



Protección de datos en Sistemas IA del Sector Público:

Metodología para Responsables y DPDs



Consejo de Transparencia
y Protección de Datos
de Andalucía



Principios Fundamentales de la Metodología

Características Principales

1

Experiencia, Mejores Prácticas y Enfoque Cualitativo

2

Adaptabilidad

3

Coordinación Normativa

4

Esfuerzo Proporcional

5

Responsabilidad Proactiva

6

Guía Estructurada

7

EIPD Integrada

8

Reflexión Profunda

Beneficios Clave

Acompañamiento Integral

Reutilización Eficiente

Elevado Nivel de Protección

Rol Central del Delegado de Protección de Datos



Configuración Automática por Proyecto

Participación de la administración según tipo de adquisición en el ciclo de vida del SIA



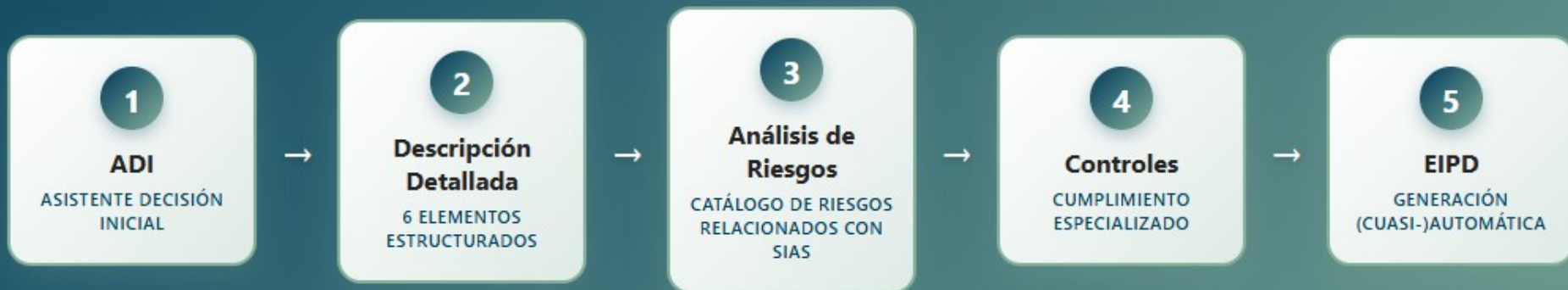
Participación de la Administración

● Participación directa ○ Responsabilidad del proveedor



Metodología Protección de Datos en Sistemas de IA

Flujo de Trabajo para Administraciones Públicas



Metodología Integrada y Adaptativa

Flujo secuencial que se adapta automáticamente al tipo de proyecto SIA y perfil de cumplimiento





1

Asistente de Decisión Inicial (ADI)

7 preguntas clave para caracterizar el proyecto

Inputs: Descripción preliminar y 7 Preguntas Estratégicas

Se caracteriza el proyecto respondiendo estas preguntas

1. Tipo de Adquisición del SIA

¿Cómo va a obtener/implementar el sistema de IA?

Ej: A) Desarrollo interno / E) Servicio tercero (API)

2. Naturaleza de las Decisiones

¿Cuál es la naturaleza de las decisiones que tomará el sistema?

Ej: B) Recomendaciones con supervisión / C) Decisiones automatizadas

3. Tipos de Datos Personales

¿Qué tipos de datos personales procesará el sistema?

Ej: Datos básicos, económicos, salud, biométricos

4. Colectivos Afectados

¿Qué colectivos se verán afectados por el sistema?

Ej: Menores, Ciudadanía en general, Empleados públicos, colectivos vulnerables

5. Evaluación Preliminar RIA

¿El sistema podría clasificarse como de alto riesgo según el Reglamento de IA?

Ej: Claramente NO / Probablemente Sí / No estoy seguro

6. Riesgos Preliminares RGPD

¿Identifica alguno de estos riesgos preliminares de protección de datos?

Ej: Falta base jurídica, impedimentos derechos, transferencias

7. Recursos y Capacidades

¿Cuáles son los recursos disponibles para la supervisión del proyecto?

Ej: Limitados / Moderados / Amplios



1

Asistente de Decisión Inicial (ADI)

7 preguntas clave para caracterizar el proyecto

GENERA AUTOMÁTICAMENTE

Outputs: Resultados del Análisis

El ADI recomienda automáticamente la configuración óptima de Cumplimiento

Perfil de Cumplimiento

Determina la intensidad y extensión de Cumplimiento requerido

ESENCIAL

30 riesgos + 62 controles

ESTÁNDAR

45 riesgos + 154 controles

EXHAUSTIVO

60 riesgos + 178 controles

Necesidad EIPD

Evalúa si es necesaria, recomendada o no necesaria la EIPD

Necesaria

Recomendada

No necesaria

Controles Aplicables

Identifica qué controles específicos se aplican según el tipo de adquisición

Configuración automática de los 8 Grupos de Controles según tipo de Adquisición A/B/C/D/E



2

Descripción Detallada del Proyecto

6 elementos esenciales

1. Definición y Evaluación Inicial

Problema a resolver, justificación del uso de IA y alcance de participación de la administración

2. Características Técnicas

Tipo de tecnología IA, funcionalidades principales, integración con sistemas existentes y limitaciones

3. Clasificación RIA

Categoría según Reglamento de IA, justificación de clasificación y obligaciones aplicables

4. Tratamientos de Datos

Actividades de tratamiento, finalidades, bases jurídicas, categorías de datos y plazos de conservación

5. Contexto Normativo y Organizativo

Marco normativo y organizativo específico, área responsable y procesos principales afectados

6. Actores y Responsabilidades

Responsable del tratamiento, roles clave, interlocutores con DPD, cadena de encargados y transferencias internacionales



3

Análisis de Riesgos (AARR)

Descripción y Análisis sistemático de 60 riesgos específicos para SIA

* Podrán añadirse otros propios del proyecto

Análisis Sistemático de Riesgos

Aplicación del catálogo de 60 riesgos específicos filtrados automáticamente según características del proyecto

Riesgos Identificados

Filtrado automático por contexto

Evaluación de Criticidad

Probabilidad × Impacto

Asignación a Controles: Riesgo Residual

Mapeo automático riesgo→controles/nivel de madurez



4

Controles de Cumplimiento

8 Grupos de Controles especializados

Adaptación por Perfil de Cumplimiento:

ESENCIAL: 62 controles

ESTÁNDAR: 154 controles

EXHAUSTIVO: 178 controles

Evaluación de Madurez de Controles:

1

No implementado

Sin implementar o solo documentación básica

2

Básico

Implementación inicial, aplicación inconsistente

3

Gestionado

Procedimientos definidos, aplicación consistente

4

Optimizado

Mejora continua, métricas, revisión periódica

1. Justificación y Diseño

Fundamentación del uso de IA, alternativas consideradas y verificación de riesgos desde el análisis sistemático

12

2. Anonimización

Técnicas aplicadas, verificación de riesgos de reidentificación identificados y controles de acceso

20

3. Obtención de Datos

Técnicas aplicadas, verificación de riesgos de reidentificación identificados y controles de acceso

20

4. Desarrollo y Entrenamiento

Arquitectura técnica, métricas de calidad y verificación de riesgos técnicos del modelo

15

5. Proveedores

Cadena de suministro, pliegos de contratación y mitigación de riesgos de gestión de proveedores

26

6. Verificación EIPD

Compleitud de EIPD, coherencia riesgo↔medida y marco de cumplimiento continuo

10

7. Validación Pre-despliegue

Pruebas funcionales, cálculo de riesgos residuales y documentación técnica

36

8. Monitorización Continua

Supervisión operativa de riesgos identificados, gestión de cambios y auditorías periódicas

39



5

Evaluación de Impacto en Protección de Datos

Generación (cuasi-)automática desde respuestas de elementos y controles

Descripción Sistemática

Información consolidada desde elementos descriptivos y controles sobre responsables, finalidades, datos y destinatarios

Necesidad y Proporcionalidad

Justificación y análisis de alternativas extraídos principalmente del Control 1 y elementos descriptivos

Análisis de Riesgos

Sección generada automáticamente desde el AARR con matriz completa de riesgos y mitigación

Medidas de Mitigación

Medidas técnicas y organizativas consolidadas desde los controles aplicables al proyecto



ADI: Caso Específico de Menores de Edad

Activación automática de protecciones reforzadas cuando el SIA trata datos de menores



Detección Automática

La presencia de datos personales de menores activa protecciones especiales



Cumplimiento Reforzado

Aumenta el nivel de Cumplimiento necesario del proyecto



EIPD Necesaria

Considera EIPD necesaria en el contexto de nuevas tecnologías



Riesgos Específicos

Activa riesgos particulares que requieren valoración y mitigación

Riesgos Siempre Activos para Menores

1

Personal No Capacitado

Falta de formación específica en IA y protección de menores

2

Reducción de Autonomía

Impacto negativo en capacidad de autodeterminación y desarrollo

3

Efectos Psicológicos

Generación de estrés, ansiedad o efectos negativos por monitorización

4

Manipulación del Comportamiento

Explotación de vulnerabilidades específicas de menores



Sistema de Alertas de Fase de Licitación

Herramienta de apoyo que evalúa el estado de preparación en relación con la fase actual del proceso de contratación pública.

Fases del Proceso de Licitación

1

Planificación

Definición de necesidades y marco básico

2

Elaboración de Pliegos

Base informativa para criterios técnicos

3

Licitación

Base informativa + análisis preliminar

4

Adjudicación

Metodología completa para evaluación

5

Ejecución

Metodología + marco de cumplimiento

6

Recepción

Metodología + evaluación cumplimiento

Estados de Criticidad



Momento Ideal

Preparación suficiente o superior para la fase



Importante

Desfase moderado en preparación



Urgente

Desfase significativo con riesgo de calidad



Crítico

Riesgo grave de decisiones incorrectas

Funcionamiento del Sistema



Evalúa elementos descriptivos completados



Analiza estado del AARR (No iniciado/Parcial/Completo)



Genera alertas contextuales según fase actual



Proporciona recomendaciones específicas