Protección de datos desde la óptica de las personas responsables y encargadas de tratamiento. Curso avanzado. Bloque IV: Delegado de protección de datos y gestión de riesgos

1. El Delegado de Protección de Datos (DPD): concepto

¿QUÉ ES? Persona física o jurídica para garantizar el cumplimiento de la protección de datos.

No asume responsabilidad de la seguridad.

¿OBLIGATORIO? No, en todo caso (arts. 37 RGPD y 34 LOPDGDD)

¿SE PUEDE NOMBRAR AUNQUE NO HAYA OBLIGACIÓN? SI.

Si se nombra, respetar sus funciones y sus requisitos de cualificación y posición.

Si hay dudas – Se recomienda analizar y documentar la decisión.

1. El Delegado de Protección de Datos (DPD): funciones

"Control del cumplimiento interno de la normativa y política de protección de datos"

- **Informar** y **asesorar** de las obligaciones.
- Supervisar el **cumplimiento** legal. En concreto:
  - la asignación de responsabilidades internas
  - la concienciación y formación del personal
  - las auditorías correspondientes
- En **evaluaciones de impacto**: asesorar y supervisar su aplicación.
- **Con las Agencias** de Protección de Datos: cooperar y actuar como contacto.

1. El Delegado de Protección de Datos (DPD): requisitos

CUALIFICACIÓN Y POSICIÓN

- ✓ **Conocimientos especializados** del derecho y de la práctica de la protección de datos.
- ✓ **Independiente** funcional y jerárquicamente en el organigrama de la empresa.

  No puede recibir instrucciones sobre sus funciones, ni ser destituido ni sancionado por el desempeño de su trabajo.
- ✓ **Reporta al más alto nivel jerárquico**.
- ✓ Sus **datos de contacto serán publicados y notificados** a la Agencia.
- ✓ **Interno (**o un servicio **externo)**.
- ✓ **No** debe existir **conflicto de intereses:** no puede ser destituido ni sancionado por el responsable

2. Análisis de riesgos: valoración

VALORACIÓN DE **RIESGOS DE TODOS LOS TRATAMIENTOS** → **MEDIDAS DE SEGURIDAD**

TENIENDO EN CUENTA:

- ✓ el estado de la **técnica**
- ✓ el **coste** de la aplicación de las medidas
- ✓ la naturaleza, ámbito, contexto y fines del **tratamiento**
- ✓ los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los **derechos y libertades de las personas físicas**.

2. Análisis de riesgos: determinación del nivel de seguridad

Nivel básico: datos identificativos recogidos en los registros de actividades del tratamiento, así como a aquellos datos a los que se le apliquen niveles medios o altos de seguridad. Ejemplos: nombre, DNI, dirección, teléfono o correo electrónico.

Nivel medio: datos que, por su finalidad de tratamiento, puedan suponer un riesgo más elevado para los derechos y libertades de los individuos. Ejemplos: datos relativos a condenas o infracciones penales, información cuyos responsables del tratamiento sean la Seguridad Social y las Administraciones tributarias

Nivel alto: categorías especiales de datos o especialmente protegidos. Ejemplos: sexo, ideología, afiliación sindical, orientación sexual, raza, religión, salud de las personas físicas o información derivada de casos de violencia de género.

2. Análisis de riesgos: la herramienta Evalúa-Riesgo v2

Evalúa-Riesgo RGPD v2:

- ayuda a responsables y encargados a identificar los factores de riesgo
- propicia una primera evaluación del riesgo intrínseco.
- estima el riesgo residual si se utilizan medidas y garantías para mitigar los factores de riesgos específicos.
- No garantiza el cumplimiento automático de las obligaciones legales.

Tras su utilización:

- La valoración del nivel de riesgo + nivel de riesgo = evaluación mínima
- Deber de especificación por el responsable para determinar (con precisión) el nivel de riesgo del tratamiento.

2. Análisis de riesgos: acciones para afrontarlos/solventarlos

- **Reducir/mitigar el riesgo:** deber de establecer medidas de control que disminuyan los niveles de probabilidad y/o los impactos asociados al riesgo inherente.
- **Evitar/eliminar el riesgo**: Si el riesgo es muy elevado o abandonar la actividad de tratamiento o modificar la naturaleza, el alcance, el contexto y la finalidad del tratamiento.
- **Aceptar/asumir el riesgo:** Si el riesgo inherente es inferior al nivel de riesgo considerado como aceptable, se puede asumir. Necesidad de continuar gestionándolo de forma continua.

2. Análisis de riesgos: medidas de seguridad

AEPD: Guía para la notificación de brechas de datos personales

Algunos ejemplos básicos para mantener la seguridad de los datos:

- ✓ Contraseñas no compartidas y seguras
- ✓ Perfiles de acceso diferenciados
- ✓ Copias de seguridad
- ✓ Recoger lo imprimido y eliminar lo escaneado
- ✓ Protector de pantalla
- ✓ ¿Almacenamiento en pendrives? ¿Fotos en móviles o cámaras?
- ✓ Utilizar CCO, al enviar *emails,* cuando sea necesario
- ✓ Datos en papel: destructoras, archivo, no sobre la mesa, impresora…

3. Autoridades de Protección de Datos

- Agencia Española de Protección de Datos (AEPD)

Autonómicas:

- - Agencia Vasca de Protección de Datos
- - Autoridad Catalana de Protección de Datos
- - Consejo de Transparencia y Protección de Datos de Andalucía
- ~~- Agencia de la Comunidad de Madrid~~ (2001 – 2012)

3. Autoridades de Protección de Datos: la AEPD

Comunica-Brecha RGPD: recurso de utilidad para que cualquier organización, responsable de un tratamiento de datos personales, pueda valorar la obligación de informar a las personas físicas afectadas por una brecha de seguridad de los datos personales.

- Herramienta que facilita la **comprensión** de dichas obligaciones y cómo abordar adecuadamente la brecha
- **Deber de adaptación** por parte de los responsables y encargados de los tratamientos de datos personales

3. Autoridades de Protección de Datos: áreas de actuación

- Canal prioritario
- Internet y redes sociales
- Reclamaciones de telecomunicaciones
- Publicidad no deseada
- Educación y menores
- Videovigilancia
- Innovación y tecnología
- Violencia de género
- Protección de datos y coronavirus
- Salud
- Administraciones públicas

3. Autoridades de Protección de Datos: guías más actuales

- Aproximación a los espacios de datos desde la perspectiva del RGPD
- Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales
- Guía para profesionales del sector sanitario
- La protección de datos en las relaciones laborales
- LOPD: Nuevas obligaciones para el Sector Público

Jorge Viguri Cordero
jviguri@uji.es

UNIVERSITAT JAUME I

#ProDigital