



Política de Privacidad y Protección de Datos Personales

Servicios Tecnológicos AVIM SpA

CÓDIGO	VERSIÓN	CLASIFICACIÓN
5.2-PL02	1.0	PÚBLICO
FECHA DE ESTA VERSIÓN	ESTADO	PRÓXIMA REVISIÓN
21-09-2026	Vigente	Enero 2027
ELABORADO POR	REVISADO POR	APROBADO POR
Responsable de privacidad	Encargado del SGI	Administración General

Este documento impreso o descargado constituye COPIA NO CONTROLADA. La versión vigente reside en el repositorio del SGI de AVIM.

Identificación y control del documento

Información documentada según ISO/IEC 27001, 27701 y 42001, cláusula 7.5.

Identificación

- Código único: 5.2-PL02
- Documento derivado de la Política del SGI (5.2-PL01)
- Versión y clasificación en cada página
- Numeración de páginas en formato N / total

Responsabilidades

- Elaboración y mantención: Responsable de privacidad
- Revisión de idoneidad: Encargado del SGI
- Aprobación y vigencia: Administración General
- Difusión y registro de acuse: Administración

Distribución y acceso

- Versión controlada: repositorio del SGI de AVIM
- Documento de clasificación pública
- Audiencia: titulares, clientes, personal y terceros
- Publicable en el sitio web y en propuestas comerciales

Vigencia, revisión y retención

- Revisión anual, o ante cambio legal o de alcance
- Próxima revisión: Enero 2027
- Cambios comunicados dentro de 45 días de aprobados
- Retención de versiones y registros: 5 años

Trazabilidad de cambios

Cada versión registra fecha, responsable y descripción del cambio.

VERSIÓN	FECHA	ELABORADO / APROBADO	DESCRIPCIÓN DEL CAMBIO
1.0	21-09-2026	Responsable de privacidad / Administración General	Creación del documento. Desarrolla la operativa de protección de datos personales que la Política del SGI (5.2-PL01) enuncia como principio: categorías de datos, finalidades y bases de licitud, ciclo de vida, transferencias, subencargados, derechos de los titulares y canal de ejercicio. Alineado a la Ley N° 21.719 y a ISO/IEC 27701.

Este documento no reemplaza los anexos de tratamiento de datos de cada contrato: los desarrolla y les da un marco común.

Estructura de la política

Catorce capítulos: del ámbito de aplicación al canal de ejercicio de derechos y la vigencia.

01	Propósito, alcance y aplicación	08	Transferencias internacionales
02	Roles: Responsable y Encargado	09	Subencargados y terceros
03	Categorías de datos que tratamos	10	Derechos de los titulares
04	Finalidades y bases de licitud	11	Vulneraciones y notificación
05	Ciclo de vida del dato personal	12	Personal: reserva y formación
06	Medidas de seguridad	13	Contacto y ejercicio de derechos
07	Datos personales en flujos de IA	14	Aprobación, vigencia y disposiciones finales

Anexos: trazabilidad normativa, definiciones y documentos relacionados.

Qué cubre esta política

Desarrolla el capítulo de privacidad de la Política del SGI y aplica a todo dato personal bajo control de AVIM.

Qué cubre

- Datos tratados por cuenta de clientes en la prestación de servicios
- Datos de nuestros propios productos y sistemas internos
- Datos de contacto comercial, postulantes y personal
- Datos que circulan por flujos de trabajo con modelos de IA

A quiénes obliga

- Socios, administradores y ejecutivos
- Trabajadores dependientes y a honorarios
- Consultores, contratistas y subcontratistas
- Proveedores y terceros que traten datos por cuenta de AVIM

PRINCIPIO RECTOR

Tratamos datos personales solo cuando existe una finalidad legítima, una base de licitud identificada y los controles necesarios para protegerlos. Ante la duda entre recopilar y no recopilar, no recopilamos.

Dos roles, obligaciones distintas

El rol que AVIM asume en cada tratamiento determina qué obligaciones le corresponden.

AVIM como Encargado

- Aplica a los servicios prestados por cuenta de clientes
- Tratamiento solo bajo instrucciones documentadas del Responsable
- Uso limitado a los fines contractualmente establecidos
- Devolución o eliminación de los datos al término del contrato
- Asistencia ante solicitudes de titulares y auditorías

AVIM como Responsable

- Aplica a productos y sistemas internos propios de AVIM
- Finalidades legítimas, explícitas y documentadas
- Base de licitud identificada y registrada para cada tratamiento
- Información transparente a los titulares sobre el tratamiento
- Atención directa de las solicitudes de derechos

DETERMINACIÓN DEL ROL

El rol se establece por contrato antes de iniciar cualquier tratamiento y queda registrado en el registro de actividades de tratamiento. No se presume.

Qué datos tratamos

Inventario por categoría. El detalle por servicio se mantiene en el registro de actividades de tratamiento.

Identificación y contacto

- Nombre, RUT, cargo, correo y teléfono corporativo
- Datos de contraparte en contratos, propuestas y licitaciones
- Origen: el titular, el cliente o fuentes de acceso público

Datos operativos y técnicos

- Registros de acceso, trazas de auditoría y métricas de uso
- Identificadores de sesión y de equipo en entornos gestionados
- Origen: generados por la operación de los sistemas

Datos en fuentes del cliente

- Datos presentes en repositorios, bases y documentos del cliente
- Tratados como Encargado y dentro del entorno acordado
- Origen: el cliente, en el marco del contrato de servicio

Datos sensibles

- Solo cuando el contrato lo exige y existe base legal expresa
- Medidas reforzadas de cifrado, control de acceso y registro
- Nunca se incorporan a entornos no productivos

Para qué tratamos cada dato

Toda finalidad nueva requiere base legal identificada y registro previo.

FINALIDAD	ROL DE AVIM	BASE DE LICITUD
Prestación de los servicios contratados	Encargado	Instrucción documentada del Responsable
Gestión contractual, facturación y cobranza	Responsable	Ejecución del contrato
Soporte, comunicación y atención al cliente	Responsable	Ejecución del contrato
Seguridad, trazabilidad y prevención de incidentes	Responsable	Interés legítimo y obligación legal
Cumplimiento de obligaciones legales	Responsable	Obligación legal
Comunicación comercial a contactos de negocio	Responsable	Consentimiento revocable

LÍMITE ABSOLUTO

No utilizamos datos de clientes para entrenar modelos públicos o compartidos, ni para finalidades distintas de las declaradas, sin consentimiento explícito y documentado.

Del ingreso a la eliminación

Cada etapa tiene un control asociado y deja evidencia.

01

Recopilación

- Solo los datos necesarios para la finalidad
- Origen identificado y registrado
- Información al titular como Responsable

02

Uso y acceso

- Mínimo privilegio y necesidad de conocer
- Registro de accesos sobre datos sensibles
- Sin uso para fines no autorizados

03

Conservación

- Plazos por tipo de dato y obligación legal
- Revisión de los datos ya innecesarios
- Sin conservación indefinida por defecto

04

Eliminación

- Eliminación segura o anonimización
- Devolución o destrucción al fin del contrato
- Certificado de destrucción si se requiere

EVIDENCIA

Cada etapa del ciclo deja registro en el sistema documental del SGI. Sin evidencia, el control no es auditable y se considera no implementado.

Cómo protegemos los datos

Medidas técnicas y organizativas proporcionales al riesgo, gobernadas por el SGSI certificado.

01

Control de acceso

Mínimo privilegio, autenticación reforzada y revisión periódica de permisos. El acceso se concede por función, no por persona.

02

Cifrado

Cifrado en tránsito y en reposo, con gestión de claves separada de los datos.

03

Segregación de entornos

Los entornos de desarrollo y prueba no contienen datos personales reales.

04

Respaldo y recuperación

Respaldos periódicos con restauración probada, para garantizar disponibilidad e integridad.

05

Registro y trazabilidad

Trazas de auditoría conservadas de modo que no puedan alterarse sin dejar rastro.

06

Privacidad desde el diseño

La arquitectura considera la protección de datos antes del desarrollo, no como capa añadida.

El dato que llega al modelo

Compromisos específicos para el tratamiento de datos personales en sistemas de IA.

Qué hacemos

- Detección y enmascaramiento antes del envío al modelo
- Pseudonimización reversible cuando el caso de uso lo requiere
- Registro de qué categorías de datos alcanzan cada modelo
- Evaluación de impacto previa al despliegue de un sistema nuevo

Qué no hacemos

- No entrenamos modelos públicos con datos de clientes sin consentimiento
- No incorporamos datos personales reales a conjuntos de prueba
- No permitimos decisiones autónomas que afecten derechos
- No operamos modelos sobre los sistemas productivos del cliente

SUPERVISIÓN HUMANA

Toda salida de un sistema de IA que pueda afectar a una persona queda sujeta a revisión humana antes de producir efectos.

Dónde residen los datos

La soberanía de los datos es una decisión de arquitectura, no un efecto secundario del proveedor.

Condiciones de la transferencia

- Base legal identificada antes de cualquier transferencia
- Resguardos contractuales con el destinatario
- Registro de las jurisdicciones de almacenamiento y proceso
- Información al cliente sobre la ubicación de sus datos

Opciones de residencia

- Despliegue en territorio nacional cuando el contrato lo exige
- Arquitecturas soberanas sobre infraestructura del cliente
- Restricción de regiones en los proveedores de nube
- Verificación documentada de la residencia efectiva

COMPROMISO

Cuando un cliente exige residencia nacional de los datos, esa exigencia se traduce en una restricción técnica verificable, no en una declaración contractual.

Quién más puede tocar los datos

La cadena de tratamiento se declara, se controla y se puede auditar.

Condiciones de incorporación

- Autorización previa del cliente antes de incorporar un subencargado
- Debida diligencia documentada de seguridad y privacidad
- Traslado íntegro de las obligaciones por contrato
- Inventario de subencargados y de su ámbito de acceso

Control durante la relación

- Revisión periódica de certificaciones e informes
- Notificación al cliente ante cambio de subencargados
- Término de la relación ante incumplimiento
- Verificación de la eliminación de datos al cierre

RESPONSABILIDAD NO DELEGABLE

La contratación de un tercero no transfiere nuestra responsabilidad ante el cliente ni ante los titulares de los datos. Respondemos por la cadena que elegimos.

Qué puede exigir un titular

Derechos reconocidos por la Ley N° 21.719, ejercibles de forma gratuita.

Acceso

Conocer qué datos tratamos, con qué finalidad, de qué fuente provienen y a quién han sido comunicados.

Rectificación

Corregir los datos inexactos, desactualizados o incompletos que obren en nuestros sistemas.

Cancelación

Solicitar la eliminación cuando los datos ya no son necesarios o el tratamiento carece de base legal.

Oposición

Oponerse a un tratamiento determinado, incluida la comunicación comercial y las decisiones automatizadas.

Portabilidad

Recibir los datos en formato estructurado o solicitar su transferencia a otro responsable.

Bloqueo

Suspender el tratamiento mientras se resuelve una solicitud de rectificación u oposición.

Qué ocurre cuando algo falla

Una vulneración de datos personales se gestiona como incidente del SGI, con plazos y evidencia.

01

Detección

Toda sospecha se reporta y registra de inmediato, con hora, alcance estimado y categorías de datos involucradas.

02

Evaluación

Análisis del riesgo para los derechos de los titulares afectados, que determina el alcance de la notificación.

03

Notificación

Comunicación al cliente Responsable, a la autoridad de protección de datos y a los titulares cuando corresponda.

04

Remediación

Corrección de la causa raíz, verificación del control fallido y actualización de la matriz de riesgos.

PLAZOS

Los plazos de notificación se rigen por la Ley N° 21.719 y por lo pactado en cada contrato, prevaleciendo el más exigente de ambos.

Quien accede al dato responde por él

El deber de secreto no termina con la relación laboral o contractual.

Deber de reserva

- Compromisos individuales de confidencialidad firmados por todos
- Vigencia posterior al término de la relación contractual
- Prohibición de extraer o divulgar datos personales
- Consecuencias disciplinarias y legales ante el incumplimiento

Formación y conciencia

- Inducción obligatoria dentro de los primeros 30 días de ingreso
- Al menos una sesión anual de protección de datos personales
- Refuerzo por rol para quienes operan datos, modelos o infraestructura
- Registro de asistencia y evaluación de comprensión

ALCANCE

Estas obligaciones se extienden a consultores, contratistas y a cualquier tercero que acceda a datos personales por cuenta de AVIM.

Cómo ejercer un derecho

Canal único, gratuito y con plazo de respuesta.

CANAL DE PRIVACIDAD

privacidad@avim.ai

Consultas y ejercicio de derechos sobre datos personales.

DIRECCIÓN

Av. Providencia 1208

Oficina 207, Providencia, Santiago de Chile.

PLAZO DE RESPUESTA

Según Ley N° 21.719

Acuse de recepción y respuesta dentro del plazo legal.

Qué incluir en la solicitud

- Identificación del titular y acreditación de identidad
- Derecho que se ejerce y datos sobre los que recae
- Medio y dirección para recibir la respuesta

Si el dato es de un cliente

- Como Encargado, la solicitud se deriva al Responsable
- Informamos al titular a quién corresponde atenderla
- Asistimos al Responsable con la información y los plazos

Si la respuesta no le satisface, el titular puede reclamar ante la Agencia de Protección de Datos Personales.

Vigencia y disposiciones finales

VERSIÓN 1.0 — 21-09-2026	ESTADO Vigente	PRÓXIMA REVISIÓN Enero 2027	APROBACIÓN Administración General
Obligatoriedad El cumplimiento es obligatorio para todas las personas y entidades alcanzadas por el capítulo 01. Su incumplimiento se trata conforme al Programa de Integridad (5.2-PL03).	Relación con otros documentos Desarrolla el capítulo de privacidad de la Política del SGI (5.2-PL01). Los anexos de tratamiento de cada contrato la complementan y prevalecen en lo específico.		
Prevalencia Ante conflicto prevalece la norma legal aplicable y la obligación contractual, sin perjuicio de los estándares internos más exigentes que AVIM haya adoptado.	Vigencia Entra en vigencia en la fecha de aprobación. Sus actualizaciones se comunican a clientes y titulares dentro de los 45 días siguientes.		

Qué requisito cubre cada capítulo

Matriz de referencia para auditoría interna y de certificación.

CAPÍTULO	REFERENCIA LEGAL	REFERENCIA DE NORMA
01 Propósito y aplicación	Leyes N° 19.628 y 21.719	ISO/IEC 27701 — cl. 5.2 y 6
02 Roles	Ley N° 21.719 — responsable y encargado	ISO/IEC 27701 — cl. 7 y 8
03 y 04 Categorías y finalidades	Ley N° 21.719 — licitud y finalidad	ISO/IEC 27701 — 7.2 y 8.2
05 Ciclo de vida del dato	Ley N° 21.719 — conservación	ISO/IEC 27701 — 7.4 y 8.4
06 Medidas de seguridad	Ley N° 21.719 — medidas de seguridad	ISO/IEC 27001 — Anexo A
07 Datos en flujos de IA	Ley N° 21.719 — decisiones automatizadas	ISO/IEC 42001 — A.5 y A.8
08 Transferencias internacionales	Ley N° 21.719 — flujos transfronterizos	ISO/IEC 27701 — 7.5 y 8.5
09 Subencargados y terceros	Ley N° 21.719 — encargados	ISO/IEC 27701 — 8.5; 27001 — A.5.19
10 Derechos de los titulares	Ley N° 21.719 — derechos ARCOP	ISO/IEC 27701 — 7.3 y 8.3
11 Vulneraciones y notificación	Ley N° 21.719 — notificación	ISO/IEC 27001 — A.5.24 a A.5.28
12 a 14 Personal, contacto y vigencia	Ley N° 21.719 — deber de secreto	ISO/IEC 27001 — cl. 7.2, 7.3 y 7.5

Definiciones y documentos relacionados

Definiciones

Dato personal

Información vinculada o referida a una persona natural identificada o identificable.

Dato sensible

Dato que revela la esfera íntima o cuyo uso indebido puede generar discriminación.

Titular

Persona natural a quien se refieren los datos personales.

Responsable de Tratamiento

Quien determina las finalidades y medios del tratamiento.

Encargado de Tratamiento

Quien trata datos por cuenta del Responsable, según sus instrucciones.

Vulneración de datos

Incidente que provoca pérdida, alteración o acceso no autorizado a datos.

Documentos y registros relacionados

CÓDIGO	DOCUMENTO O REGISTRO
5.2-PL02	Política de Privacidad (este documento)
5.2-PL01	Política del Sistema de Gestión Integrado
5.2-PL03	Programa de integridad y código de ética
5.2-DG01	Acuerdos individuales de confidencialidad
8.3-RG01	Registro de actividades de tratamiento
8.1-RG01	Registro de solicitudes de titulares
8.1-DG01	Inventario de subencargados autorizados
8.1-PR01	Procedimiento de gestión de incidentes

QUÉ ESPERAMOS DEL EQUIPO

Cuatro reglas que no se negocian

01

Minimizar

Trate solo los datos personales que la finalidad declarada realmente necesita.

02

Instruirse

Trate datos de clientes solo conforme a las instrucciones documentadas del contrato.

03

Registrar

Deje evidencia de accesos, decisiones y plazos: sin registro no hay auditoría.

04

Reportar

Informe de inmediato cualquier sospecha de vulneración de datos personales.

La protección de datos no se declara en un documento: se demuestra en cada tratamiento.

