



Solución push-to-talk

DOCUMENTACIÓN INSTITUCIONAL Y CONTRACTUAL

Política de Uso Aceptable corePTT

Conductas permitidas restricciones y respuesta al uso indebido

Plataforma corePTT

Cumplimiento normativo y gobernanza
Seguridad y protección de datos

05

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 Uso Aceptable corePTT

Conductas permitidas restricciones y respuesta al uso indebido

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
Código postal	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 establece reglas prácticas para la comunicación, grabación, localización, APIs, dispositivos y seguridad. Se aplica a la operación contratada y a la evaluación gratuita de 7 días, respetando los recursos, límites, finalidades y responsabilidades documentados en cada instrumento.

Este documento forma parte del conjunto documental 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 el cuadro de activación. En la operación de pago, se aplican los documentos identificados en la Orden de Contratación. Su incorporación exige que se ponga a disposición antes de la aceptación, con título, revisión y fecha; las futuras modificaciones no tienen efectos contractuales automáticos ni retroactivos.

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 letras 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 Finalidad

Esta Política protege a las personas, redes, dispositivos, clientes y a la propia plataforma. Se aplica a usuarios, administradores, integraciones, APIs, aplicaciones conectadas y a cualquier persona que utilice una credencial o un recurso de corePTT.

2 Uso autorizado

El servicio debe utilizarse para comunicaciones profesionales legítimas, dentro del alcance aprobado por el CLIENTE y de los permisos asignados. El usuario no puede eludir controles, aprovechar una función con una finalidad oculta ni utilizar el entorno de otra organización sin autorización.

3 Contenido y conductas prohibidos

- amenazas, persecución, acoso, discriminación, explotación, extorsión o incitación a la violencia;
- material ilícito, fraudulento, difamatorio o que vulnere la confidencialidad, la imagen, la propiedad intelectual o la privacidad;
- uso para coordinar delitos, obstruir a las autoridades u ocultar actividades ilegales;
- grabación, filmación o localización de una persona sin fundamento jurídico e información adecuada;
- divulgación de credenciales, datos personales o información confidencial más allá de la necesidad operativa;
- comunicación deliberadamente falsa que pueda comprometer la seguridad, la continuidad o la respuesta a un incidente.

4 Seguridad e integridad

- no realizar pruebas de carga, intrusión o seguridad, escaneos, interceptación de tráfico, explotación de vulnerabilidades ni intentos de acceso a otros entornos sin autorización escrita específica;
- no introducir malware, código destructivo, automatización abusiva ni mecanismos de persistencia;
- no eludir la autenticación, los límites, los registros de auditoría, las restricciones de licencia ni los controles administrativos;
- no utilizar una cuenta genérica cuando el entorno exija trazabilidad individual;
- no conectar dispositivos comprometidos, con sus protecciones eliminadas o con una versión sin soporte cuando ello aumente el riesgo.

5 Uso de APIs e integraciones

Las integraciones deberán respetar la documentación, los límites de llamadas, el alcance de las credenciales y el entorno autorizado. Se prohíben la extracción sin finalidad y autorización legítimas, la reidentificación de datos anonimizados, la replicación o reventa no autorizada del servicio y las copias sin controles compatibles. Las claves y los secretos deberán protegerse y sustituirse cuando se hayan expuesto; las APIs no habilitadas en el alcance quedan fuera de la prueba.

6 Privacidad y monitorización

El CLIENTE debe configurar la grabación y la localización de forma proporcional a la finalidad comunicada. Se prohíbe utilizar corePTT para vigilancia clandestina, elaboración de perfiles discriminatorios, control de la vida privada o decisiones exclusivamente automatizadas sin las salvaguardas exigidas por la ley. El acceso al contenido operativo debe responder a una necesidad funcional y quedar registrado en la auditoría.

7 Uso en entornos críticos

El usuario deberá mantener medios alternativos y no depender exclusivamente de corePTT para asistencia o mando cuyo fallo pueda causar la muerte, lesiones graves, daños ambientales o pérdidas materiales relevantes. Cualquier compromiso comercial de uso crítico exige un proyecto específico, pruebas, redundancia, contingencia y aceptación formal con evidencia técnica. En la prueba gratuita, el uso como sistema de emergencia o infraestructura de misión crítica queda fuera del alcance. La plataforma no sustituye a los servicios públicos de emergencia.

8 Recursos de red

Se prohíbe generar una carga desproporcionada, llamadas automatizadas no autorizadas, envíos masivos, interferencias, suplantación de identidad, ocultación del origen o un uso que degrade la experiencia de otros clientes. El PROVEEDOR puede aplicar límites técnicos razonables para preservar la seguridad y la disponibilidad.

9 Equipos y números de serie

Los dispositivos suministrados en alquiler o comodato deben utilizarse en el lugar, para la finalidad y con la configuración acordados. El CLIENTE no puede retirar la identificación patrimonial, modificar el firmware sin autorización, romper un precinto ni transferir el equipo a un tercero fuera del contrato.

10 Comunicación responsable de vulnerabilidades

Las sospechas de vulnerabilidades deberán remitirse de forma confidencial a legal@coreptt.com, con descripción, evidencias minimizadas y un contacto seguro. La comunicación no autoriza el acceso a datos de terceros, la persistencia, la interrupción ni las pruebas invasivas, ni genera una recompensa automática. Las eventuales pruebas exigen autorización escrita con alcance, ventana temporal y responsabilidades; la divulgación deberá respetar los derechos, la confidencialidad y la seguridad.

11 Investigación

El PROVEEDOR podrá preservar los registros pertinentes, limitar los accesos y solicitar la información necesaria para investigar una infracción. Considerará la gravedad, la recurrencia, el impacto y la cooperación, y limitará las medidas a lo necesario. El tratamiento de evidencias deberá respetar la finalidad, la base jurídica, el acceso restringido y un plazo justificado, sin autorizar la vigilancia indiscriminada del contenido.

12 Consecuencias

La infracción podrá dar lugar a orientación, bloqueo, sustitución de credenciales, suspensión o terminación, según la gravedad, el riesgo, la ley y el contrato. El PROVEEDOR informará del motivo cuando esté permitido y ofrecerá la oportunidad de corregir la situación cuando sea compatible con el riesgo. Las medidas urgentes podrán ser inmediatas. Las comunicaciones a autoridades o terceros requieren fundamento jurídico y un alcance proporcional; la gratuidad no elimina los deberes de buena fe, seguridad y protección de datos.

13 Responsabilidad del CLIENTE

El CLIENTE debe formar a los usuarios, mantener actualizados a los administradores, revisar los accesos, desactivar las cuentas de las personas desvinculadas e investigar el uso indebido bajo su control. Debe cooperar con el PROVEEDOR en la contención de incidentes y no instruir a los usuarios para que infrinjan esta Política.

14 Consultas y excepciones

Las excepciones operativas requieren aprobación escrita del PROVEEDOR y del responsable autorizado por el CLIENTE, con alcance, plazo, riesgos y controles. No pueden autorizar conductas ilícitas ni excluir normas obligatorias. La ausencia de respuesta no significa autorización. Las modificaciones de los recursos y de la duración de la prueba deberán registrarse, y el contacto comercial no prorroga el acceso.

Derechos de terceros e integraciones autorizadas

El usuario no podrá eludir licencias, copiar software, utilizar marcas o logotipos sin autorización, extraer código, manipular firmware, crear integraciones no aprobadas ni infringir los términos de los fabricantes y proveedores conectados al entorno.

Uso de entornos de evaluación

La prueba estándar dura 7 días naturales, equivalentes a 168 horas a partir de la activación comunicada, con una licencia de R\$ 0,00 y un alcance validado en el cuadro de activación. No incluye SLA comercial ni disponibilidad continua. Se prohíbe utilizarla para emergencias, producción crítica, vigilancia ilícita, tratamiento fuera de la finalidad autorizada o elusión de licencias, seguridad y procedimientos de contratación. Quedan excluidos los datos sensibles y los datos de niños o adolescentes, salvo acuerdo específico previo y cumplimiento de los requisitos legales.

El CLIENTE deberá dar preferencia a datos ficticios, anonimizados o minimizados y realizar sus exportaciones antes del final de la prueba. No hay renovación automática ni conversión automática a una modalidad de pago, obligación de compra ni cobro retroactivo de la licencia gratuita. Para continuar, deberá formalizar la contratación a través de sales@coreptt.com; teléfono registrado: (11) 9839-0601. Si no existe contratación o conservación lícita, el contenido operativo se eliminará o anonimizará en un plazo máximo de 30 días después de la finalización, y las copias de seguridad residuales se purgarán en un plazo máximo de 90 días después de la finalización, sin reutilización operativa; los plazos están sujetos a la validación de la arquitectura antes de la firma. La prueba no garantiza la restauración ni grabaciones durante 90 días.

Los organismos públicos y las empresas deberán autorizar internamente la prueba, designar a un responsable y permitir únicamente datos compatibles con la finalidad y la clasificación de la información. Las partes cumplirán la legislación aplicable sobre integridad y anticorrupción, sin ventajas indebidas, fraude ni favoritismo ilícito. Las aprobaciones, los cambios de alcance y las prórrogas se documentarán. Las comunicaciones de irregularidades podrán enviarse a legal@coreptt.com, con investigación restringida y prohibición de represalias por actuaciones de buena fe.

Esta revisión y las demás políticas solo formarán parte del acuerdo si se ponen a disposición antes de la aceptación y se identifican por título, versión y fecha. Las nuevas versiones no se incorporarán automáticamente ni modificarán retroactivamente las obligaciones. Esta Política no declara certificaciones, auditorías ni conformidad técnica que no se hayan demostrado.

Control documental

Campo	Registro
Responsable de la documentación	COREPTT TECNOLOGIA LTDA
Estado documental	Borrador para revisión jurídica

Campo	Registro
Canal de ventas	sales@coreptt.com
Asuntos jurídicos privacidad e integridad	legal@coreptt.com