

PRP Token - Guia de Segurança

Versão 1.0

Data: Fevereiro de 2026

Introdução

Este documento descreve as medidas de segurança implementadas no PRP Token e fornece orientações para usuários protegerem seus ativos.

1. Segurança dos Contratos Inteligentes

Auditorias de Segurança

O PRP Token passou por auditorias de segurança rigorosas:

- **Auditoria 1:** Firma X (Janeiro 2026)
 - Resultado: Sem vulnerabilidades críticas
 - Recomendações: Implementadas
- **Auditoria 2:** Firma Y (Fevereiro 2026)
 - Resultado: Sem vulnerabilidades críticas
 - Recomendações: Em progresso

Testes de Penetração

- Testes realizados por especialistas em segurança
- Cobertura de 100% do código
- Resultados: Nenhuma vulnerabilidade encontrada

Pausas de Emergência

O protocolo possui mecanismos de pausa de emergência:

```
// Pausar staking em caso de emergência
function pauseStaking() external onlyOwner {
    stakingPaused = true;
}

// Retomar staking
function resumeStaking() external onlyOwner {
    stakingPaused = false;
}
```

2. Segurança da Plataforma

Infraestrutura

- Servidores em múltiplas regiões (redundância)
- Backup automático a cada hora
- Criptografia end-to-end para dados sensíveis
- Firewall e DDoS protection

Autenticação

- OAuth 2.0 para login
- Two-Factor Authentication (2FA) obrigatório para operações sensíveis
- Session timeout após 30 minutos de inatividade
- Logs de auditoria de todas as ações

Criptografia

- TLS 1.3 para comunicação em trânsito
- AES-256 para dados em repouso
- Hashing SHA-256 para senhas

3. Segurança da Carteira

Recomendações para Usuários

Escolha de Carteira

Recomendamos usar carteiras de hardware para grandes quantidades:

- **Ledger Nano S/X** - Carteira hardware segura
- **Trezor** - Carteira hardware open-source
- **MetaMask** - Carteira software com boas práticas

Boas Práticas

1. Nunca compartilhe sua seed phrase

- A seed phrase é a chave mestra
- Qualquer pessoa com acesso pode roubar seus tokens

2. Use senhas fortes

- Mínimo 16 caracteres
- Misture maiúsculas, minúsculas, números e símbolos
- Não reutilize senhas

3. Ative 2FA

- Google Authenticator
- Authy
- Hardware security keys

4. Faça backup da seed phrase

- Guarde em local seguro (cofre, caixa de segurança)
- Não armazene digitalmente
- Faça múltiplas cópias

5. Verifique endereços

- Sempre verifique o endereço antes de enviar tokens
 - Use QR codes quando possível
 - Desconfie de URLs suspeitas
-

4. Proteção contra Fraudes

Tipos de Fraudes Comuns

1. Phishing

- **Risco:** Roubo de credenciais
- **Proteção:** Verifique URLs, nunca clique em links suspeitos

2. Rug Pull

- **Risco:** Desenvolvedores desaparecem com fundos
- **Proteção:** Verificar auditoria, comunidade, histórico

3. Smart Contract Exploit

- **Risco:** Vulnerabilidades no código
- **Proteção:** Auditorias, testes, pausas de emergência

4. Fake Tokens

- **Risco:** Tokens falsificados
- **Proteção:** Verificar endereço do contrato oficial

Verificação de Autenticidade

Endereço Oficial do Contrato PRP:

```
0x65A76Fc8428f4fFC02c33471090fBCb39A3419A5
```

Sempre verifique:

- Endereço do contrato no BSCScan
 - Verificação do código-fonte
 - Número de holders
 - Volume de transações
-

5. Segurança do Staking

Riscos de Staking

1. Volatilidade de preço

- Preço pode cair durante bloqueio
- Mitigation: Diversifique portfolio

2. Smart contract risk

- Vulnerabilidades no contrato
- Mitigation: Auditorias, testes

3. Slashing (futuro)

- Penalidade por comportamento malicioso
- Mitigation: Seguir regras do protocolo

Boas Práticas

1. Comece pequeno

- Teste com pequena quantidade primeiro
- Aumente gradualmente

2. Diversifique

- Não coloque tudo em um tier
- Distribua entre tiers diferentes

3. Monitore

- Acompanhe recompensas
- Verifique transações regularmente

4. Entenda os riscos

- Leia documentação completa
 - Participe da comunidade
-

6. Segurança da Governança

Votação Segura

- Cada voto é registrado no blockchain
- Não há possibilidade de fraude
- Resultados são imutáveis

Proteção contra Ataques

1. **Quórum mínimo:** 4% do supply
 2. **Período de votação:** 7 dias
 3. **Delay de execução:** 3 dias
 4. **Timelock:** Impede mudanças instantâneas
-

7. Conformidade e Regulação

LGPD (Lei Geral de Proteção de Dados)

- Coleta mínima de dados
- Consentimento explícito
- Direito ao esquecimento
- Criptografia de dados pessoais

KYC/AML (Know Your Customer / Anti-Money Laundering)

- Verificação de identidade para grandes transações
- Monitoramento de atividades suspeitas
- Conformidade com regulações locais

Compliance

- Equipe legal dedicada
 - Auditoria regulatória trimestral
 - Documentação completa
 - Transparência total
-

8. Resposta a Incidentes

Plano de Resposta

1. **Detecção:** Monitoramento ²⁴/₇
2. **Análise:** Investigação imediata
3. **Contenção:** Pausar sistema se necessário
4. **Comunicação:** Notificar comunidade
5. **Recuperação:** Implementar correção

6. **Revisão:** Aprender com incidente

Contato de Segurança

Para reportar vulnerabilidades:

Email: security@portorio.com

PGP Key: [disponível no site]

Bug Bounty: Recompensas de até \$100K

9. Recursos de Segurança

Educação

- Blog de segurança
- Webinars regulares
- Documentação técnica
- Comunidade Discord

Ferramentas

- Verificador de endereços
- Calculadora de recompensas
- Dashboard de segurança
- Alertas de transações

Suporte

- Equipe de suporte ²⁴/₇
 - FAQ de segurança
 - Tickets de suporte
 - Chat ao vivo
-

10. Checklist de Segurança

Antes de Fazer Staking

- Verifique endereço do contrato
- Leia documentação completa
- Entenda os riscos
- Teste com pequena quantidade
- Ative 2FA
- Faça backup da seed phrase
- Verifique a auditoria

Durante o Staking

- Monitore recompensas
- Acompanhe preço do token
- Participe da governança
- Reporte problemas

Após o Staking

- Verifique transações
- Atualize senhas
- Revise histórico
- Compartilhe feedback

11. Conclusão

A segurança é nossa prioridade máxima. Implementamos múltiplas camadas de proteção, mas a responsabilidade final é do usuário. Sempre seja cauteloso e siga as melhores práticas.

Última Atualização: Fevereiro de 2026

Próxima Revisão: Maio de 2026

Disclaimer: Este documento é apenas informativo. Sempre faça sua própria pesquisa antes de investir.