Tercera Letra

NARRATIVA · EVIDENCIA · TECNOLOGÍA

DOCUMENTO PÚBLICO · CREDENCIAL

Credencial de Seguridad y Privacidad

Marco operativo de Tercera Letra SpA en protección de datos personales y seguridad de la información

VERSIÓN	FECHA	PRÓXIMA REVISIÓN	CARÁCTER
1.0	24 de junio de 2026	24 de junio de 2027	Público

Tercera Letra SpA
RUT 77.237.103-9
Bremen 229, Casa C, Ñuñoa
Santiago, Chile
terceraletra.cl

Este documento describe cómo Tercera Letra SpA aborda la protección de datos personales y la seguridad de la información en las plataformas que desarrolla y opera. Su propósito es entregar a clientes actuales y potenciales una vista clara, verificable y operativa de las prácticas que aplicamos, los principios que las ordenan y los compromisos que asumimos.

Lo publicamos para ahorrar idas y vueltas en evaluaciones de proveedor, para que cualquier organización con la que conversamos pueda revisar nuestro marco antes de pedir información detallada, y para que las decisiones de contratación se tomen con evidencia.

1. Por qué publicamos este documento

Tercera Letra construye plataformas de inteligencia de datos para sectores donde la información tratada es por naturaleza sensible para sus titulares: educación, regulación ambiental, gestión territorial, comunidades de barrio. La protección de datos personales no es un cumplimiento periférico de nuestra operación: es una condición de posibilidad del producto. Una plataforma que no respeta la privacidad de sus usuarios no es defendible como herramienta de política pública ni como activo de negocio.

Publicamos este marco porque entendemos que cada cliente, especialmente del sector regulado, debe verificar que sus proveedores cumplen estándares mínimos a lo largo de su cadena de suministro. La Ley 21.663 sobre Marco de Ciberseguridad lo hace explícito para los Operadores de Importancia Vital y los Prestadores de Servicios Esenciales. La Ley 21.719 sobre Protección de Datos Personales lo hace exigible para todo responsable que delega tratamientos en un encargado.

Este documento es la respuesta sintética. Para profundizar, ponemos a disposición la **plantilla del Contrato de Tratamiento de Datos (DPA)** que firmamos con cada cliente, los **avisos de privacidad** de cada producto y los **canales** que detallamos al final.

2. Marco normativo

Nuestro programa de cumplimiento se enmarca en el ordenamiento jurídico chileno vigente, principalmente en:

- **Ley 21.719** sobre Protección de Datos Personales, que entra en plena vigencia el 1 de diciembre de 2026.
- **Ley 21.663** sobre Marco de Ciberseguridad.
- **Ley 21.459** sobre Delitos Informáticos.
- **Ley 20.416** sobre empresas de menor tamaño, en lo aplicable al régimen de atenuante por MiPyme.

Cuando un producto tiene por audiencia estudiantes de enseñanza media o niños, niñas y adolescentes, aplicamos las protecciones reforzadas que la propia Ley 21.719 reconoce, junto con el principio general de interés superior del menor. Cuando un producto se ofrece a titulares fuera del territorio nacional, consideramos la regulación local aplicable. Para actividades que utilizan modelos de inteligencia artificial, observamos como referencia operativa el proyecto de ley sobre sistemas de IA en tramitación (Boletín 16.821-19).

3. Principios que ordenan el tratamiento de datos

El diseño de cada producto y de cada operación interna de Tercera Letra se rige por seis principios operativos. No son enunciados: son criterios de decisión que se traducen en elecciones arquitectónicas concretas, verificables en el código y en la documentación interna.

3.1 Privacidad por diseño y por defecto

Las plataformas se diseñan, desde su arquitectura inicial, para tratar el mínimo de datos personales necesarios para cumplir su finalidad declarada. Cuando un dato sensible o de mayor riesgo puede sustituirse por uno agregado, anónimo o derivado, optamos por la alternativa de menor riesgo. La configuración por defecto de las opciones que afectan la privacidad —por ejemplo, la visibilidad de la ubicación en aplicaciones comunitarias— es siempre la de mayor protección, exigiendo una acción explícita del titular para reducirla.

3.2 Separación de capas

Cuando un producto sirve a un cliente institucional para administrar información de su población objetivo, la arquitectura separa la **capa de usuarios** de la plataforma (cuentas institucionales protegidas por autenticación) de la **capa de información** tratada (datos agregados o públicos por defecto). El caso paradigmático es nuestra plataforma de inteligencia territorial para Servicios Locales de Educación Pública: los usuarios institucionales acceden a un panel cuya información subyacente proviene de fuentes públicas del Ministerio de Educación y se presenta en agregados por establecimiento, evitando estructuralmente el tratamiento individualizado de datos personales de niños, niñas y adolescentes.

3.3 Aislamiento por cliente

Cuando operamos una misma plataforma para varios clientes institucionales, la arquitectura garantiza que un usuario de un cliente no acceda nunca a información de otro. Este aislamiento se implementa mediante **reglas de seguridad a nivel de fila** en la base de datos (Row Level Security), verificadas en cada despliegue, y se documenta como medida técnica en el contrato con cada cliente.

3.4 Minimización y proporcionalidad en la retención

Cada actividad de tratamiento tiene definido un plazo de conservación. Los datos que dejan de ser necesarios para la finalidad declarada se suprimen o anonimizan. Cuando un dato es transitorio por naturaleza —por ejemplo, la ubicación geográfica de un usuario durante un paseo en una aplicación comunitaria—, el sistema lo elimina automáticamente mediante una política de Time-to-Live a nivel de base de datos, sin intervención manual ni dependencia de procesos diferidos.

3.5 Transparencia accionable

Los titulares de los datos reciben información clara sobre qué datos se recogen, para qué, con quién se comparten y por cuánto tiempo, en el momento mismo en que entregan esos datos. El canal de ejercicio de derechos ARCO+P (acceso, rectificación, cancelación, oposición, portabilidad y bloqueo temporal) está disponible en cada producto y se responde en los plazos legales. Los avisos de privacidad se escriben en lenguaje claro, dirigidos al titular, no al fiscalizador.

3.6 Trazabilidad y reversibilidad

Cada cambio relevante en la arquitectura de seguridad, en las reglas de acceso a datos o en la configuración de subprocesadores queda registrado en el control de versiones del código y referenciado en el Registro de Actividades de Tratamiento. Cuando un titular solicita la supresión de sus datos, la operación es efectiva en nuestros sistemas y se traslada a los subprocesadores con instrucciones equivalentes.

4. Cómo trabajamos con cada cliente

4.1 Determinación del rol

Antes de cualquier intercambio de datos personales, declaramos por escrito el rol que asumimos: **Responsable** del tratamiento o **Encargado** por cuenta del cliente. Este punto, aparentemente formal, fija la asignación de obligaciones bajo la Ley 21.719 y es la base de toda la conversación posterior.

En general, somos Responsables cuando ofrecemos al público directamente uno de nuestros productos propios. Somos Encargados cuando un cliente institucional nos contrata para operar una plataforma cuyos titulares son su responsabilidad.

4.2 Contrato de Tratamiento de Datos (DPA)

Cuando actuamos como Encargado, formalizamos la relación mediante un Contrato de Tratamiento de Datos (DPA) que cumple con los requisitos del artículo 15 bis de la Ley 21.719. La plantilla maestra de este contrato es pública y está disponible para revisión previa en `terceraletra.cl/seguridad/dpa`.

El DPA define el objeto, la duración, la naturaleza y finalidad del tratamiento, las categorías de datos y de titulares, los derechos y obligaciones de las Partes, el régimen de subprocesadores y transferencias internacionales, los procedimientos de respuesta a incidentes y de ejercicio de derechos, los mecanismos de devolución o supresión al término del encargo, y la ley aplicable.

4.3 Documentación interna

Mantenemos un **Registro de Actividades de Tratamiento (RAT)** actualizado, que inventaría todas las operaciones de tratamiento que ejecutamos, sus finalidades, los datos involucrados y los subprocesadores. El RAT es documento interno; se exhibe ante la Agencia de Protección de Datos Personales en procedimientos de fiscalización, ante auditores externos contratados y ante clientes que lo soliciten en procesos formales de due diligence bajo acuerdo de confidencialidad.

4.4 Acuerdos con colaboradores

Toda persona externa que colabora con Tercera Letra y accede a información confidencial firma un **Acuerdo de Confidencialidad y Tratamiento de Información** que cubre la información comer-

cial, la información de clientes, los datos personales tratados y la propiedad intelectual de los desarrollos producidos. Los accesos otorgados se registran de manera trackeable en el anexo del acuerdo, lo que permite revocación efectiva al término del vínculo.

5. Medidas técnicas y organizativas

Aplicamos las siguientes medidas, agrupadas en seis categorías. Su detalle específico para cada encargo se documenta en el Anexo correspondiente del DPA suscrito con cada cliente.

Control de acceso e identidad. Autenticación gestionada por proveedores especializados (Firebase Authentication, Supabase Auth, según el producto). Autenticación multifactor opcional o requerida según rol. Privilegios mínimos. Revisión periódica de cuentas activas.

Aislamiento por cliente. Row Level Security en bases de datos para productos multi-cliente. Separación lógica entre datos de distintos clientes verificada en cada despliegue.

Protección en tránsito y en reposo. Comunicación cliente-servidor cifrada vía HTTPS / TLS 1.2 o superior. Cifrado en reposo gestionado por los subprocesadores de almacenamiento. Cabeceras de seguridad desplegadas: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, X-Content-Type-Options. Cifrado de disco completo (BitLocker) en los equipos donde se almacenen copias locales de datos sensibles.

Respaldo y continuidad operativa. Respaldos automáticos gestionados por los subprocesadores de almacenamiento. Procedimiento de recuperación documentado.

Registro de eventos y monitoreo. Registro de accesos, errores y operaciones administrativas relevantes, con conservación de treinta días para diagnóstico. Revisión periódica de alertas.

Procedimientos organizativos. Acuerdos de confidencialidad para todo colaborador externo con acceso a sistemas o datos. Procedimiento documentado de respuesta a vulneraciones de seguridad con plazo de notificación al cliente Responsable de **veinticuatro horas** desde el conocimiento del incidente. Registro de Actividades de Tratamiento revisado al menos cada doce meses. Procedimiento documentado de atención a derechos ARCO+P con plazo legal de treinta días.

6. Subprocesadores

Para hacer funcionar las plataformas que operamos, utilizamos los siguientes proveedores externos. Cada uno trata datos exclusivamente bajo nuestras instrucciones, está sujeto a acuerdos contractuales que extienden las obligaciones de la Ley 21.719 y cumple estándares industriales de seguridad. Comunicamos a nuestros clientes Responsables cualquier modificación de esta lista con anticipación razonable.

PROVEEDOR	SERVICIOS	PAÍS
Google LLC	Workspace (correo, almacenamiento), Firebase (autenticación, base de datos, hosting), API de modelos de lenguaje	Estados Unidos
Supabase Inc.	Autenticación y base de datos Postgres con Row Level Security	Estados Unidos
Netlify Inc.	Hosting estático y CDN	Estados Unidos
Render Services Inc.	Hosting de servicios backend	Estados Unidos
Resend Inc.	Envío transaccional de correo	Estados Unidos
GitHub Inc. (Microsoft Corp.)	Repositorios de código y automatización de despliegue	Estados Unidos
NIC Chile	Registro de dominios .cl	Chile

Las transferencias internacionales se sostienen en las cláusulas contractuales tipo incluidas en los términos de servicio de cada proveedor. Cuando la Agencia de Protección de Datos Personales publique el listado de países con nivel adecuado de protección, actualizaremos esta declaración.

7. Tus derechos como titular

Si te ofrecemos directamente un producto y nuestro tratamiento de tus datos te afecta, la Ley 21.719 te reconoce los siguientes derechos, que puedes ejercer en cualquier momento, sin justificación y sin costo: **Acceso, Rectificación, Cancelación, Oposición, Portabilidad y Bloqueo temporal**.

Para ejercerlos, escríbenos a `privacidad@terceraletra.cl`. Respondemos en un plazo máximo de **treinta días corridos** desde la recepción de tu solicitud. Si por la complejidad necesitamos más tiempo, te lo informamos dentro de ese mismo plazo.

Cuando el responsable de tus datos no es Tercera Letra sino un cliente nuestro (por ejemplo, una institución educativa que opera una plataforma desarrollada por nosotros), te trasladamos al canal del responsable y te informamos del traslado.

Tienes derecho a presentar reclamo ante la **Agencia de Protección de Datos Personales** si nuestra respuesta no te resulta satisfactoria.

8. Divulgación responsable de vulnerabilidades

Si eres investigador de seguridad y detectas una vulnerabilidad en alguno de los productos o servicios que operamos, te invitamos a reportarla a `seguridad@terceraletra.cl`. Te pedimos:

- Describir la vulnerabilidad con el detalle suficiente para reproducirla.
- No acceder a datos de otros usuarios más allá de lo estrictamente necesario para demostrar el problema.
- No divulgar públicamente la vulnerabilidad hasta que hayamos tenido oportunidad razonable de remediarla.
- Si necesitas establecer un canal cifrado, pídelo en tu primer mensaje y lo coordinamos.

Nos comprometemos a:

- Acusar recibo de tu reporte dentro de **cinco días hábiles**.
- Mantenerte informado del progreso de la remediación.
- Reconocer públicamente tu contribución, si así lo deseas.
- No emprender acciones legales contra investigadores que actúen de buena fe dentro de los términos descritos.

9. Documentos públicos disponibles

DOCUMENTO	UBICACIÓN
Plantilla del Contrato de Tratamiento de Datos (DPA)	`terceraletra.cl/seguridad/dpa`
Avisos de privacidad por producto	Dentro de cada aplicación y en su sitio público
security.txt	`terceraletra.cl/.well-known/security.txt`

10. Contactos

Para consultas sobre datos personales y ejercicio de derechos

`privacidad@terceraletra.cl`

Para reportes de vulnerabilidades de seguridad

`seguridad@terceraletra.cl`

Para incidentes urgentes

`sergio.molina@terceraletra.cl`

Tercera Letra SpA
RUT 77.237.103-9
Bremen 229, Casa C, Ñuñoa, Santiago, Chile
`terceraletra.cl`

Aprobación

Este documento fue elaborado y aprobado por el representante legal de Tercera Letra SpA. Su archivo institucional se mantiene bajo control de versiones en el repositorio interno de cumplimiento de Tercera Letra (`_seguridad-y-cumplimiento/06-credencial-publica/`).