

Solucionario / CTRG0012

Curso básico de protección de datos

Soluciones

Actividades

Test de Repaso



SOLUCIONES ACTIVIDADES

ACTIVIDAD 1

Consentimiento del interesado	Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
Datos biométricos	Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.
Datos genéticos	Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.
Destinatario	La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

Empresa	La persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.
Encargado del tratamiento	La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
Fichero	Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
Representante	La persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del Reglamento (UE) 2016/679.
Responsable del tratamiento	La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.
Tratamiento	Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

ACTIVIDAD 2

La seudonimización es un proceso de tratamiento de datos personales que se utiliza para proteger la privacidad y la identidad de las personas. Este proceso implica la sustitución de datos identificables, como nombres, direcciones o números de identificación, con pseudónimos o identificadores ficticios.

La seudonimización se realiza de tal manera que los datos ya no pueden atribuirse a una persona sin utilizar información adicional. Esta información adicional se mantiene separada y está sujeta a medidas técnicas y organizativas para garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Por ejemplo, en un centro de salud, los registros médicos de las personas pacientes podrían ser seudonimizados antes de ser utilizados en una investigación. Los nombres de las personas pacientes podrían ser reemplazados por códigos únicos, de modo que las personas investigadoras puedan analizar los datos sin saber a quién pertenecen. Sin embargo, si se necesita acceder a la información de la persona paciente, el centro de salud tendría la “clave” para revertir la seudonimización.

Es importante destacar que la seudonimización no es lo mismo que el anonimato. Aunque ambos procesos buscan proteger la privacidad de las personas, la seudonimización todavía permite la posibilidad de reidentificar a la persona si se tiene acceso a la información adicional que permite revertir el proceso. En cambio, con los datos anónimos, la reidentificación no es posible.

Si bien la seudonimización es una herramienta valiosa en la protección de datos personales, especialmente en contextos donde

se manejan grandes volúmenes de datos sensibles, es solo una de las muchas medidas que se pueden tomar para garantizar la privacidad y la seguridad de los datos personales.

SOLUCIÓN ACTIVIDAD 3

La pintora debe identificar qué datos personales está recogiendo y tratando. Esto puede incluir nombres, direcciones de envío, información financiera como los detalles de la tarjeta de crédito de las personas compradoras, y posiblemente sus preferencias artísticas.

Una vez identificados los datos personales que se están tratando, la pintora debe identificar cualquier amenaza o vulnerabilidad que pueda dar lugar a un incumplimiento de la normativa de protección de datos. Esto puede incluir la posibilidad de un ataque cibernético a su sitio web, un error humano como enviar un cuadro a la dirección incorrecta, o un fallo en los sistemas de seguridad de su plataforma de venta en línea.

Tras identificar las amenazas y vulnerabilidades, la pintora debe evaluar la probabilidad de que ocurran y la gravedad de las consecuencias si lo hacen. Por ejemplo, si su sitio web no tiene una seguridad adecuada, el riesgo de un ataque cibernético podría ser alto. La gravedad de este riesgo también sería alta, ya que podría resultar en la pérdida de confianza de las personas compradoras y en posibles sanciones legales.

Finalmente, la pintora debe identificar y evaluar las medidas que puede tomar para mitigar estos riesgos. Esto podría incluir la implementación de medidas de seguridad adicionales en su sitio web, la contratación de un servicio de cumplimiento de la normativa de protección de datos para asegurarse de que está cumpliendo con todas las leyes y regulaciones pertinentes, y la

formación en seguridad de datos para ella misma y para cualquier persona que pueda tener acceso a los datos personales de las personas compradoras.

SOLUCIONES TEST DE REPASO

1. d) Fichero
2. d) Todas las respuestas anteriores son correctas
3. d) Remunerada
4. c) Maximización de datos
5. d) Está prohibido
6. a) Obtener el consentimiento de las personas tan pronto como se hayan tratado sus datos personales
7. d) Todas las respuestas anteriores son correctas
8. c) Técnicas y organizativas
9. a) Derecho de oposición
10. c) Derecho de acceso
11. d) Seudonimización
12. d) Todas las respuestas anteriores son correctas
13. c) Un año
14. a) Tres años
15. d) Todas las respuestas anteriores son correctas

16. c) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679
17. d) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles
18. d) Dos años
19. d) Ninguna de las respuestas anteriores es correcta
20. b) Identificación de las fortalezas y habilidades