



POL-017_POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

ADMINISTRACIÓN DEL DOCUMENTO**Registro de Emisión**

Autor		Aprobación	
Nombre	Doris Di Pasquale	Nombre	Daniel Astudillo Alvaro Roman
Rol	Gerente de Operaciones	Rol	Alta Dirección
Fecha	19-03-2026	Fecha	29-04-2026

Control de Cambios

Versión	Modificación		Aprobación		Descripción de la Modificación
	Fecha	Nombre	Fecha	Nombre	

TABLA DE CONTENIDO

I.	Objetivo General	4
II.	Alcance	4
III.	Marco de Referencia y Documentos Relacionados	4
IV.	Definiciones.....	5
V.	Principios de Protección de Datos	5
VI.	Bases Legales para el Tratamiento	6
VII.	Derechos de los Titulares de Datos.....	7
VIII.	Seguridad de los Datos Personales.....	7
IX.	Gestión de Incidentes y Brechas de Datos	8
X.	Encargados del Tratamiento y Terceros	8
XI.	Transferencia de Datos Personales.....	8
XII.	Conservación de los Datos.....	9
XIII.	Capacitación y Concientización.....	9
XIV.	Cumplimiento y Supervisión	9
XV.	Actualización y Vigencia.....	10

I. Objetivo General

La presente Política de Protección de Datos Personales establece los principios, normas y responsabilidades que regulan el tratamiento de datos personales dentro de la organización, con el objetivo de garantizar el respeto de los derechos de los titulares, asegurar la confidencialidad, integridad y disponibilidad de la información, y cumplir con la normativa vigente en materia de protección de datos personales.

Esta política busca asegurar que el tratamiento de datos personales se realice de manera lícita, leal, transparente y proporcional, protegiendo los derechos y libertades de las personas.

II. Alcance

La presente política aplica a:

- Todos los trabajadores, colaboradores, directivos y proveedores críticos de la organización.
- Todos los procesos de negocio que impliquen tratamiento de datos personales.
- Todos los sistemas, plataformas, bases de datos y medios físicos o digitales que contengan datos personales.
- Todos los terceros que actúen como encargados del tratamiento de datos por cuenta de la organización.

Esta política aplica a todo tratamiento de datos personales realizado por la organización, ya sea de clientes, trabajadores, proveedores, usuarios o cualquier otra persona natural.

III. Marco de Referencia y Documentos Relacionados

La presente política se basa en el cumplimiento de la normativa aplicable en materia de protección de datos personales, incluyendo, entre otras:

- Ley N°21.719 de Protección de Datos Personales de Chile.
- Normativa y directrices emitidas por la autoridad competente en materia de protección de datos personales.
- Legislación complementaria aplicable en materia de privacidad, seguridad de la información y derechos fundamentales.

Cuando corresponda, esta política se complementará con otras normativas internas relacionadas con seguridad de la información, confidencialidad y gestión de riesgos.

IV. Definiciones

Para efectos de esta política se entenderá por:

Datos personales: Cualquier información relacionada con una persona natural identificada o identificable.

Datos sensibles: Datos personales que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada, tales como datos de salud, origen racial o étnico, convicciones religiosas o ideológicas, entre otros definidos por la normativa vigente.

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, tales como recolección, almacenamiento, uso, comunicación, transferencia, eliminación o modificación.

Titular de los datos: Persona natural a quien se refieren los datos personales.

Responsable del tratamiento: La organización o entidad que decide sobre la finalidad y medios del tratamiento de datos personales.

Encargado del tratamiento: Persona natural o jurídica que realiza el tratamiento de datos personales por cuenta del responsable.

V. Principios de Protección de Datos

5.1 Principio de licitud

Los datos personales serán tratados únicamente cuando exista una base legal válida que lo permita.

5.2 Principio de finalidad

Los datos personales serán recolectados para fines específicos, explícitos y legítimos, y no serán utilizados para finalidades incompatibles con aquellas para las cuales fueron recolectados.



5.3 Principio de proporcionalidad

Solo se tratarán los datos personales estrictamente necesarios para cumplir con las finalidades definidas.

5.4 Principio de calidad de los datos

Los datos personales deberán ser exactos, actualizados y pertinentes en relación con las finalidades del tratamiento.

5.5 Principio de seguridad

La organización adoptará medidas técnicas y organizativas adecuadas para proteger los datos personales contra accesos no autorizados, pérdida, alteración o divulgación indebida.

5.6 Principio de transparencia

La organización proporcionará información clara y accesible a los titulares sobre el tratamiento de sus datos personales.

5.7 Principio de responsabilidad

La organización será responsable de demostrar el cumplimiento de la normativa de protección de datos personales y de las obligaciones establecidas en esta política.

VI. Bases Legales para el Tratamiento

El tratamiento de datos personales solo se realizará cuando exista alguna de las siguientes bases legales:

- Consentimiento del titular.
- Ejecución de un contrato o medidas precontractuales.
- Cumplimiento de una obligación legal.
- Protección de intereses vitales del titular.
- Interés legítimo del responsable del tratamiento, siempre que no prevalezcan los derechos del titular.
- Otras bases legales reconocidas por la normativa vigente.

VII. Derechos de los Titulares de Datos

La organización garantiza a los titulares el ejercicio de los derechos establecidos por la normativa vigente, incluyendo:

- Derecho de acceso a sus datos personales.
- Derecho de rectificación de datos inexactos o incompletos.
- Derecho de supresión o eliminación de los datos cuando corresponda.
- Derecho de oposición al tratamiento en determinadas circunstancias.
- Derecho de portabilidad de los datos cuando sea aplicable.
- Derecho a solicitar la limitación o bloqueo del tratamiento en los casos previstos por la ley.

La organización dispondrá de mecanismos adecuados para facilitar el ejercicio de estos derechos dentro de los plazos establecidos por la normativa.

VIII. Seguridad de los Datos Personales

La organización implementará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, entre otras:

- Control de acceso a sistemas y bases de datos
- Mecanismos de autenticación y gestión de identidades
- Protección de redes y sistemas
- Cifrado o seudonimización cuando corresponda
- Registro y monitoreo de accesos
- Respaldo y recuperación de información
- Gestión de incidentes de seguridad

Estas medidas serán revisadas periódicamente y ajustadas de acuerdo con la evolución de los riesgos y la tecnología disponible.

IX. Gestión de Incidentes y Brechas de Datos

La organización contará con procedimientos para la detección, análisis y gestión de incidentes de seguridad que involucren datos personales.

Cuando corresponda, se realizarán las notificaciones a la autoridad competente y a los titulares afectados conforme a los requisitos establecidos por la normativa vigente.

X. Encargados del Tratamiento y Terceros

Cuando el tratamiento de datos personales sea realizado por terceros en nombre de la organización, estos deberán cumplir con las obligaciones establecidas en la normativa aplicable y en los contratos correspondientes.

La organización exigirá a los encargados del tratamiento la implementación de medidas adecuadas para garantizar la protección de los datos personales.

XI. Transferencia de Datos Personales

Las transferencias de datos personales a terceros o a otros países se realizarán únicamente cuando exista una base legal válida y se implementen las salvaguardas necesarias para garantizar un nivel adecuado de protección.

En Nastec, las transferencias de datos personales se realizan principalmente mediante el uso de plataformas tecnológicas corporativas (tales como correo electrónico, herramientas de seguridad y servicios cloud autorizados como BUK), asegurando:

- Uso de proveedores que cumplen estándares de seguridad
- Aplicación de controles de acceso y autenticación
- Transmisión mediante canales protegidos
- Evaluación previa de los datos a transferir (principio de minimización)

XII. Conservación de los Datos

Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir con las finalidades para las cuales fueron recolectados, o durante los plazos establecidos por la normativa aplicable.

Una vez cumplida la finalidad del tratamiento o vencidos los plazos legales, los datos serán eliminados o anonimizados de manera segura.

En Nastec, los períodos de conservación de los datos personales se definen y documentan en el Inventario de Datos, donde se establece el tiempo de retención aplicable a cada tratamiento, considerando criterios legales, contractuales y operativos.

La empresa realiza revisiones periódicas de los datos almacenados con el objetivo de asegurar su eliminación o anonimización cuando ya no sean necesarios.

XIII. Capacitación y Concientización

La organización promoverá la capacitación y concientización de sus trabajadores respecto de las obligaciones relacionadas con la protección de datos personales y el manejo adecuado de la información.

XIV. Cumplimiento y Supervisión

Nastec define una estructura de gobernanza para la protección de datos personales, asignando roles y responsabilidades para asegurar el cumplimiento normativo, incluyendo un responsable del tratamiento y las funciones de supervisión correspondientes.

La organización establece mecanismos de coordinación interna para la gestión de datos personales, asegurando la adecuada implementación de políticas, controles y mejora continua.



Se realizarán revisiones periódicas para asegurar la mejora continua del modelo de protección de datos.

XV. Actualización y Vigencia

La presente política será revisada periódicamente y actualizada cuando sea necesario para reflejar cambios en la normativa, en las actividades de la organización o en las mejores prácticas en materia de protección de datos.

La política entra en vigor a partir de su aprobación por la alta dirección de la organización y será de cumplimiento obligatorio para toda la organización y partes interesadas.