

Segurança e Confiança corePTT

Governança, controles, responsabilidade compartilhada e incidentes

Plataforma corePTT

Compliance e governança
Segurança e proteção de dados

06

Governança corePTT

Revisão 1.3 • 14 de outubro de 2026

sales@coreptt.com

COREPTT TECNOLOGIA LTDA

CNPJ 69.599.966/0001-93 • Campinas SP

Revisão 1.3 | 14 de outubro de 2026

MINUTA PARA REVISÃO JURÍDICA

Segurança e Confiança corePTT

Governança, controles, responsabilidade compartilhada e incidentes

Fornecedor responsável	COREPTT TECNOLOGIA LTDA
Nome fantasia	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Sede	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Comercial e contratação	sales@coreptt.com
Telefone cadastral	(11) 9839-0601
Jurídico privacidade e integridade	legal@coreptt.com
Marca e plataforma	corePTT
Revisão	1.3
Data da revisão	14 de outubro de 2026

Este documento apresenta compromissos de segurança que podem ser verificados e separa controles da FORNECEDORA, do Cliente, dos usuários, das operadoras e dos fornecedores.

Este documento estabelece os controles e responsabilidades de segurança para o corePTT, coordenados com os Termos de Uso, a Política de Privacidade, a Política de Uso Aceitável e, quando contratados, a Ordem, o Contrato Empresarial, o DPA e o SLA. A avaliação gratuita segue o termo de 7 dias e não recebe automaticamente as metas comerciais de produção.

Documentos externos somente integram a relação se disponibilizados ao Cliente antes do aceite e identificados por título, versão e data. Políticas futuras não serão incorporadas automaticamente e nenhuma revisão alterará retroativamente uma contratação; mudanças contratuais exigem ajuste escrito aceito pelas partes, preservadas as normas obrigatórias.

Identificação da fornecedora

A FORNECEDORA é COREPTT TECNOLOGIA LTDA, nome fantasia COREPTT TECNOLOGIA, inscrita no CNPJ sob nº 69.599.966/0001-93, com sede na Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270.

Comercial e contratação: sales@coreptt.com. Telefone cadastral: (11) 9839-0601. Jurídico, privacidade, integridade e segurança: legal@coreptt.com.

A FORNECEDORA é a pessoa jurídica responsável pelos compromissos que assumir nos instrumentos corePTT. O Cliente e os representantes de ambas as partes serão qualificados no instrumento aplicável, com poderes para aprovar o escopo e assinar.

1 Escopo e transparência

Este documento descreve o modelo de segurança esperado para a oferta corePTT. Ele não deve ser interpretado como certificado, relatório de auditoria ou garantia de inexistência de incidentes. A versão publicada deve corresponder aos controles efetivamente implantados e às evidências que a FORNECEDORA possa apresentar sob confidencialidade.

2 Responsabilidade compartilhada

Responsável	Obrigações principais
FORNECEDORA	proteger os componentes sob sua administração, gerir acessos internos, responder a incidentes e supervisionar fornecedores
Cliente	definir usuários, grupos, permissões, retenção, dispositivos autorizados e regras internas de gravação e localização
Usuário	proteger credenciais e dispositivo, instalar atualizações, seguir orientações e comunicar suspeitas
Operadora e fornecedores	cumprir suas obrigações de rede, infraestrutura, produto, suporte e segurança conforme contrato próprio

3 Governança

A FORNECEDORA deve manter responsáveis definidos para segurança, privacidade, operação e resposta a incidentes; inventário dos ativos relevantes; avaliação periódica de riscos; critérios de aceitação de fornecedores; regras de mudança; e registros que permitam demonstrar as decisões tomadas. Exceções devem possuir proprietário, justificativa, prazo e controle compensatório.

4 Identidade e acesso

Contas administrativas devem ser individuais, concedidas pelo menor privilégio necessário e revistas periodicamente. A autenticação multifator deve ser exigida para funções administrativas sempre que o componente suportar o recurso. Credenciais, chaves e segredos não devem ser armazenados em texto aberto ou compartilhados por canais inadequados.

5 Ambientes e mudanças

Ambientes de desenvolvimento, teste e produção devem ser separados de acordo com a arquitetura. Dados pessoais reais não devem ser usados em teste salvo necessidade documentada e proteção equivalente. Mudanças relevantes devem ter solicitação, avaliação, aprovação, teste, plano de reversão e registro compatíveis com o risco.

6 Proteção de dados em trânsito e armazenamento

O Anexo Técnico deve identificar protocolos de transporte, criptografia disponível, gestão de chaves, regiões de armazenamento e exceções. A FORNECEDORA não declara criptografia ponta a ponta quando servidores precisam processar, gravar, transcodificar ou distribuir a comunicação. O Cliente receberá descrição suficiente para compreender esse desenho antes de ativar gravações ou dados de alto risco.

7 Registros e monitoramento

Eventos administrativos, autenticações, alterações de permissão e ações críticas devem gerar registros proporcionais ao risco. O acesso a logs é restrito, e sua retenção observa finalidade de segurança, Marco Civil da Internet, DPA e Ordem de Contratação. Monitoramento não autoriza vigilância indiscriminada de trabalhadores ou conteúdo.

8 Vulnerabilidades e atualizações

A FORNECEDORA deve acompanhar vulnerabilidades que afetem componentes sob sua gestão, priorizar correções conforme criticidade e risco de exploração e manter processo para atualizações emergenciais. Componentes sem suporte devem ser substituídos, isolados ou protegidos por controle compensatório documentado.

9 Desenvolvimento e integrações

Alterações de software devem passar por revisão compatível, controle de dependências e teste. APIs devem exigir autenticação, restringir escopo e aplicar limites contra abuso. Integrações fornecidas pelo Cliente devem ser avaliadas antes de receber acesso a dados ou funções de alto impacto.

10 Cópias de segurança e continuidade

Frequência de backup, período de retenção, região, testes de restauração, objetivo de ponto de recuperação e objetivo de tempo de recuperação devem constar do Anexo Técnico quando forem compromissos contratuais. Backup não equivale a arquivo permanente e não substitui exportação pelo Cliente.

11 Fornecedores

Fornecedores com acesso a dados ou infraestrutura devem ser avaliados conforme criticidade e assumir obrigações de confidencialidade, segurança, incidentes, exclusão e cooperação. A FORNECEDORA deve manter a lista de suboperadores e verificar se transferências internacionais possuem mecanismo válido.

12 Pessoas e confidencialidade

Colaboradores e prestadores com acesso devem estar vinculados a dever de confidencialidade, receber orientação compatível com sua função e perder o acesso quando a necessidade terminar. Acesso excepcional para suporte deve ser autorizado, limitado no tempo e registrado sempre que a arquitetura permitir.

13 Resposta a incidentes

O processo contemplará recebimento do alerta, classificação, preservação de evidências, contenção, erradicação, recuperação, análise de impacto e lições aprendidas. A FORNECEDORA, como operadora dos dados do Cliente, comunicará ao controlador incidentes identificados sem demora injustificada, com informações disponíveis e atualizações, sem aguardar o encerramento da investigação. O controlador avaliará e realizará as comunicações à ANPD e aos titulares quando exigidas, nos prazos legais. Cada parte conserva suas obrigações próprias. O registro dos incidentes com dados pessoais observará o prazo legal, inclusive cinco anos quando aplicável, conforme a LGPD e a Resolução CD ANPD nº 15 de 2024.

14 Evidências e auditorias

Mediante solicitação razoável e compromisso de confidencialidade, a FORNECEDORA poderá fornecer questionários respondidos, descrições de arquitetura, políticas, relatórios de teste ou outra evidência

disponível. A entrega deve preservar segredo comercial, segurança de outros clientes e informações que aumentem risco de ataque.

15 Certificações e declarações

Certificações ISO, relatórios de auditoria, homologações e conformidade técnica, inclusive padrões 3GPP, somente poderão ser anunciados ou contratados com evidência válida, escopo definido e período vigente. Este documento não declara certificação ou auditoria independente. Compatibilidade funcional e evolução de produto não equivalem a certificação.

16 Ativos, mídias e descarte

Ativos que armazenem ou processem informação devem possuir responsável, classificação e ciclo de vida compatível com o risco. A devolução, reutilização, venda ou descarte de equipamento ou mídia deve incluir remoção segura dos dados, verificação do resultado e registro quando a criticidade justificar. Dispositivos do Cliente permanecem sujeitos às regras internas dele.

17 Infraestrutura física e provedores

Controles físicos de datacenters, telecomunicações e instalações de terceiros seguem a responsabilidade e as evidências do respectivo provedor. A FORNECEDORA deve avaliar esses controles conforme criticidade e não anunciar localização, redundância, certificação ou vigilância que não possa demonstrar. Instalações sob gestão direta devem restringir e registrar acessos compatíveis com o risco.

18 Testes de resiliência

Planos de continuidade, restauração de backup e resposta a incidentes devem ser exercitados em periodicidade proporcional ao risco. Resultados, lacunas e responsáveis por correção devem ser registrados. RTO, RPO, região alternativa e frequência de teste somente constituem compromisso contratual quando constarem da Ordem ou do Anexo Técnico.

19 Revisão e indicadores

A FORNECEDORA deve revisar este documento e o conjunto de controles diante de mudança relevante, incidente material ou, no mínimo, em ciclo periódico definido internamente. A análise pode considerar acessos privilegiados, vulnerabilidades, restaurações, fornecedores, incidentes, exceções e planos de correção, sem divulgar informação que aumente o risco de ataque.

20 Contato de segurança

Alertas de segurança e relatos responsáveis de vulnerabilidade podem ser enviados a legal@coreptt.com. Informações sobre incidente em andamento devem ser tratadas de forma confidencial para não comprometer contenção, investigação ou terceiros.

Segurança da cadeia de fornecedores

A FORNECEDORA avalia as dependências relevantes de infraestrutura, software, API e equipamento de acordo com o risco e o escopo contratado. Mudanças de fornecedor ou de suboperador que afetem segurança, privacidade ou continuidade devem seguir o processo contratual e o DPA.

A página de Segurança e Confiança descreve práticas e controles, mas não deve afirmar certificação, auditoria independente ou conformidade integral com norma que não tenha sido formalmente obtida e mantida.

Segregação em infraestrutura compartilhada

Ambientes compartilhados deverão adotar segregação lógica de contas, perfis, dados e permissões compatível com a arquitetura validada. Recursos de computação, armazenamento, rede e serviços de apoio podem ser comuns a vários Clientes. Os controles e testes serão proporcionais ao risco; não haverá declaração de isolamento físico sem contratação e evidência específica.

Ambientes dedicados e gerenciamento de servidores

Em ambiente dedicado, a FORNECEDORA gerencia os recursos expressamente reservados ao Cliente, dentro da camada contratada. Isso pode abranger provisionamento, configuração segura, atualização, monitoramento, capacidade, contas administrativas, registro técnico, backup, recuperação e resposta a incidentes. Itens excluídos ou cogestionados devem constar da Ordem de Contratação.

A responsabilidade da FORNECEDORA pela administração do ambiente não transforma em recursos próprios a infraestrutura física, a nuvem, a conectividade ou o software licenciados de terceiros. A FORNECEDORA responde pela seleção, configuração e gestão que assumir; o provedor responde por sua camada; e o Cliente responde por usuários, dados, terminais e decisões sob seu controle.

Backup e recuperação

Periodicidade, retenção, escopo, criptografia, localização, testes de restauração, RPO e RTO somente constituem compromisso quando registrados no plano ou na Ordem aceita. Backup é controle de recuperação e não substitui arquivo histórico. A avaliação gratuita de 7 dias não inclui garantia de backup ou recuperação, salvo obrigação expressamente aceita antes da ativação; continuam exigíveis as medidas proporcionais de segurança e os deveres legais.

No teste gratuito, o Cliente deverá realizar ou solicitar as exportações necessárias antes do término. Sem contratação ou preservação juridicamente necessária, o conteúdo operacional será eliminado ou anonimizado em até 30 dias corridos após o término; eventuais cópias residuais de backup serão expurgadas em até 90 dias após o término, com acesso restrito e sem reutilização operacional. Os prazos serão validados com a arquitetura antes da assinatura. Guarda legal e exercício regular de direitos seguem seus prazos e finalidades próprios. O teste não assegura retenção de gravações por 90 dias nem recuperação de conteúdo já eliminado.

Controle documental

Campo	Registro
Responsável pelo documento	COREPTT TECNOLOGIA LTDA
Coordenação e revisão jurídica	Responsável a designar pela FORNECEDORA antes da assinatura
Comercial e contratação	sales@coreptt.com
Jurídico privacidade e integridade	legal@coreptt.com
Revisão e data	1.3 • 14 de outubro de 2026
Situação	Minuta para revisão jurídica