UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

GUÍA PRÁCTICA PARA LAS EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE LOS DATOS SUJETAS AL RGPD

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD

Enfoque ejecutivo de privacidad, gestión de riesgos y ciberseguridad

Documento fuente: Agencia Española de Protección de Datos (AEPD) | Síntesis técnica en español

1. Síntesis ejecutiva

La guía de la Agencia Española de Protección de Datos desarrolla un marco práctico para realizar Evaluaciones de Impacto en la Protección de Datos (EIPD) conforme al Reglamento General de Protección de Datos (RGPD). Su tesis central es que la protección de datos debe gestionarse de forma preventiva, basada en riesgos y desde el diseño. La EIPD no es un trámite documental aislado: es un proceso de gobierno que permite anticipar daños potenciales sobre los derechos y libertades de las personas, determinar si un tratamiento es viable y establecer controles técnicos, organizativos y legales antes de que el riesgo se materialice.

El RGPD exige una EIPD cuando sea probable que un tratamiento entrañe un alto riesgo. La evaluación debe realizarse antes de la puesta en marcha del tratamiento y revisarse cuando cambie de manera relevante el contexto o el nivel de riesgo. La guía enfatiza la responsabilidad proactiva del responsable del tratamiento: conocer qué datos procesa, con qué finalidad, mediante qué tecnologías, quién interviene, qué amenazas existen y qué salvaguardas son necesarias.

Idea clave: una EIPD eficaz conecta privacidad, cumplimiento, seguridad de la información y gestión de riesgos en un único proceso de decisión.

2. Alcance y contenido mínimo de una EIPD

De acuerdo con el artículo 35.7 del RGPD, la evaluación debe contener, como mínimo:

- Descripción sistemática de las operaciones de tratamiento y de sus finalidades.
- Evaluación de la necesidad y proporcionalidad del tratamiento respecto de la finalidad perseguida.
- Evaluación de los riesgos para los derechos y libertades de los interesados.
- Medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que permitan demostrar conformidad con el RGPD.

La guía organiza la EIPD en tres grandes bloques: contexto del tratamiento, gestión de riesgos y conclusión/validación. A ello añade la comunicación y consulta previa a la autoridad de control cuando el riesgo residual siga siendo elevado, así como la supervisión posterior de la implantación de los controles.

3. Gobierno, responsabilidades y participación

La obligación de realizar la EIPD corresponde al responsable del tratamiento. El Delegado de Protección de Datos (DPD), cuando exista, cumple una función de

asesoramiento y monitorización, pero no sustituye la responsabilidad del responsable. La ejecución puede apoyarse en personal interno o externo y requiere involucrar a quienes conocen el tratamiento: seguridad de la información, tecnología, riesgos, asesoría jurídica, áreas de negocio y, cuando corresponda, encargados del tratamiento e interesados o sus representantes.

Actor	Papel principal	Enfoque
Responsable del tratamiento	Asume y rinde cuentas por la EIPD	Decide viabilidad y controles
DPD	Asesora y monitoriza	Cumplimiento y derechos de los interesados
Encargado	Colabora y aporta garantías/información	Riesgos del servicio y medidas aplicadas
Seguridad/TI/Jurídico/Negocio	Aporta conocimiento especializado	Amenazas, arquitectura, legitimación y operación

4. Metodología práctica para la EIPD

La metodología propuesta busca objetividad, trazabilidad, repetibilidad y comparabilidad. Antes de comenzar deben definirse el equipo, las tareas, los hitos y la forma de documentar análisis, decisiones, conclusiones y plan de acción.

1. Describir el ciclo de vida: Identificar captura, clasificación/almacenamiento, uso/tratamiento, cesión o acceso por terceros y destrucción; mapear datos, sistemas, intervinientes, tecnologías y flujos.

2. Analizar necesidad y proporcionalidad: Verificar base legitimadora, finalidad, minimización, conservación y si existen alternativas menos invasivas.

3. Identificar amenazas y riesgos: Determinar escenarios capaces de causar daño o vulnerar derechos y libertades a lo largo de todo el ciclo de vida.

4. Evaluar riesgos: Estimar probabilidad e impacto desde el punto de vista de la persona afectada y calcular el riesgo inherente.

5. Tratar riesgos: Seleccionar controles y recalcular el riesgo residual. El objetivo no es riesgo cero, sino un nivel aceptable.

6. Plan de acción y conclusión: Asignar controles, responsables y plazos; decidir si el tratamiento puede realizarse o requiere rediseño/consulta previa.

7. Supervisar y revisar: Comprobar la implantación real de las medidas y actualizar la EIPD cuando cambien el tratamiento o sus riesgos.

5. Contexto: ciclo de vida, datos y legitimación

La calidad de la EIPD depende de comprender el tratamiento con suficiente detalle. Debe documentarse qué se hará con los datos, para qué, qué categorías se utilizarán, de quién proceden, dónde se almacenan, qué terceros acceden, qué sistemas intervienen y cómo se eliminan. Este inventario permite identificar puntos de exposición que un análisis exclusivamente tecnológico podría omitir.

La guía exige aplicar el principio de minimización: los datos deben ser adecuados, pertinentes y limitados a lo necesario. La necesidad y proporcionalidad se valoran preguntando si la finalidad puede alcanzarse razonablemente sin tratar datos personales o mediante medios menos invasivos. El juicio de proporcionalidad comprende idoneidad, necesidad y proporcionalidad en sentido estricto.

Si el tratamiento no es necesario o proporcional, debe reformularse o rediseñarse antes de continuar con la evaluación de riesgos.

6. Gestión de riesgos con enfoque de ciberseguridad

La guía distingue la EIPD de un análisis de riesgos corporativo tradicional: el centro de la evaluación es el impacto sobre el interesado, no únicamente la pérdida para la organización. Las amenazas deben analizarse a lo largo del ciclo de vida e incluyen acceso ilegítimo, fuga de información, ataques de hacking o suplantación, modificación no autorizada, errores de captura, uso ilegítimo, pérdida o indisponibilidad de datos y fallos tecnológicos u organizativos.

El riesgo inherente se estima antes de considerar controles mediante la relación Riesgo = Probabilidad × Impacto. La guía propone cuatro niveles para cada variable: despreciable (1), limitado (2), significativo (3) y máximo (4). Con la matriz resultante, el riesgo se clasifica como bajo (1-2), medio (>2 y ≤6), alto (>6 y ≤9) o muy alto (>9).

Prob. \ Impacto	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

Una vez identificados los riesgos, pueden adoptarse cuatro respuestas: reducción, retención, transferencia o anulación. Los controles pueden ser organizativos (procedimientos, gestión de incidentes y vulnerabilidades), legales (cláusulas, consentimiento y garantías contractuales) o técnicos (control de acceso, cifrado, copias de seguridad, autenticación, pseudonimización, entre

otros). Después de aplicarlos se recalculan probabilidad e impacto para obtener el riesgo residual.

7. Controles, riesgo residual y plan de acción

El riesgo residual representa la exposición que permanece después de aplicar las medidas de control. La guía ilustra este enfoque con datos de salud almacenados en un dispositivo móvil: autenticación reforzada, cifrado y pseudonimización pueden reducir de forma sustancial tanto la probabilidad de acceso no autorizado como el impacto para el interesado. Cada riesgo debe tratarse de forma individual y con tantas medidas como sean necesarias hasta alcanzar un nivel aceptable.

La EIPD concluye con un plan de acción que, como mínimo, identifica el control, su descripción, el responsable de implantación y el plazo. Para tratamientos nuevos, las medidas deben incorporarse a los requerimientos desde el diseño. Para tratamientos existentes, debe impulsarse una iniciativa de adecuación y fijarse un plazo máximo; si el riesgo residual no es aceptable, puede ser necesario interrumpir el tratamiento hasta implantar las salvaguardas.

8. Consulta previa, decisión y supervisión

Si el riesgo residual permanece alto o muy alto y no puede mitigarse adecuadamente, el responsable debe consultar a la autoridad de control antes de proceder. La consulta debe aportar información sobre responsabilidades, fines y medios del tratamiento, medidas y garantías, datos de contacto del DPD, la propia EIPD y cualquier otra información solicitada. Un tratamiento con riesgo residual elevado no debe iniciarse sin resolver esta situación.

Una conclusión favorable tampoco cierra el proceso: la viabilidad está condicionada a que los controles comprometidos se implanten. La guía recomienda supervisar la implantación y realizar una revisión posterior. La EIPD debe actualizarse cuando exista una variación relevante del contexto, por ejemplo, incorporación de nuevos canales, automatización, externalización, nuevas tecnologías, nuevas finalidades o categorías de datos.

9. Cuestiones operativas relevantes

- Encargados del tratamiento: deben apoyar al responsable y proporcionar garantías e información suficiente. Si no conocen todo el contexto, pueden realizar un análisis de riesgos del servicio y mantener un inventario de controles aplicables.

- Códigos de conducta: una metodología prevista en un código de conducta puede utilizarse para la EIPD, pero la adhesión no elimina la obligación de realizarla cuando corresponda.
- Opinión de los interesados: cuando proceda, el RGPD permite recabar la opinión de los interesados o sus representantes, protegiendo a la vez intereses comerciales o de negocio.
- Documentación: debe mantenerse trazabilidad suficiente para justificar las decisiones, los criterios de riesgo y la eficacia esperada de las medidas.

10. Valor de los anexos y aplicación práctica

La guía incorpora plantillas para documentar el ciclo de vida de los datos, analizar necesidad y proporcionalidad, gestionar riesgos y formalizar el plan de acción y la conclusión. También incluye un catálogo orientativo de amenazas y otro de amenazas con posibles soluciones. Estos anexos convierten el marco conceptual en una herramienta utilizable por equipos de privacidad, cumplimiento, seguridad de la información, tecnología y auditoría.

Desde una perspectiva de ciberseguridad, el principal aporte es integrar controles de confidencialidad, integridad y disponibilidad con riesgos jurídicos y de derechos fundamentales. Una fuga de información, una mala configuración, una suplantación de identidad, un malware o la pérdida de un dispositivo no se valoran solo por su impacto operativo, sino por las consecuencias concretas que pueden generar sobre las personas cuyos datos son tratados.

11. Conclusiones ejecutivas

- La EIPD debe incorporarse al gobierno del tratamiento desde la fase de diseño y no tratarse como una validación posterior.
- La decisión de continuar un tratamiento debe basarse en el riesgo residual y en la implantación efectiva de controles.
- Privacidad y ciberseguridad deben trabajar de forma coordinada: las salvaguardas técnicas son esenciales, pero no sustituyen la legitimación, minimización, proporcionalidad ni la gobernanza.
- El análisis debe centrarse en los derechos y libertades del interesado; esta perspectiva diferencia la EIPD del análisis de riesgos puramente empresarial.
- La revisión continua es obligatoria en la práctica: cambios tecnológicos, organizativos o funcionales pueden modificar el riesgo y exigir una nueva evaluación.

Conclusión: la EIPD es un mecanismo de decisión y control preventivo que permite demostrar responsabilidad proactiva y traducir los principios del RGPD en medidas concretas de privacidad y seguridad.

Nota sobre el idioma y la fuente

El archivo fuente ya se encuentra redactado en español. Por ello, este documento no realiza una traducción literal, sino una síntesis ejecutiva técnica en español, conservando la terminología esencial del RGPD y de la guía de la AEPD.

Fuente base: Agencia Española de Protección de Datos, «Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD».