10ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ANÁLISIS DE RIESGOS EVALUACIÓN IMPACTO BRECHAS DE SEGURIDAD

Andrés Calvo y Charo Heras
Unidad de Evaluación y Estudios Tecnológicos

¿Te pesa el Reglamento?

SI

LA AEPD

¿BENEFICIA O DIFICULTA?

CONCLUSIÓN

- El RGPD es una herramienta que favorece el desarrollo de la economía digital
- Entre sus objetivos está que los ciudadanos confíen en los tratamientos de sus datos personales
- En consecuencia, potenciar el mercado interior

RESPONSABILIDAD PROACTIVA

Los responsables, aplicarán

- Las medidas técnicas y organizativas apropiadas para garantizar
- Y estar en condiciones de demostrar
- Que el tratamiento de datos personales se lleva a cabo de conformidad con el Reglamento.

Tales medidas se revisarán y actualizarán cuando sea necesario

LA SEGURIDAD

- Las medidas de seguridad es uno de los aspectos que ha sufrido más cambios con la aplicación del RGPD
- No existen medidas definidas según la tipología de los datos tratados
- Desaparecen los niveles de seguridad, es decir no se habla de nivel de seguridad bajo, medio o alto
- Desaparecen las medidas de seguridad asociadas a dichos niveles pero eso no significa que las medidas ya implantadas haya que eliminarlas

LA SEGURIDAD

- Art. 9 LOPD:

  El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las **medidas de índole técnica y organizativas necesarias …**

- Título VIII RD 1720/2007:

  artículo 81.7: Las medidas incluidas en cada uno de los niveles descritos anteriormente **tienen la condición de mínimos exigibles,** sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

DOS FORMAS DE VER LA SEGURIDAD

TÍTULO VIII

RD 1720/2007

INTEGRIDAD

CONFIDENCIALIDAD

DISPONIBILIDAD

LA SEGURIDAD

LA SEGURIDAD

- El responsable debe aplicar medidas de **seguridad técnicas** y organizativas para garantizar un nivel de seguridad adecuado al riesgo.

- Debe tener en cuenta:
  - Estado de la técnica
  - Costes de aplicación
  - Naturaleza, alcance, contexto y fines del tratamiento
  - Riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas

LA SEGURIDAD

- **Medidas a incluir**:
  - Seudonimización y cifrado
  - Garantizar confidencialidad, integridad, disponibilidad y resiliencia permanente de sistemas y servicios de tratamiento
  - Capacidad de restaurar la disponibilidad y el acceso a los datos (rápido ante incidente físico o técnico)
  - Proceso de verificación, evaluación y valoración regular de la eficacia de las medidas

- Se deben tener en cuenta los **riesgos** como consecuencia de la destrucción, pérdida o alteración de los datos personales
  - Transmitidos, conservados o tratados de otra forma
  - La comunicación o acceso no autorizado

RIESGO

- Aparece el concepto de **riesgo**
- **Riesgo** para los derechos y libertades de los ciudadanos
- El concepto de seguridad va más allá de la implantación de medidas de seguridad técnicas
- El responsable del tratamiento debe decidir qué medidas técnicas y organizativas son las apropiadas en su organización para garantizar el nivel de seguridad adecuado a la probabilidad y gravedad del riesgo

RIESGO

Riesgos para los **derechos y libertades de las personas físicas**:

Tratamiento de datos que pudieran provocar:

- daños y perjuicios físicos
- problemas de discriminación
- usurpación de identidad o fraude
- pérdida financiera
- daños para la reputación
- perdida de confidencialidad de datos sujetos al secreto profesional
- reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo

EVALUACIONES DE IMPACTO

Herramienta preventiva que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos.

"ANTES DEL TRATAMIENTO" si es de alto riesgo

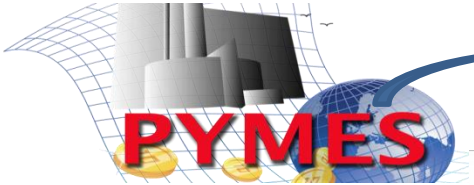
Debe realizarla el Responsable no el DPD

Cuándo:

- Evaluación sistemática y exhaustiva de aspectos personales (perfiles)
- Tratamientos a gran escala
- Observación sistemática a gran escala de una zona de acceso público

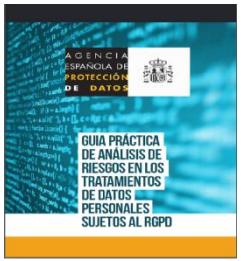
HAY QUE AYUDAR

2.800.000 inscritos en la SS



RGPD FACILITA
HERRAMIENTA PARA TRATAMIENTOS DE ESCASO RIESGO

Tratamientos que no son de escaso riesgo



FACILITA

- Herramienta gratuita
- Tratamientos de escaso riesgo
- Tres pantallas:
  - Sector de actividad (sanidad, banca)
  - Tipo de datos tratados (origen racial, salud)
  - Tratamientos realizados (perfiles)
- Documentos mínimos indispensables
  - Clausula informativa
  - Registro actividades tratamiento
  - Contratos
  - Medidas de seguridad

FACILITA

Si la actividad de su organización pertenece a alguno de estos sectores, márquelo:

- ☐ Sanidad
- ☐ Solvencia patrimonial y crédito
- ☐ Generación y uso de perfiles
- ☐ Actividades políticas, sindicales o religiosas
- ☐ Servicios de telecomunicaciones
- ☐ Seguros
- ☐ Entidades bancarias y financieras
- ☐ Actividades de servicios sociales
- ☐ Publicidad
- ☐ Videovigilancia masiva (Videovigilancia de grandes infraestructuras como estaciones de ferrocarril o centros comerciales)
- ○ Ninguno de los anteriores

FACILITA

HERRAMIENTA PARA TRATAMIENTOS DE ESCASO RIESGO

Los datos que incorpore en el programa desde esta pantalla hasta la finalización del programa, se van a utilizar para elaborar los documentos que se generan automáticamente adaptados a su organización

Nombre de la empresa

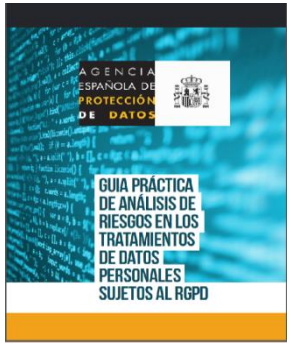
Dirección completa de la empresa

N.I.F.:

Teléfono

GUIA ANALISIS DE RIESGOS

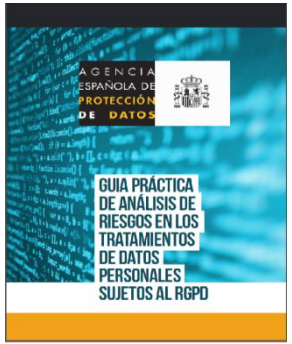
Hoja de ruta ante una actividad de tratamiento



1. ¿Puedo usar Facilita?

2. ¿PIA? Analizar
   - Listas de tratamientos previstos en art. 35
   - Naturaleza (categorías especiales, gran escala …)
   - Alcance (toma decisiones con efectos jurídicos ..)
   - Contexto (uso nuevas tecnologías …)
   - Fines de tratamiento (elaboración perfiles …)

GUIA ANALISIS DE RIESGOS



Gestión de riesgos:

Tareas para controlar la incertidumbre que provoca una amenaza.

Etapas:

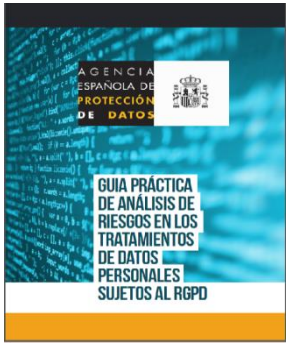
Monitorización continua

- Identificar amenazas
- Evaluar los riesgos
- Tratar los riesgos

Análisis de riesgos:
Proceso sistemático para estimar la magnitud de los riesgos a que está expuesto un sistema o una organización.

GUIA ANALISIS DE RIESGOS

Contenido



- Registro de actividades de tratamiento
  - Qué es y qué debe incluir
- Análisis básico de riesgos
  - Descripción de las operaciones de las actividades de tratamiento
  - Gestión de riesgos por defecto
- Anexos (plantillas)
  - Análisis de necesidad de EIPD
  - Descripción de actividades de tratamiento
  - Documentar el análisis básico de riesgos

GUIA DE EVALUACION DE IMPACTO

Debe incluir:

- Descripción sistemática de la actividad de tratamiento
- Evaluación de la necesidad y proporcionalidad del tratamiento
- Evaluación de los riesgos
- Medidas previstas para afrontar los riesgos

Etapas:

- Análisis preliminar (necesidad de EIPD)
- Contexto (ciclo vida datos y necesidad y proporcionalidad tratamiento)
- Gestión de riesgos (identificar amenazas e identificar, evaluar y tratar riesgos)
- Conclusiones (plan de acción)
- Supervisión (supervisar y revisar la implantación)

GUIA DE EVALUACION DE IMPACTO

Contenido

- Metodología
- Cuestiones
  - Cuándo revisarla
  - Qué ocurre si adherido a un código de conducta
  - Puedo realizar el tratamiento cuando la EIPD presenta un riesgo elevado
- Anexos (plantillas)
  - Análisis de documentación del ciclo de vida de datos asociados a una actividad de tratamiento
  - Análisis de la necesidad y proporcionalidad del tratamiento
  - Gestión de riesgos
  - Plan de acción
- Catálogo de amenazas

LISTADO CUMPLIMIENTO NORMATIVO

- ✓ Referenciado en Guías
- ✓ Riesgos asociados al cumplimiento de requisitos regulatorio relacionados con los derechos y libertades de las personas
- ✓ Método básico para que responsables y encargados puedan valorar su nivel de cumplimiento del RGPD
- ✓ Documento de ayuda al DPD en tareas de supervisión y asesoramiento

LISTADO CUMPLIMIENTO NORMATIVO

LISTADO DE CUMPLIMIENTO DEL RGPD	CUMPLE SI / NO
PRINCIPIOS RELATIVOS AL TRATAMIENTO	
Se recogen los datos personales con fines determinados	
Se recogen los datos personales con fines explícitos	
Se recogen los datos personales con fines legítimos	
Se tratan ulteriormente de manera incompatible con otros fines	
Los datos personales se mantienen exactos	
Se mantienen actualizados	
Se rectifican los datos personales inexactos respecto de la finalidad	
Se suprimen los datos personales inexactos respecto de la finalidad	
Se mantienen durante más tiempo del necesario respecto de la finalidad	
Se tratan con fines de archivo en interés público	
Se tratan con fines de investigación científica	
Se tratan con fines históricos	
Los datos personales se tratan con fines estadísticos	

LISTADO CUMPLIMIENTO NORMATIVO

LICITUD DEL TRATAMIENTO	
Se tiene consentimiento para cada finalidad del tratamiento	
El tratamiento es necesario para ejecutar un contrato o precontrato	
Existe obligación legal	
El tratamiento es necesario para proteger intereses vitales	
El tratamiento es necesario para el cumplimiento de interés público	
El tratamiento es necesario para satisfacer intereses legítimos	

CONDICIONES PARA EL CONSENTIMIENTO	
Se puede demostrar que el afectado dio su consentimiento para el tratamiento	
Se puede demostrar que el tratamiento se realiza como resultado del cumplimiento de una obligación legal	
Se solicita el consentimiento de forma clara e independiente de los demás asuntos	
Se solicita el consentimiento de forma inteligible y de fácil acceso	
Se solicita usando lenguaje claro y sencillo	
Se informa con carácter previo a recabar el consentimiento	

BRECHAS DE SEGURIDAD

- ✓ El registro de incidencias sigue siendo necesario (Art. 90 RD 1720/2007)
- ✓ Obligación de notificar salvo cuando sea improbable que exista un riesgo para los derechos y libertades de las personas
- ✓ No todos los incidentes de seguridad se deben notificar
- ✓ Obligación de notificar: de la LGT al RGPD

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.aepd.es

@AEPD_es #10SesiónAEPD

10ª Sesión Anual Abierta de la Agencia Española de Protección de Datos