OKLAWORKS® SERVIÇOS DE INFORMÁTICA

Caldas Novas e Morrinhos, Goiás

SEGURANÇA DA INFORMAÇÃO

OklaOS | versão de 04/11/2026

OklaOS 1.10.0 | versão dos documentos 2026-11-04-3

Caldas Novas, 2026

OKLAWORKS® SERVIÇOS DE INFORMÁTICA

SEGURANÇA DA INFORMAÇÃO

OklaOS | versão de 04/11/2026

Documento jurídico publicado pelo controlador do sistema, conforme a versão vigente em 04/11/2026. Texto idêntico ao exibido na página legal.php.

Caldas Novas

2026

RESUMO

Este documento reúne as regras de uso e as informações de privacidade e proteção de dados pessoais do OklaOS, nos termos da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e do Marco Civil da Internet (Lei nº 12.965/2014): direitos e deveres do usuário, finalidades e bases legais do tratamento, compartilhamentos, cookies, medidas de segurança, resposta a incidentes, prazos de retenção e meios de exercer os direitos do titular.

Palavras-chave: LGPD; termos de uso; privacidade; proteção de dados; segurança da informação

SUMÁRIO

1 SEGURANÇA DA INFORMAÇÃO 5

1 SEGURANÇA DA INFORMAÇÃO

Medidas técnicas e administrativas adotadas, nos termos do art. 46 da LGPD:

• Senhas armazenadas com hash forte e salgado, nunca em texto aberto, com política de senha forte e verificação em duas etapas opcional (TOTP) com códigos de recuperação. Reautenticação exigida em operações administrativas sensíveis.

• Criptografia AES-256 com autenticação para dados sensíveis em repouso (cookies de sites do OklaWeb e segredos de 2FA) e HTTPS com HSTS nas conexões.

• Aviso na conta quando há acesso a partir de um novo endereço IP.

• Sessões por cookie HttpOnly e SameSite, token anti-CSRF em toda ação de escrita e encerramento remoto de sessões.

• Limite de tentativas de login, cadastro, 2FA e contato por endereço IP.

• Isolamento total entre contas: cada usuário acessa somente os próprios dados, com cotas de armazenamento definidas por perfil.

• Pastas de dados protegidas contra acesso direto pela internet, com teste de exposição no Okla Update.

• Auditoria de ações administrativas, de aceites dos termos, de exportações de dados e de acessos a redes internas.

• Guardian Live: captura persistente de erros, falhas e eventos de segurança, com autoteste e relatórios.

• OklaWeb em quadro isolado, sem acesso à sessão do Sistema, com bloqueio de endereços de metadados de nuvem, validação de redirecionamentos e política de rede controlada pelo administrador.

• Rotinas de limpeza e verificação de integridade do banco pelo Agente Guardião e pelo Okla Update.

• Cópias de segurança feitas pelo administrador e chave de criptografia que pode ser guardada em arquivo selado por senha, separada do backup do banco.

Sua parte

Use senhas longas e únicas, não compartilhe a conta, encerre sessões em computadores de terceiros e avise o administrador sobre qualquer suspeita. Para relatar uma vulnerabilidade, escreva para os canais de contato informados na página inicial ou o administrador do sistema sem divulgar o problema publicamente antes da correção.