

# Conclusión

## Evaluación del Impacto sobre la Protección de Datos (DPIA)

Una Pre-DPIA evalúa si el tratamiento previsto de datos personales plantea un alto riesgo para el interesado. Dependiendo de la jurisdicción, el tamaño y la naturaleza del proyecto, y el tipo de datos que vayan a tratarse, puede ayudar a determinar si entonces puede ser necesaria una DPIA completa.

Una evaluación completa del impacto sobre la protección de datos (DPIA) está diseñada para evaluar los riesgos para la privacidad. Cuando así lo exijan las leyes o normativas locales, será necesario realizar una DPIA al iniciar un nuevo proyecto, introducir uno nuevo o modificar significativamente una aplicación, producto o servicio existente con un alto impacto en los datos personales.

## Registros de Actividades de Tratamiento (ROPA)

El tratamiento de datos personales debe documentarse en los Registros de Actividades de Tratamiento (ROPA). Detalla qué tipo de datos personales se están tratando, dónde y por qué se conservan, y quién tiene acceso a ellos. Para más información, ponte en contacto con tu equipo local de Information Governance, el Delegado/a de Protección de Datos o con el equipo de Compliance.

## Riesgos de la IA

El uso de la IA conlleva algunos riesgos que hay que mitigar. Entre ellos figuran:

- Prejuicios y discriminación: La IA solo puede tomar decisiones sobre los datos a los que tiene acceso y no sobre todo el contexto.
- Falta de transparencia: puede ser difícil explicar cómo se toman las decisiones, especialmente cuando no hay intervención humana en la toma de decisiones.
- Seguridad de la información: existe la posibilidad de que los grandes sistemas sean pirateados, accediendo y exponiendo grandes volúmenes de datos personales.

Zurich trabaja de forma responsable con su conjunto de principios de IA Responsable, como la seguridad, la transparencia, la responsabilidad y la fiabilidad.

## Marco de gestión de riesgos

Además de trabajar de acuerdo con los principios de la IA Responsable, nuestro uso de la IA se rige por nuestro marco de gestión de riesgos, incluidas las políticas de Privacidad de Datos y Seguridad de la Información, así como nuestra guía AIAF. Estas orientaciones incorporan las mejores prácticas del sector para evaluar los sistemas de IA en términos de precisión, explicabilidad e imparcialidad, entre otros factores, a lo largo de su ciclo de vida.

Para obtener más información, ponte en contacto con tu equipo local de Information Governance, el Delegado/a de Protección de Datos o con el equipo de Compliance.

## A quién dirigirse

Ponte en contacto con tu equipo local de Information Governance, el Delegado/a de Protección de Datos o con el equipo de Compliance para cualquier consulta sobre IA.

