

Decálogo sobre el ISO/IEC 27701

1. Privacidad a otro nivel: Este estándar es como una extensión del famoso ISO 27001 (gestión de seguridad de la información), pero enfocado en la privacidad. Es decir, te ayuda a gestionar los datos personales de una manera segura y correcta.
2. Cumple con las leyes: Te asegura que tu organización esté alineada con leyes de protección de datos, como el GDPR en Europa o cualquier otra legislación de privacidad que aplique.
3. Rol de controlador y procesador: Define claramente si tu organización es un "controlador" (el que decide qué se hace con los datos) o un "procesador" (el que solo los maneja según indicaciones).
4. Mapas de privacidad: Te obliga a tener bien claro dónde están los datos personales, cómo los usas y con quién los compartes.
5. Riesgos bajo control: Te ayuda a identificar riesgos relacionados con los datos personales y te dice cómo mitigarlos para evitar problemas.
6. Políticas claras: Establece que debes crear políticas y procedimientos claros para la protección de los datos personales.
7. Protección en la práctica: No basta con tener políticas; también debes asegurarte de que se apliquen en la vida diaria de la empresa.
8. Derechos de los individuos: Debes garantizar que las personas (dueños de los datos) puedan ejercer sus derechos, como pedir acceso, corrección o eliminación de sus datos personales.
9. Cultura de privacidad: El estándar fomenta que todos en la organización, desde el becario hasta el CEO, estén concienciados con la privacidad y sepan cómo actuar en su día a día.

10. Mejora continua: No es solo implementar el sistema y olvidarse. ISO/IEC 27701 requiere que revises, midas y mejores continuamente la forma en que manejas los datos personales.