



Solución push-to-talk

DOCUMENTACIÓN INSTITUCIONAL Y CONTRACTUAL

Política de Privacidad corePTT

Tratamiento de datos personales en el sitio la relación comercial y la plataforma

Plataforma corePTT

Cumplimiento normativo y gobernanza
Seguridad y protección de datos

03

Gobernanza corePTT

Revisión 1.3 • 14 de octubre de 2026

sales@coreptt.com

COREPTT TECNOLOGIA LTDA

CNPJ 69.599.966/0001-93 • Campinas SP

Revisión 1.3 | 14 de octubre de 2026

BORRADOR PARA REVISIÓN JURÍDICA

Política de Privacidad corePTT

Tratamiento de datos personales en el sitio la relación comercial y la plataforma

Responsable legal y comercial	COREPTT TECNOLOGIA LTDA
CNPJ	69.599.966/0001-93
Nombre comercial	COREPTT TECNOLOGIA
Domicilio registrado	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Municipio y estado	Campinas/SP
CEP	13025-270
Marca y plataforma	corePTT
Revisión	1.3
Fecha de revisión	14 de octubre de 2026
Estado documental	Borrador para revisión jurídica

Esta Política presenta los datos que podrán tratarse, sus finalidades, los roles del PROVEEDOR y del CLIENTE, los criterios de conservación y los medios para que los titulares ejerzan sus derechos. Abarca la relación comercial, los portales, la operación contratada y la evaluación gratuita de 7 días.

Este documento forma parte del conjunto documental de corePTT y deberá leerse junto con los instrumentos aplicables a su finalidad. En la prueba gratuita se aplican el Contrato de Prueba de 7 días y la ficha de activación. En la operación de pago se aplican los documentos identificados en la Orden de Contratación. Su incorporación exige que se faciliten antes de la aceptación, con título, revisión y fecha; los cambios futuros no tienen efecto contractual automático ni retroactivo.

Identificación del PROVEEDOR

COREPTT TECNOLOGIA LTDA, nombre comercial COREPTT TECNOLOGIA, inscrita en el CNPJ con el nº 69.599.966/0001-93, con domicilio en Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270, en adelante el PROVEEDOR.

La marca utilizada es corePTT, con core en minúsculas y PTT en mayúsculas. El PROVEEDOR deberá identificarse en los instrumentos comerciales, fiscales y de evaluación; la marca no sustituye la identificación de la persona jurídica.

Ventas y contratación: sales@coreptt.com; teléfono registrado: (11) 9839-0601. Asuntos jurídicos, privacidad e integridad: legal@coreptt.com. Revisión 1.3 del 14 de octubre de 2026. Borrador para revisión jurídica.

1 Quién trata los datos

COREPTT TECNOLOGIA LTDA, CNPJ 69.599.966/0001-93, con domicilio en Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270, actúa como responsable del

tratamiento para las finalidades propias que efectivamente determine, como la relación comercial, gestión contractual, prevención del fraude, seguridad y cumplimiento de obligaciones. El canal de privacidad es legal@coreptt.com.

El CLIENTE define las finalidades y los medios esenciales del tratamiento de los datos de sus usuarios, comunicaciones y localización. Cuando el PROVEEDOR trate estos datos según instrucciones lícitas y documentadas del CLIENTE, actuará como encargado del tratamiento, también en la prueba. Para sus finalidades propias, podrá actuar como responsable independiente. La clasificación depende de cada finalidad concreta y se documentará en el DPA o en el instrumento de evaluación.

2 A quién se aplica esta política

Esta Política abarca a los visitantes de los portales, representantes de clientes y socios, usuarios de la plataforma, personas que participan en demostraciones, contactos de soporte y titulares cuyos datos se introduzcan en un entorno corePTT. No sustituye los avisos específicos presentados por el CLIENTE en su condición de responsable del tratamiento.

3 Datos que pueden tratarse

Categoría	Ejemplos
Registro profesional	nombre, empresa, cargo, correo electrónico corporativo, teléfono e identificador de usuario
Cuenta y autenticación	nombre de acceso, identificadores, factores de autenticación, historial de acceso y cambios de permisos
Dispositivo y red	IP, modelo, sistema operativo, versión de la aplicación, identificadores técnicos, operador y diagnósticos
Uso operativo	grupos, canales, eventos PTT, presencia, estado, horarios, registros de despacho y metadatos de comunicación
Contenido	audio, vídeo, mensajes, adjuntos y grabaciones cuando la función esté habilitada
Localización	coordenadas, fecha, hora, precisión e historial, según la configuración del CLIENTE
Soporte	solicitudes de soporte, grabaciones de atención, pruebas, registros y comunicaciones con el equipo técnico
Comercial y fiscal	propuestas, contratos, contactos de cobro, documentos fiscales, pagos y datos bancarios estrictamente necesarios
Sitio y cookies	páginas visitadas, preferencias de consentimiento, origen del acceso y datos de navegación descritos en la Política de Cookies

El contenido de voz, vídeo o mensajes podrá revelar información sensible. Por regla general, la plataforma no exige estas categorías. Los datos personales sensibles y los datos de niños o adolescentes quedan fuera de la prueba gratuita, salvo acuerdo específico previo y cumplimiento de los requisitos legales. Los proyectos que los impliquen deberán documentar la finalidad, base jurídica, necesidad, salvaguardas, permisos y conservación antes de la activación.

4 Cómo se obtienen los datos

- directamente del titular, en registros, formularios, reuniones, demostraciones y solicitudes de soporte;
- del CLIENTE, que crea cuentas, grupos, permisos y configuraciones;
- automáticamente, durante el uso de la aplicación, los dispositivos y las integraciones;
- de socios, revendedores, fabricantes, operadores o bases públicas, cuando sea necesario para la relación comercial y esté permitido por la ley.

5 Finalidades y bases jurídicas

Finalidad	Base jurídica habitual y observaciones
Negociar contratar y ejecutar servicios	actuaciones precontractuales y ejecución de un contrato; interés legítimo para contactos empresariales compatibles
Crear cuentas y proporcionar funciones	base jurídica definida por el responsable para la finalidad y los titulares; el PROVEEDOR ejecuta instrucciones lícitas y documentadas cuando actúa como encargado
Prestar soporte y mantener la calidad	ejecución de un contrato; interés legítimo sujeto a una evaluación de necesidad y ponderación
Proteger cuentas e investigar abusos	cumplimiento de una obligación legal, ejercicio legítimo de derechos o interés legítimo cuando proceda, documentados según la necesidad, proporcionalidad y ponderación
Facturar y mantener registros	ejecución de un contrato y cumplimiento de obligaciones legales, fiscales y contables
Enviar comunicaciones comerciales	consentimiento cuando sea exigible o interés legítimo en una relación empresarial existente, siempre con un mecanismo de oposición
Atender a titulares y autoridades	cumplimiento de una obligación legal o regulatoria y ejercicio legítimo de derechos
Utilizar cookies no necesarias	consentimiento, con posibilidad de rechazo y retirada

Cada tratamiento deberá tener una base jurídica adecuada a su finalidad y a los titulares implicados. Aceptar la contratación o esta Política no constituye un consentimiento genérico de los usuarios. Las instrucciones del CLIENTE no sustituyen la identificación de una base jurídica por el responsable. Cuando sea aplicable el consentimiento, será específico e informado, con posibilidad de rechazo y retirada; la retirada no afecta a los tratamientos realizados válidamente antes de ella.

6 Rol del CLIENTE como responsable del tratamiento

El CLIENTE deberá informar previamente a los titulares sobre el monitoreo, grabación, localización, finalidades, acceso de administradores y conservación; adoptar una base jurídica adecuada; limitar los permisos; y atender los derechos. La decisión sobre el monitoreo de trabajadores depende de la necesidad, proporcionalidad y legislación aplicable. El PROVEEDOR tratará los datos operativos conforme a instrucciones lícitas y documentadas y no sustituirá esta evaluación por la aceptación contractual.

7 Comunicación de datos

El PROVEEDOR comunica datos solo cuando sea necesario para prestar el servicio, cumplir una obligación, ejercer derechos o realizar una operación empresarial legítima. Los destinatarios pueden incluir proveedores de nube, comunicación, monitoreo, soporte, firma, cobro, contabilidad, fabricantes e integradores vinculados al entorno. Cada proveedor debe recibir únicamente los datos necesarios para su función y asumir obligaciones compatibles de confidencialidad y seguridad.

Los datos también pueden facilitarse a una autoridad competente mediante una orden o una base legal válida. Siempre que esté permitido, el PROVEEDOR evaluará la regularidad y el alcance de la solicitud y registrará su atención.

8 Subencargados del tratamiento

Los prestadores y subencargados aplicables al entorno, su función, los países de tratamiento y los canales pertinentes deberán identificarse en un anexo o listado facilitado al CLIENTE antes de la activación. Los cambios seguirán el procedimiento del DPA o un acuerdo escrito. Las objeciones basadas en la protección de datos se evaluarán y podrán exigir una alternativa viable o la finalización de la función, conforme a los instrumentos aplicables.

9 Transferencias internacionales

Los datos solo podrán consultarse o almacenarse fuera de Brasil cuando la arquitectura contratada utilice un proveedor o equipo en el extranjero. El PROVEEDOR y el CLIENTE deberán identificar los países, destinatarios y finalidades en el DPA o Anexo Técnico y adoptar un mecanismo válido del art. 33 de la LGPD.

Cuando se utilicen las cláusulas estándar de la Resolución CD ANPD n° 19 de 2024, el texto oficial se incorporará íntegramente y sin modificación al instrumento firmado entre el exportador y el importador. La Política o página específica deberá informar, en lenguaje claro, sobre la forma, duración, destino, responsabilidades y canal para el ejercicio de derechos.

10 Conservación

Registro	Criterio de conservación
Datos de cuenta	vigencia de la cuenta y período necesario para su cierre, auditoría y ejercicio de derechos
Voz vídeo mensajes y localización	plazo seleccionado por el CLIENTE en la Orden de Contratación, sujeto a bloqueo legal o preservación válida
Registros de acceso a la aplicación	mínimo legal aplicable a los proveedores de aplicaciones, en un entorno controlado y seguro, y plazo adicional justificado
Solicitudes de soporte y pruebas técnicas	tiempo necesario para el soporte, historial de cambios, prevención de recurrencias y defensa de derechos
Datos fiscales y contractuales	plazos legales, regulatorios y de prescripción aplicables
Registros de incidentes	al menos cinco años desde el registro, conforme a la Resolución CD ANPD n° 15 de 2024
Cookies	plazo indicado en el centro de preferencias o hasta la retirada, cuando proceda

Registro	Criterio de conservación
Contenido operativo de la prueba	eliminación o anonimización en un plazo máximo de 30 días después de la finalización; copias de seguridad residuales en un plazo máximo de 90 días después de la finalización; validación técnica antes de la firma y reservas legales aplicables

Los datos eliminados del entorno activo podrán persistir en copias de seguridad protegidas durante el ciclo informado en la contratación, con acceso restringido y sin uso operativo. En la prueba, los residuos se purgarán en un plazo máximo de 90 días después de su finalización, plazo sujeto a la validación de la arquitectura antes de la firma. La conservación por obligación legal o ejercicio legítimo de derechos tendrá una finalidad limitada, acceso restringido y el plazo aplicable.

11 Decisiones automatizadas

corePTT puede generar alertas, indicadores técnicos y reglas automáticas configuradas por el CLIENTE. El PROVEEDOR no debe utilizar estos resultados para tomar por su cuenta decisiones que afecten a los intereses del titular. Si el CLIENTE configura un proceso decisorio automatizado, deberá informar sobre la lógica relevante y garantizar los derechos previstos en el art. 20 de la LGPD, cuando proceda.

12 Seguridad

El PROVEEDOR mantendrá medidas técnicas y administrativas proporcionales a la naturaleza del tratamiento y al riesgo, conforme a los controles efectivamente aplicables al entorno y los compromisos del DPA o de la prueba. El CLIENTE y los usuarios deberán proteger las credenciales, dispositivos, redes, integraciones y perfiles bajo su responsabilidad. Esta Política no declara certificación, auditoría independiente, cifrado de extremo a extremo ni ausencia de incidentes.

13 Incidentes de seguridad

La parte que identifique un incidente con datos personales lo comunicará a la otra sin demora injustificada, con la información disponible y actualizaciones para la contención, investigación y evaluación. El responsable evaluará y realizará las comunicaciones a la ANPD y a los titulares cuando sean exigibles, dentro de los plazos legales; el encargado prestará la cooperación necesaria. La distribución de roles no excluye las obligaciones propias de cada parte. Los incidentes y decisiones se registrarán conforme a las disposiciones aplicables.

14 Derechos del titular

- confirmar la existencia de tratamiento y obtener acceso a los datos;
- corregir datos incompletos, inexactos o desactualizados;
- solicitar la anonimización, bloqueo o eliminación de datos innecesarios, excesivos o tratados de forma no conforme;
- solicitar la portabilidad conforme a la regulación y protegiendo los secretos comerciales e industriales;
- obtener información sobre las comunicaciones de datos y sobre la posibilidad de negar o retirar el consentimiento;
- oponerse al tratamiento irregular y solicitar la revisión de decisiones automatizadas, cuando proceda;
- presentar peticiones ante la ANPD y ejercer derechos ante los organismos de defensa competentes.

Las solicitudes podrán enviarse a legal@coreptt.com con información suficiente para localizar los datos y confirmar la identidad. El PROVEEDOR podrá solicitar pruebas proporcionadas para evitar el fraude. Cuando el CLIENTE sea el responsable del tratamiento, la solicitud se remitirá al responsable o se atenderá conforme a sus instrucciones lícitas, sin excluir las obligaciones propias del PROVEEDOR. Las

respuestas observarán los plazos legales aplicables, incluida la declaración completa de acceso en un plazo máximo de quince días cuando sea exigible.

15 Encargado de protección de datos

El canal público para titulares y autoridades es legal@coreptt.com. La identificación y los datos profesionales del encargado de protección de datos, cuando sean exigibles, deberán divulgarse conforme a la LGPD y la regulación aplicable. El encargado de protección de datos recibe comunicaciones, orienta a la organización y desempeña las actividades legales pertinentes. La indicación del canal no atribuye a una persona no identificada un cargo ni un nombramiento formal.

16 Actualizaciones

Las actualizaciones podrán reflejar cambios legales, técnicos u operativos y se identificarán mediante revisión y fecha. Los cambios materiales se comunicarán de forma compatible con el tratamiento y la relación existente. No validarán retroactivamente tratamientos irregulares ni se incorporarán automáticamente a contratos vigentes. Las políticas incorporadas al contrato deberán haberse facilitado e identificado antes de la aceptación; los cambios observarán el procedimiento acordado y las normas imperativas.

Datos en integraciones externas

Una integración solo debe transmitir los datos necesarios para la función contratada. La Política, el DPA o el listado de subencargados deben informar sobre las categorías de proveedores, finalidades, categorías de datos, ubicación del tratamiento y mecanismo aplicable a las transferencias internacionales.

El uso de infraestructura o software de terceros no excluye las obligaciones del PROVEEDOR sobre los tratamientos realizados bajo su responsabilidad. Cuando un proveedor actúe como responsable independiente, esta condición y el canal de atención correspondiente deberán presentarse claramente al titular.

Conservación del contenido operativo

En la operación de pago, las grabaciones estarán disponibles durante un máximo de 90 días naturales en ventana móvil únicamente cuando se contraten la función y ese plazo. Los plazos de mensajes, archivos, localización y demás contenidos se definirán en la Orden de Contratación y en el DPA, según la finalidad, base jurídica, capacidad y controles. El contenido podrá eliminarse al finalizar el plazo aplicable, salvo preservación lícita.

El plazo contractual de las grabaciones no se extiende automáticamente al registro, facturación, registros de acceso, seguridad, solicitudes de soporte, incidentes, acreditación contractual ni atención de derechos. Cada categoría se conservará únicamente durante el período necesario para su finalidad y las obligaciones aplicables. La prueba gratuita no garantiza la conservación ni disponibilidad de grabaciones durante 90 días.

Datos de evaluación y prueba de concepto

La prueba estándar dura 7 días naturales, equivalentes a 168 horas desde la activación comunicada. Deben preferirse datos ficticios, anonimizados o minimizados. Al finalizar, el acceso podrá cerrarse, sin conversión automática a un plan de pago. El CLIENTE deberá realizar las exportaciones antes del vencimiento. Sin contratación ni preservación lícita, el contenido operativo se eliminará o anonimizará en un plazo máximo de 30 días después de la finalización; las copias de seguridad residuales se purgarán en un plazo máximo de 90 días después de la finalización, sin reutilización operativa. Estos plazos deben validarse en la arquitectura antes de la firma.

El alojamiento, los países de tratamiento, los prestadores, las funciones de grabación y localización y las instrucciones del CLIENTE deberán informarse y validarse antes de activar la prueba. El contenido de las comunicaciones no se destinará a publicidad, venta a terceros ni entrenamiento de modelos de IA sin un acuerdo específico y una base jurídica adecuada. La continuidad después de la prueba depende de la contratación formal a través de sales@coreptt.com y no garantiza la recuperación de contenido ya eliminado.

Los órganos y entidades públicas siguen siendo responsables de definir la finalidad pública, competencia, base jurídica, publicidad, clasificación de la información y autorizaciones internas. Los datos relacionados con la seguridad pública, defensa nacional, seguridad del Estado o investigación penal solo podrán utilizarse en una prueba dentro de su propio régimen jurídico y bajo la tutela pública aplicable.

Copias de seguridad y solicitudes de eliminación

Las copias de seguridad sirven para la continuidad y recuperación, no para el archivo ni la consulta ordinaria. Durante el ciclo de purga, el contenido eliminado se aislará del uso normal, protegerá y borrará mediante una rotación segura. Si una recuperación técnicamente necesaria vuelve a introducir datos cuya eliminación se haya solicitado, deberá aplicarse de nuevo la instrucción de eliminación. La prueba no garantiza copias de seguridad, restauración ni recuperación de datos ya eliminados.

Control documental

Campo	Registro
Responsable de la documentación	COREPTT TECNOLOGIA LTDA
Estado documental	Borrador para revisión jurídica
Canal comercial	sales@coreptt.com
Asuntos jurídicos privacidad e integridad	legal@coreptt.com