Grupo Logístico Chile SpA

Política de Tratamiento y Protección de Datos Personales

Versión con control de cambios

Documento para revisión ejecutiva

Responsable del documento: Administración y Finanzas

Elaborado por: Victorino Rodríguez | Consultor TI

Aprobación: Paola Díaz | Gerencia de Administración y Finanzas

Aprobación: Gloria Nail | Gerencia de Operaciones

Emisión base: 29/03/2026

Actualización: 03/05/2026

Grupo Logístico Chile SpA

Política de Tratamiento y Protección de Datos Personales

Documento corporativo formal para aprobación de gerencia

Razón social	Grupo Logístico Chile SpA
RUT	76.010.628-3
Giro	Transporte de carga por carretera
Domicilio	José Joaquín Pérez 969, San Bernardo
Responsable del documento	Administración y Finanzas
Revisión	Anual

Paola Díaz
Gerencia de Administración y Finanzas

Gloria Nail
Gerencia de Operaciones

Grupo Logístico Chile SpA
76.010.628-3
Fono: +569 4029 8614

Control documental

Documento	Código	Emisión	Próxima revisión
Política de Tratamiento y Protección de Datos Personales	POL-GLC-001	29/03/2026	29/03/2027
Elaborado por	Victorino Rodríguez Consultor TI	**Responsable**	Administración y Finanzas
Aprobado por	Paola Díaz Gerencia de Administración y Finanzas	**Aprobado por**	Gloria Nail Gerencia de Operaciones
Ámbito	Aplica a toda la empresa y terceros con acceso a datos	**Territorio**	Chile

Índice

1. Objetivo

Establecer los lineamientos, principios y controles aplicables al tratamiento y protección de los datos personales tratados por Grupo Logístico Chile SpA, con el fin de resguardar los derechos de sus titulares, asegurar un *tratamiento lícito, proporcional y seguro de la información, y cumplir con la normativa vigente en Chile*, especialmente la Ley N° 21.719.

Esta política regula la forma en que la organización recopila, utiliza, almacena, conserva, resguarda y, cuando corresponda, elimina datos personales en el marco de sus actividades administrativas, operacionales, laborales, comerciales, tecnológicas y de seguridad física.

2. Alcance

La presente política aplica a toda la empresa Grupo Logístico Chile SpA, RUT 76.010.628-3, con domicilio en José Joaquín Pérez 969, San Bernardo, y cubre todos los tratamientos de datos personales efectuados en el desarrollo de su giro principal de transporte de carga por carretera.

Su aplicación alcanza a trabajadores, extrabajadores, postulantes, clientes, contactos comerciales, proveedores, contratistas, subcontratistas y terceros que operen sistemas de la empresa o accedan a datos personales por cuenta de ésta.

La política rige para las operaciones efectuadas en Chile y aplica a las áreas de Administración y Finanzas, Operaciones, TI y cualquier otra función que trate datos personales dentro de la organización.

3. Responsabilidades

3.1 Gerencia de Administración y Finanzas

- Aprobar, promover y supervisar el cumplimiento de esta política.
- Actuar como responsable interno principal en materias de protección de datos personales.
- Canalizar y coordinar la atención de requerimientos de titulares de datos.

Supervisar que el tratamiento de datos personales se ajuste a la presente política, a la normativa aplicable y a las instrucciones internas que emita la empresa.

Designar formalmente al Delegado o Responsable Interno de Protección de Datos Personales y proveerle medios razonables para el cumplimiento de sus funciones.

3.2 Gerencia de Operaciones

- Velar por la correcta aplicación de la política en procesos operacionales, trazabilidad de vehículos, coordinación logística y actividades que involucren información de trabajadores, contratistas y clientes.

3.3 Área de Administración

- Gestionar documentalmente los antecedentes personales y comerciales tratados por la empresa.
- Recibir solicitudes de titulares por los canales definidos y derivarlas al responsable correspondiente.

3.4 Área TI

- Implementar y mantener medidas técnicas y organizativas de protección de la información.
- Administrar controles de acceso, perfiles, respaldos y resguardo de sistemas que contengan datos personales.

3.5 Delegado o Responsable Interno de Protección de Datos Personales

La empresa designa como responsable interna de coordinación en materias de protección de datos personales a Paola Díaz, Gerenta de Administración y Finanzas.

Tendrá facultades para recibir y canalizar solicitudes de titulares, coordinar respuestas con las áreas involucradas, requerir antecedentes internos necesarios para su gestión, proponer medidas de mejora y escalar incidentes o incumplimientos a la gerencia cuando corresponda.

Contará con apoyo del área TI y de las jefaturas responsables de proceso para levantar información, evaluar incidentes, coordinar medidas correctivas y mantener actualizada la documentación relacionada con protección de datos personales.

3.6 Jefaturas, trabajadores y terceros

- Tratar datos personales solo dentro del marco de sus funciones y mantener reserva y confidencialidad.
- Reportar incidentes o accesos indebidos de forma inmediata.
- Cumplir esta política cuando traten datos personales por cuenta de Grupo Logístico Chile SpA.

Participar en las actividades de inducción, difusión o capacitación que la empresa defina en materias de confidencialidad, seguridad de la información y protección de datos personales.

Informar oportunamente cualquier incumplimiento, error operativo o desviación detectada en los procesos que involucren datos personales.

4. Términos y definiciones

Término	Definición
Dato personal	Cualquier información vinculada o referida a una persona natural identificada o identificable.
Dato sensible o de categoría especial	Información que requiere una protección reforzada, como datos de salud o biométricos.
Tratamiento de datos	Cualquier operación sobre datos personales, como recolección, almacenamiento, uso, consulta, comunicación o eliminación.
Titular de datos	Persona natural a quien corresponden los datos personales objeto de tratamiento.
Incidente de seguridad	Evento que afecte la confidencialidad, integridad, disponibilidad o acceso autorizado a los datos personales.

5. Política de tratamiento y protección de datos personales

5.1 Principios generales

La empresa se compromete a tratar los datos personales conforme a criterios de licitud, finalidad, proporcionalidad, seguridad, confidencialidad y responsabilidad, procurando que el tratamiento sea adecuado a la finalidad informada y limitado a lo estrictamente necesario.

5.2 Categorías de titulares

La empresa trata datos personales de trabajadores, extrabajadores, postulantes, clientes, contactos comerciales, proveedores, contratistas y subcontratistas.

5.3 Tipos de datos tratados

Nombre completo, RUT, teléfono, correo electrónico, dirección, cargo, contacto de emergencia patente del vehículo, geolocalización de camiones, antecedentes laborales, remuneraciones, datos bancarios, antecedentes previsionales, datos de salud vinculados a licencias médicas y datos biométricos utilizados exclusivamente para control de asistencia.

5.4 Finalidades del tratamiento

Contratación laboral, administración de personal, pago de remuneraciones, control de asistencia, gestión comercial, facturación y cobranzas, coordinación de despachos, monitoreo y trazabilidad de flota, cumplimiento de obligaciones legales y contractuales, seguridad física, soporte informático y marketing corporativo cuando corresponda.

5.5 Bases que justifican el tratamiento

Consentimiento del titular cuando corresponda, ejecución de una relación contractual o precontractual y cumplimiento de obligaciones legales.

5.6 Origen de los datos

Los datos pueden obtenerse directamente del titular o desde terceros legítimamente relacionados con la finalidad del tratamiento, tales como clientes mandantes, portales laborales, mutuales y proveedores.

5.7 Tratamiento por terceros

La empresa podrá apoyarse en proveedores de GPS o trazabilidad de flota, software de RR.HH., servicios de nube o hosting, Microsoft 365 y sistemas ERP, de forma genérica, siempre bajo obligaciones de confidencialidad y seguridad.

5.8 Videovigilancia y biometría

La empresa mantiene cámaras perimetrales en el recinto de San Bernardo con la única finalidad de seguridad física. Las cámaras graban solo video y sus grabaciones solo pueden ser revisadas por la gerencia. El uso de huella dactilar se limita exclusivamente al control de asistencia y es administrado por una solución externa.

5.9 Ámbito territorial, bases de datos y universo de titulares

La empresa opera y trata datos personales dentro del territorio de Chile. Sus bases de datos y registros se relacionan principalmente con procesos laborales, operacionales, administrativos, comerciales, de seguridad física y de soporte tecnológico. El universo de titulares comprende principalmente trabajadores, ex trabajadores, postulantes, clientes, contactos comerciales, proveedores, contratistas y subcontratistas.

5.10 Actividades y procesos con mayor riesgo de infracción

Se consideran actividades o procesos de mayor riesgo aquellos en que se recopilan, consultan, comunican, almacenan o resguardan datos personales en un volumen relevante o con categorías de mayor sensibilidad, tales como: administración de carpetas laborales, tratamiento de licencias médicas, uso de datos biométricos para control de asistencia, gestión de trazabilidad de vehículos, acceso a repositorios compartidos, tratamiento de datos en sistemas cloud, intercambio de información por correo electrónico, atención de requerimientos de titulares, gestión de incidentes de seguridad y tratamiento por terceros proveedores o prestadores de servicios.

5.11 Información que debe mantenerse disponible al público

La empresa procurará mantener a disposición del público, a través de su sitio web corporativo o un medio equivalente de fácil acceso, al menos la presente política con su fecha y versión, la identificación del responsable del tratamiento, los canales de contacto para solicitudes de titulares, las categorías de datos tratados, las finalidades, las bases de legitimidad, los destinatarios o categorías de destinatarios, la existencia o no de transferencias internacionales, el período de conservación de los datos, la procedencia de los datos y la referencia a los derechos que asisten a los titulares, incluyendo la posibilidad de reclamar ante la Agencia de Protección de Datos Personales cuando corresponda.

5.12 Consentimiento, retiro del consentimiento y decisiones automatizadas

Cuando el tratamiento se funde en el consentimiento del titular, éste podrá retirarlo en cualquier momento por los canales establecidos, sin afectar la licitud del tratamiento realizado con anterioridad a dicho retiro. A la fecha, la empresa declara no efectuar decisiones automatizadas ni elaboración de perfiles sobre la base de datos personales tratados en sus operaciones.

6. Medidas de seguridad de la información

Grupo Logístico Chile SpA mantiene medidas de seguridad proporcionales a la naturaleza de los datos tratados y a los riesgos asociados.

- Cuentas individuales nominativas
- Contraseñas robustas
- Control de accesos y segregación de funciones
- Bloqueo automático de sesión por inactividad
- Firewall
- Respaldos en la nube
- Gestión de incidentes
- Política de seguridad de la información

6.1 Reglas y procedimientos específicos de prevención

Acceder únicamente a los datos personales estrictamente necesarios para el desempeño de las funciones asignadas.

Utilizar solo cuentas individuales autorizadas, quedando prohibido compartir credenciales, reutilizar accesos de terceros o mantener sesiones abiertas sin supervisión.

Almacenar información personal únicamente en repositorios corporativos autorizados por la empresa.

Evitar el envío de datos personales a destinatarios incorrectos, verificando previamente identidad, dirección de correo y legitimidad del requerimiento.

Resguardar especialmente los datos de salud, biométricos, bancarios, previsionales y laborales, aplicando principio de necesidad y mínima exposición.

Mantener documentos físicos bajo custodia y no dejarlos expuestos en escritorios, vehículos o lugares de tránsito.

Gestionar altas, cambios y bajas de accesos conforme a perfiles de cargo y segregación de funciones.

Sin perjuicio de lo anterior, actualmente no se encuentran formalizados MFA, antivirus o EDR administrado, cifrado general ni registros de auditoría; estos controles deberán evaluarse como parte de la mejora continua y del fortalecimiento progresivo del sistema de prevención de infracciones y de seguridad de la información.

7. Conservación, almacenamiento y revisión de datos

Los datos personales se conservarán únicamente por el tiempo necesario para cumplir la finalidad para la cual fueron recopilados, dar cumplimiento a obligaciones legales o contractuales y atender eventuales requerimientos administrativos, laborales, comerciales o judiciales.

- Datos de trabajadores: durante la vigencia de la relación laboral y posteriormente por el plazo necesario para cumplimiento legal, defensa de intereses legítimos y respaldo histórico sujeto a revisión periódica.
- Datos de postulantes: por un plazo razonable vinculado al proceso de selección y eventuales procesos futuros, sujeto a revisión periódica.
- Datos de clientes y proveedores: mientras se mantenga la relación comercial o contractual y luego como respaldo histórico, sujeto a revisión periódica.
- Datos contenidos en CCTV: por un período de 30 días, salvo requerimiento fundado de conservación por motivos de seguridad.
- Los documentos físicos se mantienen archivados en bodega dentro de las dependencias de la empresa bajo criterio de custodia y conservación documental.

8. Derechos de los titulares y canal de atención

La empresa dispondrá de canales para que los titulares puedan formular solicitudes relacionadas con sus datos personales, incluyendo requerimientos de acceso, rectificación, actualización, eliminación, oposición u otras acciones que procedan conforme a la normativa aplicable.

Las solicitudes podrán ingresarse a través del formulario o canal de contacto disponible en la página web corporativa y mediante el correo electrónico auditoria@grupologistico.cl.

La responsable interna para la coordinación de estas materias será Paola Díaz, Gerenta de Administración y Finanzas.

Como buena práctica de gestión interna, la empresa procurará responder las solicitudes en un plazo máximo de 10 días hábiles, sin perjuicio de los plazos legales aplicables.

8.1 Derechos de los titulares

Solicitar acceso a sus datos personales y a la información asociada a su tratamiento.

Solicitar rectificación, actualización o corrección de datos inexactos, desactualizados o incompletos.

Solicitar supresión, eliminación u oposición al tratamiento cuando proceda legalmente.

Solicitar portabilidad cuando resulte aplicable conforme a la ley.

Retirar su consentimiento en los tratamientos que se funden en dicha base de legitimidad.

Reclamar ante la Agencia de Protección de Datos Personales en caso de rechazo o de falta de respuesta oportuna por parte del responsable.

8.2 Publicación y transparencia

La empresa procurará publicar o mantener accesible esta política y la información mínima exigible para conocimiento de titulares y terceros interesados, mediante su sitio web corporativo o un medio de información equivalente.

9. Incidentes de seguridad y protección de datos

Ante cualquier incidente que comprometa o pueda comprometer la confidencialidad, integridad, disponibilidad o acceso autorizado a datos personales, la empresa deberá actuar con celeridad y coordinación interna.

Todo trabajador, jefatura, proveedor o tercero que detecte un incidente deberá reportarlo inmediatamente al área TI y a la Gerencia de Administración y Finanzas.

- Identificar el evento
- Contener el impacto
- Resguardar evidencias
- Evaluar los datos afectados
- Determinar la causa preliminar
- Definir acciones correctivas y preventivas
- Documentar el incidente

Evaluar si corresponde comunicación interna, contractual, regulatoria o reporte a la Agencia de Protección de Datos Personales

9.1 Reporte interno y reporte a la autoridad

Cuando un incidente constituya o pueda constituir una vulneración relevante de las medidas de seguridad aplicables a datos personales, la empresa deberá escalarlo inmediatamente a la Gerencia de Administración y Finanzas, al área TI y al responsable interno designado para su evaluación.

Si de acuerdo con la normativa vigente corresponde informar a la Agencia de Protección de Datos Personales o a los titulares afectados, la empresa realizará dicho reporte por los canales y dentro de los plazos que resulten aplicables conforme a la ley y a las instrucciones de la autoridad competente.

9.2 Denuncias internas y medidas disciplinarias

El incumplimiento de esta política, de los procedimientos internos asociados o de las instrucciones emitidas en materia de tratamiento y protección de datos personales podrá dar lugar a medidas administrativas internas de acuerdo con la normativa laboral, reglamentos internos, contratos y demás instrumentos aplicables, sin perjuicio de otras responsabilidades legales que correspondan.

Las denuncias o reportes de incumplimiento podrán realizarse a la jefatura directa, al área de Administración y Finanzas, al área TI o al responsable interno de protección de datos, debiendo resguardarse la debida revisión del caso y la aplicación de medidas correctivas cuando proceda.

10. Control documental y revisión

La presente política será administrada por el área de Administración y Finanzas, con apoyo del área TI y de la gerencia correspondiente.

La política deberá revisarse anualmente o antes si ocurre una modificación normativa relevante, un cambio significativo en los procesos de tratamiento de datos, la implementación de nuevas tecnologías o sistemas, incidentes relevantes de seguridad, o cambios organizacionales que afecten responsabilidades o flujos de información.

10.1 Integración contractual y normativa interna

La empresa procurará incorporar las obligaciones de tratamiento y protección de datos personales, confidencialidad, deber de reporte y cumplimiento de esta política en los contratos de trabajo, anexos, reglamentos internos y contratos de prestación de servicios que resulten pertinentes, incluyendo funciones directivas cuando corresponda.

Asimismo, cualquier proveedor, contratista, subcontratista o tercero con acceso a datos personales deberá sujetarse contractualmente a obligaciones de confidencialidad, seguridad, reporte de incidentes y cumplimiento de los lineamientos que la empresa establezca en esta materia.

11. Histórico de revisiones

Revisión	Descripción
00	Creación del documento
01	Ajustes derivados de revisión legal, operativa o tecnológica