PAYNOTAS · DOCUMENTO JURÍDICO

Política Pública de Segurança da Informação

Versão 1.1 · 17/11/2026

1. Objetivo

Esta Política apresenta os princípios de segurança que o PayNotas adota para proteger dados, credenciais, certificados digitais e notas fiscais, sem revelar detalhes técnicos que possam facilitar um ataque.

2. Princípios

A segurança do PayNotas segue confidencialidade, integridade, disponibilidade, rastreabilidade, menor privilégio, defesa em camadas, mínimo de dados necessário e resposta proporcional ao risco.

3. Medidas adotadas

- conexão cifrada em todo o site, painel e aplicativo
- senha guardada só como resumo criptográfico resistente a ataque, nunca a senha em si
- cookie de acesso protegido, válido por 12 horas e invisível para scripts da página
- código de verificação adicional na entrada, quando disponível para a conta
- certificado digital e segredos guardados cifrados
- dados de cada empresa separados, com emissão presa ao CNPJ do certificado da própria empresa
- ambientes de desenvolvimento e de produção separados
- acesso administrativo aos servidores restrito e somente por rede privada cifrada
- travas contra tentativas repetidas de acesso e contra automação abusiva
- registros de auditoria das operações
- correção de falhas e atualização de componentes
- cópias de segurança cifradas, frequentes e guardadas em local separado, com ensaio de restauração
- procedimento de resposta a incidentes
- escolha e acompanhamento de fornecedores

4. Certificado digital e dados fiscais

O certificado digital é importado pelo TITULAR no fluxo do PayNotas criado para isso, guardado cifrado e usado só para assinar e transmitir as notas pedidas pelo CLIENTE.

O CLIENTE nunca deve enviar certificado, senha ou código por e-mail, mensagem ou atendimento. O PayNotas nunca pede essas informações por esses canais.

5. Cuidados do CLIENTE

O CLIENTE deve:

- usar senha forte e exclusiva
- ativar o código de verificação adicional quando disponível
- não compartilhar o acesso da conta
- proteger os aparelhos e as redes que usa
- manter o certificado digital válido e guardado com cuidado
- avisar o PayNotas na hora se suspeitar de acesso indevido

6. Desenvolvimento e mudanças

Mudanças relevantes no software passam por revisão, testes automáticos e implantação controlada, com volta automática à versão anterior em caso de falha. Correções críticas de segurança podem ser implantadas em caráter emergencial.

7. Relato de vulnerabilidades

Relatos de falha de segurança devem ser enviados para contato@paynotas.com.br. É proibido explorar falhas de forma destrutiva, acessar dados de terceiros, manter acesso, copiar dados, interromper o serviço ou divulgar a falha antes de um prazo razoável de correção.

8. Incidentes

O PayNotas mantém procedimento para identificar, conter, investigar, recuperar e comunicar incidentes. Clientes, titulares e autoridades são avisados quando a lei exigir ou quando o aviso for necessário para reduzir o risco. Quando o PayNotas for operador, o CLIENTE será avisado em até 24 (vinte e quatro) horas depois da confirmação interna do incidente, como meta, sempre que tecnicamente possível.

9. Continuidade

O PayNotas mantém cópias de segurança e procedimentos de restauração compatíveis com os objetivos internos de recuperação. Prazos de recuperação ou garantias específicas só valem quando constarem da oferta ou do contrato.

10. Atualizações

Esta Política pode ser atualizada conforme mudanças de risco, arquitetura ou legislação.