



TERMOS DE USO - CMR Services

Última atualização: 13/02/2026

Operadora	CMR Services
CNPJ	54.673.492/0001-05
E-mail	financeiro@cmrservices.com.br
Endereço	Av Alto da Boa Vista, 295 – Itacaré-BA

Ao contratar, acessar ou utilizar qualquer serviço de hospedagem de **VPS** da CMR Services (“**Serviços**”), você (“**Cliente**” ou “**Contratante**”) declara que leu, entendeu e concorda integralmente com estes Termos de Uso, com a Política de Uso Aceitável (AUP) e com as políticas técnicas e operacionais aplicáveis.

Estes Termos também refletem requisitos e boas práticas usuais de datacenter e upstreams de rede, incluindo medidas de mitigação/filtragem para proteção da infraestrutura e de terceiros (ex.: bloqueios temporários, rate-limit, blackhole, etc.).

1. Definições

VPS: servidor virtual com recursos computacionais alocados conforme plano contratado.

Infraestrutura/Datacenter: ambiente físico e rede onde os Serviços são executados, operado por fornecedor(es) de infraestrutura da CMR.

Incidente de Segurança: evento envolvendo tentativa de intrusão, malware, abuso, spam, varredura/exploração, ou ataque de negação de serviço (DoS/DDoS).

2. Objeto e escopo dos Serviços

A CMR Services disponibiliza VPS e conectividade conforme o plano contratado (CPU, RAM, armazenamento, tráfego e IP, quando aplicável).

Serviços adicionais (ex.: migrações assistidas, hardening, troubleshooting avançado, otimização de performance) poderão ser cobrados à parte, mediante orçamento.

3. Uso aceitável (AUP) e condutas proibidas

O Cliente deve utilizar os Serviços de forma lícita, ética e compatível com boas práticas de internet e segurança.

É proibido: (i) envio de spam; (ii) phishing, fraude, roubo de credenciais; (iii) hospedagem/distribuição de malware; (iv) varredura e exploração de vulnerabilidades sem autorização; (v) ataques DoS/DDoS (origem, coordenação, amplificação); (vi) violação de direitos autorais e propriedade intelectual; (vii) qualquer atividade ilegal.

O Cliente é responsável por todo conteúdo, tráfego e operações executadas em sua VPS, inclusive ações de usuários finais, aplicações e integrações.



4. Segurança, rede e medidas de proteção

Para proteger a infraestrutura, a CMR Services poderá aplicar políticas de firewall, mitigação, rate-limit, filtragem e/ou blackhole para conter tráfego abusivo ou suspeito.

Em caso de incidente (ex.: comprometimento, abuso, ataque contínuo), a CMR poderá restringir portas, limitar recursos, suspender temporariamente a VPS e exigir correções antes da reativação.

O Cliente deve manter o sistema atualizado, credenciais seguras (preferencialmente com MFA onde aplicável), firewall na VPS e boas práticas de hardening.

5. Proteção de DDoS (Cloudflare) - melhor esforço e limitações

A CMR Services poderá disponibilizar **proteção anti-DDoS via Cloudflare** (ou tecnologia equivalente) conforme plano/contratação.

A mitigação é fornecida em regime de **melhor esforço**, pois ataques podem variar em volume, vetores e características. A CMR poderá ajustar regras, rotas e filtros para reduzir impacto global na rede.

Se o ataque for persistente, direcionado, ou gerar risco à rede/terceiros, podem ser aplicadas medidas como **blackhole temporário**, restrição de portas, ou suspensão preventiva até estabilização e/ou correção do serviço do Cliente.

6. Backups e responsabilidade por dados

O Cliente é integralmente responsável por manter backups de todos os dados e configurações, inclusive antes de mudanças, atualizações e migrações.

Backups opcionais ofertados pela CMR (quando existentes/contratados) são camada adicional e não substituem a obrigação do Cliente.

A CMR não garante recuperação de dados em casos de exclusão acidental, corrupção lógica, comprometimento, erro de configuração ou falhas em software do Cliente.

7. Suporte e atendimento

O suporte será prestado pelos canais oficiais e dentro do escopo do plano contratado.

Demandas fora do escopo (ex.: projetos, performance tuning, intervenções complexas) podem ser atendidas mediante orçamento e disponibilidade técnica.

8. Pagamentos, inadimplência e suspensão

Os valores e prazos de cobrança constam na proposta/contrato/plano contratado.

Em caso de inadimplência, a CMR poderá suspender os Serviços e restringir acesso até a regularização, além de aplicar encargos conforme acordado comercialmente.

A CMR pode condicionar reativação à quitação integral e/ou à mitigação comprovada de incidentes de segurança/abuso.



8.1. Política de Reembolso e Direito de Arrependimento

8.1.1. Direito de arrependimento (CDC - art. 49): quando a contratação ocorrer fora do estabelecimento comercial (ex.: compra online), o Cliente pessoa física poderá exercer o direito de arrependimento em até **7 (sete) dias corridos** a contar da confirmação da contratação ou do início da prestação do serviço, o que ocorrer primeiro, **desde que não tenha havido uso relevante/consumo do serviço** que descaracterize a reversibilidade da contratação.

8.1.2. Início imediato do serviço: por se tratar de serviço digital com provisionamento imediato (criação da VPS, alocação de IP, liberação de acesso, instalação/ativação de recursos), o Cliente reconhece que a execução pode começar imediatamente após a confirmação de pagamento. Havendo arrependimento dentro do prazo legal, a CMR Services poderá avaliar o nível de uso/consumo e **descontar valores proporcionais** quando houver utilização efetiva, custos não recuperáveis e/ou evidência de uso que inviabilize a devolução integral.

8.1.3. Reembolso fora do arrependimento: fora das hipóteses legais aplicáveis, **não há reembolso automático** de mensalidades já pagas. Eventuais créditos, abatimentos ou reembolsos serão analisados **caso a caso**, conforme o motivo e o histórico do Cliente.

8.1.4. Exclusões de reembolso: não haverá reembolso em casos de: (i) violação destes Termos/AUP, abuso, spam, ataques, uso ilegal; (ii) suspensão por incidente de segurança não mitigado; (iii) bloqueios/blackhole/filtragens aplicadas para proteção de rede devido a tráfego originado ou direcionado ao serviço do Cliente; (iv) falhas decorrentes de configuração, software, aplicação, credenciais, ou ações do próprio Cliente.

8.1.5. Procedimento: solicitações devem ser feitas pelo e-mail **financeiro@cmrservices.com.br**, informando CPF/CNPJ, identificação do serviço, data da contratação e motivo. A devolução, quando aprovada, ocorrerá pelo mesmo meio de pagamento, respeitando prazos operacionais de bancos/operadoras.

9. Suspensão e rescisão por violação

A CMR poderá suspender ou rescindir imediatamente em caso de: violação destes Termos/AUP, risco à infraestrutura, incidentes não tratados, exigência legal/autoridade competente ou inviabilidade técnica.

Em caso de rescisão, obrigações financeiras pendentes permanecem exigíveis.

10. Limitação de responsabilidade

A CMR não se responsabiliza por lucros cessantes, perda de receita, perda de dados, paralisação de atividades, falhas em software do Cliente, ou danos indiretos/incidentais.

O Cliente reconhece que serviços de hospedagem envolvem riscos inerentes (atualizações, falhas de terceiros, upstreams, ataques), e se compromete a manter plano de contingência e backups.



11. Privacidade e LGPD

Quando houver tratamento de dados pessoais, as partes se comprometem a cumprir a LGPD (Lei 13.709/2018).

O Cliente declara possuir base legal para tratar dados inseridos em suas aplicações e é responsável por seus avisos de privacidade, consentimentos e atendimento a titulares.

12. Alterações destes Termos

A CMR poderá atualizar estes Termos para refletir mudanças técnicas, legais ou operacionais. O uso contínuo após atualização implica aceitação.

13. Foro e legislação aplicável

Estes Termos são regidos pelas leis da República Federativa do Brasil.

Fica eleito o foro da comarca de **Itacaré/BA** para dirimir controvérsias, salvo disposição diversa em contrato específico.



ANEXO A - POLÍTICA TÉCNICA VPS (FAIR USE)

CPU e I/O: planos VPS são compartilhados. Uso contínuo e anormal (ex.: 100% CPU 24/7, IOPS excessivo) pode gerar limitação (throttling) para preservar estabilidade do nó.

Armazenamento: é vedado utilizar a VPS como “repositório de arquivos” para distribuição massiva, storage público não autorizado ou backup de terceiros sem contratação específica.

Tráfego e portas: tráfego abusivo, scan, brute force ou serviços que gerem reclamações podem ser bloqueados. Portas comumente associadas a abuso poderão ser filtradas.

E-mail: envio de e-mail em massa/SMTP não autorizado é proibido e pode resultar em bloqueio imediato de portas e/ou suspensão.

Se você tiver dúvidas sobre o escopo do seu plano, limites técnicos ou políticas antiabuso, entre em contato pelos canais oficiais.