
Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación

Unidad de Aprendizaje 1

1. ¿En qué fecha se aplicó el Reglamento General de Protección de Datos (RGPD)?

- a. 17 de mayo de 2016.
- b. 25 de mayo de 2018.**
- c. 5 de diciembre de 2018.
- d. 14 de julio de 2016.

2. El objetivo principal del Reglamento General de Protección de Datos es:

- a. Proteger los derechos y libertades fundamentales de las personas físicas respecto al tratamiento de sus datos personales y sin garantizar la libre circulación de estos datos dentro de la UE.
- b. Permitir que las empresas recopilen y utilicen libremente los datos personales de los ciudadanos sin restricciones.
- c. Regular exclusivamente el uso de datos personales por parte de grandes corporaciones, excluyendo a las pequeñas empresas y autónomos.
- d. Proteger los derechos y libertades fundamentales de las personas físicas respecto al tratamiento de sus datos personales y garantizar la libre circulación de estos datos dentro de la UE.**

3. Una empresa sudamericana que vende sus productos en Norteamérica debe cumplir con el Reglamento General de Protección de Datos:

- Verdadero
- Falso

4. Los artículos que hablan sobre sanciones en el Reglamento General de Protección de Datos se recogen en el:

- a. Capítulo III
- b. Capítulo XI
- c. Capítulo VIII**
- d. Capítulo V

5. Completa la siguiente frase:

- a. La Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales introduce disposiciones específicas relacionadas con **los derechos digitales**, la videovigilancia, el uso de datos en el ámbito laboral y **la protección de menores en entornos digitales**.

6. La Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales fue publicada el:

- a. 17 de mayo de 2016
- b. 25 de mayo de 2018
- c. 5 de diciembre de 2018**
- d. 14 de julio de 2016

7. La Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se estructura en diez títulos, seis disposiciones transitorias, veintidós disposiciones adicionales, una disposición derogatoria y dieciséis disposiciones finales:

- Verdadero
- Falso

8. Completa la siguiente frase:

- a. La evaluación de impacto sobre la protección de datos (EIPD) es un análisis que las empresas deben realizar cuando un tratamiento de datos personales puede suponer un riesgo alto para los **derechos y libertades** de las personas.

9. ¿Cuál es el principio básico de la protección de datos?

- a. La recopilación ilimitada de datos sin restricciones
- b. El almacenamiento de datos personales de forma indefinida
- c. La cesión de datos a terceros sin necesidad de autorización
- d. El consentimiento explícito**

10. ¿En qué título de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales se define el régimen sancionador, clasificando infracciones en muy graves, graves y leves?

- a. Título III
- b. Título IX**
- c. Título VIII
- d. Título V

Ejercicios de autoevaluación

Unidad de Aprendizaje 2

1. Determina si la siguiente oración es verdadera o falsa: “Según el RGPD, cualquier entidad, ya sea persona física o jurídica, que trate datos personales en el curso de sus actividades económicas o profesionales está sujeta a sus disposiciones”.

- Verdadero
- Falso

2. ¿A qué se refiere el tratamiento de datos?

- a. **A cualquier operación o conjunto de operaciones realizadas sobre datos personales.**
- b. Solo al almacenamiento de datos personales sin realizar ninguna otra acción sobre ellos.
- c. Exclusivamente al uso de datos para fines comerciales y publicitarios.
- d. A la recopilación de datos, pero sin necesidad de protegerlos ni gestionarlos adecuadamente.

3. ¿Cuál es el primer paso en el tratamiento de datos personales?

- a. Registro de los datos en bases de datos
- b. Adaptación y modificación de los datos
- c. Eliminación de datos innecesarios
- d. **Recopilación de los datos**

4. ¿Qué implica la consulta de datos en el tratamiento de información?

- a. **Acceder a los datos sin alterarlos, permitiendo su revisión y análisis.**
- b. Eliminar automáticamente los datos almacenados en una base de datos.
- c. Modificar los datos según la necesidad del negocio, sin restricciones.
- d. Compartir los datos personales con cualquier tercero sin consentimiento.

5. Un autónomo que maneja datos personales de sus clientes debe asegurarse de cumplir con la normativa de protección de datos. ¿Cuál de las siguientes afirmaciones es correcta respecto a sus obligaciones?

- a. Solo necesita obtener el consentimiento de sus clientes si almacena datos financieros o bancarios.
- b. Está obligado a permitir que los clientes accedan, rectifiquen o soliciten la eliminación de sus datos personales.**
- c. No necesita informar a la autoridad competente en caso de una brecha de seguridad, ya que es un negocio pequeño.
- d. Puede almacenar datos personales indefinidamente sin necesidad de justificar el período de conservación.

6. ¿En qué consiste la conservación de datos en el tratamiento de información?

- a. Compartir los datos con terceros sin restricciones.
- b. Eliminar los datos inmediatamente después de su recopilación.
- c. Almacenar los datos por un período determinado según su finalidad.**
- d. Modificar los datos según las necesidades del negocio.

7. Ordena la estructura de un registro de actividades de tratamiento.

- a. Actividad de tratamiento, categoría de datos, categoría de interesados, finalidad del tratamiento y base legal.**

8. ¿Por qué es recomendable designar a un delegado de protección de datos?

- a. Para gestionar el tratamiento de datos cuando es una parte clave del negocio.**
- b. Porque todos los autónomos están obligados a hacerlo.
- c. Para evitar cumplir con otras normativas de seguridad.
- d. Para encargarse de la contabilidad y otros aspectos financieros.

9. ¿Qué derecho no se incluye dentro de los derechos de los interesados en el RGPD?

- a. Derecho de acceso
- b. Derecho a la portabilidad
- c. Derecho a recibir una compensación económica**
- d. Derecho al olvido

10. ¿Por qué es importante realizar copias de seguridad de los datos de los clientes?

- a. Para compartir los datos con terceros sin autorización.
- b. Para evitar que los clientes ejerzan sus derechos sobre sus datos.
- c. Para eliminar datos antiguos sin posibilidad de recuperación.
- d. Para garantizar la recuperación de información en caso de pérdida.**

Ejercicios de autoevaluación

Unidad de Aprendizaje 3

1. ¿Qué permite el derecho a la portabilidad de los datos?

- a. **Obtener y reutilizar los datos personales en un formato estructurado para transferirlos a otro proveedor.**
- b. Eliminar cualquier dato personal almacenado por una empresa en un plazo de 30 días.
- c. Restringir el acceso a los datos personales a cualquier empresa que los esté tratando.
- d. Oponerse a la recopilación de datos personales en redes sociales.

2. Determina si la siguiente oración es verdadera o falsa: “El derecho de rectificación permite a los titulares corregir datos inexactos o erróneos”.

- Verdadero
- Falso

3. ¿Cuál de las siguientes opciones no se refiere al derecho de acceso?

- a. Permite al titular conocer si sus datos están siendo tratados y obtener información sobre ello.
- b. Da derecho a recibir una copia de los datos personales tratados por el responsable.
- c. **Permite solicitar la eliminación inmediata de los datos personales almacenados.**
- d. Facilita la transparencia y el control del individuo sobre sus datos personales.

4. Relaciona:

- b. Se permite el uso de sistemas de geolocalización para control laboral, pero los trabajadores deben ser informados previamente sobre su uso y sus derechos.
- c. Familiares y herederos pueden acceder o gestionar los contenidos digitales de una persona fallecida, salvo que esta haya indicado lo contrario. Se regula el mantenimiento o eliminación de perfiles en redes sociales.

- d. La educación debe garantizar la integración digital, promoviendo el uso seguro y responsable de la tecnología. Se incluirá en los planes de estudio la formación en competencias digitales y riesgos en línea.
- a. Se garantiza la posibilidad de corregir información que afecte el honor o la intimidad de una persona en redes sociales y medios digitales, incluyendo avisos aclaratorios en archivos de noticias.

5. **Determina si la siguiente oración es verdadera o falsa: “El artículo 88 de la LOPDGDD establece que el trabajador no puede desconectarse, aunque no esté en su jornada laboral”.**

- Verdadero
- Falso

6. **¿Qué artículo establece que los convenios colectivos pueden incluir garantías adicionales para la protección de los datos personales y derechos digitales de los trabajadores?**

- a. Artículo 96
- b. Artículo 80
- c. Artículo 89
- d. Artículo 91

7. **¿Qué tipo de sanción puede implicar una compensación económica a las víctimas de una infracción de protección de datos?**

- a. Sanción administrativa
- b. Sanción penal
- c. Sanción disciplinaria
- d. **Sanción civil**

8. **¿Cuál de las siguientes opciones no es una sanción penal en protección de datos?**

- a. Multas penales adicionales a las sanciones administrativas.
- b. **Multas económicas impuestas por organismos reguladores de protección de datos.**

- c. Penas de prisión para los responsables en casos de dolo o negligencia grave.
- d. Sanciones aplicadas cuando se detecta una conducta criminal intencionada.

9. ¿Qué acción podría reducir la severidad de una sanción impuesta a una empresa por una infracción de protección de datos?

- a. Cooperar con las autoridades durante la investigación.**
- b. No informar a los titulares de los datos sobre la brecha de seguridad.
- c. Borrar evidencias para evitar sanciones más graves.
- d. Ignorar los requerimientos de las autoridades de protección de datos.

10. ¿Cuál de los siguientes factores no influye en la determinación de la sanción por una infracción de protección de datos?

- a. La naturaleza de la infracción, incluyendo el tipo de datos comprometidos.
- b. La rapidez con la que la empresa responde para mitigar el impacto de la infracción.
- c. La cantidad de empleados que tiene la empresa infractora.**
- d. El historial de cumplimiento de la organización.

Ejercicios de autoevaluación

Unidad de Aprendizaje 4

1. ¿Qué es un delegado de protección de datos?

- a. Es un asesor externo que solo interviene en caso de una brecha de seguridad.
- b. Es un empleado responsable de supervisar las actividades de *marketing* digital.
- c. Es un profesional designado para asegurar que una organización cumpla con las leyes de protección de datos.**
- d. Es el encargado de gestionar únicamente las bases de datos comerciales de la empresa.

2. ¿Cuáles son las principales funciones del delegado de protección de datos según el RGPD y la LOPDGDD?

- a. Gestionar las campañas de *marketing* y las estrategias comerciales de la organización.
- b. Controlar el acceso físico a las instalaciones de la empresa y garantizar la seguridad informática.
- c. Elaborar informes financieros y supervisar el cumplimiento fiscal de la organización.
- d. Informar y asesorar, supervisar el cumplimiento del RGPD y actuar como intermediario con las autoridades de supervisión.**

3. Clasifica las siguientes afirmaciones en ventajas y desventajas:

Ventajas:

- c. Un DPD bien informado puede optimizar el manejo seguro de datos dentro de la empresa, estableciendo procesos más eficientes que reduzcan errores y mejoren la gestión de la información.
- e. Implementar y mantener un sistema de protección de datos adecuado requiere una gestión constante de registros, auditorías y documentación, lo que puede aumentar la carga de trabajo en la empresa.
- f. Gracias a la correcta implementación de medidas de protección de datos, la empresa puede evitar sanciones económicas severas derivadas del incumplimiento de la normativa.

Desventajas

- a. Un DPD debe estar altamente capacitado en normativas como el RGPD y la LOPDGDD, lo que puede requerir inversiones en formación y actualización constante para cumplir con las regulaciones.
- b. Adaptar los procesos internos para cumplir con la protección de datos puede generar resistencia entre los empleados, especialmente si implica cambios en la forma en que manejan la información.
- d. El DPD lleva un registro detallado de todas las actividades de procesamiento de datos, lo que permite que la empresa esté siempre lista para demostrar su cumplimiento ante auditorías o inspecciones.

4. ¿Qué formación se recomienda que tenga el delegado de protección de datos?

- a. Formación jurídica, preferiblemente en Derecho, y habilidades técnicas**
- b. Formación exclusiva en informática
- c. Experiencia en *marketing* digital
- d. Formación en administración de empresas

5. ¿Cuál de las siguientes opciones cumple con los requisitos de experiencia para un DPD?

- a. 1 año de experiencia sin formación adicional.
- b. 3 años de experiencia + 60 h de formación reconocida.**
- c. 2 años de experiencia sin formación adicional.
- d. 6 meses de experiencia + 20 h de formación reconocida.

6. ¿Qué activos deben identificarse en el análisis de riesgo de protección de datos?

- a. Exclusivamente las bases de datos digitales.
- b. Únicamente los documentos en formato físico.
- c. Tangibles e intangibles relacionados con el tratamiento de datos personales.**
- d. Solo los dispositivos físicos como servidores y ordenadores.

7. ¿Cómo se debe evaluar cada riesgo identificado?

- a. Según la probabilidad de que ocurra y el impacto potencial.**
- b. Únicamente por el impacto financiero que pueda causar.
- c. Basándose solo en experiencias previas de la empresa.
- d. Evaluando la dificultad de implementar soluciones.

8. Relaciona cada concepto con su definición.

- a. Fortalezas
 - b. Oportunidades
 - c. Debilidades
 - d. Amenazas
-
- b.** Factores externos que pueden afectar negativamente la empresa o proyecto.
 - c.** Ventajas y puntos fuertes que tiene la empresa o el proyecto.
 - d.** Factores del entorno que pueden representar ventajas o crecimiento.
 - a.** Aspectos que la empresa o el proyecto deben mejorar.

9. ¿Qué tipo de medidas pueden implementarse para mitigar los riesgos de privacidad?

- a. Implementar medidas técnicas como la encriptación y organizativas como la capacitación del personal.**
- b. Contratar a un experto externo en protección de datos.
- c. Limitar el acceso a los datos a los directivos de la empresa.
- d. Eliminar todos los registros de datos personales.

10. ¿Cuál es el objetivo de la evaluación de la necesidad y proporcionalidad?

- a. Comprobar que el tratamiento de datos cumple con los objetivos comerciales.
- b. Evaluar si los empleados conocen las políticas internas de la empresa.
- c. Validar que los datos personales no caducan.
- d. Determinar si el tratamiento de datos es necesario y si existen alternativas menos intrusivas.**

