

Checklist descargable: ¿está tu EIPD / DPIA listo para la Ley 21.719?

Antes de cerrar una EIPD, conviene verificar que cubra todo lo que la Ley 21.719 espera de un análisis de alto riesgo. Este checklist resume los elementos que no pueden faltar. Funciona como control final: si alguna respuesta es “no”, probablemente necesitas ajustar, ampliar o documentar mejor tu evaluación.

¿El tratamiento está claramente descrito?

Un **sí** significa que el tratamiento está definido con precisión: qué datos se usarán, para qué, quién participa y cómo fluye la información. Un **no** indica falta de claridad operativa, lo que deja la EIPD sin base para evaluar riesgos y vuelve imposible justificar decisiones ante la Agencia.

¿Se identifican bases legales y categorías de datos?

Un **sí** implica que dejaste registrado por qué puedes tratar esos datos y qué tipo de información manejas (comunes, sensibles, menores, laborales). Un **no** revela un riesgo inmediato: no puedes demostrar legitimidad del tratamiento ni dimensionar correctamente la sensibilidad y exposición de los titulares.

¿Se ha evaluado necesidad y proporcionalidad?

Un **sí** confirma que revisaste si todos los datos son necesarios y si el tratamiento no es excesivo. Un **no** sugiere posible sobre-recolección o finalidades poco justificadas, lo cual puede aumentar sanciones e incluso invalidar el tratamiento por falta de minimización y claridad de propósito.

¿Se ha hecho un análisis de riesgos con criterios claros?

Un **sí** indica que aplicaste escalas coherentes de impacto y probabilidad, y priorizaste riesgos de forma razonada. Un **no** muestra que el análisis es superficial o inconsistente, dificultando decidir qué medidas adoptar y dejando la EIPD vulnerable ante auditorías por falta de trazabilidad metodológica.

¿Se definieron medidas de mitigación concretas (incluyendo en dispositivos)?

Un **sí** refleja que las medidas son reales, aplicables y medibles: controles técnicos, organizativos, contractuales y acciones sobre endpoints (inventario, borrado remoto, bloqueo). Un **no** significa que la EIPD quedó en diagnóstico sin acciones, lo que no demuestra diligencia ni reduce riesgos para los titulares.

¿La EIPD ha sido aprobada por los responsables adecuados?

Un **sí** confirma revisión formal del DPO, el comité de privacidad y la dirección, dejando evidencia del proceso. Un **no** implica que la EIPD carece de validación institucional, lo que debilita su fuerza legal y puede dejar decisiones sin respaldo ante la Agencia o auditorías internas.