

Organiza:



Partners Estratégicos:



IV Congreso Privacidad "Diálogos de DPDs"

14 Diciembre 2021
Salón de Actos. Distrito C. Telefónica

Partners Estratégicos



“Análisis de riesgos y evaluaciones de impacto: aclarando algunos conceptos”

Javier Villegas Flores

Lead Advisor, GOVERTIS



<https://www.linkedin.com/in/javier-villegas-flores/>

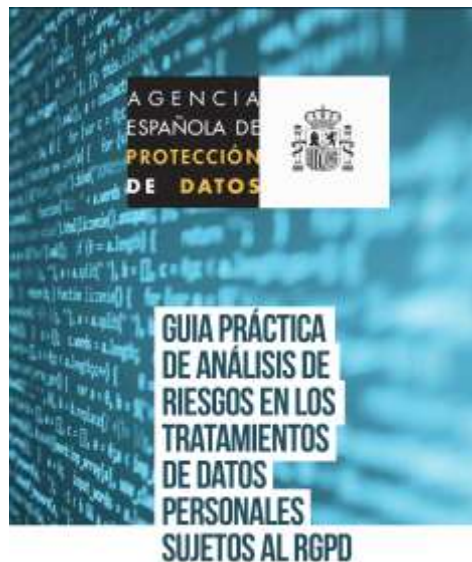


j.villegas@govertis.com



[@JavierVillegasF](https://twitter.com/JavierVillegasF)





Otros contenidos	
Guías generales	Descargas
Guía sobre el uso de videocámaras para seguridad y otras finalidades	83.126
Guía sobre el uso de las cookies	77.804
Guía para el responsable de tratamiento de datos personales	56.919
Protección de datos: guía para el ciudadano	49.233
Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD	42.225
Guía para pacientes y usuarios de la Sanidad	40.721
Guía para el cumplimiento del deber de informar	33.130
Guía de evaluación de impacto en la protección de datos personales	31.487
Directrices para la elaboración de contratos entre responsables y encargados del tratamiento	26.768
Guía para la gestión y notificación de brechas de seguridad	26.702
Listado de elementos para el cumplimiento normativo	16.113
Guía de Privacidad desde el diseño	15.845
Drones y Protección de Datos	8.099
Guía de Privacidad desde el diseño (versión en inglés)	6.580
Guía sobre el uso de las cookies (versión en inglés)	4.532
Guía para la gestión y notificación de brechas de seguridad (versión en inglés)	3.248
Drones y Protección de Datos (versión en inglés)	939

Organiza:



Partners Estratégicos:



Datos extraídos de Memoria AEPD 2020

Herramienta Gestiona ⁸		
Sección	Abierto	Finalizado
Evaluaciones de impacto en la privacidad (EIPD)	5.403	2.750
Análisis de riesgos	5.398	2.651

⁸ Gestiona EIPD: Asistente para el análisis de riesgos y evaluaciones de impacto en protección de datos.

*Desde julio 2019

Herramienta Facilita RGPD ⁶			
	2018	2019	2020
Accesos a Facilita RGPD	622.550	197.279	124.460
Cuestionarios finalizados	150.360	49.086	26.504

⁶ Facilita RGPD, herramienta para facilitar la adecuación al RGPD de empresas y profesionales, implantada en septiembre de 2017.

RESOLUCIONES SANCIONADORAS

Resolución	Infracción - sanción	Detalle
PS/00050/2021: Empresa logística	Infracción del artículo 35 del RGPD: 20.000 euros. Incorrecto análisis de riesgos y evaluación necesidad EIPD	<i>Aporta copia de análisis de riesgos de actividades de tratamiento, (modelo cuestionario y notas al mismo). “Aplicando como primer paso la adaptación de la herramienta FACILITA RGPD el 8/04/2019 se obtiene el resultado de la actividad de “escaso riesgo”. Indica que evaluaron la necesidad de realizar o no una EIPD. “El resultado determinó que no se precisaba realizar una evaluación de impacto en protección de datos (EIPD) (...)” Se realizó un “análisis de riesgos básicos” “para determinar si era preciso implantar procesos y protocolos adicionales a los diseñados”</i>
PS/00120/2021: Empresa supermercados	Infracción del artículo 35 del RGPD: 50.000 euros. Evaluación de impacto deficiente o incompleta	<i>No consta acreditado el correcto análisis de riesgos y la preceptiva evaluación de impacto, toda vez que no contempla, ni en uno ni en la otra, todos los sujetos afectados (FD V), como es el caso de trabajadores y menores</i>
PS/00120/2021: Servicio público de Salud	Infracción del artículo 35 del RGPD: apercibimiento tras notificación brecha de seguridad No consta análisis de riesgos ni EIPD previa	

RESPONSABILIDAD PROACTIVA - ACCOUNTABILITY

*“El **análisis de riesgos y la evaluación de impacto** nos ayudan a encontrar el equilibrio entre:*

- *objetivos del **negocio***
 - ***derechos** de los titulares de datos personales,*
- llevando a cabo las acciones necesarias para **tratar el riesgo a la privacidad**”*



- ☐ Las medidas estaban tasadas
- ☐ Se definían sólo por un criterio: el nivel de los datos: BÁSICO, MEDIO Y ALTO



- ☐ Las medidas NO estan tasadas
- ☐ Se definen a partir de **análisis de riesgo** (tratamientos alto riesgo → **EIPD**).
- ☐ Además del tipo de datos se deben tener en cuenta otros criterios: cesiones, volumen, tid etc.



RESPONSABILIDAD PROACTIVA

RESPONSABLE DE TRATAMIENTO decide:

- **QUÉ** medidas implantar
- y el diseño de los mecanismos que hagan posible dicha implantación (**CÓMO**)
- Realizando un **Análisis de Riegos (AR)** y **Evaluación de impacto (EIPD)**, en su caso
- Hay que evidenciar para demostrar el cumplimiento del mismo

Y “ACCOUNTABILITY”

- Hay que evidenciar para demostrar el cumplimiento:

1. **Por qué** se ha optado por esas medidas
2. Que se han **adoptado** esas medidas
3. Que se han **aplicado** esas medidas

PROCESOS	INDICADORES					
	INDICADOR	UN	20	21	22	23
PROCESO 1	INDICADOR 1	20	21	22	23	24
PROCESO 2	INDICADOR 2	25	26	27	28	29
PROCESO 3	INDICADOR 3	30	31	32	33	34
PROCESO 4	INDICADOR 4	35	36	37	38	39
PROCESO 5	INDICADOR 5	40	41	42	43	44
PROCESO 6	INDICADOR 6	45	46	47	48	49
PROCESO 7	INDICADOR 7	50	51	52	53	54
PROCESO 8	INDICADOR 8	55	56	57	58	59
PROCESO 9	INDICADOR 9	60	61	62	63	64
PROCESO 10	INDICADOR 10	65	66	67	68	69

DOCUMENTO DE POLÍTICA DE PRIVACIDAD

1. OBJETIVO

2. ALCANCE

3. DEFINICIONES

4. POLÍTICA DE PRIVACIDAD

5. MEDIDAS DE PROTECCIÓN DE DATOS

6. PROCEDIMIENTOS DE TRATAMIENTO DE DATOS

7. RESPONSABILIDADES

8. MONITORIZACIÓN Y EVALUACIÓN

9. ACTUALIZACIÓN

10. ANEXOS

Reverso del “Risk based approach”



“Accountability”



Organiza:



Partners Estratégicos:

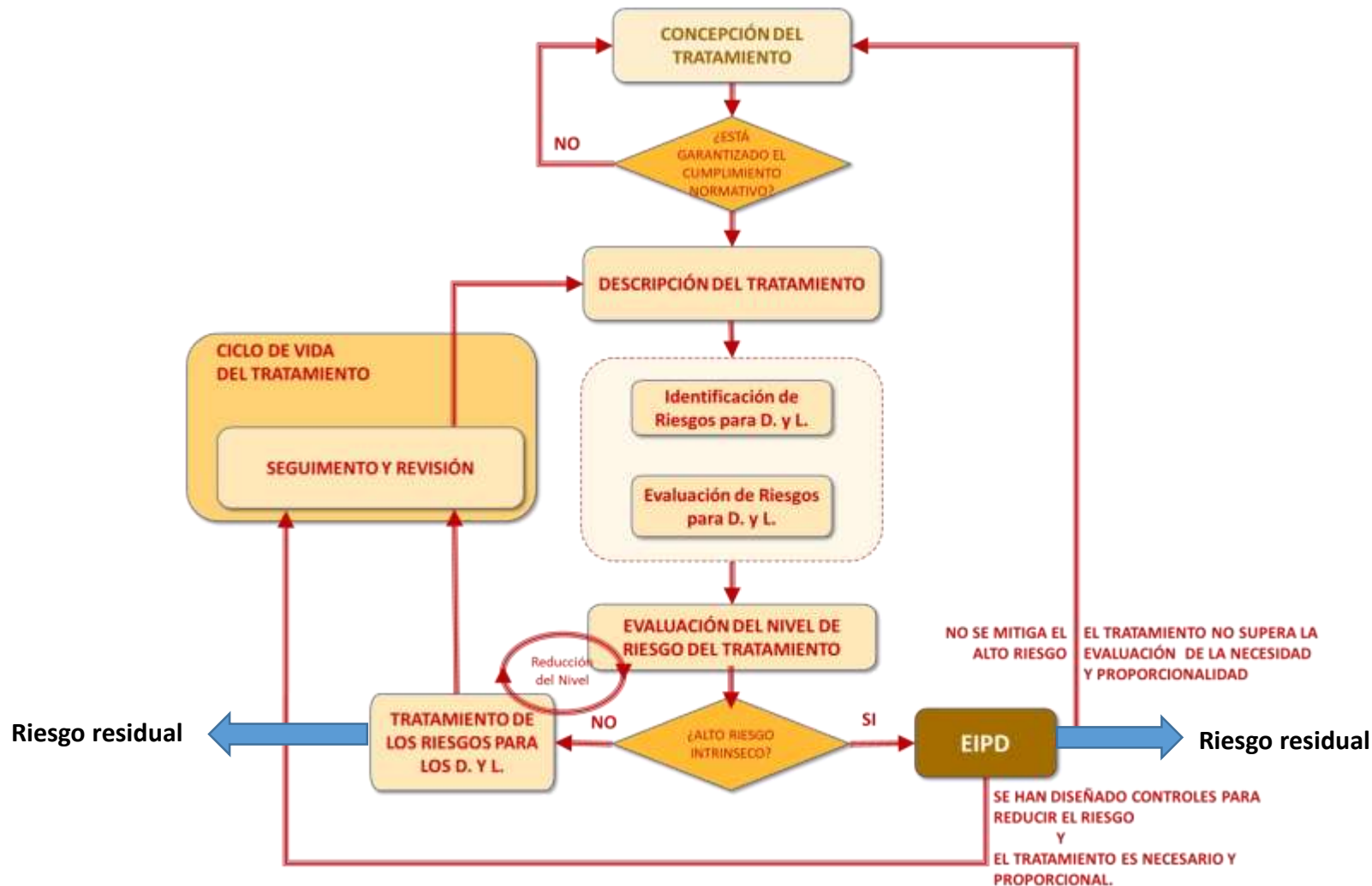


ACLARANDO ALGUNOS CONCEPTOS

1. **Proceso de realización de un análisis de riesgos y una evaluación de impacto. Aspectos comunes y diferencias**
2. **Diferencia entre Análisis de riesgos y cumplimiento normativo**
3. **Evaluaciones de impacto: ¿solo sobre nuevos tratamientos? ¿uno o varios tratamientos?**
4. **Herramientas de las autoridades para análisis de riesgos, ¿son suficientes?:**
 - *Sector público: análisis de riesgos en Pil@r (herramienta CCN).*
 - *Gestiona EIPD – Evalúa RGPD (herramientas AEPD)*

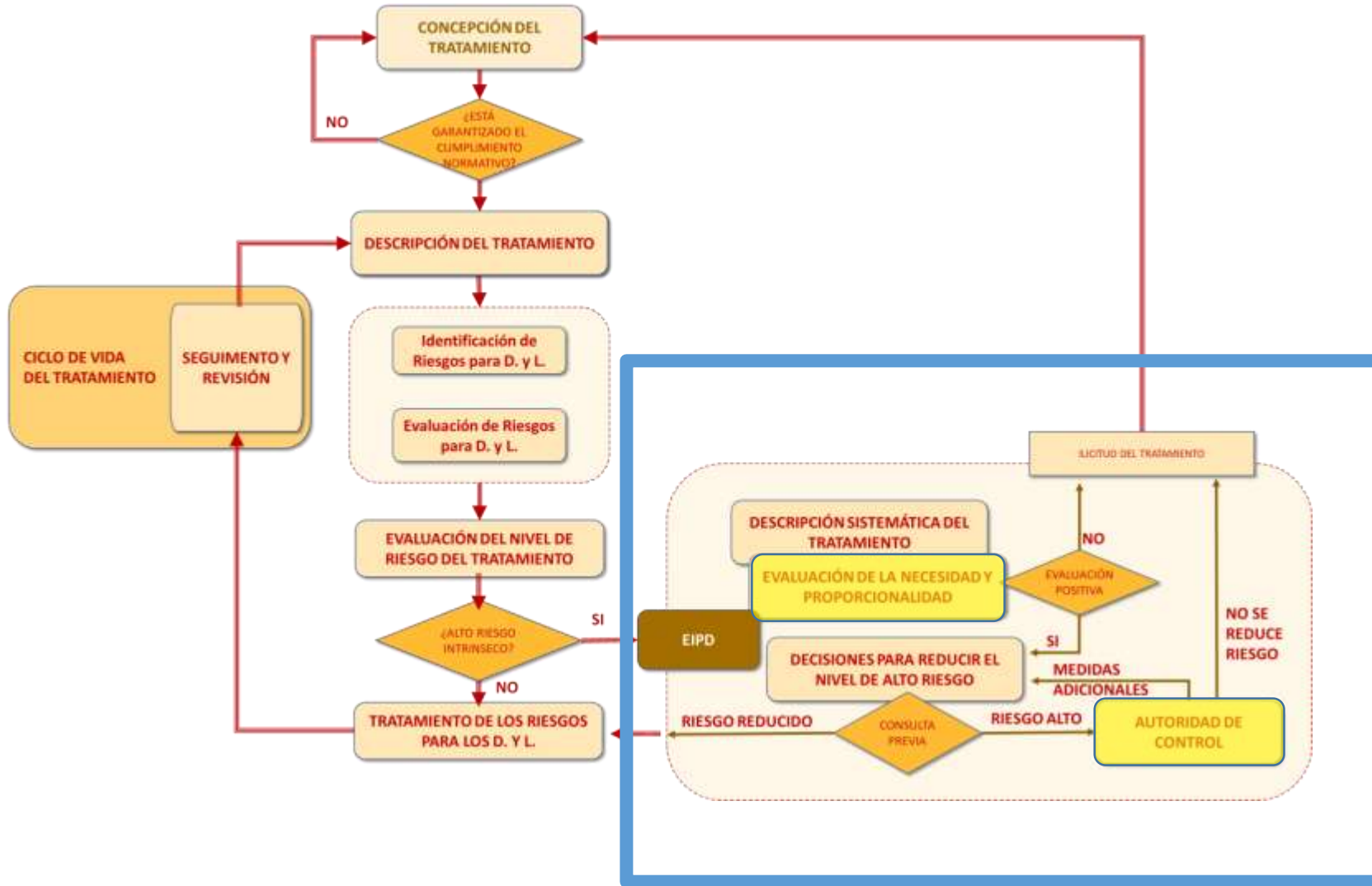


1. Análisis de riesgos y EIPD. Aspectos comunes



1. Chequear **cumplimiento normativo**
2. **Descripción del tratamiento**, tanto en lo que respecta a su naturaleza, como al ámbito, contexto y fines del mismo.
3. **Identificación y análisis** de los riesgos en el tratamiento.
4. **Evaluación** del nivel de riesgo y determinación de si procede o es necesario realizar una EIPD.
5. **Tratamiento** del riesgo.
6. **Seguimiento y verificación** de la eficacia de las medidas adoptadas y decisión sobre cuándo es necesario realizar un proceso de revisión y **reevaluación** de las medidas.

1. Análisis de riesgos y EIPD. Diferencias



1. Solo cuando hay **alto riesgo**
2. Para **TRATAMIENTOS EN DESARROLLO**, aunque excepcionalmente EN PRODUCCIÓN.
3. Sobre **UN TRATAMIENTO**, aunque excepcionalmente VARIOS.
4. Exige **juicio necesidad y proporcionalidad**.
5. Exige **asesoramiento DPD**
6. Contenido **Informe EIPD tasado**.
7. **Consulta previa AEPD**.

2. Evaluaciones de impacto: ¿solo sobre nuevos tratamientos? ¿uno o varios tratamientos?

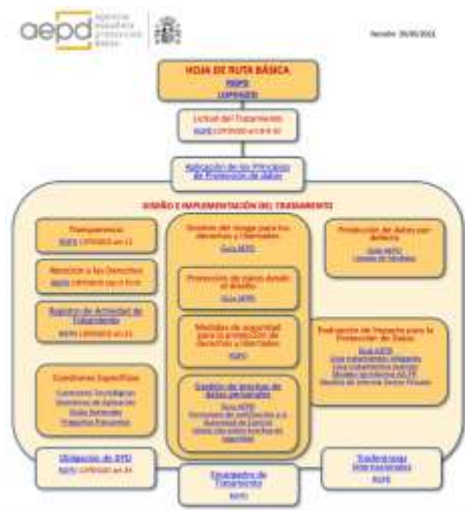
Ámbito de aplicación EIPD:

- Tratamientos **EN DESARROLLO (NUEVOS)** que supongan un riesgo elevado
- Tratamientos **EN PRODUCCIÓN** que sufran cambios sustanciales y que supongan un riesgo elevado
- **UNO o VARIOS TRATAMIENTOS**, cuando sean y entrañen riesgos similares (aplica igual a los análisis de riesgos)



3. Diferencia entre Análisis de riesgos y cumplimiento normativo

- La **GESTIÓN DEL RIESGO PARA LOS DERECHOS Y LIBERTADES (OBJETO AARR y EIPD)**
 - Impacto y la probabilidad de causar **daño** a los **derechos y libertades** de las personas, a nivel individual o social, como consecuencia de un **tratamiento de datos personales**.
- La **GESTIÓN DE RIESGO DE CUMPLIMIENTO NORMATIVO**
 - Impacto y probabilidad de que la entidad incurra en **sanciones legales o administrativas, pérdidas financieras significativas o de reputación** por incumplimiento de la normativa legal



No cumplir con requisitos legales puede suponer riesgos para los derechos y libertades

4. Herramientas de las autoridades para análisis de riesgos, ¿son suficientes? HERRAMIENTAS AEPD

No es posible ejecutar una EIPD si no existe una gestión de riesgos para los derechos y libertades y no se realiza en el marco de la misma. **AARR -> riesgo intrínseco -> alto riesgo (evaluación necesidad EIPD) -> EIPD**



AARR -> riesgo intrínseco -> bajo riesgo / riesgo medio no EIPD



4. Herramientas de las autoridades para análisis de riesgos, ¿son suficientes? HERRAMIENTAS AEPD

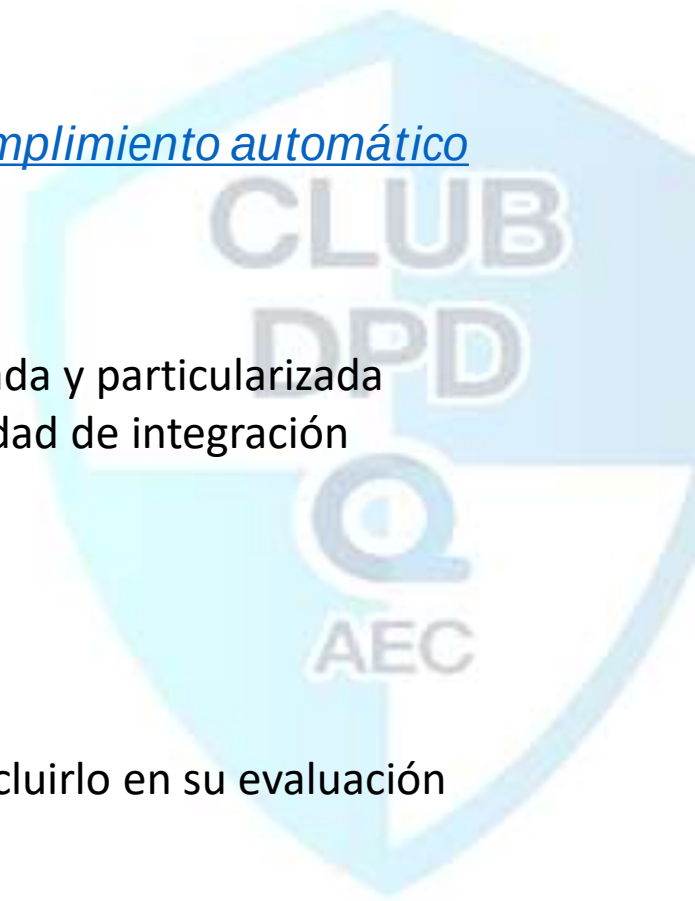
Son herramientas de ayuda, orientativas. Los documentos obtenidos no suponen cumplimiento automático

GESTIONA EIPD

- Genera la documentación **básica** y, en ningún caso exhaustiva, que debe ser completada y particularizada
- No es adecuada para entidades que tenga otros marcos de gestión de riesgos (necesidad de integración procesos)

EVALÚA RGPD

- Factores de riesgo desplegados no tienen carácter exhaustivo
- Responsable deberá identificar aquellos que sean específicos para el tratamiento e incluirlo en su evaluación
- Resultado es una **evaluación mínima que debe ser ajustada**



5. Herramientas de las autoridades para análisis de riesgos, ¿son suficientes? PIL@R



- Hace análisis de riesgos y EIPD, incluyendo la dimensión privacidad, y amenazas específicas de protección de datos
- Incluye amenazas específicas que se confunden con aspectos de cumplimiento normativo. No está actualizado conforme nueva Guía
- No aplicación automática de medidas del ENS por nivel de riesgo:
 - Las medidas que se deriven del AR-EIPD pueden ir más allá de las contempladas en el ENS

Nivel de riesgo para los derechos y libertades	Categoría ENS
Muy Alto	Alto
Alto	Alto
Medio	Medio
Bajo	Bajo

IDEAS CLAVE

Metodología libre, salvo aspectos específicos EIPD

- El RGPD no establece un criterio práctico-metodológico para la gestión de los riesgos (**AARR**): **libertad elección**
- **Para EIPD sí establece requisitos mínimos:** artículos 35 y 36 RGPD “Evaluación de impacto relativa a la protección de datos”

Objetivo: protección derechos y libertades

- Protección de la persona, en su dimensión individual y social: **derechos y libertades del interesado:** *daños físicos, materiales o inmateriales, discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, perjuicios económicos o sociales, privación a los interesados de sus derechos y libertades, etc.*
- **NO proteger intereses propios del responsable o encargado** (continuidad del tratamiento, su eficacia o su eficiencia, el cumplimiento normativo, reputación, pérdidas económicas...)

Análisis de riesgos simplificado es incompleto

Hay que evaluar los riesgos de todos los tratamientos, sea EIPD o AR (art. 24)

IDEAS CLAVE

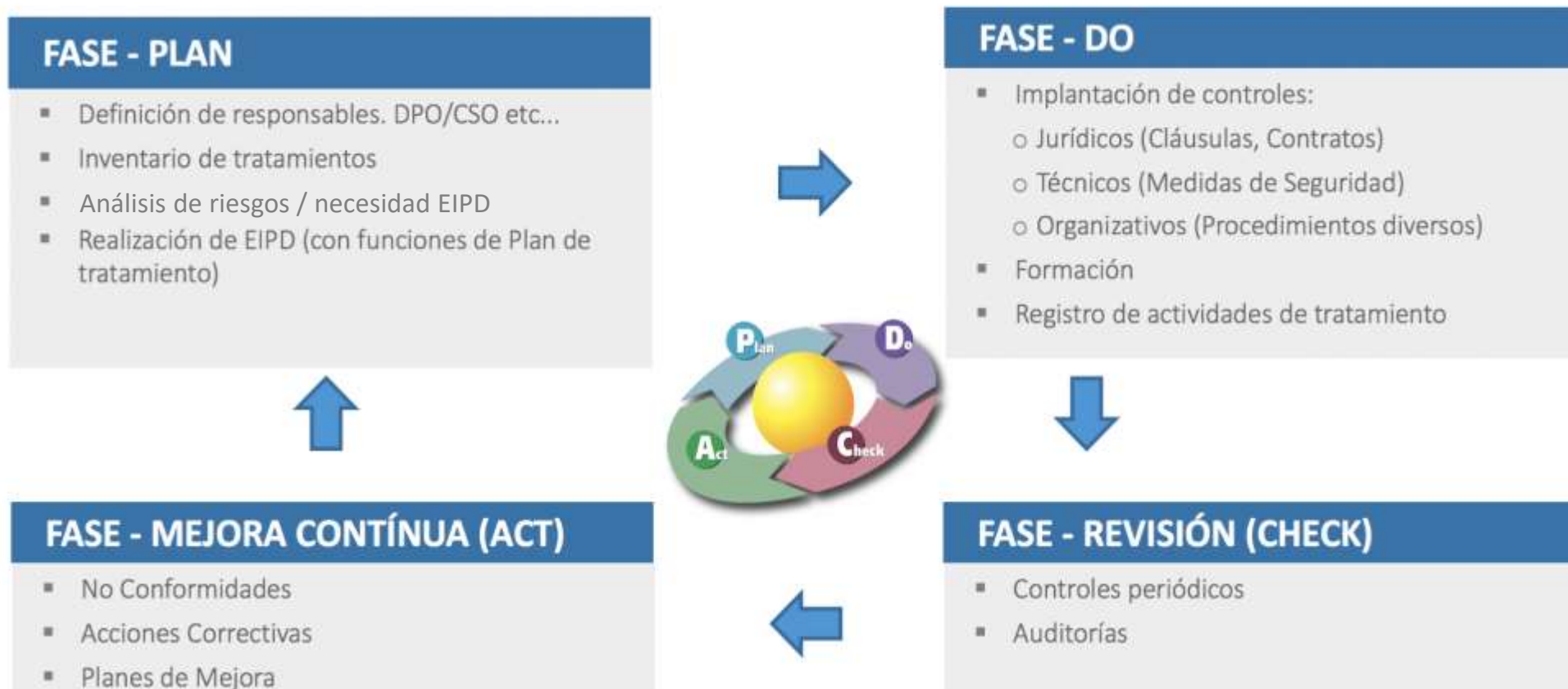
Definir factores de riesgo específicos, más allá de los generales

Operaciones relacionadas con los fines de tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal.
Tipos de datos utilizados	Factores de riesgo relacionados con el ámbito del tratamiento que se derivan de los datos recogidos, procesados o inferidos en el tratamiento.
Extensión y alcance del tratamiento	Factores de riesgo relacionados con el ámbito del tratamiento relativos al número de sujetos afectados, la diversidad de datos o aspectos tratados, la duración en el tiempo, el volumen de datos, la extensión geográfica, la exhaustividad sobre la persona, la frecuencia de recogida, etc.
Categorías de interesados	Factores de riesgo relacionados con el ámbito del tratamiento relativos a la categoría de interesados, como empleados, menores, mayores, personas en situación de vulnerabilidad, víctimas, discapacitados, etc.

Factores técnicos del tratamiento	Factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnologías.
Recogida y generación de datos	Factores de riesgo que se derivan de la naturaleza del tratamiento al recogerse o generarse datos de forma específica.
Efectos colaterales del tratamiento	Factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento.
Categoría del responsable/encargado	Factores de riesgo que se derivan del contexto específico del sector de actividad, modelo de negocio o tipo de entidad.
Comunicaciones de datos	Factores de riesgo que se derivan del contexto en el que se realizan las comunicaciones de datos a terceros en el marco del tratamiento.
Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales.

IDEAS CLAVE

No es un documento, es un proceso



IDEAS CLAVE

Enfoque de riesgos es **pilar esencial de la gestión de la protección del derecho fundamental a la protección de datos**

CAPÍTULO IV. Responsable del tratamiento y encargado del tratamiento

SECCIÓN 1. Obligaciones generales

Artículo 24. Responsabilidad del responsable del tratamiento.

“1. Teniendo en cuenta:

- *la **naturaleza, el ámbito, el contexto y los fines** del tratamiento*
- *así como los **riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas,***
- *el **RESPONSABLE DEL TRATAMIENTO** aplicará **medidas técnicas y organizativas apropiadas** a fin de garantizar y poder **demostrar** que el tratamiento es conforme con el presente Reglamento. Dichas medidas se **revisarán y actualizarán** cuando sea necesario”.*

Muchas gracias

