



POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

APLICACIÓN OPERACIONES 360 SANTIAGO

Gran Américas Santiago Chile S.A.
Santiago de Chile

Gran Américas Santiago Chile S.A. (en adelante, la “Empresa”), en su calidad de Responsable del Tratamiento de datos personales, establece la presente Política de Protección de Datos Personales aplicable a la aplicación denominada “Operaciones 360 Santiago” (en adelante, la “Aplicación”), de conformidad con la Ley N° 19.628 sobre Protección de la Vida Privada, la Ley N° 21.459 sobre Delitos Informáticos, normativa complementaria vigente en la República de Chile y considerando la reforma legal en curso que contempla la creación de la Agencia de Protección de Datos Personales.

I. IDENTIFICACIÓN DEL RESPONSABLE

La Empresa actúa como Responsable del Tratamiento respecto de los datos personales tratados en el marco de la Aplicación.

Ámbito de aplicación: Usuarios autorizados en virtud de vínculo laboral o contractual.

I BIS. BASE JURÍDICA DEL TRATAMIENTO

El tratamiento de datos personales realizado a través de la Aplicación se funda en las siguientes bases de licitud:

- a) La relación laboral o contractual vigente entre el Usuario y la Empresa, en los términos del contrato de trabajo o instrumento contractual respectivo.
- b) El ejercicio legítimo de las facultades de dirección, organización y supervisión propias del empleador, conforme a la legislación laboral chilena.
- c) El cumplimiento de obligaciones legales aplicables a la Empresa.
- d) La autorización expresa otorgada por el titular, cuando corresponda.

En el contexto laboral, el tratamiento de datos no se fundamenta exclusivamente en el consentimiento del trabajador, sino en el marco jurídico propio de la relación contractual y en el ejercicio legítimo de facultades empresariales, siempre bajo criterios de razonabilidad y proporcionalidad.

II. OBJETO Y FINALIDAD

La Aplicación tiene por finalidad el control y supervisión de la operación de flota, la visualización de información operativa, la validación mediante códigos QR y el apoyo a la toma de decisiones en terreno.

Los datos serán tratados exclusivamente para autenticación, control de acceso, personalización del entorno, supervisión operativa y cumplimiento de obligaciones legales.

III. DATOS TRATADOS

- a) Datos de identificación: nombre, usuario corporativo, correo electrónico y rol.
- b) Datos de autenticación: credenciales cifradas.
- c) Datos de geolocalización en tiempo real.
- d) Datos derivados de lectura de códigos QR (tratamiento efímero).

IV. PRINCIPIOS APLICABLES

El tratamiento se regirá por los principios de licitud, lealtad, transparencia, minimización, limitación de finalidad, exactitud, limitación de conservación, integridad, confidencialidad y responsabilidad activa.

V. CONSENTIMIENTO EXPRESO

En cumplimiento de la Ley N° 19.628 sobre Protección de la Vida Privada y considerando las mejores prácticas internacionales en materia de protección de datos personales, el Usuario declara que:

Al momento de instalar, acceder y autenticarse en la Aplicación **Operaciones 360 Santiago**, deberá aceptar expresamente la presente Política de Protección de Datos mediante un mecanismo electrónico de aceptación (check box o botón de “Aceptar”).

La aceptación implicará:

1. Reconocimiento de haber leído la presente Política.
2. Comprensión de las finalidades del tratamiento.
3. Autorización expresa para el tratamiento de sus datos personales en los términos aquí establecidos.

4. Autorización específica para el uso de:
 - Geolocalización en tiempo real.
 - Cámara del dispositivo para lectura de códigos QR.
5. Aceptación del almacenamiento y tratamiento en infraestructura tecnológica en la nube.

El consentimiento será:

- Libre.
- Específico.
- Informado.
- Inequívoco.

La Aplicación almacenará evidencia técnica de la aceptación (fecha, hora, usuario, versión de la política aceptada).

En caso de no aceptar la presente Política, el Usuario no podrá acceder ni utilizar la Aplicación.

V BIS. PRINCIPIO DE PROPORCIONALIDAD Y RESPETO DE DERECHOS FUNDAMENTALES

La Empresa declara que el tratamiento de datos personales realizado mediante la Aplicación, incluyendo la geolocalización en tiempo real, se ajusta estrictamente a los principios de proporcionalidad, necesidad y finalidad legítima.

Dicho tratamiento:

- No constituye un sistema de vigilancia permanente.
- No implica intromisión indebida en la vida privada del trabajador.
- No vulnera los derechos fundamentales consagrados en el artículo 19 N° 4 de la Constitución Política de la República.
- Se limita exclusivamente al cumplimiento de fines operacionales vinculados a la gestión de flota y supervisión funcional.

Cualquier tratamiento que exceda dichas finalidades requerirá fundamento jurídico específico.

VI. GEOLOCALIZACIÓN

La Aplicación podrá tratar datos de geolocalización en tiempo real del dispositivo móvil del Usuario exclusivamente con la finalidad de:

- Mostrar información contextual de la operación de flota.
- Optimizar la toma de decisiones operativas.
- Validar ubicación en procesos específicos de supervisión.

Características del tratamiento:

- No se realiza monitoreo permanente fuera del uso activo de la Aplicación.
- No se generan perfiles de comportamiento.
- No se almacenan historiales de trazabilidad con fines disciplinarios automatizados.
- El uso del GPS es proporcional y limitado a la finalidad operativa.

El Usuario podrá deshabilitar el permiso de ubicación desde su dispositivo, entendiendo que ello limitará funcionalidades esenciales.

VII. USO DE CÁMARA Y QR

La Aplicación solicita acceso a la cámara únicamente para:

- Escaneo de códigos QR asociados a conductores.
- Consulta de información operativa vinculada a registros maestros.

Se deja constancia de que:

- No se almacenan imágenes.
- No se realiza reconocimiento facial.
- No se capturan datos biométricos.
- El procesamiento es inmediato y efímero.

VIII. INFRAESTRUCTURA CLOUD

La Aplicación **Operaciones 360 Santiago** puede estar alojada en infraestructura tecnológica en la nube, específicamente en servicios provistos por:

Microsoft

Plataforma: Microsoft Azure

El tratamiento de datos en infraestructura cloud implica que:

- Los servidores pueden estar ubicados dentro o fuera del territorio de la República de Chile.
- Se aplican estándares internacionales de seguridad (ISO 27001, SOC 2, cifrado en tránsito y en reposo).
- Se establecen contratos de encargo de tratamiento con el proveedor cloud.
- Se aplican controles de seguridad lógica, autenticación multifactor y segregación de ambientes.

En caso de transferencia internacional de datos, esta se realizará bajo:

- Cláusulas contractuales que garanticen nivel adecuado de protección.
- Estándares equivalentes a la normativa chilena.
- Principio de responsabilidad demostrada.

VIII BIS. ENCARGADOS DEL TRATAMIENTO

Cuando la Empresa utilice servicios tecnológicos de terceros, incluyendo proveedores de infraestructura cloud, dichos proveedores actuarán en calidad de Encargados del Tratamiento.

La Empresa declara que:

- Mantiene el control y la determinación de las finalidades del tratamiento.
- Suscribe contratos que regulan expresamente confidencialidad, seguridad y limitación de uso.
- Exige estándares equivalentes a la normativa chilena en materia de protección de datos.

La externalización de infraestructura tecnológica no implica cesión de titularidad ni transferencia de responsabilidad respecto del tratamiento de datos personales.

IX. MEDIDAS DE SEGURIDAD

La Empresa implementa medidas técnicas y organizativas para garantizar confidencialidad, integridad y disponibilidad de la información, incluyendo control de acceso basado en roles, registros de trazabilidad, protocolos de respuesta ante incidentes y evaluaciones de impacto cuando proceda.

IX BIS. DEBER DE SECRETO

Conforme al artículo 7 de la Ley N° 19.628, las personas que intervengan en cualquier fase del tratamiento de datos personales estarán obligadas a guardar secreto respecto de los mismos, obligación que subsistirá aun después de finalizada su relación contractual.

La Empresa implementa medidas de seguridad destinadas a prevenir:

- Pérdida.
- Alteración.
- Acceso no autorizado.
- Tratamiento indebido.

En caso de incidentes de seguridad que pudieren afectar datos personales, se activarán protocolos internos de respuesta y, cuando corresponda, se informará a la autoridad competente y a los titulares afectados.

X. DERECHOS DEL TITULAR

Los titulares podrán ejercer derechos de acceso, rectificación, cancelación y oposición conforme a la Ley 19.628.

Las solicitudes deberán canalizarse a través de los medios oficiales definidos por la Empresa.

X BIS. PROCEDIMIENTO DE EJERCICIO DE DERECHOS

El titular podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición mediante solicitud escrita dirigida al canal formal que la Empresa determine.

La solicitud deberá:

- Identificar al solicitante.
- Acreditar identidad mediante mecanismo razonable.
- Especificar el derecho que se desea ejercer.

La Empresa dará respuesta dentro del plazo legal aplicable y, en ausencia de regulación específica, dentro de un plazo razonable acorde a la naturaleza de la solicitud.

La cancelación o supresión no procederá cuando exista obligación legal de conservación.

XI. ADECUACIÓN A LA FUTURA REFORMA LEGAL

Gran Américas Santiago declara que la presente Política se ajustará automáticamente a la reforma en curso de la Ley 19.628 que contempla:

- Creación de la Agencia de Protección de Datos Personales.
- Principio de responsabilidad proactiva.
- Evaluaciones de impacto en protección de datos (cuando aplique).
- Notificación de brechas de seguridad.
- Mayor regulación de transferencias internacionales.
- Sanciones administrativas reforzadas.

En virtud de lo anterior, la Empresa adopta desde ya los siguientes principios avanzados:

1. Principio de licitud, lealtad y transparencia.
2. Principio de minimización de datos.
3. Principio de limitación de finalidad.
4. Principio de exactitud.
5. Principio de limitación del plazo de conservación.
6. Principio de integridad y confidencialidad.
7. Principio de responsabilidad activa.

En caso de producirse un incidente de seguridad que afecte datos personales:

- Se activará protocolo interno de respuesta.
- Se notificará a la autoridad competente cuando la normativa lo exija.

Se informará a los titulares si el riesgo es significativo.

XII. OFICIAL DE PROTECCIÓN DE DATOS

Gran Américas Santiago podrá designar un Encargado o Delegado de Protección de Datos (DPO), responsable de:

- Supervisar el cumplimiento normativo.
- Atender derechos ARCO.
- Gestionar incidentes de seguridad.
- Coordinar auditorías de cumplimiento.

XIII. CONSERVACIÓN Y TRAZABILIDAD

La Empresa mantendrá:

- Registro de actividades de tratamiento.
- Versionamiento de la Política aceptada.
- Registro de consentimientos electrónicos.
- Evidencia técnica de autenticación.

Los datos se conservarán:

- Mientras exista relación contractual o laboral.
- Durante el plazo exigido por normativa laboral o tributaria.
- Posteriormente, serán eliminados o anonimizados.

XIV. CONFIDENCIALIDAD

Todo el personal con acceso a datos personales estará sujeto a deber de confidencialidad contractual y legal.

XV. MODIFICACIONES

La presente Política podrá ser actualizada para adecuarse a cambios normativos o funcionales, siendo informadas oportunamente a los Usuarios.

XVI. RESPONSABILIDAD EN EL USO DE CREDENCIALES

El Usuario es responsable de:

- Mantener la confidencialidad de sus credenciales.
- No compartir su usuario y contraseña.
- Utilizar dispositivos seguros.
- Notificar de inmediato cualquier uso no autorizado.

La Empresa no será responsable por accesos indebidos derivados de negligencia del Usuario en el resguardo de sus credenciales.

XVII. LEY APLICABLE Y COMPETENCIA

La presente Política se rige por las leyes de la República de Chile.

Cualquier controversia derivada de su interpretación o aplicación será sometida a la competencia de los tribunales ordinarios de justicia con asiento en la ciudad de Santiago.