



Política de Protección de Datos Personales

Uso interno — POL-PDP-001

PG VALDÉS ADVISORY CHILE SpA

Villarrica, Región de La Araucanía · Cobertura desde Santiago al sur

POL-PDP-001 · Versión 2.2

Versión 2.2 — 22 de septiembre de 2026 (corrige la cita del Reglamento del Modelo de Prevención de Infracciones y actualiza su estado de verificación)

Aprobado por: Pamela González Valdés — Directora Ejecutiva

www.pgvaldesadvisory.cl · contacto@pgvaldesadvisory.cl · +56 9 3779 8535

Documento sujeto a aprobación formal. Esta política se emite como documento independiente a solicitud de la Dirección Ejecutiva, para facilitar su aprobación y comunicación individual. Un resumen de esta política, junto con el resto del sistema de gestión, se mantiene en el Manual Corporativo de Políticas y Procedimientos.

Declaración de política

PG Valdés Advisory Chile SpA tratará datos personales de manera lícita, leal, transparente y limitada a finalidades determinadas. La consultora aplicará privacidad desde el diseño y por defecto, podrá demostrar sus decisiones y dará a las personas mecanismos claros para ejercer sus derechos. Ninguna urgencia comercial habilita a recolectar, reutilizar, compartir o conservar datos sin base, información o controles adecuados.

Objetivo y vigencia normativa

Establecer las reglas para gobernar el tratamiento de datos personales durante todo su ciclo de vida, prevenir daños a los titulares, cumplir la Ley N° 19.628 en su texto vigente y preparar la operación para las modificaciones introducidas por la Ley N° 21.719, cuya entrada en vigor general está prevista para el 1 de diciembre de 2026, mientras no exista una modificación legal publicada. Esta política adopta, además, el Reglamento de los artículos 49 a 53 de la Ley N° 21.719 (Decreto N° 662 de 2025, del Ministerio de Hacienda, firmado el 13 de junio de 2025) como marco de referencia para el Modelo de Prevención de Infracciones que se describe más adelante, y su artículo 8 como base para la línea de reporte directo de la Delegada de Protección de Datos a la máxima autoridad de la organización.

Actualización de verificación (22-sept-2026). Una revisión posterior con fuentes externas (análisis de estudios jurídicos y de IAPP) corrobora que el Decreto N° 662 de 2025 del Ministerio de Hacienda existe, fue firmado el 13 de junio de 2025, regula los artículos 49 a 53 de la Ley N° 21.719 (Modelo de Prevención de Infracciones) y fue tomado de razón por la Contraloría General de la República el 28 de agosto de 2026; su artículo 8 establece que la Delegada de Protección de Datos reporta directamente a la máxima autoridad de la organización. No obstante, no fue posible ubicar el decreto en Ley Chile / BCN ni confirmar su número de edición y CVE de publicación en el Diario Oficial, probablemente porque su trámite ante Contraloría concluyó recién en agosto de 2026. Antes de invocar formalmente este decreto ante un cliente, una auditoría o la propia Agencia de Protección de Datos Personales, Legal/DPO debe confirmar esa referencia exacta en el Diario Oficial.

El doble rol de PG Valdés Advisory: Responsable y Encargada de Tratamiento

Por la naturaleza de su actividad de consultoría en auditoría, riesgos, compliance y sistemas de gestión, PG Valdés Advisory trata datos personales en dos calidades distintas:

Calidad	Cuándo aplica	Ejemplos
Responsable de datos	Respecto de los datos que PG Valdés Advisory recolecta y decide por sí misma para operar su propio negocio.	Datos de contacto de clientes y prospectos; datos de facturación; datos recolectados en el sitio web; datos de profesionales a honorarios.
Encargada de tratamiento	Cuando, en ejecución de un servicio de auditoría, diagnóstico GRC, implementación de normas ISO o preparación de certificación, accede a datos personales que son propiedad de un cliente.	Registros de colaboradores del cliente auditado; evidencias de auditoría con datos personales; información de proveedores del cliente revisada en una auditoría de segunda parte.

Cuando actúa como Encargada, PG Valdés Advisory trata los datos del cliente exclusivamente conforme a las instrucciones y al contrato de encargo suscrito con ese cliente, sin reutilizarlos para fines propios ni combinarlos con sus propias bases de datos. En la estructura actual, la Directora Ejecutiva ejerce los roles internos de responsable, dueña del tratamiento y DPO. Solo dará acceso a un profesional independiente o empresa tercera cuando el proyecto lo necesite y exista un acuerdo escrito que delimite instrucciones, datos, sistemas, confidencialidad, seguridad, incidentes, subcontratación y eliminación o devolución.

Principios obligatorios

Principio	Qué exige en la práctica
Licitud y lealtad	Toda recolección debe apoyarse en una base de licitud válida y no puede engañar al titular sobre el uso real de sus datos.
Finalidad	Los datos recolectados para un fin no pueden reutilizarse para otro distinto sin nueva base legal o consentimiento.
Proporcionalidad y minimización	Solo se solicitan los campos estrictamente necesarios; se prohíbe la recolección "por si acaso".
Calidad	Los datos deben ser exactos, completos, actuales y vinculados a su fuente; debe existir un mecanismo de corrección.
Responsabilidad demostrada	La organización debe poder demostrar cumplimiento en cualquier momento mediante el registro de actividades, esta política y sus registros asociados.
Seguridad y confidencialidad	El nivel de protección será proporcional al riesgo, sensibilidad, volumen, contexto y consecuencias para las personas.
Transparencia	El titular debe poder conocer, sin esfuerzo desproporcionado, qué se hace con sus datos (Política de Privacidad pública).
Conservación limitada	Los datos se eliminarán o anonimizarán cuando dejen de ser necesarios, salvo obligación legal o defensa de derechos documentada.

Ciclo de vida del tratamiento de datos



Figura 1. Controles del ciclo de vida de los datos personales.

Bases de licitud y gestión del consentimiento

Base de licitud	Se usa cuando...	Ejemplo
Consentimiento	No existe otra base aplicable y el tratamiento depende de la voluntad del titular.	Suscripción a comunicaciones comerciales.
Ejecución de un contrato	El dato es necesario para cumplir lo pactado con el titular.	Ejecución del servicio de auditoría o consultoría contratado.
Obligación legal	Una norma exige el tratamiento.	Retención de boletas y facturas para el SII.
Interés legítimo	Existe un interés real de la consultora que no prevalece sobre los derechos del titular; debe documentarse el balance.	Prospección comercial B2B con contactos profesionales.
Formulación o defensa de un derecho	El dato se necesita para un litigio o procedimiento.	Prueba documental en un reclamo o juicio.

Cuando la base de licitud sea el consentimiento: debe solicitarse de forma granular, sin casillas premarcadas ni silencio como aceptación; debe registrarse evidencia (fecha, hora, canal, versión del texto); el titular debe poder revocarlo con la misma facilidad con que lo otorgó; y, revocado, el tratamiento debe cesar salvo que exista otra base independiente. No se condicionará un servicio a datos no necesarios para prestarlo.

Transparencia y avisos

Cada punto de recolección debe enlazar o entregar un aviso coherente con el registro de actividades: identidad del responsable y su contacto; datos de contacto de la persona responsable de privacidad; categorías de datos; finalidades; bases; destinatarios; transferencias; conservación; decisiones automatizadas relevantes; carácter obligatorio o voluntario; y derechos y modo de ejercerlos. La Política de Privacidad publicada en el sitio web (versión pública, documento PUB-PDP-001) desarrolla este aviso para visitantes y contactos, y debe mantenerse coherente con la configuración productiva real del sitio, sus formularios, proveedores y tecnologías de seguimiento.

Datos sensibles y personas en situación de especial protección

El tratamiento de datos sensibles exige consentimiento expreso y controles reforzados. La consultora evitará recibir antecedentes de salud, biométricos, políticos, sindicales, religiosos, de vida u orientación sexual u otros sensibles si no son imprescindibles para el servicio. Cuando una evidencia de cliente los contenga, se aplicará acceso restringido, cifrado, minimización de copias, registro de acceso y supresión prioritaria. Los servicios no se dirigen a niños, niñas o adolescentes; en formularios de registro que pudieran involucrarlos, se aplicará verificación de edad y consentimiento parental antes de continuar la recolección.

Solicitudes de derechos (ARCO+)

Los derechos de acceso, rectificación, cancelación o supresión, oposición, portabilidad y bloqueo son personales, intransferibles e irrenunciables. Este procedimiento asegura respuestas dentro de plazo y de forma gratuita.

Derecho	Plazo legal de referencia	Consideración de ejecución
---------	---------------------------	----------------------------

Acceso	30 días corridos (+30 con aviso)	La respuesta incluye los datos tratados, su origen, finalidad, destinatarios y plazo de conservación.
Rectificación	30 días corridos (+30 con aviso)	Requiere que el titular acredite la inexactitud; se propaga a todos los sistemas y encargados.
Supresión	30 días corridos (+30 con aviso)	Se verifica antes si existe obligación legal de conservación o interés legítimo vigente.
Oposición	30 días corridos (+30 con aviso)	Se distingue si es total o parcial; el cese es inmediato una vez verificada la identidad.
Portabilidad	30 días corridos (+30 con aviso)	Se entrega en formato electrónico estructurado (ej. CSV/JSON) cuando esté vigente este derecho.
Bloqueo	2 días hábiles	Suspensión temporal y reversible del tratamiento mientras se resuelve la solicitud subyacente.

Flujo: (1) recepción por el canal habilitado y registro con fecha y hora; (2) acuse de recibo dentro de 48 horas; (3) verificación proporcional de identidad; (4) evaluación de procedencia y de causales de excepción (obligación legal de conservación, afectación de derechos de terceros, necesidad probatoria, o imposibilidad de verificar identidad); (5) ejecución coordinada con quien custodie los datos; (6) respuesta fundada al titular, indicando la acción tomada o el motivo de la denegación y los mecanismos de reclamación; (7) registro y cierre para trazabilidad y KPIs.

Atención de derechos de las personas



Figura 2. Flujo de atención de derechos de titulares.

Gestión de brechas de seguridad

Toda pérdida, acceso no autorizado, divulgación, alteración o destrucción de datos personales debe reportarse de inmediato al responsable de privacidad, incluso si existe duda sobre su materialidad. Ocultar deliberadamente una brecha constituye una infracción grave; ninguna persona puede decidir por sí sola no reportar un incidente.

Nivel	Criterio	Tiempo máximo de contención	Acción
Bajo	Datos comunes, pocos titulares, sin evidencia de explotación.	72 horas	Registro interno y corrección de la causa raíz.
Medio	Datos comunes con volumen significativo, o acceso indebido interno.	24 horas	Notificación a la autoridad competente cuando corresponda + plan de remediación.
Alto	Datos sensibles, de niños/niñas o económicos comprometidos.	Inmediato (mismo día)	Notificación a la autoridad y a los titulares afectados, más comunicación a la Dirección.

Etapas: detección y reporte inmediato; activación de la respuesta y contención (aislar el sistema, cortar accesos comprometidos, preservar evidencia); evaluación de riesgo según tipo de datos y volumen de titulares; notificación a la autoridad competente "sin dilaciones indebidas" cuando la ley lo exija, indicando naturaleza, categorías y volumen de datos afectados, consecuencias probables y medidas adoptadas; notificación a los titulares afectados cuando la brecha involucre datos sensibles, de menores o económicos; remediación de la causa raíz; y cierre con registro completo y revisión post-incidente dentro de los 15 días siguientes. Este procedimiento es la referencia vigente para toda brecha que involucre datos personales, incluidas las que se detecten en el marco de la Política de Seguridad de la Información (POL-SI-001).

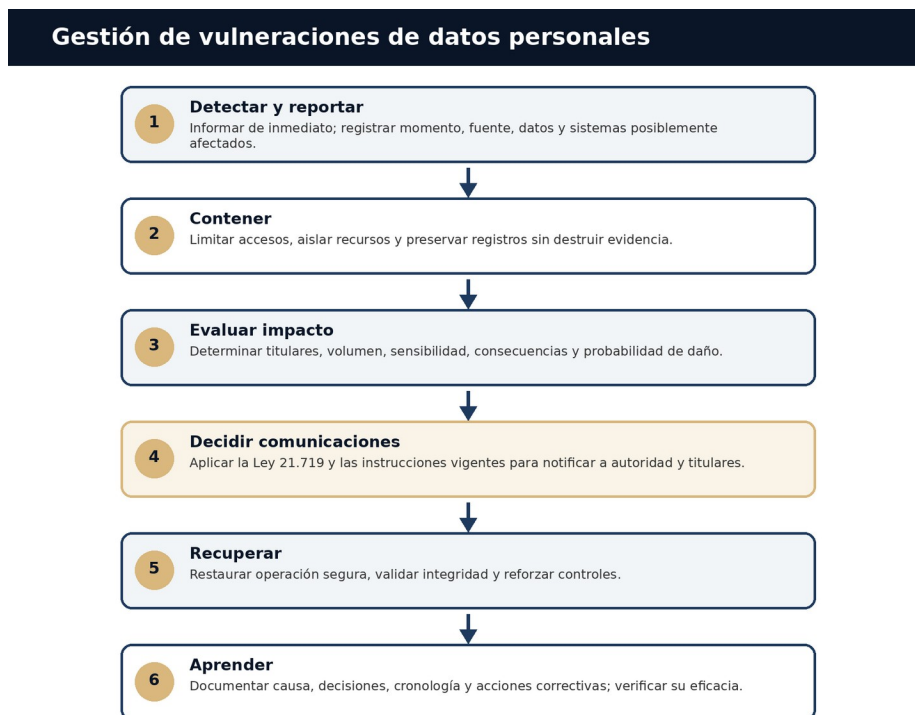


Figura 3. Flujo de gestión de una vulneración de datos personales.

Evaluación de impacto en protección de datos (EIPD)

Obligatoria antes de implementar tratamientos de alto riesgo: perfilamiento con efectos jurídicos significativos, tratamiento masivo de datos, monitoreo sistemático de zonas de acceso público, tratamiento de datos sensibles a gran escala, o decisiones automatizadas con efectos sobre el titular. La evaluación describe el tratamiento

propuesto, identifica riesgos concretos para los titulares, califica cada riesgo (probabilidad/impacto), define medidas de mitigación y determina el riesgo residual; si este permanece alto, se consulta al responsable de privacidad y se evalúa la consulta previa a la autoridad competente.

Conservación, bloqueo y eliminación

Categoría	Criterio de plazo	Disposición
Prospectos y marketing	Hasta retiro del consentimiento, oposición o vencimiento del plazo informado (referencia: 2 años sin contacto).	Supresión o anonimización de listas y respaldos operativos.
Clientes y contratos	Vigencia contractual más plazos legales, tributarios y de defensa de derechos.	Bloqueo cuando corresponda y supresión segura al vencer.
Evidencias de proyectos (rol de Encargada)	Plazo contractual o el mínimo necesario para soporte, auditoría y defensa.	Devolución, eliminación certificada o anonimización según contrato con el cliente.
Postulantes	Proceso de selección y plazo adicional informado y justificado.	Supresión si no existe consentimiento o finalidad vigente.
Proveedores y personal	Relación vigente más obligaciones laborales, tributarias, previsionales o contractuales.	Acceso restringido, bloqueo y eliminación controlada.

Los respaldos (backups) deben incluirse en el ciclo de eliminación, no solo las bases de producción. Vencido el plazo o la finalidad, los datos deben eliminarse, anonimizarse o seudonimizarse; toda excepción (litigio en curso, obligación legal vigente, bloqueo solicitado por el titular) debe documentarse con su fundamento y una fecha estimada de reevaluación.

Encargados, proveedores y transferencias internacionales

Todo tercero que trate datos por cuenta de la consultora será evaluado antes de contratar. El contrato de encargo definirá objeto, duración, finalidad, datos, titulares, instrucciones, confidencialidad, seguridad (incluyendo medidas técnicas mínimas), prohibición de subcontratar sin autorización previa, obligación de reportar brechas sin dilación, derecho de auditoría y destino de los datos al término del contrato (devolución o eliminación certificada). Si el encargado se desvía del encargo y trata los datos para fines propios o no autorizados, pasa a ser responsable solidario.

Las transferencias internacionales se realizarán solo con un mecanismo admitido por la normativa aplicable (país con nivel adecuado, cláusulas contractuales tipo, normas corporativas vinculantes, u otra causal legal puntual) y una evaluación documentada del país, receptor, salvaguardas y acceso gubernamental cuando sea pertinente. Debe documentarse en el registro de actividades de tratamiento y, cuando corresponda, informarse en la Política de Privacidad pública.

Gobernanza: delegado/a de protección de datos y comité

PG Valdés Advisory designa a Pamela González Valdés como responsable de privacidad y, en la medida en que la organización avance en su Modelo de Prevención de Infracciones, como Delegada de Protección de Datos (DPO), aplicando la facilidad prevista para micro, pequeñas y medianas empresas de concentrar ambos roles en la máxima autoridad. Si la organización crece o certifica su modelo, deberá reevaluar si esta concentración sigue siendo compatible con la autonomía exigida al DPO. El Comité de Protección de Datos se constituye como una

instancia liviana de revisión trimestral, presidida por la DPO, que revisa el registro de actividades de tratamiento, la matriz de riesgos, las evaluaciones de impacto de alto riesgo y los incidentes del período.

Rol	Decisiones y responsabilidades mínimas
Dirección Ejecutiva	Aprueba el apetito de riesgo de privacidad, las evaluaciones de alto riesgo y las comunicaciones de incidentes relevantes; designa formalmente al DPO.
Responsable de privacidad / DPO	Mantiene el inventario y registro de tratamientos, atiende derechos ARCO+, gestiona brechas, asesora proyectos, coopera con la autoridad y capacita.
Dueño del tratamiento	Define finalidad, datos, base, plazo, destinatarios y controles; mantiene exactitud y evidencia.
Seguridad de la información	Aplica controles técnicos, gestiona vulneraciones y preserva evidencia.
Encargados y subencargados	Tratan solo conforme a instrucciones, mantienen confidencialidad y cooperan con derechos e incidentes.

Registro de actividades de tratamiento (RAT)

Antes de operar un tratamiento nuevo o significativamente modificado, el dueño debe registrarlo. El registro contendrá, como mínimo: tipo de datos (incluyendo si hay sensibles), ámbito territorial, categorías de titulares, fines, fuente de los datos, base de licitud, destinatarios o cesionarios (incluidos terceros países), existencia y destino de transferencias internacionales, plazos de supresión, y existencia de decisiones automatizadas o perfilamiento. El DPO consolida y valida el registro al menos semestralmente y antes de cada reunión del Comité de Protección de Datos; debe estar disponible para la autoridad competente y para los clientes que, como responsables, requieran acreditar la debida diligencia de PG Valdés Advisory como encargada.

Excepciones e incumplimientos

Toda excepción debe identificar el requisito afectado, el motivo, el riesgo para las personas o la operación, la duración, el control compensatorio y la aprobación de la persona propietaria y de la Dirección. No se autorizan excepciones que eliminen un derecho irrenunciable o contradigan una prohibición legal.

Todo incumplimiento se registra, se evalúa según su riesgo, se contiene cuando corresponde y se somete a análisis de causa y acción correctiva. Las medidas laborales o contractuales deben respetar la normativa vigente, el debido proceso y la proporcionalidad.

Control y revisión

La persona propietaria de POL-PDP-001 revisará esta política al menos una vez al año y cuando cambien la normativa, los servicios, la estructura, los riesgos, la tecnología o las expectativas relevantes de las partes interesadas; y cuando la organización avance hacia la certificación de su Modelo de Prevención de Infracciones. La incorporación de cualquier persona dependiente, profesional a honorarios o integrante de una empresa tercera constituye un cambio organizacional que exige revisar, antes o al inicio de su participación, el alcance, los roles, la segregación de funciones, los accesos, las inducciones, las cláusulas contractuales y los controles aplicables; cuando corresponda, se aprobará y comunicará una versión actualizada. La copia vigente es la publicada en el repositorio corporativo; las impresiones son copias no controladas.

Referencias

- Ley N° 21.719 y su Reglamento de los artículos 49 a 53 (Decreto N° 662 de 2025, Ministerio de Hacienda) — citación corroborada por fuentes externas; pendiente confirmar en Ley Chile / Diario Oficial el número de edición y CVE exactos (ver nota anterior).
- Ley N° 19.628 sobre protección de la vida privada, en Ley Chile.
- ISO/IEC 27701, sistema de gestión de privacidad.
- Política de Privacidad y Tratamiento de Datos Personales, versión pública (PUB-PDP-001) de PG Valdés Advisory Chile SpA.
- Manual de Cumplimiento de la Ley N° 21.719 (Modelo de Prevención de Infracciones) — documento independiente recomendado, pendiente de elaboración, que en el futuro desarrollaría en mayor detalle esta política.

Historial de versiones

Versión	Fecha	Cambios principales	Aprobado por
1.0 – 1.2	10-sept-2026	Versiones preliminares independientes (una preparada externamente dentro del Manual Corporativo, otra preparada internamente como Manual de la Ley N° 21.719).	Pendiente
2.0	10-sept-2026	Unificación de ambas versiones dentro del Manual Corporativo, con corrección de la vigencia de la Ley N° 21.719.	Pendiente
2.1	10-sept-2026	Se emite como documento independiente, a solicitud de la Dirección Ejecutiva, para facilitar su aprobación individual.	Pamela González Valdés
2.2	22-sept-2026	Se corrige la cita del Reglamento del Modelo de Prevención de Infracciones (era Ley N° 19.628, corresponde a Ley N° 21.719) y se actualiza la nota de verificación del Decreto N°	Pamela González Valdés

		662 de 2025 con hallazgos de fuentes externas (ver nota en "Objetivo y vigencia normativa").	
--	--	--	--