



Política del Sistema de Gestión Integrado

Servicios Tecnológicos AVIM SpA

CÓDIGO	VERSIÓN	CLASIFICACIÓN
5.2-PL01	2.0	PÚBLICO
FECHA DE ESTA VERSIÓN	ESTADO	PRÓXIMA REVISIÓN
21-09-2026	Vigente	Enero 2027
ELABORADO POR	REVISADO POR	APROBADO POR
Encargado del SGI	Administración General	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-PL01
- Versión y clasificación en cada página
- Estado del documento explícito
- Numeración de páginas en formato N / total

Responsabilidades

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

Distribución y acceso

- Versión controlada: repositorio del SGI de AVIM
- Toda copia impresa o descargada es no controlada
- Audiencia: personal, consultores, clientes y terceros
- Disponible para las partes interesadas que lo soliciten

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	14-09-2026	Administración General	Emisión inicial de la Política General Integrada (ISO/IEC 27001 e ISO/IEC 27701).
2.0	21-09-2026	Encargado del SGI / Administración General	Ampliación del alcance a ISO/IEC 42001 y al rol de Responsable de Tratamiento; gobernanza de terceros, gestión de incidentes de IA y marco de objetivos; la operativa de datos personales se traslada a la Política de Privacidad (5.2-PL02).

Estructura de la política

Trece capítulos: del propósito y el alcance certificado a la vigencia y las disposiciones finales.

01	Propósito y alcance general
02	Alcance certificado del SGI
03	Compromiso de la Alta Dirección
04	Seguridad y robustez técnica
05	Privacidad: roles y principios
06	IA responsable y transparente
07	Evaluación de impacto y sostenibilidad

08	Gobernanza de terceros
09	Personas: reserva y competencia
10	Gestión de incidentes
11	Objetivos, indicadores y mejora
12	Gobernanza del SGI y responsabilidades
13	Aprobación, vigencia y disposiciones finales

Anexos: trazabilidad normativa, definiciones y documentos relacionados.

Qué establece y a quiénes obliga

Marco de principios y compromisos de la Alta Dirección para proteger la información, la privacidad y el uso responsable de la IA.

Qué establece

- Principios rectores del Sistema de Gestión Integrado
- Compromisos exigibles ante clientes y autoridades
- Marco para definir y medir los objetivos del SGI
- Base para las políticas y procedimientos específicos

A quiénes obliga

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

OBJETIVO PRINCIPAL

Proteger la información empresarial y personal que se nos confía, y gobernar el ciclo de vida de los sistemas de IA que proveemos, de modo que la adopción de IA de nuestros clientes no obligue a elegir entre innovación y cumplimiento.

Marco legal de referencia: Leyes N° 19.628 y 21.719 sobre protección de datos personales; Ley N° 19.886 de compras públicas; RGPD de la Unión Europea cuando resulte aplicable.

Tres sistemas, un solo perímetro

El SGI integra tres normas sobre el mismo perímetro operativo, cada una desde su ángulo.

ISO/IEC 27001

Seguridad de la información

Protección de la información empresarial y personal durante el diseño, desarrollo, provisión, implementación, soporte y operación de Servicios de Plataforma en la Nube Pública-Privada e infraestructura y soluciones de IA.

ISO/IEC 27701

Privacidad de la información

El mismo perímetro, actuando como Encargado de Tratamiento para los servicios prestados por cuenta de clientes y como Responsable de Tratamiento respecto de los productos y sistemas internos propios de AVIM.

ISO/IEC 42001

Gestión de IA

Provisión de servicios de plataforma de IA y de sistemas basados en PLN y modelos de lenguaje de gran tamaño, para la habilitación segura de cargas de trabajo de IA y la protección de datos personales en flujos con LLM.

DOCUMENTOS DE REFERENCIA

El alcance formal de cada sistema, con su redacción certificada y la Declaración de Aplicabilidad vigente, se mantiene en el documento de alcance del SGI. Esta política no lo reemplaza: lo respalda.

Lo que la Dirección asume

La Alta Dirección asume la responsabilidad sobre la eficacia del Sistema de Gestión Integrado.

DECLARACIÓN

La Alta Dirección de Servicios Tecnológicos AVIM SpA se compromete a cumplir los principios de esta política, alineados con ISO/IEC 27001, ISO/IEC 27701 e ISO/IEC 42001, y a aplicar a la propia organización cada control de gobernanza que recomienda a sus clientes.

RECURSOS

Provisión asegurada

Recursos técnicos, financieros y humanos para el desarrollo, mantenimiento y mejora del SGI.

CUMPLIMIENTO

Requisitos aplicables

Cumplimiento de los requisitos legales, regulatorios y contractuales que nos obligan.

MEJORA CONTINUA

Revisión periódica

Revisión por la Dirección de la eficacia del SGI y de la vigencia de esta política.

Esta política se comunica a todo el personal, está disponible para las partes interesadas que corresponda y constituye el marco para los objetivos del SGI.

Proteger la infraestructura y los modelos

Aplica con independencia de si la carga de trabajo involucra Inteligencia Artificial.

Protección de la infraestructura

- Confidencialidad, integridad y disponibilidad de la información
- Arquitecturas de IA, cómputo y nube pública, privada e híbrida
- Control de accesos con principio de mínimo privilegio
- Cifrado en tránsito y en reposo; respaldo y recuperación probados

Seguridad de los sistemas de IA

- Prevención de envenenamiento de datos y manipulación de modelos
- Controles frente a inyección de instrucciones en flujos con LLM
- Prevención de extracción no autorizada de información
- Segregación entre desarrollo, prueba y producción

PRINCIPIO DE NO INTRUSIÓN

La IA no opera sobre los sistemas productivos del cliente. Trabajamos sobre capas de datos preparadas y controladas, diseñadas para que el acceso del modelo quede acotado, registrado y reversible.

Dos roles, obligaciones distintas

El rol que asumimos en cada tratamiento determina qué obligaciones nos corresponden.

Encargado de Tratamiento

- Aplica a los servicios prestados por cuenta de clientes
- Tratamiento solo bajo instrucciones documentadas del Responsable
- Uso limitado a los fines contractualmente establecidos
- Sin uso de datos de clientes para entrenar modelos sin consentimiento

Responsable de Tratamiento

- Aplica a productos y sistemas internos propios de AVIM
- Finalidades legítimas, explícitas y documentadas
- Minimización: solo los datos necesarios para la finalidad
- Base de licitud identificada y registrada para cada tratamiento

DESARROLLO OPERATIVO

Las categorías de datos, finalidades, plazos de conservación, transferencias, derechos de los titulares y canales de ejercicio se desarrollan en la Política de Privacidad y Protección de Datos Personales (5.2-PL02), que forma parte de este Sistema de Gestión Integrado.

Seis compromisos sobre la IA

Criterios de decisión cuando una situación no está resuelta por una regla explícita.

01

Rol en el ciclo de vida

Cada contrato declara qué responsabilidades del ciclo de vida asumimos como proveedor y cuáles permanecen en el cliente.

02

Transparencia

Informamos sobre capacidades, limitaciones y naturaleza de los modelos empleados, distinguiendo entre pesos abiertos y modelos propietarios de terceros.

03

Uso previsto y límites

Nuestros sistemas asisten la decisión humana y hacen cumplir controles. No adoptan decisiones autónomas que afecten los derechos de las personas.

04

Equidad y no discriminación

Evaluamos los sistemas que diseñamos, integramos y operamos para identificar y mitigar sesgos algorítmicos.

05

Control humano

Mantenemos capacidad de intervención y supervisión humana en los sistemas críticos y en aquellos cuyas salidas puedan afectar a personas.

06

Propiedad intelectual

Respetamos la propiedad intelectual y las licencias del software, los datos y los modelos que utilizamos.

Evaluar antes de desplegar

La evaluación considera el riesgo para la organización y el impacto sobre las personas y la sociedad.

Antes del despliegue

- Evaluación de impacto del sistema de IA para nuevos servicios
- Evaluación de impacto en protección de datos cuando corresponda
- Registro de la decisión y de las medidas de mitigación

Durante la operación

- Monitoreo del comportamiento y de las salidas del sistema
- Reevaluación ante cambios de modelo, datos o finalidad
- Revisión de los controles cuando cambia el contexto de uso

Sostenibilidad

- Consideración del consumo energético del cómputo de IA
- Dimensionamiento proporcional a la necesidad real
- Arquitecturas que reduzcan la huella sin degradar el control

CONDICIÓN DE DESPLIEGUE

Ningún sistema de IA nuevo entra en operación sin evaluación de impacto documentada y aprobada. El resultado puede condicionar el despliegue, restringir el uso previsto o detenerlo.

Proveedores, plataformas y modelos

Nuestro modelo de servicio se apoya en infraestructura y modelos de terceros. Esa dependencia se gobierna.

Evaluación y selección

- Criterios documentados de seguridad, privacidad y gobernanza de IA
- Debida diligencia proporcional al riesgo antes de contratar
- Registro de certificaciones e informes de aseguramiento
- Verificación de licencias de modelos y conjuntos de datos

Control durante la relación

- Cláusulas de confidencialidad, datos y término por incumplimiento
- Inventario de proveedores críticos y de su ámbito de acceso
- Revisión periódica del desempeño y de sus certificaciones
- Las obligaciones se trasladan a los subencargados

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.

Quien opera sostiene la política

Compromisos exigibles a todo el personal, consultores y terceros que actúan por cuenta de AVIM.

Deber de reserva

- Compromisos individuales de confidencialidad firmados por todos
- Vigencia posterior al término de la relación laboral o contractual
- Acceso a información sensible solo en lo necesario para la función
- Prohibición de extraer o divulgar información de clientes

Competencia y conciencia

- Inducción obligatoria dentro de los primeros 30 días de ingreso
- Sesión anual de seguridad, privacidad y uso responsable de IA
- Refuerzo por rol para quienes operan datos, modelos o infraestructura
- Registro de asistencia y evaluación de comprensión

CONOCIMIENTO COMPROBABLE

Sin registro no hay difusión acreditada. El acuse de recibo firmado o la aceptación electrónica de esta política es parte del cumplimiento y se conserva como evidencia.

Detectar, contener, notificar, aprender

Aplica a incidentes de seguridad, vulneraciones de datos personales y comportamientos no previstos de los sistemas de IA.

01

Detección y registro

Todo incidente o sospecha se registra desde su detección, con hora, alcance y sistemas involucrados.

02

Evaluación y contención

Clasificación por severidad e impacto sobre personas; medidas inmediatas para contener el incidente.

03

Notificación

Comunicación al cliente afectado y a la autoridad de protección de datos en los plazos que la normativa establezca.

04

Remediación

Corrección de la causa raíz, restauración del servicio y verificación de que el control fallido quedó operativo.

05

Lecciones aprendidas

Actualización de la matriz de riesgos, de los controles y de la capacitación a partir de lo ocurrido.

06

Incidentes de IA

Los comportamientos no previstos de un sistema de IA se tratan como incidente, aunque no haya vulneración de datos.

Cómo se mide el cumplimiento

Esta política es el marco desde el cual se establecen y revisan los objetivos del SGI.

Indicadores mínimos

- Porcentaje de personal con capacitación vigente
- Incidentes registrados y porcentaje cerrado dentro del plazo
- Solicitudes de titulares atendidas dentro del plazo legal
- Proveedores críticos con debida diligencia completada
- Sistemas de IA con evaluación de impacto vigente
- Hallazgos de auditoría y planes de acción cerrados

Auditoría y revisión

- Auditoría interna anual sobre los controles críticos
- Revisión por la Dirección al menos una vez al año
- Revisión extraordinaria ante incidentes o cambios normativos
- Auditoría externa de certificación por el organismo acreditado
- Reporte periódico de indicadores a la Administración General

MEJORA CONTINUA

Los objetivos del SGI son definidos, medidos y revisados por la Alta Dirección, y se ajustan cuando cambian el negocio, la estructura, la cartera de clientes o la legislación aplicable.

Roles y responsabilidades

Estructura proporcional al tamaño de la Empresa, con independencia funcional del Encargado del SGI.

ROL	RESPONSABILIDADES	ENTREGABLES Y FRECUENCIA
Administración General y socios	Aprobar la política y sus actualizaciones; asignar recursos; realizar la revisión por la Dirección; decidir sobre riesgos no aceptables.	Aprobación anual; revisión por la Dirección; acta de decisiones.
Encargado del SGI	Mantener el sistema documental; coordinar riesgos, auditorías e incidentes; reportar el desempeño a la Administración General.	Plan anual del SGI; reporte periódico de indicadores.
Responsable de privacidad	Gestionar el registro de tratamientos, las solicitudes de titulares y las evaluaciones de impacto en protección de datos.	Registro de tratamientos; evidencia de solicitudes atendidas.
Líderes de proyecto y dueños de proceso	Operar los controles definidos en su ámbito; levantar alertas; mantener evidencias; apoyar auditorías.	Evidencias por proyecto; revisión periódica.
Todo el personal y terceros	Conocer y cumplir esta política; reportar incidentes y sospechas; participar en la capacitación.	Acuse de recibo; capacitación anual.

Vigencia y disposiciones finales

VERSIÓN 2.0 — 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).	Consulta Las dudas de interpretación se dirigen al Encargado del SGI antes de actuar. Las consultas sobre datos personales se canalizan según la Política de Privacidad (5.2-PL02).		
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 Este documento entra en vigencia en la fecha de aprobación y reemplaza a todas las versiones anteriores, que quedan marcadas como obsoletas.		

Qué requisito cubre cada capítulo

Matriz de referencia para auditoría interna y de certificación.

CAPÍTULO	REFERENCIA LEGAL	REFERENCIA DE NORMA
01 y 02 Propósito y alcance	Leyes N° 19.628 y 21.719; Ley N° 19.886	ISO/IEC 27001, 27701 y 42001 — cl. 4
03 Compromiso de la Dirección	Control interno de la Empresa	ISO/IEC 27001, 27701 y 42001 — cl. 5.1 y 5.2
04 Seguridad y robustez técnica	Ley N° 21.719 — medidas de seguridad	ISO/IEC 27001 — Anexo A; ISO/IEC 42001 — Anexo A
05 Privacidad: roles y principios	Leyes N° 19.628 y 21.719; RGPD	ISO/IEC 27701 — cl. 7 y 8
06 IA responsable y transparente	Ley N° 21.719 — decisiones automatizadas	ISO/IEC 42001 — A.5, A.6 y A.8
07 Evaluación de impacto	Ley N° 21.719 — evaluación de impacto	ISO/IEC 42001 — cl. 6.1 y A.5; ISO/IEC 27701 — cl. 5.4
08 Gobernanza de terceros	Ley N° 21.719 — encargados y subencargados	ISO/IEC 27001 — A.5.19 a A.5.23; ISO/IEC 42001 — A.10
09 Personas	Ley N° 21.719 — deber de secreto	ISO/IEC 27001 — cl. 7.2 y 7.3; A.6
10 Gestión de incidentes	Ley N° 21.719 — notificación de vulneraciones	ISO/IEC 27001 — A.5.24 a A.5.28; cl. 10
11 a 13 Objetivos, gobernanza y vigencia	Control interno de la Empresa	ISO/IEC 27001, 27701 y 42001 — cl. 6.2, 9 y 7.5

Definiciones y documentos relacionados

Definiciones

Sistema de Gestión Integrado (SGI)

Políticas, procesos y controles con que AVIM cumple ISO/IEC 27001, 27701 y 42001.

Responsable de Tratamiento

Quien determina las finalidades y medios del tratamiento de datos personales.

Encargado de Tratamiento

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

Sistema de IA

Sistema que genera predicciones, contenidos, recomendaciones o decisiones a partir de datos.

Evaluación de impacto

Análisis previo de los efectos de un sistema sobre la organización y las personas.

Copia no controlada

Ejemplar impreso o descargado cuya vigencia no está garantizada.

Documentos y registros relacionados

CÓDIGO	DOCUMENTO O REGISTRO
5.2-PL01	Política del SGI (este documento)
5.2-PL02	Política de Privacidad y Protección de Datos
5.2-PL03	Programa de integridad y código de ética
5.2-DG01	Acuerdos individuales de confidencialidad
4.0-DG01	Alcance del SGI y Declaración de Aplicabilidad
8.1-PR01	Procedimiento de gestión de incidentes
8.2-RG01	Registro de evaluaciones de impacto de IA
9.1-RG02	Registro de proveedores críticos evaluados

QUÉ ESPERAMOS DEL EQUIPO

Cuatro acciones concretas

01

Conocer

Revise esta política y deje registro de su acuse de recibo o aceptación electrónica.

02

Aplicar

Opere los controles definidos para su rol, en cada proyecto y en cada entorno.

03

Registrar

Mantenga la evidencia de lo que hace: sin registro, el control no existe.

04

Reportar

Informe de inmediato cualquier incidente, sospecha o comportamiento no previsto.

La gobernanza no es un trámite: es la condición que hace posible adoptar IA sin elegir entre innovación y cumplimiento.

