:element name="GetPriceResponse">
   <s:complexType>
    <s:sequence>
     <s:element minOccurs="1" maxOccurs="1" name="GetPriceResult" type="s:int" />
    </s:sequence>
   </s:complexType>
  </s:element>
 </s:schema>
</wsdl:types>
<wsdl:message name="ConnectToBDSoapIn">
 <wsdl:part name="parameters" element="tns:ConnectToBD" />
</wsdl:message>
<wsdl:message name="ConnectToBDSoapOut">
 <wsdl:part name="parameters" element="tns:ConnectToBDResponse" />
</wsdl:message>
<wsdl:message name="GetPriceSoapIn">
 <wsdl:part name="parameters" element="tns:GetPrice" />
</wsdl:message>
<wsdl:message name="GetPriceSoapOut">
 <wsdl:part name="parameters" element="tns:GetPriceResponse" />
```

```
</wsdl:message>
<wsdl:portType name="WSPrecios1Soap">
  <wsdl:operation name="ConnectToBD">
    <wsdl:input message="tns:ConnectToBDSoapIn" />
    <wsdl:output message="tns:ConnectToBDSoapOut" />
  </wsdl:operation>
  <wsdl:operation name="GetPrice">
    <wsdl:input message="tns:GetPriceSoapIn" />
    <wsdl:output message="tns:GetPriceSoapOut" />
  </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="WSPrecios1Soap" type="tns:WSPrecios1Soap">
  <soap:binding transport="http://schemas.xmlsoap.org/soap/http" />
  <wsdl:operation name="ConnectToBD">
    <soap:operation soapAction="http://tempuri.org/ConnectToBD" style="document" />
    <wsdl:input>
      <soap:body use="literal" />
    </wsdl:input>
    <wsdl:output>
      <soap:body use="literal" />
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="GetPrice">
    <soap:operation soapAction="http://tempuri.org/GetPrice" style="document" />
    <wsdl:input>
      <soap:body use="literal" />
    </wsdl:input>
    <wsdl:output>
      <soap:body use="literal" />
    </wsdl:output>
  </wsdl:operation>
 </wsdl:binding>
 <wsdl:service name="WSPrecios1">
   <wsdl:port name="WSPrecios1Soap" binding="tns:WSPrecios1Soap">
     <soap:address location="http://localhost:63890/WSPrecios.asmx" />
   </wsdl:port>
 </wsdl:service>
</wsdl:definitions>
```

11. Explique que es una declaración de aplicabilidad en el contexto de las normas ISO 27001 y 27002 (hasta 2 puntos).

12. Explique en qué consisten las vulnerabilidades Meltdown y Spectre (hasta 2 puntos)

13. Al objeto de alertar ante un fallo en un proceso de copia de seguridad que se ejecuta en un sistema GNU/Linux, codificar un shell script en el que se detecte la ejecución (estado R) de un proceso llamado copiadm y que envíe un correo electrónico a la dirección sistemas.dp@juntadeandalucia.es informando en el caso de que dicho proceso NO se esté ejecutando (hasta 2 puntos).