Examen de muestra

Edición 201708

Índice

Introducción

Éste es el examen de muestra de EXIN Privacy & Data Protection Foundation (PDPF.SP). Las normas y reglamentos de exámenes EXIN se aplican a este examen.

Este examen consiste en 40 preguntas de tipo test. Cada pregunta tiene un número de respuestas posibles, de las cuales sólo una es correcta.

El número máximo de puntos que se pueden obtener en este examen es de 40. Cada respuesta correcta tiene un valor de un punto. Si usted consigue 26 puntos o más, habrá aprobado el examen.

El tiempo permitido para este examen es de 60 minutos.

¡Buena suerte!

Examen de muestra

1 / 40
La obtención, almacenamiento, modificación, divulgación o difusión ilegal de datos personales es una infracción de la legislación europea.

¿Qué tipo de infracción es ésta?

A) Un delito relacionado con el contenido
B) Un delito económico
C) Un delito de propiedad intelectual
D) Un delito contra la intimidad

2 / 40
¿Cómo se relacionan la privacidad y la protección de los datos?

A) La protección de los datos es un subconjunto de la privacidad.
B) La privacidad es un subconjunto de la protección de los datos.
C) Son lo mismo.
D) No se puede tener privacidad sin la protección de los datos.

3 / 40
¿Cuál es el propósito principal del RGPD?

A) Ser una base común sobre la cual los estados miembros puedan construir sus propias leyes.
B) Hacer que los países no pertenecientes a la UE respeten el derecho a la privacidad de los individuos dentro de la UE.
C) Proteger la privacidad como un derecho humano fundamental para todos.
D) Reforzar y unificar la protección de datos para los individuos dentro de la UE.

4 / 40
El RGPD está relacionado con la protección de los datos personales.

¿Cuál es la definición de datos personales?

A) Toda información sobre una persona física identificada o identificable
B) Cualquier información que los ciudadanos europeos quisieran proteger
C) Datos que directa o indirectamente revelen el origen racial o étnico, opniones religiosas, y datos relacionados con la salud o los hábitos sexuales
D) Preservación de la confidencialidad, integridad y disponibilidad de la información

5 / 40
De acuerdo con RGPD, ¿qué categoría de datos personales se consideran como sensibles?

A) Los detalles de la tarjeta de crédito
B) El número de la seguridad social
C) El número del pasaporte
D) La afiliación sindical

6 / 40
Según el RGPD, ¿cuál es la definición del "tratamiento" de datos personales?

A) Cualquier operación que se puede realizar sobre datos personales
B) Cualquier operación que se puede realizar sobre datos personales, excepto la eliminación y la destrucción
C) Sólo las operaciones en las que los datos se comparten en las redes sociales o son tranferidos por correo electrónico o de otra forma a través de internet
D) Sólo las operaciones en las que los datos personales se utilizan para los fines para los que se obtuvieron

7 / 40
Una autoridad pública independiente establecida por un Estado Miembro de conformidad con el artículo 51.

¿Qué rol en la protección de datos se define aquí?

A) Responsable
B) Encargado
C) Autoridad de control
D) Tercero

8 / 40
El "consentimiento informado" es una base legal para tratar datos personales en virtud del RGPD. Los fines del tratamiento para el que se da consentimiento deberían estar documentados.

¿En qué momento del tratamiento se debería obtener el consentimiento del interesado?

A) Después de que se presenten los fines específicos del tratamiento y antes de que se obtengan los datos personales.
B) Antes de que se traten los datos personales.
C) Antes de que los datos personales se publiquen o difundan.
D) Antes de que se conciban y presenten los fines específicos del tratamiento.

9 / 40
El RGPD está basado en los principios de proporcionalidad y subsidiariedad.

¿Cuál es el significado de "proporcionalidad" en este contexto?

A) Los datos personales sólo se pueden tratar de acuerdo a los fines específicos del tratamiento.
B) Los datos personales no se pueden reutilizar sin el consentimiento explícito e informado.
C) Los datos personales sólo se podrían tratar en caso de que no haya otros medios para lograr los fines del tratamiento.
D) Los datos personales deben ser adecuados, pertinentes y limitados en relación a los fines del tratamiento.

10 / 40
El tratamiento de los datos personales debe cumplir las reglas generales de calidad.

¿Cuál es una de estas reglas definidas por el RGPD?

A) Los datos tratados deben ser archivados.
B) Los datos tratados deber ser encriptados.
C) Los datos tratados deben ser indexados.
D) Los datos tratados deben ser pertinentes.

11 / 40
Cada vez que se tratan datos personales, se debe comprobar la proporcionalidad y la subsidiariedad.

¿Cuál es el requisito para que se traten los datos personales?

A) Deber manejarse por el menor número posible de empleados y ellos deben trabajar para el responsable o un afiliado.
B) Debe limitarse siempre a lo que es necesario para alcanzar los objetivos definidos y debe limitarse a los datos menos "intrusivos".
C) Debe limitarse a un tamaño de almacenamiento predefinido y el sistema que se utilice debe estar financiado por el responsable.
D) Debe utilizarse para el menor número posible de fines del tratamiento y esto no se puede hacer fuera de las instalaciones del encargado.

12 / 40
"El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que (...) sólo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento."

¿Qué término del RGPD se define aquí?

A) Cumplimiento
B) Protección de datos por defecto
C) Protección de datos desde el diseño
D) Protección integrada

13 / 40
¿Cuál es el término usado en el RGPD para la divulgación de, o el acceso a, datos personales no autorizada?

A) Violación de la confidencialidad
B) Violación de la seguridad de los datos
C) Incidente
D) Incidente de seguridad

14 / 40
Se ha comprobado que se ha producido una violación de la seguridad de los datos personales sensibles.

¿A quién se le debe reportar en última instancia de acuerdo con el RGPD?

A) Delegado de protección de datos (DPD)
B) La autoridad de control
C) El director del departamento
D) La policía

15 / 40
Mientras se está realizando una copia de seguridad, el disco del servidor se daña. Tanto los datos como la copia de seguridad se han perdido. El disco contenía datos personales pero no datos sensibles.

¿De qué tipo de incidente se trata?

A) Violación de la seguridad de los datos
B) Violación de la seguridad
C) Incidente de Seguridad

16 / 40
Alguien que trabaja para un sindicato se llevó un borrador de un boletín a casa para terminarlo para los miembros. La memoria USB que contenía el borrador y la lista de correo se perdió.

¿A quién(es), entre otros, habría que reportar esta violación de la seguridad de los datos?

A) A todos los miembros de la lista de correo
B) A la junta directiva del sindicato
C) A la policía

17 / 40
Una organización de servicios sociales planea diseñar una nueva base de datos para administrar sus clientes y la atención que necesitan.

Para solicitar el permiso a la autoridad de control, ¿cuál es uno de los primeros pasos importantes que se deben tomar?

A) Obtener datos acerca de los clientes y la cantidad y tipo de atención que necesitan y reciben.
B) Realizar una evaluación de impacto en la protección de datos (EIPD) para evaluar los riesgos del tratamiento previsto.
C) Obtener el consentimiento de los clientes para el tratamiento previsto de sus datos personales.

18 / 40
¿En qué caso se debería notificar siempre a los interesados de una violación de la seguridad de los datos?

A) La violación de la seguridad de los datos no condujo a una probabilidad significativa de consecuencias perjudiciales para la protección de los datos personales.
B) Los datos personales fueron tratados en una instalación del encargado que no está ubicada dentro de las fronteras de la UE.
C) Los datos personales fueron tratados por una parte que todavía no había firmado un contrato vinculante con el responsable.
D) El sistema en el que se trataban los datos personales fue atacado, causando daños a sus dispositivos de almacenamiento.

19 / 40
Un responsable holandés ha contratado el tratamiento de los datos personales sensibles a un encargado del tratamiento en un país del norte de África, sin consultar a la autoridad de control. Fue descubierto y penalizado por la autoridad de control. Seis meses más tarde la misma autoridad descubrió que el responsable es culpable de nuevo de la misma transgresión para otra operación de tratamiento.

¿Cuál es la penalización máxima que la autoridad puede imponer en este caso?

A) € 750.000
B) € 1.230.000
C) € 10.000 o 2% del volumen de negocio total anual global con un mínimo de € 10.000.000, el de mayor cuantía
D) € 20.000.000 o 4% del volumen de negocio total anual global con un mínimo de € 20.000.000, el de mayor cuantía

20 / 40
A las autoridades de control se les asignan una serie de responsabilidades encaminadas a garantizar el cumplimiento de los reglamentos de protección de datos.

¿Cuál es una de esas responsabilidades?

A) Evaluar códigos de conducta para sectores específicos relacionados con el tratamiento de los datos personales.
B) Definir un conjunto mínimo de medidas que se deben tomar para proteger los datos personales.
C) Investigar todas las violaciones de la seguridad de los datos de las que hayan sido notificados.
D) Revisar los contratos y las NCV sobre el cumplimiento de los reglamentos.

21 / 40
Una asociación religiosa quiere compartir datos personales con su autoridad religiosa en un país no europeo para cumplir con una solicitud legal del gobierno involucrado.

¿Qué regulación del RGPD se aplica en este caso?

A) Como una excepción, a una asociación religiosa se le permite el tratamiento de datos sensibles que revelan convicciones religiosas.
B) No es lícito transferir datos personales fuera de la UE como respuesta a un requerimiento legal de un tercer país.
C) El tratamiento es lícito siempre y cuando se haya adquirido un consentimiento específico e inequívoco del interesado.
D) El tratamiento de datos personales fuera de la UE está permitido usando las clásulas modelo de contrato diseñadas por la Comisión Europea.

22 / 40
El 12 de Julio del 2016, la Comisión Europea implementó una resolución en relación a la transferencia de datos personales con EE.UU (Escudo de la Privacidad UE-EE.UU.).

En términos del RGPD, ¿qué tipo de resolución es ésta?

A) Una decisión de adecuación
B) Un decreto de excepción
C) Un contrato vinculante estándar
D) Un tratado que sustituye al RGPD

23 / 40
Las normas corporativas vinculantes son un medio para que las organizaciones alivien su carga administrativa al cumplir con el RGPD.

¿Cómo les ayudan estas normas?

A) Les permiten tener contratos con terceros con todas las partes involucradas en el extranjero.
B) Les permiten dejar que terceros países fuera del Espacio Económico Europeo traten datos personales.
C) Evitan la necesidad de dirigirse a cada autoridad de control en la UE por separado.
D) Les evitan tener que pedir permiso a una autoridad de control para el tratamiento de datos una vez se aceptan sus NCV.

24 / 40
En caso de que un contratista contrate el tratamiento de datos personales, las partes celebrarán un contrato por escrito. Este contrato establece el objeto y la duración del tratamiento, la naturaleza y los fines del tratamiento, el tipo de datos personales y las categorías de los interesados.

¿Qué otro aspecto debe regirse por este contrato escrito?

A) La responsabilidad del encargado
B) La obligación de notificación de la violación de la seguridad de los datos
C) Las obligaciones y los derechos del responsable
D) La obligación de que los encargados deben cooperar con la autoridad de control

25 / 40
¿Qué se debería hacer para que un responsable pueda externalizar el tratamiento de datos personales a un encargado?

A) El responsable debe pedir permiso a la autoridad de control para externalizar el tratamiento de los datos.
B) El responsable debe preguntar a la autoridad de control si el contrato escrito acordado cumple con los reglamentos.
C) El responsable y el encargado deben redactar y firmar un contrato escrito garantizando la confidencialidad de los datos.
D) El encargado debe demostrar al Responsable que se cumplen todas las demandas acordadds en el Acuerdo de Nivel de Servicio (SLA).

26 / 40
La protección de datos desde el diseño, tal como está descrito en el artículo 25 del RGPD, se basa en siete principios básicos. Uno de estos se suele denominar "Funcionalidad - Suma-Positiva, no Suma-Cero".

¿Cuál es la esencia de este principio?

A) Las normas de seguridad aplicadas deben asegurar la confidencialidad, integridad y disponibilidad de los datos a lo largo de su ciclo de vida.
B) Si diferentes tipos de objetivos legítimos son contradictorios, los objetivos de privacidad deben tener prioridad sobre los objetivos de seguridad.
C) Al integrar la privacidad dentro de una determinada tecnología, proceso o sistema, debería hacerse de tal manera que la funcionalidad completa no se vea afectada.
D) Siempre que sea posible, se deberían realizar y publicar evaluaciones detalladas del impacto en la privacidad y de riesgos, documentando claramente los riesgos de privacidad.

27 / 40
A menudo, el personal que trabaja con datos personales considera la privacidad y la seguridad de la información como cuestiones separadas.

¿Por qué esto está mal?

A) La privacidad no se puede garantizar sin identificar, implementar y monitorizar las medidas apropiadas de seguridad de la información.
B) La autoridad de control espera que se integren los roles de delegado de protección de Datos y responsable de la seguridad de la información.
C) Los reglamentos identifican medidas de seguridad de la información que se deben tomar antes de que se permita la manipulación de datos personales.

28 / 40
Uno de los objetivos de la evaluación de impacto relativa a la protección de datos (EIPD) es "fortalecer la confianza de los clientes o de los ciudadanos en la forma que se tratan los datos personales y se respeta la privacidad".

¿Cómo un EIPD puede "fortalecer la confianza"?

A) La organización minimiza el riesgo de costosos ajustes en los procesos o rediseño de sistemas en una etapa posterior.
B) La organización evita el no cumplimiento con el RGPD y minimiza el riesgo de multas.
C) La organización demuestra que se toma en serio la privacidad y busca el cumplimiento con el RGPD.

29 / 40
¿Cuál es el propósito de una auditoría de privacidad por parte de una autoridad de control?

A) Cumplir la obligación del RGPD de implementar medidas técnicas y organizativas apropiadas para la protección de datos.
B) Supervisar y ejecutar la aplicación del RGPD evaluando que el tratamiento se realice de conformidad con el RGPD.
C) Asesorar al responsable en la mitigación de los riesgos de la privacidad para proteger al responsable de reclamanciones de responsabilidad por el incumplimiento del RGPD.

30 / 40
¿Qué describe **mejor** el principio de minimización de datos?

A) Se debe tener cuidado de obtener el menor número de datos posible para proteger los intereses y la privacidad de los interesados.
B) Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
C) Con el fin de mantener los datos manejables, se debe almacenar de tal manera que requiera una cantidad mínima de almacenamiento.
D) El número de elementos que son obtenidos por interesado no debe exceder el límite superior establecido por la autoridad de control.

31 / 40
Las cookies de sesión son uno de los tipos más comunes de cookie.

¿Qué hace una cookie de sesión?

A) Contiene información sobre lo que se está haciendo, por ejemplo, los productos que se seleccionan en una tienda online antes de que realmente se haga el pedido.
B) Revela el historial del navegador, de manera que otros sitios web pueden averiguar qué sitios web se han visitado antes de llegar allí.
C) Almacena el historial del navegador, de manera que se puede rastrear dónde se ha estado en la red y volver a visitar esos sitios si se desea.
D) Obtiene los datos personales, por lo que el sitio web puede saludar por el nombre y reutilizar su configuración cuando se regrese.

32 / 40
Algunas veces los sitios web monitorizan a los visitantes y almacenan su información con fines de marketing.

¿Está el sitio web obligado a notificar al vistante de que su información se está utilizando con fines de marketing?

A) Sí
B) No

33 / 40
Una compañía puede presentarse como un experto en un área concreta de especialización haciendo uso de las redes sociales.

¿Cuál es la **mejor** forma de demostrar la especialización en un campo específico?

A) Publicando información sobre la compañía en las Redes Sociales.
B) Respondiendo activamente las preguntas sobre su producto en las Redes Sociales.
C) Publicando cómo el producto del competidor es inferior al de la compañía.
D) Publicando los productos que la compañía está desarrollando.

34 / 40
Ha ocurrido una violación de la seguridad de los datos en un sistema de información que también guarda datos personales.

¿Qué es lo primero que debe hacer el responsable?

A) Determinar si la violación de la seguridad de los datos puede haber ocasionado una pérdida o un tratamiento ilícito de los datos personales.
B) Evaluar el riesgo de efectos adversos para los interesados utilizando una evaluación del impacto en la protección de datos (EIPD).
C) Evaluar si los datos personales de una naturaleza sensible han sido o podrían haber sido tratados ilícitamente.
D) Informar de la violación inmediatamente a la Autoridad de Control pertinente.

35 / 40
La palabra "privacidad" no se menciona en el RGPD.

¿Cómo se relaciona la "privacidad" con la "protección de datos"?

A) La protección de datos es un conjunto de normas y reglas sobre el tratamiento de datos personales. La privacidad es el resultado de la protección de datos.
B) La privacidad es el derecho a ser protegido de interferencias en asuntos personales. La protección de los datos es el medio para implementar esa protección.
C) La privacidad es el derecho a mantener en secreto los asuntos personales. La protección de los datos es el derecho a mantener en secreto los datos personales.
D) Los términos "privacidad" y "protección de datos" son intercambiables. No hay una diferencia real en el significado.

36 / 40
El reglamento (UE) 2016/679, conocido como el RGPD, deroga una directiva UE anterior.

¿Qué directiva está siendo derogada (sustituida)?

A) Directiva 2002/58/CE del 12 de julio del 2002
B) Directiva 2006/24/CE del 15 de marzo del 2006
C) Directiva 95/46/CE del 24 de octubre de 1995
D) Directiva 97/66/CE del 15 de diciembre de 1997

37 / 40
¿Qué derecho de los Interesados se define explícitamente en el RGPD?

A) Se debe proporcionar una copia de los datos personales en el formato solicitado por el Interesado.
B) Acceso a los datos personales sin coste alguno para el Interesado.
C) Los datos personales siempre deben ser modificados a petición del Interesado.
D) Los datos personales deben ser eliminados siempre que el Interesado lo solicite.

38 / 40
El RGPD distingue los "datos personales sensibles" como una categoría especial de datos personales.

¿Cuál es un ejemplo de dichos datos?

A) Una cita en un hospital con un médico especialista
B) Un Código Internacional de Cuenta Bancaria (IBAN)
C) Una suscripción a una revista científica para la política
D) La pertenencia a una asociación interprofesional

39 / 40
¿Qué rol en la protección de datos determina los fines y los medios del tratamiento de datos personales?

A) Responsable
B) Delegado de protección de datos
C) Encargado

40 / 40
¿Qué información se considera como datos personales de acuerdo con el RGPD?

A) Información sobre una persona, que podría perjudicar la privacidad de esa persona, incluso cuando es falsa.
B) Cualquier información sobre una persona física identificable.
C) Información, sobre una persona física identificable, que esté digitalizada.

Soluciones

1 / 40
La obtención, almacenamiento, modificación, divulgación o difusión ilegal de datos personales es una infracción de la legislación europea.

¿Qué tipo de infracción es ésta?

A) Un delito relacionado con el contenido
B) Un delito económico
C) Un delito de propiedad intelectual
D) Un delito contra la intimidad

A) Incorrecto. Un delito relacionado con el contenido se refiere a la difusión de declaraciones racistas, pornografía (infantil) o información que incite a la violencia.
B) Incorrecto. Los delitos económicos se refieren al acceso no autorizado a sistemas (hackeo, distribución de virus, etc.) espionaje informático, falsificación y fraude.
C) Incorrecto. Los delitos de propiedad intelectual atañan a las violaciones del copyright y derechos relacionados.
D) Correcto. Cualquier tipo de tratamiento ilegal de datos personales es un delito. Fuente: Ninguna. Se considera conocimiento básico.

2 / 40
¿Cómo se relacionan la privacidad y la protección de los datos?

A) La protección de los datos es un subconjunto de la privacidad.
B) La privacidad es un subconjunto de la protección de los datos.
C) Son lo mismo.
D) No se puede tener privacidad sin la protección de los datos.

A) Incorrecto. La privacidad abarca muchos conceptos como la privacidad espacial, relacional, corporal y de la información. La protección de los datos no tiene relación con algunos de estos.
B) Incorrecto. La privacidad abarca muchos conceptos como la privacidad espacial, relacional, corporal y de la información. La protección de los datos ayuda a garantizar algunos de estos.
C) Incorrecto. La protección de los datos no tiene nada que ver, por ejemplo, con la privacidad espacial.
D) Correcto. Para los gobiernos y las compañías una buena protección de la privacidad es difícil de conseguir. Sin una regulación clara en la protección de datos no habría ninguna privacidad. Fuente: White Paper – Privacy, Personal Data and the GDPR - §1.3 Definitions y RGPD consideraciones (13)

3 / 40
¿Cuál es el propósito principal del RGPD?

A) Ser una base común sobre la cual los estados miembros puedan construir sus propias leyes.
B) Hacer que los países no pertenecientes a la UE respeten el derecho a la privacidad de los individuos dentro de la UE.
C) Proteger la privacidad como un derecho humano fundamental para todos.
D) Reforzar y unificar la protección de datos para los individuos dentro de la UE.

A) Incorrecto. El RGPD es un reglamento, lo que significa que derogará las leyes de la protección de datos en los estados miembros.
B) Incorrecto. Su objetivo principal está dirigido a defirnir los derechos de protección de los datos de individuos dentro de la UE.
C) Incorrecto. El RGPD establece explícitamente que la protección de datos es un derecho fundamental, pero su alcance se limita a los individuos dentro de la UE.
D) Correcto. El alcance del RGPD se limita a la protección de los datos como un derecho de los individuos dentro de la UE y tiene por objeto armonizar las normas para ello dentro de la UE. Fuente: EU GDPR, A pocket guide – Introduction y RGPD consideraciones (1) a (13)

4 / 40
El RGPD está relacionado con la protección de los datos personales.

¿Cuál es la definición de datos personales?

A) Toda información sobre una persona física identificada o identificable
B) Cualquier información que los ciudadanos europeos quisieran proteger
C) Datos que directa o indirectamente revelen el origen racial o étnico, opniones religiosas, y datos relacionados con la salud o los hábitos sexuales
D) Preservación de la confidencialidad, integridad y disponibilidad de la información

A) Correcto. Esta es la definición oficial de datos personales. Fuente: EU GDPR, A pocket guide - Chapter 2 Terms and definitions y RGPD 2016/679 Artículo 4: Definiciones.
B) Incorrecto. Esta definición es demasiado genérica.
C) Incorrecto. Esta es la definición de datos sensibles no de los datos personales en general.
D) Incorrecto. Esta es la definición de la seguridad de la información de la ISO/IEC 27000:2014.

5 / 40
De acuerdo con RGPD, ¿qué categoría de datos personales se consideran como sensibles?

A) Los detalles de la tarjeta de crédito
B) El número de la seguridad social
C) El número del pasaporte
D) La afiliación sindical

A) Incorrecto. Los detalles de la tarjeta de crédito no son datos sensibles de acuerdo con el RGPD.
B) Incorrecto. Un número de la seguridad social no es un dato sensible de acuerdo con el RGPD.
C) Incorrecto. Los detalles del pasaporte no son datos sensibles de acuerdo con el RGPD.
D) Correcto. La afiliación sindical es un dato sensible. Fuente: RGPD art. 9 Tratamiento de categorías especiales de datos personales.

6 / 40
Según el RGPD, ¿cuál es la definición del "tratamiento" de datos personales?

A) Cualquier operación que se puede realizar sobre datos personales
B) Cualquier operación que se puede realizar sobre datos personales, excepto la eliminación y la destrucción
C) Sólo las operaciones en las que los datos se comparten en las redes sociales o son tranferidos por correo electrónico o de otra forma a través de internet
D) Sólo las operaciones en las que los datos personales se utilizan para los fines para los que se obtuvieron

A) Correcto. Fuente: RGPD art. 4 (2)
B) Incorrecto. "Tratamiento" significa cualquier operación que se realiza sobre datos personales.
C) Incorrecto. "Tratamiento" significa cualquier operación que se realiza sobre datos personales.
D) Incorrecto. "Tratamiento" significa cualquier operación que se realiza sobre datos personales.

7 / 40
Una autoridad pública independiente establecida por un Estado Miembro de conformidad con el artículo 51.

¿Qué rol en la protección de datos se define aquí?

A) Responsable
B) Encargado
C) Autoridad de control
D) Tercero

A) Incorrecto. Fuente: RGPD 2016/679, Artículo 4.
B) Incorrecto. Fuente: RGPD 2016/679, Artículo 4.
C) Correcto. Fuente: RGPD 2016/679, Artículo 4 y Artículo 51.
D) Incorrecto. Fuente: RGPD 2016/679, Artículo 4.

8 / 40
El "consentimiento informado" es una base legal para tratar datos personales en virtud del RGPD. Los fines del tratamiento para el que se da consentimiento deberían estar documentados.

¿En qué momento del tratamiento se debería obtener el consentimiento del interesado?

A) Después de que se presenten los fines específicos del tratamiento y antes de que se obtengan los datos personales.
B) Antes de que se traten los datos personales.
C) Antes de que los datos personales se publiquen o difundan.
D) Antes de que se conciban y presenten los fines específicos del tratamiento.

A) Correcto. El consentimiento sólo puede ser informado después de que se presenten los fines específicos del tratamiento al interesado. Fuente: RGPD considerandos (32), (42).
B) Incorrecto. La obtención de datos personales es "tratamiento" y como tal necesita un consentimiento informado del interesado.
C) Incorrecto. Publicar y difundur datos personales es "tratamiento" y como tal necesita un consentimiento informado del interesado.
D) Incorrecto. El consentimiento sólo puede ser informado después de que los fines específicos del tratamiento se presenten al interesado.

9 / 40
El RGPD está basado en los principios de proporcionalidad y subsidiariedad.

¿Cuál es el significado de "proporcionalidad" en este contexto?

A) Los datos personales sólo se pueden tratar de acuerdo a los fines específicos del tratamiento.
B) Los datos personales no se pueden reutilizar sin el consentimiento explícito e informado.
C) Los datos personales sólo se podrían tratar en caso de que no haya otros medios para lograr los fines del tratamiento.
D) Los datos personales deben ser adecuados, pertinentes y limitados en relación a los fines del tratamiento.

A) Incorrecto. Esta es una de las limitaciones legales.
B) Incorrecto. Esta es una de las limitaciones legales.
C) Incorrecto. Esta es la definición de subsidiariedad.
D) Correcto. Fuente: White Paper – Privacy, Personal Data and the GDPR - § 3.1.2 Proportionality and subsidiarity y RGPD art.5(1.c), y RGPD art. 35 (7).

10 / 40
El tratamiento de los datos personales debe cumplir las reglas generales de calidad.

¿Cuál es una de estas reglas definidas por el RGPD?

A) Los datos tratados deben ser archivados.
B) Los datos tratados deber ser encriptados.
C) Los datos tratados deben ser indexados.
D) Los datos tratados deben ser pertinentes.

A) Incorrecto. Tal requisito no lo define el RGPD.
B) Incorrecto. Tal requisito no lo define el RGPD.
C) Incorrecto. Tal requisito no lo define el RGPD.
D) Correcto. Este requisito lo define el RGPD. Fuente: White Paper – Privacy, Personal Data and the GDPR - § 3.1.2 Proportionality and subsidiarity y RGPD artículo 5(1.c) Principios relativos al tratamiento

11 / 40
Cada vez que se tratan datos personales, se debe comprobar la proporcionalidad y la subsidiariedad.

¿Cuál es el requisito para que se traten los datos personales?

A) Deber manejarse por el menor número posible de empleados y ellos deben trabajar para el responsable o un afiliado.
B) Debe limitarse siempre a lo que es necesario para alcanzar los objetivos definidos y debe limitarse a los datos menos "intrusivos".
C) Debe limitarse a un tamaño de almacenamiento predefinido y el sistema que se utilice debe estar financiado por el responsable.
D) Debe utilizarse para el menor número posible de fines del tratamiento y esto no se puede hacer fuera de las instalaciones del encargado.

A) Incorrecto. El número de empleados o su afiliación a alguna filial no tiene nada que ver con estos términos.
B) Correcto. Estos términos significan que no se obtienen más datos de los necesarios para alcanzar objetivo(s) predefinidos, y siempre se intenta utilizar datos que tengan el menor impacto en la privacidad del Interesado. Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation – Lawful processing y RGPD consideraciones (156), artículo 5 principios y artículo 35(7.b)
C) Incorrecto. El tamaño del almacenamiento y quién financia los sistemas que se utilizan no tiene nada que ver con estos términos.
D) Incorrecto. Siempre y cuando el Interesado dé su consentimiento el número de objetivos no está explícitamente restringido, ni tampoco su ubicación.

12 / 40
"El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que (...) sólo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento."

¿Qué término del RGPD se define aquí?

A) Cumplimiento
B) Protección de datos por defecto
C) Protección de datos desde el diseño
D) Protección integrada

A) Incorrecto. El cumplimiento es el estado o el hecho de conformidad, o satisfacer las reglas y las normas.
B) Correcto. Por defecto se deben tratar los mínimos datos personales por el periodo de tiempo más corto posible, utilizando las mejores medidas de seguridad posibles para evitar el acceso no autorizado. Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data protection by design and by default y RGPD art.20 (2).
C) Incorrecto. La protección de datos desde el diseño hace referencia a un diseño que incluye medidas apropiadas para implementar los principios de protección de datos.
D) Incorrecto. La protección de datos integrada es el resultado de la protección de datos desde el diseño.

13 / 40
¿Cuál es el término usado en el RGPD para la divulgación de, o el acceso a, datos personales no autorizada?

A) Violación de la confidencialidad
B) Violación de la seguridad de los datos
C) Incidente
D) Incidente de seguridad

A) Incorrecto. El RGPD utiliza el término violación de la seguridad de los datos. No todas las violaciones de la seguridad de los datos son una violación de la confidencialidad.
B) Correcto. Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches y RGPD artículo 4 (12)
C) Incorrecto. RGPD utiliza el término violación de la seguridad de los datos. No todos los incidentes son una violación de la seguridad de los datos.
D) Incorrecto. El RGPD utiliza el término violación de la seguridad de los datos. No todos los incidentes de seguridad son una violación de la seguridad de los datos.

14 / 40
Se ha comprobado que se ha producido una violación de la seguridad de los datos personales sensibles.

¿A quién se le debe reportar en última instancia de acuerdo con el RGPD?

A) Delegado de protección de datos (DPD)
B) La autoridad de control
C) El director del departamento
D) La policía

A) Incorrecto. Aunque podría ser reportado a un DPD interno, en última instancia debe ser reportado a la autoridad de control.
B) Correcto. Las violaciones de la seguridad de los datos deben ser reportadas a la autoridad de control si tienen un impacto significativo en la seguridad del interesado o de sus datos personales. Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation Data breaches & GDPR article 4 (12) y RGPD artículo 33 Notificación de una violación de la seguridad de los datos personales a la autoridad de control.
C) Incorrecto. Aunque podría ser reportado al director, en última instancia debe ser reportado a la autoridad de control.
D) Incorrecto. Las violaciones de la seguridad de los datos no necesariamente tienen que ser reportadas a la policía, pero en última instancia debe ser reportado a la autoridad de control.

15 / 40
Mientras se está realizando una copia de seguridad, el disco del servidor se daña. Tanto los datos como la copia de seguridad se han perdido. El disco contenía datos personales pero no datos sensibles.

¿De qué tipo de incidente se trata?

A) Violación de la seguridad de los datos
B) Violación de la seguridad
C) Incidente de Seguridad

A) Correcto. Los datos personales irrecuperablemente perdidos se consideran como tratamiento no autorizado, lo que lo convierte en una violación de la seguridad de los datos. Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches y RGPD Sección 1, Artículo 4, Definiciones.
B) Incorrecto. Los datos personales irrecuperablemente perdidos se consideran como tratamiento no autorizado, lo que lo convierte en una violación de la seguridad de los datos.
C) Incorrecto. Los datos personales irrecuperablemente perdidos se consideran como tratamiento no autorizado, lo que lo convierte en una violación de la seguridad de los datos.

16 / 40
Alguien que trabaja para un sindicato se llevó un borrador de un boletín a casa para terminarlo para los miembros. La memoria USB que contenía el borrador y la lista de correo se perdió.

¿A quién(es), entre otros, habría que reportar esta violación de la seguridad de los datos?

A) A todos los miembros de la lista de correo
B) A la junta directiva del sindicato
C) A la policía

A) Correcto. Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches y RGPD artículo 34 Notificación del Interesado.
B) Incorrecto. Estos son datos sensibles, por lo que esta pérdida debe ser reportada tanto a la autoridad de privacidad como a los interesados.
C) Incorrecto. Estos son datos sensibles, por lo que esta pérdida debe ser reportada tanto a la autoridad de privacidad como a los interesados.

.
17 / 40
Una organización de servicios sociales planea diseñar una nueva base de datos para administrar sus clientes y la atención que necesitan.

Para solicitar el permiso a la autoridad de control, ¿cuál es uno de los primeros pasos importantes que se deben tomar?

A) Obtener datos acerca de los clientes y la cantidad y tipo de atención que necesitan y reciben.
B) Realizar una evaluación de impacto en la protección de datos (EIPD) para evaluar los riesgos del tratamiento previsto.
C) Obtener el consentimiento de los clientes para el tratamiento previsto de sus datos personales.

A) Incorrecto. La obtención de datos personales médicos es por definición "tratamiento de datos sensibles". Se necesita de antemano el permiso de la autoridad de control y del interesado.
B) Correcto. Cuando se pide el consentimiento para tratar los datos, el interesado "debe tener conocimiento de los riesgos, las normas, las garantías y los derechos..." Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation – Consent y RGPD considerando (39).). Una EIPD es necesaria para evaluar esos riesgos y garantías.
C) Incorrecto. Cuando se pide el consentimiento para tratar los datos, el interesado "debe tener conocimiento de los riesgos, las normas, las garantías y los derechos..." Una EIP es necesaria para evaluar esos riesgos y garantías.

18 / 40
¿En qué caso se debería notificar siempre a los interesados de una violación de la seguridad de los datos?

A) La violación de la seguridad de los datos no condujo a una probabilidad significativa de consecuencias perjudiciales para la protección de los datos personales.
B) Los datos personales fueron tratados en una instalación del encargado que no está ubicada dentro de las fronteras de la UE.
C) Los datos personales fueron tratados por una parte que todavía no había firmado un contrato vinculante con el responsable.
D) El sistema en el que se trataban los datos personales fue atacado, causando daños a sus dispositivos de almacenamiento.

A) Incorrecto. Si no hay un impacto negativo (potencial) significativo sobre los Interesados, no hay ninguna obligación de notificarles de la violación de la seguridad de los datos. Sin embargo se debería considerar.
B) Incorrecto. La ubicación donde se procesan los datos carece de importancia para la obligación de notificar a los Interesados de las violaciones de la seguridad de los datos.
C) Correcto. Cualquier situación en la que los datos personales sean tratados por otra parte distinta del responsable sin un contrato vinculante que garantice el cumplimiento del RGPD siempre se considera una violación de la seguridad de los datos. Fuente: White Paper – Privacy, Personal Data and the GDPR - § 5.2 Procedures on how to act when a data breach occurs y RGPD artículo 28(3) encargado del tratamiento
D) Incorrecto. El daño a los dispositivos de almacenamiento hará que el acceso a los datos sea difícil o incluso imposible, pero no implica un tratamiento ilegal. El tratamiento podría llegar a ser totalmente imposible en este caso en particular.

19 / 40
Un responsable holandés ha contratado el tratamiento de los datos personales sensibles a un encargado del tratamiento en un país del norte de África, sin consultar a la autoridad de control. Fue descubierto y penalizado por la autoridad de control. Seis meses más tarde la misma autoridad descubrió que el responsable es culpable de nuevo de la misma transgresión para otra operación de tratamiento.

¿Cuál es la penalización máxima que la autoridad puede imponer en este caso?

A) € 750.000
B) € 1.230.000
C) € 10.000.000 o 2% del volumen de negocio total anual global con un mínimo de € 10.000.000, el de mayor cuantía
D) € 20.000.000 o 4% del volumen de negocio total anual global con un mínimo de € 20.000.000, el de mayor cuantía

A) Incorrecto. De acuerdo con el RGPD art. 83.3, la multa máxima es de € 20.000.000 o 4% del volumen de negocio total anual global con un mínimo de € 20.000.000, el de mayor cuantía
B) Incorrecto. De acuerdo con el RGPD art. 83.3, la multa máxima es de € 20.000.000 o 4% del volumen de negocio total anual global con un mínimo de € 20.000.000, el de mayor cuantía
C) Incorrecto. De acuerdo con el RGPD art. 83.3, la multa máxima es de € 20.000.000 o 4% del volumen de negocio total anual global con un mínimo de € 20.000.000, el de mayor cuantía
D) Correcto. Éste es el máximo para una violación. Fuente: White Paper – Privacy, Personal Data and the GDPR - §7.3.3 General conditions for imposing administrative fines y RGPD art. 83.3.

20 / 40
A las autoridades de control se les asignan una serie de responsabilidades encaminadas a garantizar el cumplimiento de los reglamentos de protección de datos.

¿Cuál es una de esas responsabilidades?

A) Evaluar códigos de conducta para sectores específicos relacionados con el tratamiento de los datos personales.
B) Definir un conjunto mínimo de medidas que se deben tomar para proteger los datos personales.
C) Investigar todas las violaciones de la seguridad de los datos de las que hayan sido notificados.
D) Revisar los contratos y las NCV sobre el cumplimiento de los reglamentos.

A) Correcto. Una de las responsabilidades de la autoridad de control es proporcionar asesoramiento general sobre cómo cumplir con los reglamentos. Fuente: White Paper – Privacy, Personal Data and the GDPR - §7.1.4 To set standards y RGPD artículo 57(1.m.p) Funciones, dentro de la Sección 2 Competencia, funciones y poderes
B) Incorrecto. Una autoridad de control proporcionará asesoriamiento general en lo que consideran un nivel de seguridad apropiado. Sin embargo, no dirán las medidas específicas que se necesitan tomar para alcanzar ese nivel. Incluso si quisieran no podrían, porque simplemente no hay una única solución.
C) Incorrecto. Las autoridades de control no tienen la obligación, ni la capacidad de investigar todas las violaciones de la seguridad de los datos que conocen. Pero sí investigarán aquellas que consideren significativas o dignas de mención.
D) Incorrecto. Una autoridad de control no es un consejo jurídico. No revisan los contratos ni las Normas Corporativas Vinculantes. Sin embargo, en el curso de una investigación podrían echar un vistazo a un contrato específico o conjunto de NCV.

21 / 40
Una asociación religiosa quiere compartir datos personales con su autoridad religiosa en un país no europeo para cumplir con una solicitud legal del gobierno involucrado.

¿Qué regulación del RGPD se aplica en este caso?

A) Como una excepción, a una asociación religiosa se le permite el tratamiento de datos sensibles que revelan convicciones religiosas.
B) No es lícito transferir datos personales fuera de la UE como respuesta a un requerimiento legal de un tercer país.
C) El tratamiento es lícito siempre y cuando se haya adquirido un consentimiento específico e inequívoco del interesado.
D) El tratamiento de datos personales fuera de la UE está permitido usando las clásulas modelo de contrato diseñadas por la Comisión Europea.

A) Incorrecto. Las asociaciones religiosas tienen permitido tratar datos personales relacionados con miembros antiguos y actuales, pero no es lícito transferir datos personales fuera de la UE como respuesta a un requerimiento legal de un tercer país.
B) Correcto. Fuente: White Paper – Privacy, Personal Data and the GDPR - §7.5.2 Regulations applying to data transfer outside the EEA & EU GDPR, A pocket guide - Chapter 3: The regulation – International transfers y RGPD art. 48.
C) Incorrecto. No es lícito transferir datos perosnales fuera de la UE como respuesta a un requerimiento legal de un tercer país, ni siquiera con el consentimiento del interesado.
D) Incorrecto. El tratamiento de datos sensibles fuera de la UE puede ser lícito, pero no como respuesta a una solicitud del gobierno de un tercer país.

22 / 40
El 12 de Julio del 2016, la Comisión Europea implementó una resolución en relación a la transferencia de datos personales con EE.UU (Escudo de la Privacidad UE-EE.UU.).

En términos del RGPD, ¿qué tipo de resolución es ésta?

A) Una decisión de adecuación
B) Un decreto de excepción
C) Un contrato vinculante estándar
D) Un tratado que sustituye al RGPD

A) Correcto. La resolución es una decisión de adecuación conforme al RGPD en relación al tratamiento en terceros países. Fuente: : White Paper – Privacy, Personal Data and the GDPR - §7.5.4 Regulations applying to data transfer between the EEA and the USA & EU GDPR, A pocket guide - Chapter 3 The Regulation – International transfers y RGPD considerandos 104 y 106.
B) Incorrecto. Una excepción se refiere a las transferencias esenciales para responder a delitos terroristas o delitos graves (art. 11)
C) Incorrecto. La resolución es una decisión de adecuación conforme al RGPD en relación al tratamiento en terceros países.
D) Incorrecto. La resolución es una decisión de adecuación conforme al RGPD en relación al tratamiento en terceros países.

23 / 40
Las normas corporativas vinculantes son un medio para que las organizaciones alivien su carga administrativa al cumplir con el RGPD.

¿Cómo les ayudan estas normas?

A) Les permiten tener contratos con terceros con todas las partes involucradas en el extranjero.
B) Les permiten dejar que terceros países fuera del Espacio Económico Europeo traten datos personales.
C) Evitan la necesidad de dirigirse a cada autoridad de control en la UE por separado.
D) Les evitan tener que pedir permiso a una autoridad de control para el tratamiento de datos una vez se aceptan sus NCV.

A) Incorrecto. Las NCV se redactan para que las organizaciones no tengan que usar contratos con terceros para cada afiliado por separado.
B) Incorrecto. Las NCV sólo son válidos dentro de una organizaicón y todos sus afiliados. No se aplican a otras partes.
C) Correcto. Una vez se aprueban las NCV por autoridad de control dentro de la UE no es necesario pedir a otra autoridad de control dentro de la UE que las apruebe de nuevo. Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation – Binding corporate rules y RGPD artículo 47(2.d.j.k.l.m) Normas Corporativas Vinculantes.
D) Incorrecto. Las NCV deben ser autorizadas también por una autoridad de control.

24 / 40
En caso de que un contratista contrate el tratamiento de datos personales, las partes celebrarán un contrato por escrito. Este contrato establece el objeto y la duración del tratamiento, la naturaleza y los fines del tratamiento, el tipo de datos personales y las categorías de los interesados.

¿Qué otro aspecto debe regirse por este contrato escrito?

A) La responsabilidad del encargado
B) La obligación de notificación de la violación de la seguridad de los datos
C) Las obligaciones y los derechos del responsable
D) La obligación de que los encargados deben cooperar con la autoridad de control

A) Incorrecto. Esto es una obligación directa del RGPD a los encargados.
B) Incorrecto. Esto es una obligación directa del RGPD a los encargados.
C) Correcto. Esto es una obligación directa del RGPD a los encargados. Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation – Controller/processor contracts y RGPD art. 28 (3).
D) Incorrecto. Esto es una obligación directa del RGPD a los encargados.

25 / 40
¿Qué se debería hacer para que un responsable pueda externalizar el tratamiento de datos personales a un encargado?

A) El responsable debe pedir permiso a la autoridad de control para externalizar el tratamiento de los datos.
B) El responsable debe preguntar a la autoridad de control si el contrato escrito acordado cumple con los reglamentos.
C) El responsable y el encargado deben redactar y firmar un contrato escrito garantizando la confidencialidad de los datos.
D) El encargado debe demostrar al Responsable que se cumplen todas las demandas acordadds en el Acuerdo de Nivel de Servicio (SLA).

A) Incorrecto. No hay que pedir permiso a la autoridad de control en cada caso de externalización.
B) Incorrecto. La autoridad de control no es un asesor jurídico y no revisará el cumplimiento de los contratos.
C) Correcto. Debe haber un contrato escrito garantizando la confidencialidad de los datos en el que el Responsable define las metas y los medios del tratamiento. Ambas partes deben firmar este contrato. Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation – Controller/processor contracts y RGPD artículo 28(3) Encargado del tratamiento
D) Incorrecto. Un SLA no es suficiente ya que se centratá en las operaciones, no necesariamente en la definición de las metas.

26 / 40
La protección de datos desde el diseño, tal como está descrito en el artículo 25 del RGPD, se basa en siete principios básicos. Uno de estos se suele denominar "Funcionalidad - Suma-Positiva, no Suma-Cero".

¿Cuál es la esencia de este principio?

A) Las normas de seguridad aplicadas deben asegurar la confidencialidad, integridad y disponibilidad de los datos a lo largo de su ciclo de vida.
B) Si diferentes tipos de objetivos legítimos son contradictorios, los objetivos de privacidad deben tener prioridad sobre los objetivos de seguridad.
C) Al integrar la privacidad dentro de una determinada tecnología, proceso o sistema, debería hacerse de tal manera que la funcionalidad completa no se vea afectada.
D) Siempre que sea posible, se deberían realizar y publicar evaluaciones detalladas del impacto en la privacidad y de riesgos, documentando claramente los riesgos de privacidad.

A) Incorrecto. Este es un aspecto de la Seguridad de Extremo a Extremo - Protección del Ciclo de Vida, uno de los otros seis principios básicos.
B) Incorrecto. La Privacidad desde el Diseño rechaza el enfoque de que la Privacidad tenga que competir con otros intereses legítimos, objetivos de diseño, y capacidades técnicas. Todos los objetos tienen que ser incluídos en una suma-positiva de manera "ganar-ganar"
C) Correcto. Esta es la esencia. Fuente: White Paper – Privacy, Personal Data and the GDPR - § 8.1.1 The seven principles of data protection by design y RGPD art 25
D) Incorrecto. Este es un aspecto de "la privacidad integrada en el diseño", uno de los otros seis principios básicos.

27 / 40
A menudo, el personal que trabaja con datos personales considera la privacidad y la seguridad de la información como cuestiones separadas.

¿Por qué esto está mal?

A) La privacidad no se puede garantizar sin identificar, implementar y monitorizar las medidas apropiadas de seguridad de la información.
B) La autoridad de control espera que se integren los roles de delegado de protección de Datos y responsable de la seguridad de la información.
C) Los reglamentos identifican medidas de seguridad de la información que se deben tomar antes de que se permita la manipulación de datos personales.

A) Correcto. La Privacidad y la Protección de Datos tratan de garantizar la confidencialidad de los datos personales. Esto requiere la implementación de medidas de seguridad. Fuente: White Paper – Privacy, Personal Data and the GDPR - § 2.1.6 - integrity and confidentiality y RGPD Artículo 35(7.d) Evaluación de impacto relativa a la protección de datos.
B) Incorrecto. La autoridad de control no espera que estos roles se integren en absoluto.
C) Incorrecto. Los reglamentos especifican metas que se deben cumplir, pero no las medidas específicas que se deben tomar.

28 / 40
Uno de los objetivos de la evaluación de impacto relativa a la protección de datos (EIPD) es "fortalecer la confianza de los clientes o de los ciudadanos en la forma que se tratan los datos personales y se respeta la privacidad".

¿Cómo un EIPD puede "fortalecer la confianza"?

A) La organización minimiza el riesgo de costosos ajustes en los procesos o rediseño de sistemas en una etapa posterior.
B) La organización evita el no cumplimiento con el RGPD y minimiza el riesgo de multas.
C) La organización demuestra que se toma en serio la privacidad y busca el cumplimiento con el RGPD.

A) Incorrecto. Este aspecto puede fortalecer la confianza de la dirección, pero no la de los clientes o los ciudadanos.
B) Incorrecto. Evitar las multas puede fortalecer la confianza de la dirección, pero no la de los clientes o los ciudadanos.
C) Correcto. Fuente: EU GDPR, A pocket guide - Chapter 3 The Regulation - Data Protection Impact Assessments.

29 / 40
¿Cuál es el propósito de una auditoría de privacidad por parte de una autoridad de control?

A) Cumplir la obligación del RGPD de implementar medidas técnicas y organizativas apropiadas para la protección de datos.
B) Supervisar y ejecutar la aplicación del RGPD evaluando que el tratamiento se realice de conformidad con el RGPD.
C) Asesorar al responsable en la mitigación de los riesgos de la privacidad para proteger al responsable de reclamanciones de responsabilidad por el incumplimiento del RGPD.

A) Incorrecto. La auditoría no es la implementación de medidas, sino una evaluación de su eficacia.
B) Correcto. De acuerdo con el RGPD art. 57.1(a) esta es una tarea importante de la autoridad de control como autoridad de control.
C) Incorrecto. La autoridad de control tiene la tarea de supervisar el cumplimiento y asesorar sobre las mejoras, pero su propósito no es el de proteger al responsable.

30 / 40
¿Qué describe **mejor** el principio de minimización de datos?

A) Se debe tener cuidado de obtener el menor número de datos posible para proteger los intereses y la privacidad de los interesados.
B) Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
C) Con el fin de mantener los datos manejables, se debe almacenar de tal manera que requiera una cantidad mínima de almacenamiento.
D) El número de elementos que son obtenidos por interesado no debe exceder el límite superior establecido por la autoridad de control.

A) Incorrecto. De hecho, el RGPD establece que los datos obtenidos deben ser adecuados, lo que implica que no tiene que ser el mínimo absoluto.
B) Correcto. Esta es la definición de minimización de datos (artículo 5.1.c). Está dirigida a asegurar que sólo se obtienen los datos necesarios para alcanzar las metas definidas. Fuente: White Paper – Privacy, Personal Data and the GDPR - §2.1 Data processing principles y RGPD art 5.1.c.
C) Incorrecto. El tamaño del almacenamiento no tiene nada que ver con este principio.
D) Incorrecto. Las autoridades de control no establecen un límite superior de número de elementos que se obtienen siempre y cuando se limiten a los necesarios para alcanzar los objetivos definidos.

31 / 40
Las cookies de sesión son uno de los tipos más comunes de cookie.

¿Qué hace una cookie de sesión?

A) Contiene información sobre lo que se está haciendo, por ejemplo, los productos que se seleccionan en una tienda online antes de que realmente se haga el pedido.
B) Revela el historial del navegador, de manera que otros sitios web pueden averiguar qué sitios web se han visitado antes de llegar allí.
C) Almacena el historial del navegador, de manera que se puede rastrear dónde se ha estado en la red y volver a visitar esos sitios si se desea.
D) Obtiene los datos personales, por lo que el sitio web puede saludar por el nombre y reutilizar su configuración cuando se regrese.

A) Correcto. Una cookie de sesión se mantiene en la memoria para guardar la información de la sesión. Se borra cuando se cierra la sesión. Fuente: White Paper – Privacy, Personal Data and the GDPR - § 8.6.3 Cookies
B) Incorrecto. Una cookie de sesión se borra cuando se cierra la sesión, por lo que no se puede utilizar en la siguiente sesión.
C) Incorrecto. Una cookie de sesión se borra cuando se cierra la sesión, por lo que no se puede utilizar en la siguiente sesión.
D) Incorrecto. Una cookie de sesión se borra cuando se cierra la sesión, por lo que no se puede utilizar en la siguiente sesión.

32 / 40
Algunas veces los sitios web monitorizan a los visitantes y almacenan su información con fines de marketing.

¿Está el sitio web obligado a notificar al vistante de que su información se está utilizando con fines de marketing?

A) Sí
B) No

A) Correcto. El sitio web tiene la obligación de notificar al visitante de que su información se está utilizando con fines de marketing. Ttienen el derecho a oponerse al tratamiento de los datos personales relacionados con él o ella para fines de marketing. Fuente: White Paper – Privacy, Personal Data and the GDPR - § 8.6.3 Cookies
B) Incorrecto. El sitio web tiene la obligación de notificar al visitante de que su información se está utilizando con fines de marketing. Ttienen el derecho a oponerse al tratamiento de los datos personales relacionados con él o ella para fines de marketing.

33 / 40
Una compañía puede presentarse como un experto en un área concreta de especialización haciendo uso de las redes sociales.

¿Cuál es la **mejor** forma de demostrar la especialización en un campo específico?

A) Publicando información sobre la compañía en las Redes Sociales.
B) Respondiendo activamente las preguntas sobre su producto en las Redes Sociales.
C) Publicando cómo el producto del competidor es inferior al de la compañía.
D) Publicando los productos que la compañía está desarrollando.

A) Incorrecto. La sola publicación de información de la compañía no te convierte en un experto en una materia.
B) Correcto. Contestando (y contestando activamente) preguntas sobre un producto en concreto en las redes sociales podría convertir a la compañía en experta. Fuente: White Paper – Privacy, Personal Data and the GDPR - § 8.6. Practice related applications of the use of data, marketing and social media.
C) Incorrecto. Esto sólo es presumir de lo bueno que es tu producto (y a lo mejor no lo es).
D) Incorrecto. Esto sólo demuestra que la compañía está desarrollando nuevos productos y sí, puede ayudar a mejorar las ventas pero no hace que la compañía sea una experta.

34 / 40
Ha ocurrido una violación de la seguridad de los datos en un sistema de información que también guarda datos personales.

¿Qué es lo primero que debe hacer el responsable?

A) Determinar si la violación de la seguridad de los datos puede haber ocasionado una pérdida o un tratamiento ilícito de los datos personales.
B) Evaluar el riesgo de efectos adversos para los interesados utilizando una evaluación del impacto en la protección de datos (EIPD).
C) Evaluar si los datos personales de una naturaleza sensible han sido o podrían haber sido tratados ilícitamente.
D) Informar de la violación inmediatamente a la Autoridad de Control pertinente.

A) Correcto. La obligación de notificación de la violación de la seguridad de los datos establecida en RGPD artículo 33(2) y 33(3.a.c) y 33(5) exige la descripción de la naturaleza de la violación y sus posibles consecuencias, como la pérdida o el tratamiento ilícito de los datos personales. Obligación de notificación de la violación de la seguridad de los datos personales. Fuente: White Paper – Privacy, Personal Data and the GDPR - § 5.2 Procedures on how to act when a data breach occurs.
B) Incorrecto. Una EIPD se lleva a cabo al diseñar operaciones de tratamiento de datos personales.
C) Incorrecto. El responsable debe comprobar primero si el incidente de seguridad es una violación de la seguridad de los datos de la que se debe informar.
D) Incorrecto. El responsable debe comprobar primero si el incidente de seguridad es una violación de la seguridad de los datos de la que se debe informar.

35 / 40
La palabra "privacidad" no se menciona en el RGPD.

¿Cómo se relaciona la "privacidad" con la "protección de datos"?

A) La protección de datos es un conjunto de normas y reglas sobre el tratamiento de datos personales. La privacidad es el resultado de la protección de datos.
B) La privacidad es el derecho a ser protegido de interferencias en asuntos personales. La protección de los datos es el medio para implementar esa protección.
C) La privacidad es el derecho a mantener en secreto los asuntos personales. La protección de los datos es el derecho a mantener en secreto los datos personales.
D) Los términos "privacidad" y "protección de datos" son intercambiables. No hay una diferencia real en el significado.

A) Incorrecto. La privacidad es un derecho, la protección de datos es el medio para asegurarla.
B) Correcto. Fuente: White Paper – Privacy, Personal Data and the GDPR - § 1.3 Definitions.
C) Incorrecto. La privacidad es un derecho, la protección de datos es el medio para asegurarla.
D) Incorrecto. La privacidad es un derecho, la protección de datos es el medio para asegurarla.

36 / 40
El reglamento (UE) 2016/679, conocido como el RGPD, deroga una directiva UE anterior.

¿Qué directiva está siendo derogada (sustituida)?

A) Directiva 2002/58/CE del 12 de julio del 2002
B) Directiva 2006/24/CE del 15 de marzo del 2006
C) Directiva 95/46/CE del 24 de octubre de 1995
D) Directiva 97/66/CE del 15 de diciembre de 1997

A) Incorrecto. La Directiva 2002/58/CE modifica algunas partes de la Directiva 97/66/CE.
B) Incorrecto. Esta directiva trata de la retención de datos obtenidos, por ejemplo, de proveedores de internet.
C) Correcto. Esta sustitución se menciona en el (sub)título del reglamento. Fuente: RGPD.
D) Incorrecto. Esta Directiva complementa a la directiva 95/66/CE para asegurar un nivel equivalente de protección de los derechos y libertades fundamentales en los estados miembros.

37 / 40
¿Qué derecho de los Interesados se define explícitamente en el RGPD?

A) Se debe proporcionar una copia de los datos personales en el formato solicitado por el Interesado.
B) Acceso a los datos personales sin coste alguno para el Interesado.
C) Los datos personales siempre deben ser modificados a petición del Interesado.
D) Los datos personales deben ser eliminados siempre que el Interesado lo solicite.

A) Incorrecto. Tiene que proporcionarse en un formato estructurado, comúnmente utilizado y legible por máquina, pero no necesariamente en cualquier formato que el Interesado especifique.
B) Correcto. Sin embargo, sólo la primera copia se tiene que proporcionar sin coste. Fuente: EU GDPR, A pocket guide – Chapter 3 The Regulation – Data subjects' rights y RGPD artículo 15(3) Derecho de acceso del Interesado.
C) Incorrecto. Sólo los datos erróneos se tienen que modificar.
D) Incorrecto. El artículo 17 establece algunas excepciones cuando los datos son necesarios para el establecimiento, ejercicio o defensa de reclamaciones legales.

38 / 40
El RGPD distingue los "datos personales sensibles" como una categoría especial de datos personales.

¿Cuál es un ejemplo de dichos datos?

A) Una cita en un hospital con un médico especialista
B) Un Código Internacional de Cuenta Bancaria (IBAN)
C) Una suscripción a una revista científica para la política
D) La pertenencia a una asociación interprofesional

A) Correcto. Una cita con un especialista médico es "un dato personal relativo a la salud". Fuente: RGPD art. 9.1.
B) Incorrecto. Un IBAN es un dato exclusivamente relacionado con una persona, por ejemplo, datos personales. Pero no los datos personales sensibles de acuerdo con el RGPD art. 9.
C) Incorrecto. Una revista científica para política no son "datos personales que revelen las opiniones políticas, las convicciones religiosas o filosóficas" y como tal no son datos sensibles de acuerdo con el RGPD art. 9.
D) Incorrecto. Sólo la afiliación sindical y otros datos personales que "revelen (…) las opiniones políticas, las convicciones religiosas o filosóficas" son datos personales sensibles de acuerdo con el RGPD art. 9.

39 / 40
¿Qué rol en la protección de datos determina los fines y los medios del tratamiento de datos personales?

A) Responsable
B) Delegado de protección de datos
C) Encargado

A) Correcto. Responsable: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento de datos personales. Fuente: White Paper – Privacy, Personal Data and the GDPR - §1.4 Roles, responsibilities, stakeholders y RGPD Articulo 4(7) definición de Responsable.
B) Incorrecto. El RGPD define al DPD como "Una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos debería asesorar al responsable o al encargado del tratamiento para supervisar el cumplimiento interno con este Reglamento"
C) Incorrecto. El Encargado es la persona u organización que trata los datos personales, pero no necesariamente es el que determina el porqué y el cómo.

40 / 40
¿Qué información se considera como datos personales de acuerdo con el RGPD?

A) Información sobre una persona, que podría perjudicar la privacidad de esa persona, incluso cuando es falsa.
B) Cualquier información sobre una persona física identificable.
C) Información, sobre una persona física identificable, que esté digitalizada.

A) Incorrecto. Cualquier declaración sobre una persona física identificable son datos personales según el RGPD.
B) Correcto. Fuente: EU GDPR, A pocket guide – Chapter 2 Terms and definitions - Personal data y RGPD art. 4(1).
C) Incorrecto. Cualquier declaración sobre una persona física identificable son datos personales según el RGPD.

Evaluación

En la siguiente tabla se indican las respuestas correctas a las preguntas.

Número	Repuesta	Número	Repuesta
1	D	**21**	B
2	D	**22**	A
3	D	**23**	C
4	A	**24**	C
5	D	**25**	C
6	A	**26**	C
7	C	**27**	A
8	A	**28**	C
9	D	**29**	B
10	D	**30**	B
11	B	**31**	A
12	B	**32**	A
13	B	**33**	B
14	B	**34**	A
15	A	**35**	B
16	A	**36**	C
17	B	**37**	B
18	C	**38**	A
19	D	**39**	A
20	A	**40**	B

Contacto EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER