



**We build incredible
digital solutions**

¿Qué debe tener mi hoja de ruta Digital?

Para cumplir con la ley 21.719

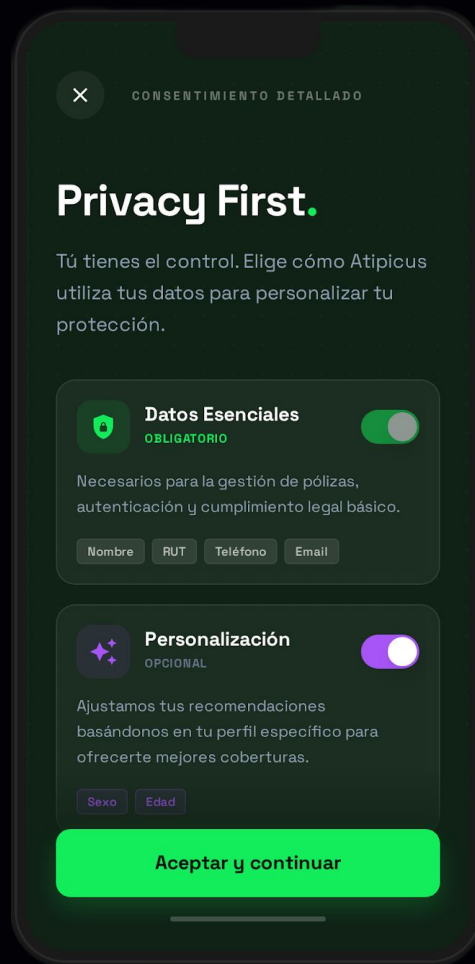


**Canales
digitales de
asegurados.**

1. Consentimiento

Base legal clara, trazable y revocable

- Consentimiento explícito y por finalidad (no genérico).
- Gestión digital: captura, versionado, revocación y evidencia.
- Beneficiarios: reglas claras de representación y trazabilidad.
- Lenguaje simple + UX clara.
- Evidencia legal auditable en todo momento.



2. Derechos ARCO

Derechos ejercibles en autoservicio

- Derechos:
 - Acceso
 - Rectificación
 - Cancelación (Supresión)
 - Oposición
- Canales digitales: web, app, email formal.
- Flujo estándar: solicitud → tracking → respuesta.
- Registro de cumplimiento para fiscalización.



3. Implementar MFA

Una barrera extra frente a contraseñas inseguras

- Qué es MFA: Contraseña + segundo factor (token sms o email).
- El problema son contraseñas débiles o filtradas son inevitables.
- El valor del MFA:
 - Bloquea accesos aún con contraseña comprometida.
 - Reduce fraude y suplantación.
 - Fortalece la defensa legal ante incidentes.



4. Decisiones automatizadas

Automatización explicable y revisable

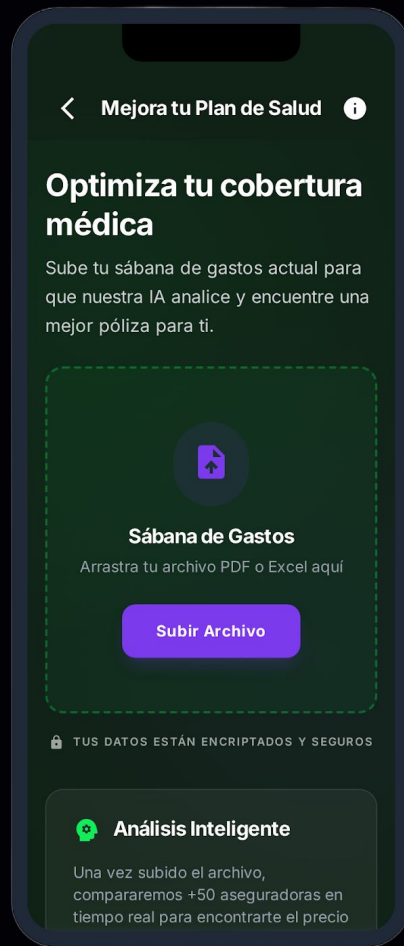
- Identificación de procesos automatizados críticos.
- Transparencia sobre datos y lógica general (difícil en legados).
- Canal para oposición y revisión humana efectiva.



5. Portabilidad

De obligación legal a ventaja competitiva

- Datos portables en formato estructurado (y ojalá común).
- Benchmark: portabilidad financiera < telco.
- Habilita ecosistemas y nuevos modelos.



**Canales
digitales de
ejecutivos.**

1. Prospección y Cotización

Venta compliant por diseño

- Uso obligatorio de CRM y herramientas oficiales.
- Eliminación de Excel, WhatsApp personal y canales informales.
- Prohibición de BD compradas sin base legal.
- Auditoría continua de fuentes de datos.

2. Suscripción

Digital, trazable y explicable

- Suscripción digital como estándar.
- Decisiones automatizadas con fallback humano.
- Minimización real de datos utilizados.
- Evidencia lista para fiscalización.

3. Administración

Uso consistente con la finalidad

- Separación de datos operacionales y analíticos.
- IoT / telemetría con consentimiento explícito.
- Retención limitada y controlada.
- Revisión periódica de permisos.

4. Siniestros

Sistemas aptos para la ley de protección de datos

- Control de accesos a terceros (liquidadores, clínicas, talleres) o software propio para liquidar.
- Contratos con obligaciones de seguridad y eliminación.
- Principio de mínimo acceso necesario.

5. Renovación

Data-driven sin datos personales

- Uso de datos anonimizados o seudonimizados.
- Modelos sin reidentificación.
- Separación analytics vs operación.
- Gobierno claro del dato.

La implementación de la ley de protección de datos es cultural

No basta solo con tecnología, tenemos que cambiar prácticas que están instauradas en la industria





**We build incredible
digital solutions**