

MODELO REFERENCIAL PARA ADAPTACIÓN Y REVISIÓN

POLÍTICA DE PRIVACIDAD

Portal de entrega y gestión de la Tarjeta Vecino

Municipalidad de La Cisterna - Chile

Documento de ejemplo - no oficial



Este texto es un modelo general para una plataforma municipal ficticia o en etapa de diseño. No utiliza logotipos, no acredita aprobación de la Municipalidad de La Cisterna y no debe publicarse sin completar los campos, verificar la operación real del portal y obtener revisión jurídica, técnica, de transparencia y de seguridad.

Documento	Política de Privacidad del Portal Tarjeta Vecino
Institución referencial	Municipalidad de La Cisterna
Versión del modelo	1.0 - 2 de agosto de 2026
Carácter	Ejemplo no oficial para adaptación y revisión
Responsable propuesto	[UNIDAD MUNICIPAL RESPONSABLE]
Canal de privacidad	[CORREO / FORMULARIO / OFICINA]

Preparado como ejemplo conforme al marco normativo chileno consultado al 2 de agosto de 2026.

Aviso previo y criterio normativo

La finalidad de este documento es explicar, en lenguaje claro, cómo podría tratar datos personales un portal destinado a solicitar, emitir, renovar, bloquear y validar una Tarjeta Vecino. La versión definitiva debe coincidir con los formularios, sistemas, contratos, bases de datos, procesos presenciales y proveedores realmente utilizados.

i	Vigencia legal relevante Al 2 de agosto de 2026 continúa operando el régimen vigente de la Ley N° 19.628. La reforma introducida por la Ley N° 21.719 tiene vigencia general desde el 1 de diciembre de 2026. Este modelo distingue ambos momentos e incorpora medidas de preparación, sin presentar anticipadamente como exigibles todas las obligaciones de la reforma.
---	--

También deben considerarse, según corresponda, las normas sobre municipalidades, procedimiento administrativo, transformación digital, transparencia y acceso a información pública, documentos electrónicos, archivo y ciberseguridad. La institución deberá revisar reglamentos, instrucciones y actos administrativos posteriores a la fecha de este modelo.

Contenido

- 1. Responsable del tratamiento y contactos
- 2. Alcance de la Política
- 3. Principios y compromisos
- 4. Datos personales que pueden tratarse
- 5. Finalidades del tratamiento
- 6. Fundamento jurídico
- 7. Datos obligatorios y opcionales
- 8. Fuentes de información
- 9. Destinatarios y comunicaciones
- 10. Proveedores y encargados
- 11. Transferencias y acceso desde el extranjero
- 12. Plazos de conservación
- 13. Seguridad e incidentes
- 14. Derechos de las personas
- 15. Niños, niñas y adolescentes
- 16. Decisiones automatizadas y perfiles
- 17. Cookies y tecnologías similares
- 18. Transparencia, archivo y acceso a información
- 19. Cambios de esta Política
- 20. Contacto y reclamos
- Anexo A. Matriz referencial de datos y conservación
- Anexo B. Matriz referencial de cookies
- Fuentes normativas consultadas

POLÍTICA DE PRIVACIDAD

Portal Tarjeta Vecino - Municipalidad de La Cisterna



Resumen en lenguaje claro

El Portal trataría sólo los datos necesarios para gestionar la Tarjeta Vecino, verificar requisitos, proteger la cuenta, atender solicitudes y validar beneficios. Los datos no se venderán ni se entregarán a comercios para marketing propio. La persona podrá consultar y solicitar correcciones o medidas sobre sus datos mediante los canales que la Municipalidad habilite.

1. Responsable del tratamiento y contactos

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]. Estos datos deben validarse antes de publicar.

- Canal de privacidad y derechos: [CORREO / FORMULARIO].
- Atención presencial: [OFICINA, DIRECCIÓN Y HORARIO].
- Canal de seguridad o reporte de vulnerabilidades: [CORREO / FORMULARIO].
- Delegado, encargado o referente de protección de datos, si existe: [CARGO Y CONTACTO].

2. Alcance de la Política

Esta Política se aplica al tratamiento de datos realizado mediante [URL DEL PORTAL], sus formularios, aplicaciones asociadas, credencial digital, soporte, procesos de impresión o entrega y registros de validación de beneficios que sean administrados por la Municipalidad.

Los sitios, plataformas o servicios de terceros enlazados se rigen por sus propias políticas. Los comercios y entidades adheridas serán responsables independientes de los datos que recopilen para sus ventas, reservas o servicios, salvo cuando actúen expresamente por encargo y bajo instrucciones de la Municipalidad.

3. Principios y compromisos

- Finalidad: Los datos se utilizarán para propósitos determinados, explícitos y vinculados con la gestión del programa.
- Minimización y proporcionalidad: Se solicitarán datos adecuados y limitados a lo realmente necesario.
- Calidad: Se procurará mantener la información exacta, completa y actualizada.
- Seguridad y confidencialidad: Se aplicarán medidas administrativas, físicas y técnicas acordes con los riesgos.
- Transparencia: Las operaciones relevantes se informarán de manera comprensible y accesible.
- Conservación limitada: Los datos no se mantendrán por más tiempo del necesario, sin perjuicio de deberes de archivo, control o defensa jurídica.
- Responsabilidad y trazabilidad: Se documentarán accesos, decisiones, proveedores, incidentes y solicitudes de derechos.

4. Datos personales que pueden tratarse

Las categorías exactas deben confirmarse mediante un inventario de formularios, bases de datos e integraciones. El Portal podría tratar:

- Identificación: nombre, apellidos, RUT, fecha de nacimiento, fotografía y datos de autenticación.
- Contacto: correo electrónico, teléfono, domicilio y comuna.
- Acreditación del vínculo con la comuna: certificados, cuentas de servicio, contratos, registros municipales u otros antecedentes definidos por el programa.
- Datos del trámite: fecha, estado, observaciones, documentos aportados, renovaciones, bloqueos, entrega y número de tarjeta.
- Representación: identidad y antecedentes que acrediten apoderamiento, tutela, cuidado o representación.
- Uso y seguridad: dirección IP, fecha y hora, dispositivo, navegador, eventos de autenticación, registros de auditoría, alertas e incidentes.

- Soporte: consultas, reclamos, archivos adjuntos y respuestas.
- Validación de beneficios: identificador de tarjeta, vigencia, entidad adherida, fecha y resultado de validación.
- Datos sensibles o especiales: únicamente cuando sean indispensables, exista habilitación jurídica y se adopten resguardos reforzados.

!	Límite recomendado No debería registrarse el detalle de compras ni solicitarse un diagnóstico médico completo cuando baste una acreditación menos invasiva. La credencial y el sistema de validación deben mostrar sólo la información mínima necesaria.
---	---

5. Finalidades del tratamiento

- Recibir, revisar y resolver solicitudes de emisión, renovación, reposición, bloqueo o cancelación de la Tarjeta Vecino.
- Verificar identidad, domicilio, representación y cumplimiento de requisitos.
- Prevenir duplicidades, errores, fraude, suplantación y uso indebido.
- Administrar la cuenta, autenticar a la persona y comunicar eventos del trámite o de seguridad.
- Permitir una validación limitada de la vigencia o categoría de la tarjeta por entidades adheridas.
- Atender consultas, solicitudes, reclamos y soporte técnico.
- Generar estadísticas y evaluar el programa, preferentemente con datos agregados o anonimizados.
- Cumplir obligaciones de auditoría, control, probidad, archivo, transparencia, continuidad, seguridad y requerimientos de autoridades competentes.
- Enviar comunicaciones opcionales sobre actividades, programas o beneficios sólo cuando exista una base jurídica adecuada y una opción de retiro cuando corresponda.

6. Fundamento jurídico

La base principal del tratamiento será el ejercicio de funciones y competencias municipales, junto con los actos administrativos, convenios, reglamentos o bases que regulen el programa. Bajo el régimen vigente de la Ley N° 19.628, los organismos públicos pueden tratar datos dentro de sus competencias y con sujeción a la ley.

El consentimiento no debe utilizarse para aparentar voluntariedad cuando el dato es necesario para resolver un trámite o ejercer una función pública. Cuando se solicite para una finalidad genuinamente opcional, debe entregarse información clara y habilitarse un mecanismo de retiro cuando corresponda.

Antes de publicar, la Municipalidad deberá documentar la norma, competencia o acto que habilita cada finalidad y evitar usos posteriores incompatibles.

7. Datos obligatorios y opcionales

Cada formulario deberá identificar los campos obligatorios y opcionales, explicar su finalidad y señalar las consecuencias de no proporcionar los obligatorios. La falta de antecedentes esenciales podría impedir verificar requisitos o resolver la solicitud; la negativa a entregar datos opcionales no debería afectar el servicio principal.

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

8. Fuentes de información

- 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 o autenticación utilizados legítimamente.
- Entidades adheridas, únicamente respecto de validaciones, incidencias o uso irregular previsto en el convenio.
- Datos técnicos generados por el uso del Portal.

9. Destinatarios y comunicaciones de datos

Los datos podrán ser conocidos o comunicados únicamente cuando resulte necesario y exista fundamento suficiente, por ejemplo a:

- Unidades municipales encargadas de tramitar, fiscalizar, controlar, atender o resolver el procedimiento, bajo perfiles de acceso y deberes de confidencialidad.
- Proveedores tecnológicos contratados para alojamiento, desarrollo, impresión, distribución, mensajería, autenticación o soporte, bajo instrucciones documentadas.
- Otros organismos públicos, tribunales, Contraloría, autoridades fiscalizadoras o de ciberseguridad cuando exista competencia y requerimiento legítimo.
- Entidades adheridas, limitándose al dato necesario para validar la tarjeta o investigar una incidencia.
- Terceros autorizados por la persona cuando la ley permita fundar la comunicación en esa autorización.



Compromiso esencial

No se venderán ni arrendarán bases de datos personales, ni se entregarán listados a comercios para marketing propio.

10. Proveedores y encargados

Los proveedores que traten datos por cuenta de la Municipalidad deberán actuar conforme a instrucciones y contratos que regulen finalidades, duración, categorías de datos, confidencialidad, subcontratación, controles de acceso, cifrado, registros, respaldo, auditoría, incidentes, devolución y eliminación.

Antes de contratar se recomienda evaluar riesgos, ubicación del alojamiento, subproveedores, certificaciones, continuidad, portabilidad, soporte remoto y capacidad de respuesta a incidentes. La Municipalidad deberá mantener un inventario actualizado de proveedores.

11. Transferencias y acceso desde el extranjero

Como criterio recomendado, los datos deberían alojarse en Chile o en ubicaciones previamente evaluadas y controladas mediante contrato. Si existe almacenamiento, respaldo, soporte o acceso desde el extranjero, esta circunstancia debe identificarse e informarse de acuerdo con las reglas aplicables.

No debe afirmarse que los datos nunca salen de Chile sin revisar servicios de nube, correo, analítica, mensajería, redes de distribución, respaldo, soporte remoto y subcontratistas. Antes del 1 de diciembre de 2026 deberán revisarse las transferencias internacionales conforme al nuevo régimen introducido por la Ley N° 21.719 y sus normas complementarias.

12. Plazos de conservación

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

Al terminar el plazo, los datos deberán eliminarse, anonimizarse o transferirse al archivo que corresponda. La desactivación de una cuenta no equivale necesariamente a la eliminación completa de los antecedentes.

13. Seguridad e incidentes

La Municipalidad y sus proveedores aplicarán controles proporcionales al riesgo, tales como gestión de identidades y privilegios, autenticación robusta, cifrado cuando corresponda, respaldo, registro de eventos, monitoreo, pruebas, gestión de vulnerabilidades, segmentación, capacitación y planes de continuidad.

Los accesos del personal deberán limitarse por función y quedar sujetos a confidencialidad y trazabilidad. Los documentos cargados deberán validarse y protegerse contra malware. La información sensible no se enviará por canales inseguros.

Ante un incidente se activarán procedimientos de detección, contención, recuperación, investigación y mejora; se preservará evidencia y se cumplirán los deberes de reporte o comunicación aplicables. Cuando corresponda informar a las personas afectadas, la comunicación debe explicar el hecho, los datos potencialmente involucrados, las medidas adoptadas y las acciones recomendadas.

14. 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, su procedencia, destinatarios y finalidad, y pueden pedir modificación, eliminación o bloqueo cuando se cumplan las condiciones legales.

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, conforme a sus requisitos y excepciones.

Para ejercer un derecho, la persona deberá identificarse razonablemente y describir su solicitud. La Municipalidad no debe pedir más antecedentes de identidad que los necesarios para evitar suplantaciones. El trámite será gratuito en los casos previstos por la ley y deberá informar plazos, subsanación y vías de reclamación.



Canales a completar

Formulario: [URL]. Correo: [CORREO]. Atención presencial: [OFICINA]. Procedimiento e identificación requerida: [DESCRIPCIÓN].

15. Niños, niñas y adolescentes

Cuando la tarjeta beneficie a una persona menor de edad, el procedimiento deberá gestionar adecuadamente la representación, considerar el interés superior y la autonomía progresiva, y limitar especialmente la visualización de identidad, fotografía, domicilio y demás datos.

El Portal no debería permitir que menores creen cuentas o autoricen tratamientos sin reglas específicas. Antes del 1 de diciembre de 2026 deberá revisarse especialmente la regulación de la Ley N° 21.719 sobre datos de menores de 16 años.

16. Decisiones automatizadas y perfiles

Este modelo supone que las solicitudes no serán rechazadas exclusivamente por una decisión automatizada sin intervención humana. Si se implementan reglas o modelos automáticos, deberá informarse su función general, permitir revisión, controlar sesgos y registrar los criterios aplicados.

Los datos de la Tarjeta Vecino no se utilizarán para elaborar perfiles comerciales, crediticios, políticos o conductuales ajenos a la finalidad municipal.

17. Cookies y tecnologías similares

El Portal podría utilizar cookies o tecnologías estrictamente necesarias para sesión, seguridad, balanceo, preferencias y accesibilidad. Las herramientas de analítica, mapas, video, redes sociales o publicidad deben identificarse mediante una auditoría técnica y gestionarse conforme a su finalidad, base jurídica y nivel de intrusión.

Cuando corresponda solicitar una elección, el panel debe ofrecer información clara, evitar casillas preseleccionadas, permitir rechazar opciones no esenciales y facilitar el cambio o retiro de la preferencia. La configuración pública debe coincidir con las tecnologías realmente cargadas.

18. Transparencia, archivo y acceso a información

La Municipalidad está sujeta a deberes de transparencia y acceso a información pública. Esto no significa que todos los datos personales de los expedientes sean públicos. Ante una solicitud de acceso deberán aplicarse la Ley N° 20.285, las causales de secreto o reserva, la comunicación a terceros cuando proceda y los principios de divisibilidad y protección de datos.

La conservación y el archivo deben armonizar la privacidad con el valor administrativo, fiscalizador, histórico y probatorio de los antecedentes.

19. Cambios de esta Política

La Política deberá revisarse periódicamente y ante cambios relevantes del Portal, finalidades, formularios, proveedores, integraciones, cookies, normativa o riesgos. La versión publicada debe indicar fecha, número de versión y un resumen de modificaciones relevantes.

- Fecha propuesta de entrada en vigencia: [DD/MM/AAAA].
- Última actualización: [DD/MM/AAAA].
- Versión aprobada mediante: [DECRETO / RESOLUCIÓN / ACTO ADMINISTRATIVO].

20. Contacto y reclamos

Las consultas sobre esta Política o el tratamiento de datos podrán dirigirse a [CANAL DE PRIVACIDAD]. Los reclamos relativos al trámite de la tarjeta podrán presentarse en [CANAL DE ATENCIÓN]. La versión final deberá identificar las vías administrativas, de transparencia, judiciales o ante la autoridad de protección de datos que resulten vigentes y aplicables en la fecha de publicación.

ANEXO A. Matriz referencial de datos, finalidades y conservación

Esta tabla es un ejemplo de trabajo. Los plazos y fundamentos deben ser aprobados por la institución y coordinados con archivo, control, transparencia, seguridad y defensa jurídica.

Categoría	Finalidad principal	Fundamento a documentar	Conservación referencial	Control recomendado
Identificación y contacto	Crear expediente, identificar y comunicar	Competencia municipal y acto del programa	Vigencia del expediente + plazo institucional	Acceso por rol y validación de identidad
Acreditación de domicilio o vínculo	Comprobar elegibilidad	Requisito formal del programa	Hasta validación o plazo probatorio definido	Minimizar documentos y ocultar datos no necesarios
Fotografía	Credencial y validación de identidad	Necesidad acreditada por el diseño del programa	Mientras la tarjeta esté vigente + plazo justificado	No mostrar en consultas públicas
Historial del trámite	Seguimiento, auditoría y revisión	Procedimiento administrativo y control	Según tabla de retención	Trazabilidad y registro de cambios
Representación	Permitir actuaciones por terceros	Normas de representación y procedimiento	Vigencia del poder + plazo del expediente	Verificar facultades y limitar copias
Eventos de validación	Confirmar beneficio y prevenir abuso	Convenio y finalidad del programa	[PLAZO BREVE Y JUSTIFICADO]	No registrar detalle de compra
Registros de seguridad	Prevenir, detectar e investigar incidentes	Seguridad y continuidad	[6-24 MESES SEGÚN RIESGO]	Acceso restringido e integridad de logs
Soporte y reclamos	Responder y acreditar atención	Gestión del servicio y procedimiento	Cierre + plazo de responsabilidad	Separar adjuntos sensibles
Comunicaciones opcionales	Informar actividades o beneficios	Base jurídica o autorización aplicable	Hasta retiro o fin de finalidad	Preferencias separadas y trazables

Criterios para completar la matriz

- Distinguir datos obligatorios, opcionales, inferidos y generados automáticamente.
- Identificar la norma, acto administrativo o convenio que habilita cada finalidad.
- Definir un plazo concreto o un criterio verificable; evitar expresiones como “indefinidamente”.
- Registrar el sistema, unidad responsable, usuarios con acceso y proveedor involucrado.
- Asegurar que la eliminación incluya copias operativas, respaldos y ambientes de prueba según un procedimiento documentado.

ANEXO B. Matriz referencial de cookies y tecnologías similares

Esta matriz no debe publicarse sin una auditoría técnica del Portal. Deben verificarse nombre, dominio, proveedor, duración, finalidad, momento de carga y transmisión de datos.

Categoría	Ejemplo de finalidad	¿Es esencial?	Duración	Proveedor/dominio	Tratamiento recomendado
Sesión y autenticación	Mantener la sesión y evitar suplantación	Sí	Sesión / plazo breve	[PROPIO / IDENTIDAD]	Activar sólo lo necesario; flags seguros
Seguridad	Detectar abuso, fraude o tráfico malicioso	Generalmente sí	[PLAZO]	[PROPIO / SEGURIDAD]	Minimizar identificadores y restringir acceso
Preferencias y accesibilidad	Recordar idioma o contraste	Depende	[PLAZO]	[PROPIO]	Explicar y permitir reinicio
Analítica	Medir uso y mejorar el Portal	No necesariamente	[PLAZO]	[PROVEEDOR]	Configurar minimización; solicitar elección cuando corresponda
Mapas o video	Mostrar contenido externo	No	[TERCERO]	[PROVEEDOR]	Carga diferida y aviso previo
Publicidad o redes sociales	Seguimiento o personalización externa	No	[TERCERO]	[PROVEEDOR]	Evitar en un trámite municipal salvo justificación excepcional

Configuración recomendada del panel

- Botones para aceptar o rechazar opciones no esenciales con visibilidad equivalente.
- Acceso permanente a "Configurar cookies" desde el pie de página.
- Categorías no esenciales desactivadas por defecto cuando corresponda solicitar una elección.
- Registro de la preferencia sin patrones engañosos ni casillas preseleccionadas.
- Posibilidad de cambiar o retirar la elección con una facilidad equivalente.

Fuentes normativas consultadas

Ley N° 19.628 sobre Protección de la Vida Privada. <https://www.bcn.cl/leychile/navegar?idNorma=141599>

Ley N° 21.719, reforma de protección de datos personales, vigencia general desde el 1 de diciembre de 2026. <https://www.bcn.cl/leychile/navegar?idNorma=1209272>

Ley N° 20.285 sobre Acceso a la Información Pública. <https://www.bcn.cl/leychile/navegar?idNorma=276363>

Ley N° 21.663, Ley Marco de Ciberseguridad. <https://www.bcn.cl/leychile/navegar?idNorma=1202434>

Ley N° 19.880 sobre Bases de los Procedimientos Administrativos. <https://www.bcn.cl/leychile/navegar?idNorma=210676>

DFL N° 1 de 2006, texto refundido de la Ley N° 18.695 Orgánica Constitucional de Municipalidades. <https://www.bcn.cl/leychile/navegar?idNorma=251693>

Ley N° 21.180 de Transformación Digital del Estado. <https://www.bcn.cl/leychile/navegar?idNorma=1138479>

Ley N° 19.799 sobre documentos electrónicos y firma electrónica. <https://www.bcn.cl/leychile/navegar?idNorma=196640>

Control previo a publicación



Completar todos los campos entre corchetes; comprobar la información solicitada y las cookies reales; aprobar tablas de conservación; revisar contratos y transferencias; definir procedimientos de derechos e incidentes; y obtener aprobación formal de las unidades jurídica, tecnológica, de transparencia, archivo y seguridad. La versión oficial deberá identificar el acto aprobatorio, su vigencia, el responsable de mantenimiento y el historial de cambios.