



Política de Seguridad de la Información

Uso interno — POL-SI-001

PG VALDÉS ADVISORY CHILE SpA

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

POL-SI-001 · Versión 2.1

Versión 2.1 — 22 de septiembre de 2026 (unifica y reemplaza la versión 1.2, y la versión incorporada en el Manual Corporativo v2.0; se emite ahora como documento independiente)

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. Sus anexos operativos (declaración de cumplimiento para terceros y checklist de incorporación/baja) se emiten en un documento separado: "Anexos — Política de Seguridad de la Información (POL-SI-001)".

Declaración de política

PG Valdés Advisory Chile SpA protegerá la confidencialidad, integridad y disponibilidad de la información propia y de clientes mediante un enfoque basado en riesgos. Los controles se diseñarán según el valor del activo, la amenaza, la vulnerabilidad, el impacto contractual y las obligaciones aplicables. La seguridad es una responsabilidad de todas las personas y forma parte del diseño, la contratación, la operación, el desarrollo y el cierre de cada servicio.

Objetivo, alcance y marco

Esta política establece el gobierno mínimo para información en cualquier formato, equipos, aplicaciones, nube, correo, repositorios, redes, respaldos, evidencias, código fuente y servicios de terceros. Se aplica a la operación unipersonal, al trabajo remoto y presencial, a dispositivos corporativos o autorizados, y a los accesos temporales otorgados a profesionales independientes o empresas terceras. No asume la existencia de un equipo interno permanente ni de un área de TI propia.

El sistema se orienta por ISO/IEC 27001:2022 y su código de prácticas ISO/IEC 27002:2022, la gestión de riesgos de ISO 31000 e ISO/IEC 27005, la Ley N° 21.663 de ciberseguridad y las instrucciones de la Agencia Nacional de Ciberseguridad cuando la consultora o un servicio queden comprendidos, y la Ley N° 21.459 sobre delitos informáticos. PG Valdés Advisory no es, a la fecha de esta política, un Operador de Importancia Vital bajo la Ley N° 21.663; aplica voluntariamente sus principios generales como buena práctica y reevaluará su clasificación si en el futuro presta servicios calificados como esenciales. La mención de estos marcos no equivale a declarar certificación.

Clasificación y manejo de la información

Nivel	Ejemplo	Control mínimo
Pública	Sitio web, brochure, propuestas de servicios genéricas.	Difusión solo desde fuentes aprobadas; proteger integridad y versión.
Interna	Metodologías propias, plantillas de trabajo, planificación comercial.	Acceso restringido a cuentas propias de la organización.
Confidencial	Contratos, correspondencia con clientes, datos personales comunes.	Almacenamiento en la nube corporativa con control de acceso; cifrado en tránsito.
Sensible / crítico	Papeles de trabajo con datos sensibles, evidencias de auditoría de alto impacto, credenciales.	Cifrado en reposo y tránsito, acceso mínimo indispensable, registro de auditoría, eliminación certificada al cierre.

Todo papel de trabajo o evidencia de un cliente se almacena conforme al nivel más alto de sensibilidad que contenga. La información confidencial o sensible/crítica no se envía por canales no corporativos ni se almacena en dispositivos personales sin cifrado. El acceso de un tercero contratado a información confidencial o sensible/crítica se otorga solo por el plazo del proyecto y se revoca al término de este.

Identidades y accesos

- Cada persona usará una identidad individual. Las cuentas compartidas se prohíben salvo necesidad técnica documentada, con custodia y trazabilidad reforzada.

- Se aplicará mínimo privilegio, necesidad de saber y segregación de funciones. Los privilegios administrativos serán separados de la cuenta de uso normal.
- La autenticación multifactor será obligatoria para correo, nube, repositorios, administración, acceso remoto y sistemas con información confidencial o restringida.
- Las altas, cambios y bajas se gestionarán con aprobación. Los accesos se revisarán al menos semestralmente y de inmediato ante cambio de función o término de la relación.
- Las contraseñas o secretos no se enviarán por correo o mensajería abierta; se usará un gestor de contraseñas autorizado y se rotarán ante indicio de compromiso.

Alta cambio revisión y baja de accesos



Figura 1. Flujo de gestión del acceso lógico.

Protección técnica y operación

- Configuración segura y endurecimiento proporcional a la exposición; eliminación o cambio de credenciales por defecto.
- Gestión de vulnerabilidades y parches según criticidad y exposición; excepciones documentadas con controles compensatorios.
- Cifrado de comunicaciones y de datos confidenciales o restringidos almacenados en equipos portátiles, respaldos y medios removibles.
- Registro de actividades de administración, autenticación, cambios y accesos sensibles; protección de logs contra alteración.
- Respaldo automático y periódico en un proveedor cloud con historial de versiones; verificación semestral de que los respaldos son recuperables. La existencia de una copia no sustituye la prueba de restauración.
- Antivirus/antimalware actualizado y autenticación de dos factores en cuentas críticas; verificación de remitentes antes de abrir adjuntos o enlaces.

Seguridad en la relación con terceros (honorarios y subcontratación)

Dado que, bajo el modelo operativo actual, todo trabajo en equipo se realiza mediante honorarios o subcontratación y no mediante colaboradores dependientes, esta sección desarrolla en detalle los controles aplicables.

Antes de incorporar a un tercero a un proyecto

1. Evaluar si el proyecto requiere acceso a información confidencial o sensible/crítica, o solo a información pública/interna.
2. Si requiere acceso a información confidencial o sensible/crítica: firmar un acuerdo de confidencialidad (NDA) específico antes de compartir cualquier dato.
3. Entregar al tercero un resumen de esta política y de las reglas de manejo de información aplicables al proyecto, junto con la declaración de cumplimiento del Anexo A (documento "Anexos — Política de Seguridad de la Información, POL-SI-001").
4. Otorgar acceso mínimo indispensable (carpeta o sistema específico del proyecto), evitando compartir el repositorio completo.
5. Documentar el acceso otorgado (qué, cuándo, por cuánto tiempo) en el registro de terceros con acceso a información (Anexo B del mismo documento de anexos).

Durante el proyecto y al término

- El tercero reporta a la Dirección cualquier incidente de seguridad del que tome conocimiento, sin dilación.
- El tercero no reenvía, copia ni almacena la información fuera de los canales acordados para el proyecto.
- Si el tercero es una empresa que subcontrata, garantiza que su propio personal cumple un estándar de confidencialidad equivalente.
- Al término del proyecto: se revocan de inmediato todos los accesos otorgados; se solicita la eliminación o devolución de la información que el tercero conserve; se registra el cierre del acceso (Anexo B).

Este procedimiento es coherente con la sección de encargados de tratamiento de la Política de Protección de Datos Personales (POL-PDP-001): cuando el tercero contratado trata datos personales de un cliente, además de esta política se aplican las reglas de encargo de tratamiento allí definidas.

Proveedores y cadena de suministro

Los proveedores se evaluarán según acceso, datos, criticidad, subcontratación y dependencia. Los contratos incluirán confidencialidad, controles, incidentes, continuidad, derecho de evaluación, ubicación y devolución o eliminación de datos. Los cambios materiales y subencargados críticos requieren revisión antes de su uso.



Figura 2. Flujo de debida diligencia y seguimiento de proveedores.

Desarrollo, adquisición, nube e inteligencia artificial

Las adquisiciones y desarrollos deben incorporar requisitos de seguridad, privacidad, continuidad, registro y salida desde su diseño. No se ingresará información confidencial, restringida, datos personales ni propiedad intelectual de clientes en herramientas de inteligencia artificial pública o no aprobada. Todo uso de IA debe tener propósito, dueño, revisión humana, evaluación de datos y validación del resultado.

Gestión de incidentes de seguridad

Se considera evento reportable cualquier anomalía que pueda afectar información o servicio: phishing, malware, acceso indebido, envío erróneo, pérdida, indisponibilidad, alteración, fuga, vulnerabilidad, fraude o incumplimiento de un control. Reportar de buena fe no genera sanción. Solo la Directora Ejecutiva o un tercero expresamente autorizado podrá efectuar comunicaciones externas sobre un incidente.

Nivel	Criterio	Acción
Bajo	Información pública o interna, sin evidencia de explotación.	Registro interno y corrección de la causa raíz.
Medio	Información confidencial expuesta, o acceso indebido de un tercero contratado.	Notificación al cliente afectado (si aplica) + plan de remediación.
Alto	Información sensible/crítica comprometida, o datos personales sensibles involucrados.	Notificación al cliente y, si aplica, a la autoridad de protección de datos; activación del procedimiento de brechas de la Política de Protección de Datos Personales (POL-PDP-001).



Figura 3. Ciclo de respuesta a incidentes de seguridad.

Continuidad y respaldo de la información

Dado que la operación depende hoy de una sola persona, la continuidad se sostiene en la disponibilidad de respaldos y en documentación mínima que permita a un tercero de confianza retomar la operación ante la pérdida de un dispositivo: gestor de contraseñas con los accesos críticos y un mecanismo de acceso de emergencia definido; identificación de una persona de confianza que sepa cómo proceder ante una indisponibilidad prolongada de la Directora Ejecutiva, sin necesariamente tener acceso permanente a la información. Esta sección se ampliará si la organización incorpora colaboradores permanentes o clientes que exijan contractualmente un plan de continuidad más formal (ISO 22301).

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-SI-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. 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

- ISO/IEC 27001:2022 y su Anexo A de controles.
- Ley N° 21.663 de ciberseguridad y normativa de la ANCI.
- Ley N° 21.459 sobre delitos informáticos.
- CSIRT de Gobierno.
- Política de Protección de Datos Personales (POL-PDP-001) de PG Valdés Advisory Chile SpA, sección "Gestión de brechas de seguridad" — procedimiento vigente para brechas que involucren datos personales.
- Anexos — Política de Seguridad de la Información (POL-SI-001): declaración de cumplimiento para terceros (Anexo A) y checklist de incorporación/baja de un tercero (Anexo B).

Historial de versiones

Versión	Fecha	Cambios principales	Aprobado por
1.0	10-sept-2026	Versión preliminar de la Política de Seguridad de la Información.	Pendiente
2.0	10-sept-2026	Unificación dentro del Manual Corporativo, con detalle operativo de terceros bajo honorarios/subcontratación.	Pendiente
2.1	22-sept-2026	Se emite como documento independiente; se separan sus anexos operativos en un documento propio.	Pamela González Valdés