



Solución push-to-talk

DOCUMENTACIÓN INSTITUCIONAL Y CONTRACTUAL

Seguridad y Confianza corePTT

Gobernanza controles responsabilidad compartida e incidentes

Plataforma corePTT

Cumplimiento normativo y gobernanza
Seguridad y protección de datos

06

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

Seguridad y Confianza corePTT

Gobernanza controles responsabilidad compartida e incidentes

Proveedor responsable	COREPTT TECNOLOGIA LTDA
Nombre comercial	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Domicilio social	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Ventas y contratación	sales@coreptt.com
Teléfono registrado	(11) 9839-0601
Asuntos jurídicos privacidad e integridad	legal@coreptt.com
Marca y plataforma	corePTT
Revisión	1.3
Fecha de revisión	14 de octubre de 2026

Este documento presenta compromisos de seguridad que pueden verificarse y separa los controles del PROVEEDOR, del CLIENTE, de los usuarios, de los operadores de telecomunicaciones y de los proveedores.

Este documento establece los controles y las responsabilidades de seguridad para corePTT, coordinados con los Términos de Uso, la Política de Privacidad, la Política de Uso Aceptable y, cuando se contraten, la Orden, el Contrato Empresarial, el DPA y el SLA. La evaluación gratuita se rige por el acuerdo de 7 días y no recibe automáticamente los objetivos comerciales de producción.

Los documentos externos solo forman parte de la relación si se ponen a disposición del CLIENTE antes de la aceptación y se identifican por título, versión y fecha. Las políticas futuras no se incorporarán automáticamente y ninguna revisión modificará retroactivamente una contratación; los cambios contractuales requieren un ajuste escrito aceptado por las partes, sin perjuicio de las normas obligatorias.

Identificación del proveedor

El PROVEEDOR es 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.

Ventas y contratación: sales@coreptt.com. Teléfono registrado: (11) 9839-0601. Asuntos jurídicos, privacidad, integridad y seguridad: legal@coreptt.com.

El PROVEEDOR es la persona jurídica responsable de los compromisos que asuma en los instrumentos corePTT. El CLIENTE y los representantes de ambas partes se identificarán en el instrumento aplicable, con facultades para aprobar el alcance y firmar.

1 Alcance y transparencia

Este documento describe el modelo de seguridad previsto para la oferta corePTT. No debe interpretarse como un certificado, un informe de auditoría ni una garantía de ausencia de incidentes. La versión publicada debe corresponder a los controles efectivamente implementados y a las evidencias que el PROVEEDOR pueda presentar bajo confidencialidad.

2 Responsabilidad compartida

Responsable	Obligaciones principales
PROVEEDOR	proteger los componentes bajo su administración, gestionar los accesos internos, responder a incidentes y supervisar a los proveedores
CLIENTE	definir usuarios, grupos, permisos, conservación, dispositivos autorizados y reglas internas de grabación y localización
Usuario	proteger las credenciales y el dispositivo, instalar actualizaciones, seguir las instrucciones y comunicar sospechas
Operador de telecomunicaciones y proveedores	cumplir sus obligaciones de red, infraestructura, producto, soporte y seguridad conforme a su propio contrato

3 Gobernanza

El PROVEEDOR debe mantener responsables definidos para seguridad, privacidad, operación y respuesta a incidentes; un inventario de los activos relevantes; evaluación periódica de riesgos; criterios de aceptación de proveedores; reglas de cambio; y registros que permitan demostrar las decisiones tomadas. Las excepciones deben tener un responsable, una justificación, un plazo y un control compensatorio.

4 Identidad y acceso

Las cuentas administrativas deben ser individuales, concederse con el mínimo privilegio necesario y revisarse periódicamente. Debe exigirse autenticación multifactor para las funciones administrativas siempre que el componente admita esta función. Las credenciales, claves y secretos no deben almacenarse en texto sin cifrar ni compartirse por canales inadecuados.

5 Entornos y cambios

Los entornos de desarrollo, prueba y producción deben separarse de acuerdo con la arquitectura. No deben utilizarse datos personales reales en las pruebas salvo que exista una necesidad documentada y una protección equivalente. Los cambios relevantes deben contar con solicitud, evaluación, aprobación, prueba, plan de reversión y registro compatibles con el riesgo.

6 Protección de datos en tránsito y almacenamiento

El Anexo Técnico debe identificar los protocolos de transporte, el cifrado disponible, la gestión de claves, las regiones de almacenamiento y las excepciones. El PROVEEDOR no declara cifrado de extremo a extremo cuando los servidores necesitan procesar, grabar, transcodificar o distribuir la comunicación. El CLIENTE recibirá una descripción suficiente para comprender este diseño antes de activar grabaciones o datos de alto riesgo.

7 Registros y monitorización

Los eventos administrativos, las autenticaciones, los cambios de permisos y las acciones críticas deben generar registros proporcionales al riesgo. El acceso a los logs es restringido, y su conservación respeta la finalidad de seguridad, el Marco Civil de Internet, el DPA y la Orden de Contratación. La monitorización no autoriza la vigilancia indiscriminada de trabajadores ni del contenido.

8 Vulnerabilidades y actualizaciones

El PROVEEDOR debe hacer seguimiento de las vulnerabilidades que afecten a los componentes bajo su gestión, priorizar las correcciones según su criticidad y el riesgo de explotación, y mantener un proceso para actualizaciones de emergencia. Los componentes sin soporte deben sustituirse, aislarse o protegerse mediante un control compensatorio documentado.

9 Desarrollo e integraciones

Los cambios de software deben someterse a una revisión compatible, control de dependencias y pruebas. Las APIs deben exigir autenticación, restringir el alcance y aplicar límites contra el abuso. Las integraciones proporcionadas por el CLIENTE deben evaluarse antes de recibir acceso a datos o funciones de alto impacto.

10 Copias de seguridad y continuidad

La frecuencia de las copias de seguridad, el período de conservación, la región, las pruebas de restauración, el objetivo de punto de recuperación y el objetivo de tiempo de recuperación deben constar en el Anexo Técnico cuando constituyan compromisos contractuales. Una copia de seguridad no equivale a un archivo permanente ni sustituye la exportación por el CLIENTE.

11 Proveedores

Los proveedores con acceso a datos o infraestructura deben evaluarse según su criticidad y asumir obligaciones de confidencialidad, seguridad, incidentes, eliminación y cooperación. El PROVEEDOR debe mantener la lista de subencargados del tratamiento y verificar que las transferencias internacionales dispongan de un mecanismo válido.

12 Personas y confidencialidad

Los empleados y prestadores con acceso deben estar sujetos a un deber de confidencialidad, recibir orientación compatible con sus funciones y perder el acceso cuando termine la necesidad. El acceso excepcional para soporte debe autorizarse, limitarse en el tiempo y registrarse siempre que la arquitectura lo permita.

13 Respuesta a incidentes

El proceso incluirá la recepción de la alerta, clasificación, preservación de evidencias, contención, erradicación, recuperación, análisis de impacto y lecciones aprendidas. El PROVEEDOR, como encargado del tratamiento de los datos del CLIENTE, comunicará al responsable del tratamiento los incidentes identificados sin demora injustificada, con la información disponible y actualizaciones, sin esperar al cierre de la investigación. El responsable del tratamiento evaluará y realizará las comunicaciones a la ANPD y a los titulares cuando sean exigidas, dentro de los plazos legales. Cada parte conserva sus propias obligaciones. El registro de incidentes con datos personales respetará el plazo legal, incluidos cinco años cuando corresponda, conforme a la LGPD y a la Resolución CD ANPD n° 15 de 2024.

14 Evidencias y auditorías

Prevía solicitud razonable y compromiso de confidencialidad, el PROVEEDOR podrá proporcionar cuestionarios respondidos, descripciones de arquitectura, políticas, informes de pruebas u otras evidencias disponibles. La entrega debe preservar los secretos comerciales, la seguridad de otros clientes y la información que aumente el riesgo de ataque.

15 Certificaciones y declaraciones

Las certificaciones ISO, los informes de auditoría, las homologaciones y la conformidad técnica, incluidos los estándares 3GPP, solo podrán anunciarse o contratarse con evidencia válida, alcance definido y período vigente. Este documento no declara certificación ni auditoría independiente. La compatibilidad funcional y la evolución del producto no equivalen a una certificación.

16 Activos soportes y eliminación

Los activos que almacenen o procesen información deben contar con un responsable, una clasificación y un ciclo de vida compatibles con el riesgo. La devolución, reutilización, venta o eliminación de equipos o soportes debe incluir la eliminación segura de los datos, la verificación del resultado y su registro cuando la criticidad lo justifique. Los dispositivos del CLIENTE siguen sujetos a sus reglas internas.

17 Infraestructura física y proveedores

Los controles físicos de los centros de datos, las telecomunicaciones y las instalaciones de terceros siguen la responsabilidad y las evidencias del proveedor correspondiente. El PROVEEDOR debe evaluar estos controles según su criticidad y no anunciar ubicación, redundancia, certificación ni vigilancia que no pueda demostrar. Las instalaciones bajo gestión directa deben restringir y registrar los accesos de forma compatible con el riesgo.

18 Pruebas de resiliencia

Los planes de continuidad, restauración de copias de seguridad y respuesta a incidentes deben ejercitarse con una periodicidad proporcional al riesgo. Deben registrarse los resultados, las carencias y los responsables de su corrección. El RTO, el RPO, la región alternativa y la frecuencia de las pruebas solo constituyen un compromiso contractual cuando consten en la Orden o en el Anexo Técnico.

19 Revisión e indicadores

El PROVEEDOR debe revisar este documento y el conjunto de controles ante un cambio relevante, un incidente significativo o, como mínimo, en un ciclo periódico definido internamente. El análisis puede considerar accesos privilegiados, vulnerabilidades, restauraciones, proveedores, incidentes, excepciones y planes de corrección, sin divulgar información que aumente el riesgo de ataque.

20 Contacto de seguridad

Las alertas de seguridad y las comunicaciones responsables de vulnerabilidades pueden enviarse a legal@coreptt.com. La información sobre incidentes en curso debe tratarse de forma confidencial para no comprometer la contención, la investigación ni a terceros.

Seguridad de la cadena de proveedores

El PROVEEDOR evalúa las dependencias relevantes de infraestructura, software, API y equipos de acuerdo con el riesgo y el alcance contratado. Los cambios de proveedor o de subencargado del

tratamiento que afecten a la seguridad, privacidad o continuidad deben seguir el procedimiento contractual y el DPA.

La página de Seguridad y Confianza describe prácticas y controles, pero no debe afirmar certificación, auditoría independiente ni conformidad integral con una norma que no se haya obtenido y mantenido formalmente.

Segregación en infraestructura compartida

Los entornos compartidos deberán adoptar una segregación lógica de cuentas, perfiles, datos y permisos compatible con la arquitectura validada. Los recursos de computación, almacenamiento, red y servicios de apoyo pueden ser comunes a varios CLIENTES. Los controles y las pruebas serán proporcionales al riesgo; no se declarará aislamiento físico sin contratación y evidencia específicas.

Entornos dedicados y gestión de servidores

En un entorno dedicado, el PROVEEDOR gestiona los recursos expresamente reservados al CLIENTE, dentro de la capa contratada. Esto puede abarcar aprovisionamiento, configuración segura, actualización, monitorización, capacidad, cuentas administrativas, registro técnico, copias de seguridad, recuperación y respuesta a incidentes. Los elementos excluidos o cogestionados deben constar en la Orden de Contratación.

La responsabilidad del PROVEEDOR por la administración del entorno no convierte en recursos propios la infraestructura física, la nube, la conectividad ni el software licenciado por terceros. El PROVEEDOR es responsable de la selección, configuración y gestión que asuma; el proveedor de infraestructura es responsable de su capa; y el CLIENTE es responsable de los usuarios, datos, terminales y decisiones bajo su control.

Copias de seguridad y recuperación

La periodicidad, conservación, alcance, cifrado, ubicación, pruebas de restauración, RPO y RTO solo constituyen un compromiso cuando se registran en el plan o en la Orden aceptada. La copia de seguridad es un control de recuperación y no sustituye al archivo histórico. La evaluación gratuita de 7 días no incluye garantía de copia de seguridad ni recuperación, salvo obligación expresamente aceptada antes de la activación; siguen siendo exigibles las medidas proporcionales de seguridad y los deberes legales.

En la prueba gratuita, el CLIENTE deberá realizar o solicitar las exportaciones necesarias antes de su finalización. Si no existe contratación o conservación jurídicamente necesaria, el contenido operativo se eliminará o anonimizará en un plazo máximo de 30 días naturales después de la finalización; las eventuales copias de seguridad residuales se purgarán en un plazo máximo de 90 días después de la finalización, con acceso restringido y sin reutilización operativa. Los plazos se validarán con la arquitectura antes de la firma. La conservación legal y el ejercicio legítimo de derechos siguen sus propios plazos y finalidades. La prueba no garantiza la conservación de grabaciones durante 90 días ni la recuperación de contenido ya eliminado.

Control documental

Campo	Registro
Responsable del documento	COREPTT TECNOLOGIA LTDA
Coordinación y revisión jurídica	Responsable que deberá designar el PROVEEDOR antes de la firma

Campo	Registro
Ventas y contratación	sales@coreptt.com
Asuntos jurídicos privacidad e integridad	legal@coreptt.com
Revisión y fecha	1.3 • 14 de octubre de 2026
Estado	Borrador para revisión jurídica