**RUNE BRITO NUÑEZ**

**SEGURIDAD INFORMATICA**

**MF0486\_3. UD5 – RESPUESTAS:**

**1. Elija la opción correcta:**

1. La LOPD limita 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.

1. La Directiva 94/46/CE3, en materia de protección de datos, garantiza la libre circulación de datos entre los estados miembros.

c. La Constitución Española establece que 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.

1. La protección de datos de carácter privado no está regulada en manera

alguna, y solo es una recomendación de la norma ISO 27000.

**2.Empareje los opciones adecuadas:**

1. Responsable del tratamiento.

2. Encargado del tratamiento.

3.Persona física o jurídica que trata los datos personales.

4. Persona física o jurídica, que decida sobre la finalidad, contenido, y uso

del tratamiento.

**3. Indique cuáles de entre los siguientes no son fuentes accesibles al público:**

a. Una guía telefónica de edición anual, y difusión a todos los clientes de una empresa de telefonía. (Según el artículo 28.3 no puede ser accesible)

b. Los diarios y boletines oficiales.

c. Un listado de una asociación de médicos, que incluye nombre, especialidad, y el domicilio.

d. Registro Mercantil.

**4. Indique, respondiendo sí o no, si las siguientes afirmaciones son objeto de la LOPD:**

1. Los datos de ciudadanos españoles de una empresa establecida fuera de la U.E. NO
2. Los datos de Fuerzas y Cuerpos de Seguridad referentes a investigaciones sobre organizaciones terroristas internacionales que puedan operan en España. NO
3. Un listado con los datos de contacto particular de sus conocidos, aficionados a las apuestas deportivas de futbol, que incluye sus números de cuenta para transferirles los beneficios. SI

**5. Marque la opción correcta**:

1. Los derechos ARCO son los derechos de acceso, revocación, cancelación, y ofuscación o cifrado.
2. Los DCP tienen los derechos ARCO, que aseguran su acceso, rectificación, cancelación, y oposición.
3. Los derechos ARCO son ejecutados por la Agencia Española de Protección de Datos, para proteger a los titulares de los datos.
4. Los derechos ARCO garantizan un poder de control sobre los datos, asegurando el derecho de acceso, el de rectificación, el de cancelación, y el de oposición.

**6. Enumere la/s condición/es necesarias para que, con su consentimiento expreso, puedan comunicar sus DCP:**

■ A los DCP que se usen para la prevención o diagnóstico médico, prestación de asistencia sanitaria, tratamiento médico, o gestión de servicios sanitarios; pero siempre por un profesional sanitario sujeto al secreto profesional, u otra persona sujeta a obligación equivalente de secreto. También podrán tratarse para salvaguardar el interés vital del afectado o de otra persona, en el supuesto que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

■ A los DCP que se usen para realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros, o cuando los DCP aparezcan de forma accesoria o incidental en ficheros no automatizados, y sin guardar relación con la finalidad del mismo (artículo 81-5).

■ A los DCP que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad, o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos (RLOPD artículo 81-6).

**7. Enumere la/s condición/es necesarias para que, sin su consentimiento expreso, puedan comunicar sus DCP:**

■Los que se refieran a ideología, afiliación sindical, religión, creencias, origen racial, salud, o vida sexual.

■ Los que se refieran a datos recabados para fines policiales, sin consentimiento de los afectados.

■ Aquellos derivados de actos de violencia de género.

■ A los datos de tráfico y de localización de los operadores que presten servicios de comunicaciones electrónicas, o exploten redes públicas de comunicaciones electrónicas, se les aplicarán además de las medidas de nivel básico y medio, la medida de nivel alto del artículo 103

**8. Califique las siguientes infracciones**

a. Divulgar DCP no respetando el deber de secreto. Grave

b. Obstaculizar el ejercicio de los derechos ARCO. Grave

c. No cumplir las medidas de seguridad del nivel reglamentario. Leve

d. No cumplir el deber de información al recabar DCP de sus titulares, y no haber solicitado su inscripción en la AEPD. Muy grave

**9. Indique la sanción esperable si se comunica a terceros un fichero sin estar legitimado para ello, reconociendo de manera espontánea la infracción:**

a. De 40.001 a 300.000, porque se trata de una infracción grave.

b. De 900 a 40.000, porque el reconocimiento espontáneo reduce la franja de sanciones a las de la categoría leve.

c. De 900 a 40.000, porque con el reconocimiento espontáneo la infracción pasa a ser de categoría leve.

d. Siempre que se reconozca la infracción, no habrá sanción alguna, por reducción.

**10. ¿Qué nivel de seguridad le aplicaría a los datos relativos a la afiliación sindical y salud, contenidos en el fichero de personal de su empresa?**

a. Básico.

b. Medio.

c. Alto.

d. Leve.

11. Que exista un registro de incidencias donde se anoten las recuperaciones de DCP a raíz de un incidente, es una medida que se debe implantar desde el nivel (incluido)...

a. ... básico.

b. ... medio.

c. ... alto.

d. No es una medida.

**12. Realizar una copia de** **respaldo semanal de los DCP es una medida de nivel...**

a. ... básico.

b. ... medio.

c. ... alto.

d. No es una medida.

**13. Complete la siguiente frase:**

Deberá designarse uno o varios responsables de seguridad, para uno o todos los ficheros, encargados de coordinar y controlar las medidas de seguridad que se establezcan.

**14. Elija la respuesta más adecuada sobre el procedimiento a seguir para realizar la inscripción de un fichero de DCP:**

1. Se solicita la inscripción, se mandan los datos de los ficheros al Registro General de Protección de Datos, y por último, se espera hasta que la AEPD responda.
2. Siempre se debe notificar la solicitud de inscripción antes de la creación del fichero, y si no hubiera respuesta de la AEPD en 30 días, se sobreentiende que el fichero está inscrito.
3. No es necesaria ninguna inscripción, porque constituye una infracción LEVE, que se podría reconocer espontáneamente, para que no se aplicara ninguna sanción económica; por lo que bastaría inscribirlos después.
4. Se rellena el formulario de la agencia en internet, abonándose las tasas de inscripción según el nivel de las medidas que se quieran aplicar.