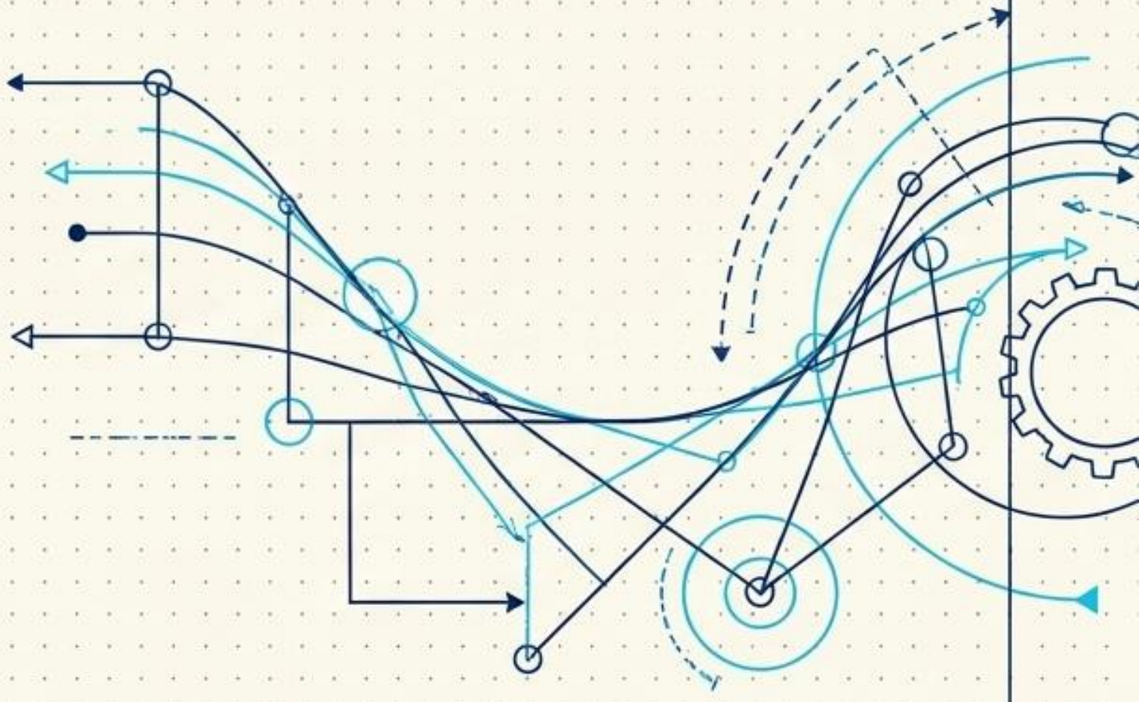
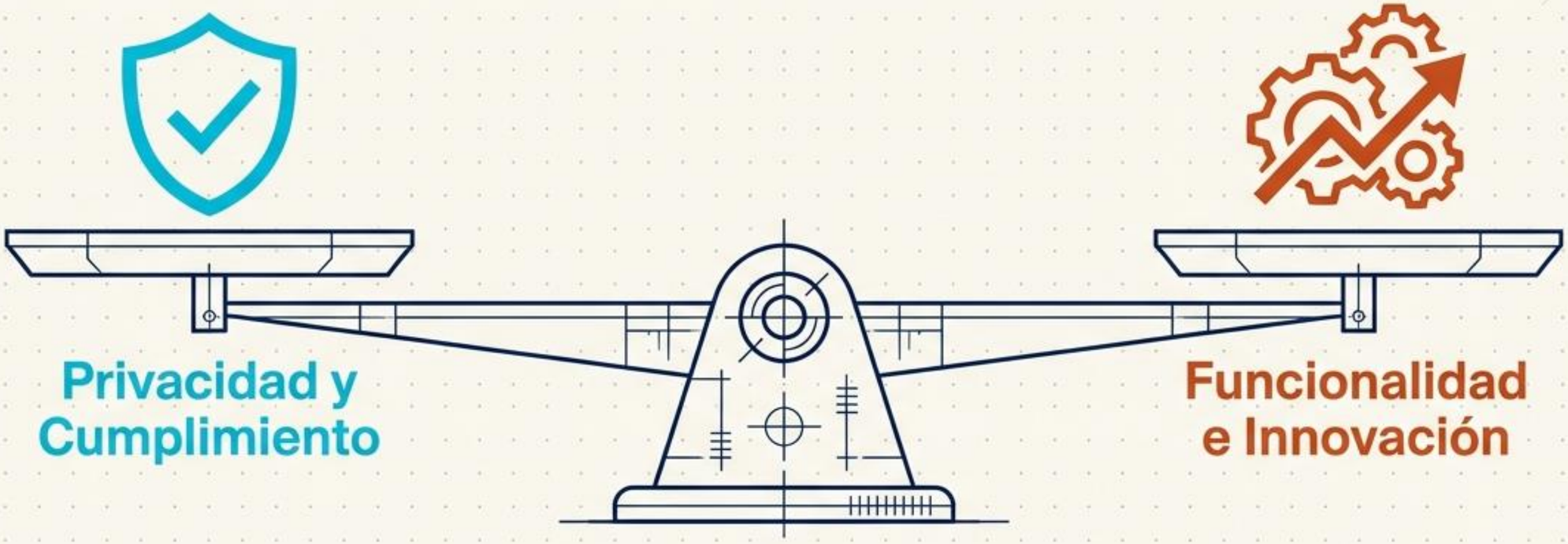
De la auditoría reactiva a la arquitectura proactiva



Evolución estratégica de la protección de datos y Privacidad por Diseño

La protección de datos exige un balance sistémico, no un sacrificio



El Mito (Suma Cero)	La Realidad (Suma Positiva)
Falsa dicotomía donde proteger los datos significa ralentizar el negocio operativo.	La privacidad integrada habilita la confianza digital y acelera la adopción de productos.

El Delegado de Protección de Datos supervisa, pero no es el auditor

El Rol (ISO 19011 apartado 6.4.2)

Actúa como observador imparcial. Acompaña al equipo auditor sin influir ni interferir en la evaluación objetiva del sistema.

La Misión

Garantizar que las conclusiones y hallazgos lleguen directamente al órgano de gobierno. Por principio de independencia, nunca audita su propio trabajo.

Una auditoría no es una fotografía fija, es la línea base de la evolución

Visión obsoleta:
Hecho aislado

Visión estratégica:
Seguimiento eficaz

- **Contexto Normativo:** Aunque la LODPD no regula el régimen de auditorías, exige una continua revisión del cumplimiento.
- **Evolución Documentada:** Cada informe debe comparar formalmente los hallazgos actuales con auditorías previas para evidenciar la trayectoria.

El motor central de la privacidad: El ciclo de mejora continua

PLANIFICAR

Identificación de riesgos, Evaluaciones de Impacto (DPIA), mapeo de datos.

HACER

Implementación técnica y organizativa de controles.

VERIFICAR

Ejecución de auditorías y medición de indicadores clave (KPIs).

ACTUAR

Ejecución de acciones correctivas y capitalización de oportunidades (ISO 19011 cap. 6.7).

La mejora continua real exige evidencia, no intenciones en papel

ERRORES FRECUENTES

- ✗ Cerrar acciones sin verificar eficacia.
- ✗ Falta de documentación en el seguimiento.
- ✗ Ignorar la comparativa con auditorías previas.
- ✗ Mejora continua meramente teórica ('en papel').

CÓMO SE DEMUESTRA EL ÉXITO

- ✓ Acciones correctivas rígidamente documentadas.
- ✓ Priorización de recursos y tiempos reales.
- ✓ Medición empírica de resultados.
- ✓ Evidencia auditable de eficacia final.

Taxonomía de las acciones de mejora en protección de datos

1. Correctivas (Ante incumplimientos)

- Implementar MFA.
- Cifrar bases de datos sensibles.
- Regularizar contratos con encargados.

2. Proactivas (De diseño)

- Automatizar gestión de incidentes.
- Mapas de datos en tiempo real.
- Ejecutar DPIAs previas.

3. De Medición

- Definir KPIs de cumplimiento.
- Monitorear tiempos de respuesta (Derechos ARCO+).

4. Culturales

- Integrar cumplimiento en el código de ética.
- Programas de concienciación continua.

El límite del modelo reactivo: La necesidad del “Desplazamiento a la Izquierda”

Reparar problemas de privacidad después de construidos los sistemas genera deuda técnica y riesgo masivo. La evolución exige empujar la responsabilidad hacia el inicio del ciclo de vida.

Privacidad por Diseño (PbD): La arquitectura como escudo preventivo

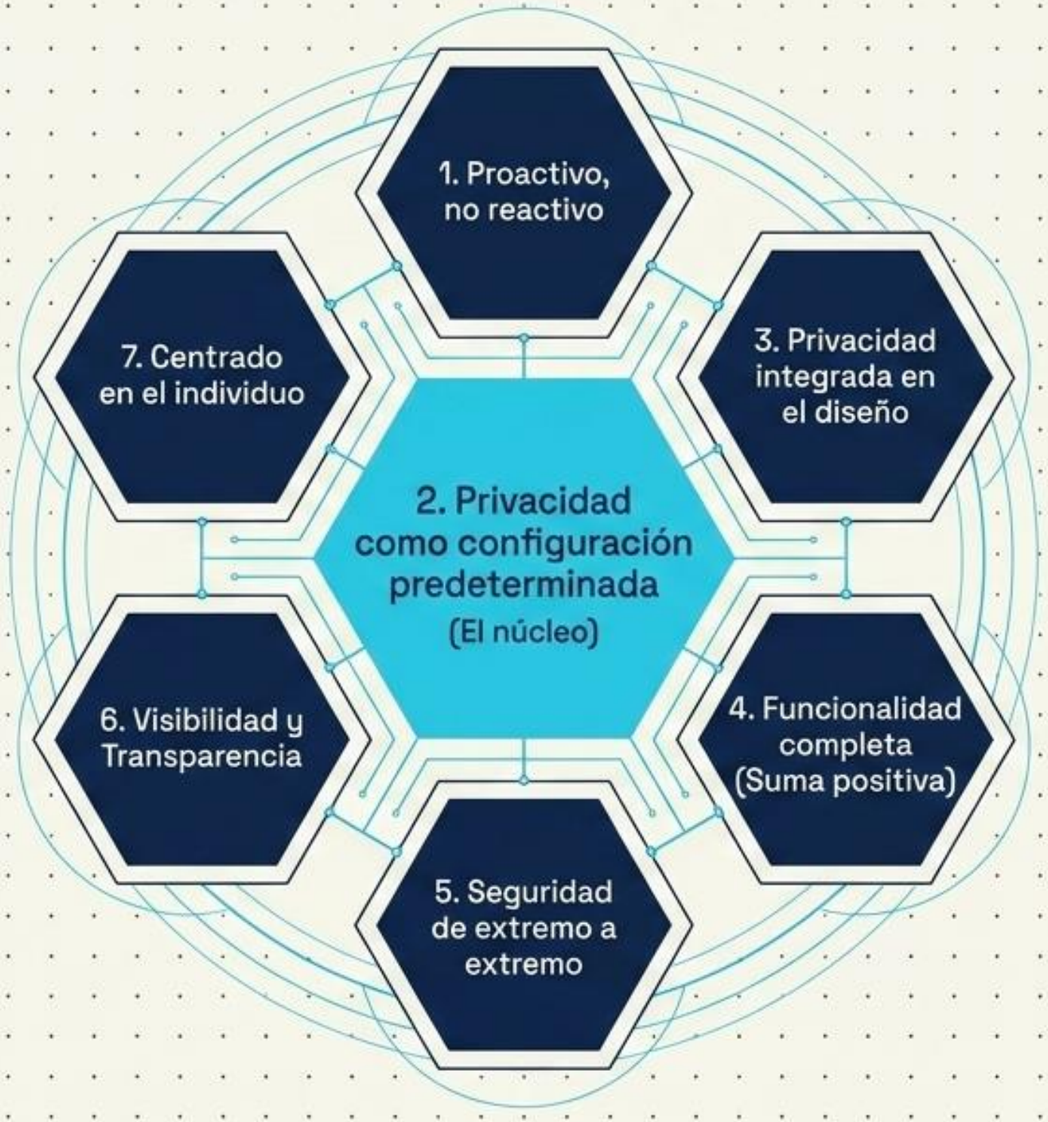
El Mandato Legal:

Entendido como el deber del responsable de tener en cuenta en las primeras fases de concepción que los tratamientos entrañan riesgos... e implementar medidas técnicas y organizativas desde el diseño.

(Art. 39 LOPDP / Art. 25 RGPD)

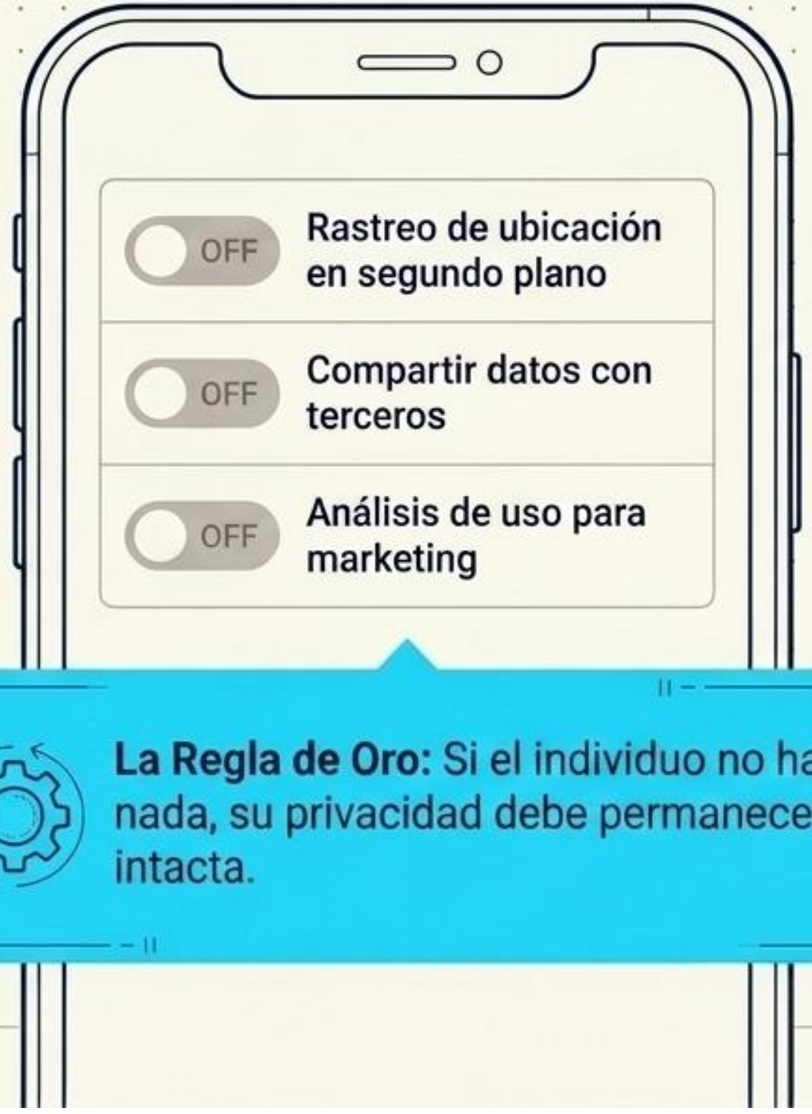
> "La privacidad debe incorporarse a los sistemas y tecnologías de datos en red, de forma predeterminada... integrada en cada estándar, protocolo y proceso."
>
> – Dra. Ann Cavoukian
> (Creadora del marco PbD en 1990)

Los 7 Principios Fundamentales de la Privacidad por Diseño



Seguridad de extremo a extremo: De la cuna a la tumba

Privacidad por Defecto: Inacción del usuario = Máxima protección



La Regla de Oro: Si el individuo no hace nada, su privacidad debe permanecer intacta.

Las 4 Dimensiones de la Minimización	
	1. Cantidad: Solo recoger los datos personales estrictamente necesarios.
	2. Extensión: Limitar la profundidad del tratamiento aplicado.
	3. Plazo: Conservación estrictamente sujeta a tiempos predefinidos.
	4. Accesibilidad: No accesible a un número indeterminado de personas sin intervención.

La cadena de suministro: Exigencia técnica a proveedores y terceros

Selección Condicionada: Seleccionar únicamente productos y encargados que garanticen la protección desde el diseño.

Vectores de Riesgo Integrados: Todo contenido de terceros (ej. SDKs móviles) debe ser auditado; heredan la responsabilidad de privacidad.

Alcance Total: Obligatorio para organizaciones de todo tamaño y vinculante incluso en el diseño de contratos públicos (Considerando 78 RGPD).

Hoja de ruta para la integración organizacional

El modelo de madurez estratégica de la privacidad

Nivel 3: Sistémico y Arquitectónico

Privacidad por Diseño y por Defecto. El cumplimiento es el cimiento técnico sobre el que se construye la confianza empresarial.

Nivel 2: Dinámico y Gestionado

Implementación del ciclo de mejora continua (PDCA). Medición de KPIs y evolución comparativa documentada.

¡GRACIAS!