



TARJETA VECINO
MODELO REFERENCIAL
Municipalidad de La Cisterna

TÉRMINOS Y CONDICIONES DE USO Y POLÍTICA DE PRIVACIDAD

Portal de entrega y gestión de la Tarjeta Vecino
Municipalidad de La Cisterna - Chile

MODELO REFERENCIAL PARA ADAPTACIÓN Y REVISIÓN JURÍDICA

Versión 1.0 | Fecha de referencia normativa: 2 de agosto de 2026

Este documento no utiliza logotipos municipales ni acredita aprobación institucional.

Aviso importante y control del documento

Carácter del documento

El presente texto es un ejemplo general de términos de uso y política de privacidad para un portal municipal chileno. No es un acto administrativo, ordenanza, decreto alcaldicio, contrato aprobado, dictamen jurídico ni publicación oficial de la Municipalidad de La Cisterna. Debe ser revisado y adaptado por la unidad jurídica, la unidad de transparencia, seguridad de la información, comunicaciones y las áreas responsables del programa Tarjeta Vecino antes de cualquier publicación.

Documento	Modelo de Términos y Condiciones de Uso y Política de Privacidad.
Servicio de referencia	Portal web para solicitud, emisión, renovación, consulta, bloqueo y gestión de la Tarjeta Vecino.
Entidad mencionada	Municipalidad de La Cisterna, únicamente para contextualizar el ejemplo.
Versión	1.0 - modelo inicial.
Fecha normativa	2 de agosto de 2026.
Campos por completar	[URL DEL PORTAL], [CORREO DE CONTACTO], [UNIDAD RESPONSABLE], [DOMICILIO], [PLAZOS DEFINITIVOS], [PROVEEDORES], [COOKIES REALES].
Revisión mínima recomendada	Jurídica; protección de datos; transparencia; ciberseguridad; archivos y gestión documental; accesibilidad; operación del programa.

Criterio normativo temporal

A la fecha de referencia de este modelo, la Ley N° 19.628 se encuentra vigente en su régimen anterior a la reforma introducida por la Ley N° 21.719. Esta última entra en vigencia el 1 de diciembre de 2026. Por ello, el texto describe los derechos vigentes y, además, incorpora medidas de preparación compatibles con el nuevo estándar, sin afirmar que todas sus obligaciones ya sean exigibles el 2 de agosto de 2026.

La Municipalidad deberá confirmar, al momento de publicar, el estado de vigencia de las leyes, reglamentos, instrucciones de autoridades, ordenanzas, decretos alcaldicios y políticas internas aplicables.

Contenido

- Parte I: Términos y Condiciones de Uso del Portal Tarjeta Vecino.
- Parte II: Política de Privacidad y Tratamiento de Datos Personales.
- Anexo 1: Matriz referencial de datos, finalidades y conservación.
- Anexo 2: Matriz referencial de cookies y tecnologías similares.
- Anexo 3: Lista de verificación antes de publicar.
- Anexo 4: Fuentes normativas consultadas.

PARTE I. TÉRMINOS Y CONDICIONES DE USO

Lectura y aceptación

El acceso y la navegación por el Portal implican el conocimiento de estos términos. La realización de una solicitud, renovación, bloqueo u otra gestión podrá requerir una aceptación expresa mediante una casilla no preseleccionada. La aceptación no limita los derechos que la ley reconoce a las personas usuarias ni exime a la Municipalidad de sus deberes legales.

1. Identificación del Portal y alcance

Estos Términos regulan el uso de [URL DEL PORTAL] (el "Portal"), plataforma de referencia destinada a apoyar la entrega y gestión de la Tarjeta Vecino de la Municipalidad de La Cisterna.

El Portal puede permitir, según las funciones efectivamente habilitadas: crear o validar una cuenta; acreditar identidad y domicilio; solicitar, renovar o bloquear una tarjeta; consultar su estado; acceder a una credencial digital; recibir comunicaciones; revisar beneficios y comercios adheridos; y formular solicitudes de soporte.

Las condiciones particulares del programa, requisitos de acceso, vigencia de la tarjeta, categorías de beneficiarios y beneficios disponibles deberán estar respaldados por el acto administrativo, convenio, bases, reglamento u otro instrumento municipal que corresponda.

2. Definiciones

- "Municipalidad": la Municipalidad de La Cisterna, cuando actúe como administradora y responsable institucional del programa.
- "Tarjeta Vecino": credencial física o digital, nominativa y de uso personal, que acredita la habilitación de una persona para acceder a prestaciones o beneficios definidos por el programa.
- "Persona usuaria" o "titular": persona natural que navega, se registra, solicita o utiliza la Tarjeta Vecino.
- "Comercio o entidad adherida": tercero que ofrece un beneficio conforme a un convenio vigente y que no representa a la Municipalidad, salvo indicación expresa.
- "Cuenta": perfil electrónico asociado a una persona usuaria, si esta funcionalidad se encuentra habilitada.
- "Proveedor tecnológico": tercero que presta servicios de desarrollo, alojamiento, soporte, mensajería, autenticación, impresión, distribución u otros, siguiendo instrucciones documentadas de la Municipalidad.

3. Requisitos para solicitar la Tarjeta Vecino

Podrán solicitarla quienes cumplan los criterios que establezca formalmente la Municipalidad, tales como residencia, domicilio, calidad de estudiante, trabajador, cuidador u otro vínculo legítimo con la comuna. Este listado es meramente ilustrativo.

La persona solicitante deberá proporcionar información veraz, actualizada y suficiente, y acompañar los antecedentes exigidos. El Portal deberá indicar claramente qué datos y documentos son obligatorios y cuáles son opcionales.

La recepción electrónica de una solicitud no garantiza su aprobación. La Municipalidad podrá verificar los antecedentes dentro de sus competencias, solicitar aclaraciones o rechazar fundadamente la solicitud cuando no se cumplan los requisitos.

Cuando el trámite deba ser realizado por un representante, apoderado, padre, madre, tutor o cuidador, deberán acreditarse las facultades correspondientes.

4. Registro, identidad y credenciales de acceso

La persona usuaria es responsable de custodiar sus claves, códigos de verificación y dispositivos. No debe compartirlos ni permitir que terceros operen su cuenta, salvo mecanismos formales de representación.

El Portal podrá emplear autenticación municipal, ClaveÚnica u otro mecanismo autorizado. Cada mecanismo puede estar sujeto a condiciones propias del proveedor de identidad.

La Municipalidad podrá bloquear temporalmente un acceso ante intentos reiterados, señales de fraude, pérdida de control de la cuenta, requerimiento del titular o incidentes de seguridad.

La persona usuaria deberá informar oportunamente cualquier acceso no autorizado, pérdida del dispositivo o uso indebido a través de [CANAL DE SOPORTE].

5. Solicitud, emisión, entrega y renovación

La emisión estará sujeta a la validación de los requisitos, disponibilidad operativa y reglas del programa. El Portal deberá informar el estado de la solicitud y, cuando corresponda, los motivos de observación o rechazo.

La entrega física podrá efectuarse en dependencias municipales, operativos territoriales o mediante un proveedor autorizado. Antes de publicar, se deberán definir los controles de identidad, constancia de entrega y tratamiento de devoluciones.

La credencial digital, cuando exista, podrá incluir código QR, número de tarjeta, fotografía u otros elementos mínimos de validación. Se deberá evitar exhibir datos excesivos.

La renovación, reposición por pérdida o deterioro y actualización de datos se registrarán por los procedimientos y eventuales costos aprobados formalmente. Este modelo no establece cobros.

6. Uso personal y correcto de la tarjeta

La Tarjeta Vecino es personal e intransferible, salvo que el programa establezca expresamente una modalidad familiar, institucional o de representación.

La persona titular debe presentarla únicamente para acceder a beneficios vigentes y podrá ser requerida para acreditar identidad mediante un medio razonable y proporcional.

No se permite alterar, copiar, vender, ceder, prestar, falsificar, automatizar, explotar comercialmente ni utilizar la tarjeta o el Portal para obtener beneficios indebidos.

El uso irregular podrá dar lugar a bloqueo preventivo, revisión, suspensión o cancelación, respetando el procedimiento aplicable y la posibilidad de formular descargos cuando corresponda.

7. Beneficios y entidades adheridas

Los beneficios, descuentos, cupos, horarios, condiciones y vigencia son definidos en cada convenio o ficha informativa y pueden variar. El Portal deberá mostrar la fecha de actualización de la información.

Los comercios adheridos son responsables de sus productos, servicios, precios, garantías, seguridad y atención al público. La Municipalidad no garantiza la disponibilidad permanente de inventario ni sustituye las obligaciones legales del tercero.

La validación por el comercio debería limitarse a confirmar la vigencia o categoría de la tarjeta y, cuando sea necesario, la identidad del titular. No deberá permitir acceso general al expediente municipal.

Las controversias sobre la aplicación de un beneficio podrán comunicarse a [CANAL DE BENEFICIOS], sin perjuicio de los derechos y acciones que correspondan.

8. Conductas prohibidas en el Portal

- Intentar acceder a cuentas, sistemas, bases de datos o funciones sin autorización.
- Eludir medidas de seguridad, realizar pruebas de vulnerabilidad no autorizadas, introducir malware o generar una carga que afecte la disponibilidad del servicio.
- Entregar antecedentes falsos, adulterados, de terceros sin autorización o destinados a suplantar identidad.
- Extraer datos de forma masiva, usar robots o reutilizar contenidos para fines incompatibles con la ley o con la finalidad pública del Portal.
- Realizar actos discriminatorios, amenazantes, fraudulentos o que vulneren derechos de otras personas.

9. Comunicaciones y notificaciones

El Portal podrá enviar mensajes transaccionales sobre validación, observaciones, aprobación, retiro, vencimiento, bloqueo, seguridad y soporte a los datos de contacto registrados.

Las comunicaciones promocionales o informativas no indispensables deberán gestionarse de forma separada, con una opción sencilla de suscripción y retiro cuando corresponda.

Una comunicación electrónica no reemplaza una notificación administrativa formal, salvo que la normativa y el procedimiento aplicable permitan utilizar ese medio.

La persona usuaria debe mantener actualizados sus datos de contacto y revisar las bandejas de correo no deseado cuando espere una comunicación.

10. Disponibilidad, mantenimiento y accesibilidad

La Municipalidad procurará mantener el Portal disponible y seguro, pero podrá interrumpirlo por mantenimiento, contingencias, actualizaciones, fuerza mayor o incidentes.

Cuando una indisponibilidad impida cumplir un plazo o realizar una gestión relevante, se deberán informar canales alternativos y aplicar las reglas del procedimiento administrativo correspondiente.

El diseño deberá considerar accesibilidad, lenguaje claro, compatibilidad razonable con dispositivos y alternativas presenciales o asistidas para personas que no puedan utilizar medios digitales.

No se garantiza compatibilidad con equipos, navegadores o sistemas obsoletos que no reciban actualizaciones de seguridad.

11. Suspensión, bloqueo y término de la cuenta o tarjeta

La Municipalidad podrá adoptar medidas temporales o definitivas por pérdida, fallecimiento, vencimiento, incumplimiento de requisitos, uso indebido, fraude, orden de autoridad, error material o razones de seguridad.

Las medidas deberán ser proporcionales, registradas y comunicadas cuando corresponda. La persona afectada podrá solicitar revisión por [CANAL Y PROCEDIMIENTO].

La eliminación de una cuenta no implica necesariamente la eliminación inmediata de todos los antecedentes, pues algunos deberán conservarse por obligaciones legales, control, auditoría, archivo, defensa jurídica o trazabilidad.

El término del programa o de un convenio deberá informarse oportunamente y no generará por sí solo un derecho adquirido a mantener beneficios futuros.

12. Propiedad intelectual y uso de contenidos

Los textos, diseños, bases, código, marcas y contenidos del Portal se encuentran protegidos por las normas aplicables o pertenecen a sus respectivos titulares.

La información pública podrá reutilizarse en los términos permitidos por la ley y por las licencias que se indiquen. No podrán utilizarse signos municipales para sugerir patrocinio, aprobación o representación inexistente.

La persona usuaria conserva los derechos sobre los documentos que aporta, pero autoriza su tratamiento exclusivamente para gestionar el trámite y cumplir las funciones legales correspondientes.

13. Enlaces y servicios de terceros

El Portal puede enlazar a sitios de autenticación, pagos, mapas, comercios, redes sociales u otros servicios. Sus términos y políticas son independientes.

La inclusión de un enlace no implica aprobación de todo el contenido o prácticas del tercero. La Municipalidad deberá revisar periódicamente los enlaces y retirar aquellos que sean inseguros o engañosos.

Antes de integrar herramientas de terceros que recolecten datos, deberá evaluarse su necesidad, configuración, transferencias, cookies y condiciones contractuales.

14. Responsabilidad y límites jurídicos

La Municipalidad responderá conforme al ordenamiento jurídico aplicable. Ninguna cláusula de este documento pretende excluir responsabilidad por actuaciones ilegales, falta de servicio, vulneración de derechos, dolo o culpa cuando la ley no permita dicha exclusión.

La persona usuaria es responsable por la exactitud de la información que entrega y por el uso que realiza de sus credenciales, sin perjuicio de la obligación institucional de implementar controles razonables.

Los beneficios ofrecidos por terceros se sujetan a sus condiciones particulares y a la normativa que resulte aplicable a dichos terceros.

15. Modificación de estos Términos

Los Términos podrán actualizarse para reflejar cambios legales, operativos, tecnológicos o del programa. La versión publicada deberá indicar fecha de vigencia y conservarse un historial accesible.

Los cambios relevantes deberán comunicarse por medios adecuados antes de su entrada en vigor, especialmente cuando alteren requisitos, usos de datos o derechos de las personas.

Una modificación de los Términos no podrá convalidar retroactivamente un tratamiento de datos o actuación que carezca de base jurídica.

16. Ley aplicable, solicitudes y contacto

El uso del Portal se rige por las leyes de la República de Chile y por la normativa municipal aplicable.

Las solicitudes, reclamos, observaciones o consultas podrán dirigirse a [UNIDAD RESPONSABLE], correo [CORREO], teléfono [TELÉFONO] o domicilio [DOMICILIO].

Los recursos administrativos, acciones judiciales, solicitudes de acceso a información pública y demás mecanismos legales se ejercerán ante las autoridades y por los procedimientos establecidos en la legislación vigente.

Fecha propuesta de vigencia de estos Términos: [DD/MM/AAAA].

Texto sugerido para la casilla de aceptación

Casilla obligatoria no preseleccionada

“Declaro haber leído y acepto los Términos y Condiciones de Uso del Portal Tarjeta Vecino. Comprendo que la aceptación de estos Términos es independiente de las autorizaciones opcionales para comunicaciones o tratamientos de datos que requieran consentimiento.”

PARTE II. POLÍTICA DE PRIVACIDAD

Resumen en lenguaje claro

El Portal tratará únicamente los datos necesarios para verificar requisitos, administrar la tarjeta, prevenir fraude, prestar soporte y cumplir funciones municipales. La información no debe venderse ni utilizarse para publicidad comercial ajena al programa. Las personas pueden consultar y corregir sus datos y ejercer los demás derechos que establezca la legislación aplicable.

1. Responsable del tratamiento

Para efectos de este modelo, el responsable del tratamiento es la Municipalidad de La Cisterna, RUT [RUT MUNICIPAL], con domicilio en [DOMICILIO], a través de [UNIDAD RESPONSABLE]. Esta identificación debe ser validada antes de publicar.

Canal de privacidad: [CORREO DE PRIVACIDAD]. Canal general: [FORMULARIO/OFICINA]. Delegado o encargado de protección de datos, si ha sido designado: [NOMBRE/CARGO/CANAL].

2. Ámbito de aplicación

Esta Política se aplica a los datos tratados mediante el Portal, sus formularios, aplicaciones asociadas, soporte, credencial digital, procesos de impresión o entrega y registros de validación de beneficios cuando sean administrados por la Municipalidad.

Los sitios y servicios de terceros enlazados tienen políticas propias. Los comercios adheridos actuarán como responsables independientes respecto de los datos que recojan para sus propias ventas o servicios, salvo que actúen expresamente por encargo de la Municipalidad.

3. Principios de tratamiento

- Finalidad: los datos se utilizarán para propósitos determinados, explícitos y legítimos.
- Proporcionalidad y minimización: se solicitarán datos adecuados, pertinentes y limitados a lo necesario.
- Calidad y actualización: se procurará que los datos sean exactos, completos y actuales.
- Seguridad y confidencialidad: se aplicarán medidas administrativas, físicas y técnicas acordes con los riesgos.
- Transparencia: se informarán las operaciones relevantes de tratamiento en lenguaje comprensible.
- Conservación limitada: los datos no se mantendrán por más tiempo del necesario, sin perjuicio de obligaciones de archivo y control.
- Responsabilidad y trazabilidad: se documentarán decisiones, accesos, proveedores, incidentes y solicitudes de derechos.

4. Categorías de datos que podrían tratarse

- Identificación: nombre, apellidos, RUT, fecha de nacimiento, nacionalidad cuando sea estrictamente necesaria, fotografía y datos de autenticación.
- Contacto: correo electrónico, teléfono, domicilio y comuna.
- Acreditación del vínculo con la comuna: certificado, cuenta de servicio, contrato, registro municipal u otro antecedente definido por el programa.
- Datos del trámite: fecha, estado, observaciones, documentos aportados, historial de renovaciones, bloqueos, entregas y número de tarjeta.
- Representación: identidad y documento que acredita la calidad de representante, tutor, apoderado o cuidador.
- Uso y seguridad: dirección IP, fecha y hora, dispositivo, navegador, eventos de autenticación, registros de auditoría, alertas de fraude e incidentes.
- Soporte y comunicaciones: consultas, reclamos, archivos adjuntos y respuestas.
- Validación de beneficios: identificador de tarjeta, estado de vigencia, comercio, fecha y resultado de validación. No se debería registrar el detalle de compras salvo que sea indispensable y esté expresamente informado.
- Datos especiales o sensibles: sólo cuando una categoría de beneficio lo requiera, exista habilitación jurídica y se apliquen resguardos reforzados. No deberán solicitarse diagnósticos completos si basta una acreditación menos invasiva.

5. Finalidades y bases que justifican el tratamiento

- Gestionar solicitudes, verificar requisitos, emitir, entregar, activar, renovar, bloquear y cancelar la tarjeta.
- Validar identidad, domicilio, representación y elegibilidad; prevenir duplicidades, errores, fraude y uso indebido.
- Administrar la cuenta, autenticar a la persona, responder soporte y comunicar eventos del trámite o de seguridad.
- Permitir la verificación limitada de la vigencia de la tarjeta por entidades adheridas.
- Generar estadísticas y evaluar el programa, preferentemente mediante datos agregados o anonimizados.
- Cumplir deberes de transparencia, auditoría, control, archivo, probidad, seguridad, continuidad operacional y requerimientos de autoridades competentes.
- Enviar información opcional sobre actividades, programas o beneficios sólo cuando exista una base jurídica adecuada y, si corresponde, consentimiento revocable.

6. Base jurídica aplicable a un organismo público

La base principal será el cumplimiento de funciones legales y competencias municipales, junto con los actos administrativos que regulen el programa. Bajo el régimen vigente de la Ley N° 19.628, un organismo público puede tratar datos dentro de sus competencias y con sujeción a la ley sin requerir consentimiento del titular.

El consentimiento no debe utilizarse para aparentar voluntariedad cuando el tratamiento es necesario para un trámite o función pública. Cuando se solicite para una finalidad opcional, deberá ser libre, informado, específico, verificable y susceptible de retiro.

Antes de publicar, la Municipalidad deberá documentar la norma, competencia, acto o convenio que habilita cada finalidad y evitar extender los datos a finalidades incompatibles.

7. Datos obligatorios y consecuencias de no entregarlos

Cada formulario deberá distinguir los campos obligatorios de los opcionales y explicar por qué se solicitan.

La falta de datos obligatorios puede impedir verificar requisitos o resolver la solicitud. La negativa a entregar datos opcionales no deberá afectar el acceso al servicio principal.

No se deberán exigir documentos completos cuando sea suficiente una validación, certificado parcial, consulta interoperable autorizada o visualización sin almacenamiento.

8. Fuentes de los datos

- Datos proporcionados por la persona titular o su representante.
- Registros y sistemas municipales, dentro del ámbito de competencia.
- Otros organismos públicos, cuando la consulta o comunicación esté autorizada y sea necesaria.
- Proveedores de identidad y autenticación utilizados legítimamente.
- Entidades adheridas, únicamente respecto de eventos mínimos de validación, incidencias o uso irregular previstos en el convenio.
- Datos técnicos generados por el uso del Portal.

9. Destinatarios y comunicaciones de datos

- Unidades municipales que requieran acceso para tramitar, fiscalizar, controlar, atender o resolver el procedimiento, bajo perfiles y deberes de confidencialidad.
- Proveedores tecnológicos contratados, que actuarán bajo instrucciones y contratos con cláusulas de seguridad, confidencialidad, subcontratación, devolución y eliminación.
- Otros organismos públicos, tribunales, Contraloría, autoridades fiscalizadoras o de ciberseguridad cuando exista competencia y requerimiento legítimo.
- Entidades adheridas, limitándose al dato estrictamente necesario para validar la tarjeta o investigar una incidencia.
- Terceros autorizados por la persona titular cuando la ley permita basar la comunicación en su autorización.
- No se venderán ni arrendarán bases de datos personales, ni se entregarán listados a comercios para marketing propio.

10. Encargados y proveedores

Antes de contratar, se evaluarán riesgos, ubicación del alojamiento, subencargados, certificaciones, continuidad, soporte, borrado, portabilidad y respuesta a incidentes.

El contrato deberá definir instrucciones, finalidades, categorías de datos, duración, controles de acceso, cifrado, registros, notificación de incidentes, auditoría y destino de los datos al terminar.

La Municipalidad mantendrá un inventario actualizado de proveedores. En la versión pública podrá informar categorías o proveedores relevantes, sin revelar antecedentes cuya divulgación comprometa la seguridad.

11. Transferencias y almacenamiento fuera de Chile

Como criterio recomendado, los datos deberán alojarse en Chile o en ubicaciones evaluadas y contractualmente controladas. Si existe tratamiento o acceso desde el extranjero, deberá informarse y cumplir las reglas aplicables.

No deberá afirmarse que los datos nunca salen de Chile sin revisar respaldos, soporte remoto, analítica, correo, mensajería, redes de distribución y subcontratistas.

Antes de la entrada en vigencia de la Ley N° 21.719, la Municipalidad deberá revisar y adecuar las transferencias internacionales al nuevo régimen y a sus reglamentos o instrucciones.

12. Plazos de conservación

Los plazos deberán fijarse en una tabla de retención aprobada, considerando la finalidad, vigencia de la tarjeta, prescripción, auditoría, responsabilidad administrativa, archivo, transparencia y defensa jurídica.

Como ejemplo: una solicitud no completada podría eliminarse o anonimizarse después de [90/180] días; los registros de seguridad podrían conservarse entre [6 y 24] meses según riesgo; y el expediente de una tarjeta podría mantenerse durante su vigencia más el plazo institucional aplicable.

Al finalizar el plazo, los datos se eliminarán, anonimizarán o transferirán al archivo que corresponda. La mera desactivación de una cuenta no equivale a eliminación total.

13. Seguridad de la información

Se aplicarán controles acordes con el riesgo, tales como gestión de identidades y privilegios, autenticación robusta, cifrado en tránsito y reposo cuando corresponda, respaldo, registro de eventos, monitoreo, pruebas, gestión de vulnerabilidades, segmentación, capacitación y planes de continuidad.

El acceso del personal se limitará por funciones y quedará sujeto a confidencialidad. Las consultas a datos de una persona deberán ser trazables.

Los documentos cargados deberán validarse, almacenarse de forma segura y protegerse contra malware. La información sensible no se enviará en texto abierto por canales inseguros.

Ningún sistema es infalible; por ello, se mantendrán procedimientos de detección, contención, recuperación, investigación y mejora.

14. Incidentes de seguridad y privacidad

Ante un incidente, la Municipalidad y sus proveedores deberán activar el procedimiento interno, preservar evidencia, contener el impacto, evaluar riesgos para las personas y cumplir los deberes de reporte y comunicación que establezca la normativa.

Las comunicaciones a personas afectadas, cuando correspondan, deberán explicar de forma clara qué ocurrió, qué datos podrían estar involucrados, medidas adoptadas y acciones recomendadas, evitando revelar información que aumente el riesgo.

Canal sugerido para reportar vulnerabilidades o incidentes: [CORREO/FORMULARIO DE SEGURIDAD].

15. Derechos de las personas

Bajo la Ley N° 19.628 vigente al 2 de agosto de 2026, las personas pueden solicitar información sobre sus datos y su procedencia, destinatarios, finalidad y personas u organismos a quienes se transmiten regularmente; además, pueden pedir modificación, eliminación o bloqueo cuando corresponda conforme a la ley.

Desde el 1 de diciembre de 2026, la reforma de la Ley N° 21.719 amplía y sistematiza derechos como acceso, rectificación, supresión, oposición, portabilidad y bloqueo, bajo las condiciones legales aplicables.

La solicitud deberá ser gratuita, identificarse de manera razonable y describir el derecho ejercido. La Municipalidad no deberá pedir más datos de identidad que los necesarios para evitar suplantación.

Canal propuesto: [FORMULARIO DE DERECHOS], [CORREO] o presentación en [OFICINA]. Se deberá informar el procedimiento, plazos, posibilidad de subsanar y vías de reclamación vigentes.

16. Datos de niños, niñas y adolescentes

El Portal no deberá estar dirigido a menores para crear cuentas o consentir tratamientos sin reglas específicas. Cuando una tarjeta beneficie a una persona menor de edad, la solicitud deberá gestionar la representación y aplicar el interés superior y la autonomía progresiva.

Se limitará la publicación y visualización de la identidad, fotografía, domicilio y demás datos de menores. La validación por comercios deberá revelar el mínimo necesario.

Antes del 1 de diciembre de 2026 deberán revisarse especialmente las reglas de la Ley N° 21.719 respecto del tratamiento de datos de menores de 16 años.

17. Decisiones automatizadas y perfiles

Este modelo asume que no se rechazarán solicitudes exclusivamente mediante decisiones automatizadas sin intervención humana. Si se implementan reglas automáticas, se deberá informar su lógica general, permitir revisión y controlar sesgos o errores.

No se utilizarán datos de la tarjeta para elaborar perfiles comerciales, crediticios, políticos o de comportamiento ajenos a la finalidad municipal.

18. Cookies y tecnologías similares

El Portal podrá usar cookies estrictamente necesarias para sesión, seguridad, balanceo, preferencias y accesibilidad. Estas no deberían requerir una opción de rechazo cuando sean indispensables para prestar el servicio solicitado.

Las cookies de analítica, mapas, video, redes sociales o publicidad deberán desactivarse por defecto cuando requieran consentimiento, ofrecer opciones equivalentes de aceptar o rechazar y documentar la elección.

La configuración real deberá reflejarse en el Anexo 2 y en un panel de preferencias accesible en todo momento. No se deben cargar herramientas de terceros antes de la elección cuando ésta sea necesaria.

19. Transparencia, acceso a información y archivos públicos

La Municipalidad está sujeta a deberes de transparencia y acceso a información pública. Esto no significa que todos los datos personales del expediente sean públicos.

Ante solicitudes de acceso, se aplicarán las reglas de la Ley N° 20.285, las causales de secreto o reserva, los procedimientos de comunicación a terceros y los principios de divisibilidad y protección de datos.

Los plazos de conservación y archivo deberán armonizar la protección de datos con la gestión documental y el valor administrativo, fiscalizador, histórico o probatorio de los antecedentes.

20. Actualizaciones de la Política

La Política se revisará periódicamente y ante cambios sustantivos del Portal, proveedores, finalidades, normativa o riesgos.

La versión vigente deberá indicar fecha, número de versión y un resumen de cambios. Las modificaciones relevantes se comunicarán de forma destacada.

Fecha propuesta de vigencia: [DD/MM/AAAA]. Última actualización: [DD/MM/AAAA].

Texto sugerido para autorizaciones opcionales

Comunicaciones voluntarias

“Autorizo opcionalmente a la Municipalidad de La Cisterna a enviarme información sobre nuevos beneficios, actividades y programas comunales al correo o teléfono registrado. Puedo retirar esta autorización en cualquier momento, sin afectar la gestión de mi Tarjeta Vecino.”

ANEXO 1. MATRIZ REFERENCIAL DE DATOS, FINALIDADES Y CONSERVACIÓN

Uso de la matriz

Los plazos son ejemplos y deben sustituirse por una tabla de retención institucional aprobada. La base jurídica concreta debe identificarse mediante la ley, competencia, decreto, reglamento, convenio o acto administrativo aplicable.

Categoría	Finalidad	Base a documentar	Conservación referencial	Control clave
Identificación y contacto	Gestionar cuenta y solicitud; comunicarse.	Función municipal y acto que regula el programa.	Vigencia del expediente + plazo institucional.	Acceso restringido; cifrado; trazabilidad.
RUT y autenticación	Verificar identidad y evitar duplicidades/fraude.	Competencia legal; servicio de identidad autorizado.	Mientras sea necesario para identificación y control.	No exhibir completo; enmascaramiento.
Domicilio y acreditación	Verificar vínculo con la comuna.	Requisito formal del programa.	Revisión periódica; eliminación de respaldos innecesarios.	Preferir validación sobre copia completa.
Fotografía	Identificación de la tarjeta cuando sea necesaria.	Acto del programa y proporcionalidad.	Vigencia de tarjeta + reposición/archivo aplicable.	Evitar acceso por comercios a copia descargable.
Documentos de representación	Gestionar solicitudes por terceros o menores.	Normas de representación y procedimiento.	Expediente + plazo legal.	Clasificación reforzada.
Estado e historial de tarjeta	Emitir, renovar, bloquear y auditar.	Gestión del beneficio y control.	Vigencia + auditoría/prescripción.	Registro inalterable de cambios relevantes.
Eventos de validación	Confirmar beneficio y detectar abuso.	Convenio y función de control.	[6-24] meses o plazo justificado.	Minimizar: comercio, fecha, resultado; no detalle de compra.
Logs técnicos y seguridad	Seguridad, diagnóstico e investigación.	Seguridad del servicio y ciberseguridad.	[6-24] meses según riesgo.	Acceso por equipo autorizado; alertas.
Soporte y reclamos	Atender solicitudes e incidencias.	Atención municipal y procedimiento.	Cierre + plazo de reclamación/archivo.	Separar adjuntos sensibles; control de acceso.
Analítica agregada	Medir uso y mejorar el programa.	Interés público; datos anonimizados cuando sea posible.	Agregados sin identificación: según necesidad estadística.	Revisión de riesgo de reidentificación.

ANEXO 2. MATRIZ REFERENCIAL DE COOKIES Y TECNOLOGÍAS SIMILARES

La siguiente tabla no debe publicarse sin una auditoría técnica del Portal. Se deberán comprobar nombres, dominios, duración, proveedor, finalidad y momento de carga de cada tecnología.

Nombre	Origen	Finalidad	Duración	Justificación	¿Rechazable?
cookie_sesion	Propia	Mantener la sesión y proteger el formulario.	Sesión	Necesaria	No
cookie_csrf	Propia	Prevenir solicitudes maliciosas.	Sesión/horas	Necesaria	No
preferencias_accesibilidad	Propia	Recordar tamaño de texto, contraste o idioma.	6 meses	Preferencia solicitada	Según configuración
analitica_municipal	[PROVEEDOR]	Medir uso agregado del Portal.	[PLAZO]	Consentimiento o configuración sin identificación, según evaluación	Sí, cuando corresponda
mapa_terceros	[PROVEEDOR]	Mostrar ubicación de puntos de atención.	[PLAZO]	Consentimiento si el tercero rastrea o transfiere datos	Sí
video_red_social	[PROVEEDOR]	Reproducir contenido incrustado.	[PLAZO]	Consentimiento previo	Sí

Configuración recomendada del panel de preferencias

- Botones “Aceptar opcionales” y “Rechazar opcionales” con igual visibilidad.
- Acceso permanente a “Configurar cookies” desde el pie de página.
- Categorías desactivadas por defecto cuando requieran consentimiento.
- Registro de la elección sin usar patrones engañosos ni casillas preseleccionadas.
- Posibilidad de retirar o cambiar la elección con la misma facilidad con que se otorgó.

ANEXO 3. LISTA DE VERIFICACIÓN ANTES DE PUBLICAR

Gobernanza y legalidad

- ☐ Existe acto administrativo o instrumento que regula el programa, requisitos, vigencia y causales de suspensión.
- ☐ Se identificó la unidad responsable y el canal de contacto.
- ☐ La unidad jurídica revisó el documento y la versión final fue aprobada formalmente.
- ☐ Se documentó la base jurídica de cada dato y finalidad.
- ☐ Se definió un procedimiento para derechos, reclamos y revisión de rechazos.

Privacidad y transparencia

- ☐ Los formularios separan datos obligatorios y opcionales.
- ☐ No se solicitan documentos o datos excesivos.
- ☐ Existe inventario de tratamientos, proveedores y transferencias.
- ☐ La política coincide con la operación real y con las cookies observadas.
- ☐ Se armonizaron privacidad, transparencia, archivo y acceso a información pública.
- ☐ Se preparó un plan de adecuación a la Ley N° 21.719 antes del 1 de diciembre de 2026.

Seguridad y operación

- ☐ Se realizó evaluación de riesgos y pruebas de seguridad.
- ☐ Los roles de acceso son mínimos y los accesos quedan registrados.
- ☐ Los contratos con proveedores incluyen seguridad, incidentes y eliminación.
- ☐ Existe plan de continuidad, respaldo, recuperación y respuesta a incidentes.
- ☐ Se definieron canales alternativos cuando el Portal no esté disponible.

Experiencia y accesibilidad

- ☐ El contenido utiliza lenguaje claro y cumple estándares de accesibilidad aplicables.
- ☐ Las casillas de aceptación no están preseleccionadas.
- ☐ Aceptar o rechazar cookies opcionales es igualmente sencillo.
- ☐ La credencial revela sólo los datos mínimos.
- ☐ Los comercios reciben únicamente información necesaria para validar el beneficio.

ANEXO 4. FUENTES NORMATIVAS CONSULTADAS

Nota de actualización

Las normas pueden ser modificadas. Los enlaces se incluyen como referencia de consulta en la Biblioteca del Congreso Nacional de Chile y deben verificarse nuevamente al aprobar la versión oficial.

Ley sobre Protección de la Vida Privada (Ley N° 19.628, versión vigente hasta el 30 de noviembre de 2026). Biblioteca del Congreso Nacional de Chile, LeyChile. <https://www.bcn.cl/leychile/Navegar?idNorma=141599>

Reforma integral de protección de datos personales (Ley N° 21.719, vigencia general desde el 1 de diciembre de 2026). Biblioteca del Congreso Nacional de Chile, LeyChile. <https://www.bcn.cl/leychile/navegar?idNorma=1209272>

Ley Orgánica Constitucional de Municipalidades (DFL N° 1 de 2006, texto refundido de la Ley N° 18.695). Biblioteca del Congreso Nacional de Chile, LeyChile. <https://www.bcn.cl/leychile/Navegar?idNorma=251693>

Bases de los procedimientos administrativos (Ley N° 19.880). Biblioteca del Congreso Nacional de Chile, LeyChile. <https://www.bcn.cl/leychile/navegar?idNorma=210676>

Transformación Digital del Estado (Ley N° 21.180). Biblioteca del Congreso Nacional de Chile, LeyChile. <https://www.bcn.cl/leychile/navegar?idNorma=1138479>

Documentos electrónicos y firma electrónica (Ley N° 19.799). Biblioteca del Congreso Nacional de Chile, LeyChile. <https://www.bcn.cl/leychile/navegar?idNorma=196640>

Acceso a la Información Pública (Ley N° 20.285). Biblioteca del Congreso Nacional de Chile, LeyChile. <https://www.bcn.cl/leychile/navegar?idNorma=276363>

Ley Marco de Ciberseguridad (Ley N° 21.663). Biblioteca del Congreso Nacional de Chile, LeyChile. <https://www.bcn.cl/leychile/navegar?idNorma=1202434>

Cláusula final del modelo

La versión oficial deberá indicar el acto que la aprueba, la fecha de entrada en vigencia, el responsable de su mantenimiento y el historial de cambios. La publicación de este modelo sin completar los campos, revisar la operación real o validar la normativa podría generar información inexacta o insuficiente para las personas usuarias.

Elaboración técnica	[NOMBRE / UNIDAD]
Revisión jurídica	[NOMBRE / UNIDAD]
Aprobación	[ACTO ADMINISTRATIVO / FECHA]