

## — CRIPTOGRAFIA E HSM

# A chave que protege seus dados nunca deveria estar em um arquivo.



Custódia de chaves em hardware certificado, do data center ao campo, com algoritmos pós-quânticos já validados.

## O DESAFIO

Criptografia forte perde valor quando a chave fica em software, no mesmo servidor da aplicação. Quem acessa o servidor acessa a chave.

Dados com vida longa enfrentam um segundo risco: material cifrado hoje pode ser guardado e decifrado no futuro por computação quântica.

### kNET

HSM de rede. Chaves geradas, usadas e guardadas dentro do equipamento, sem nunca saírem dele.

### KeyGuardian

Custódia portátil de chaves e proteção de credenciais para operações fora do data center.

### Pronto para o pós-quântico

O kNET executa algoritmos pós-quânticos validados pelo NIST CAVP, o que permite planejar a migração sobre a mesma base certificada.

## ONDE SE APLICA

### PKI e assinatura

Certificação digital ICP-Brasil e eIDAS

### Dados e aplicações

Chaves de bancos de dados, backups e APIs

### Cerimônias de chaves

Geração e custódia com controle de quórum

### Transição PQC

Migração por criticidade e vida útil do dado

## CERTIFICAÇÕES DO KNET



FIPS 140-3 L3



CC EAL4+



NIST CAVP PQC



ICP-Brasil



Inmetro



NCC 26.12596

**Projetos decididos até 30 de novembro entram no ciclo de implantação de 2026.**

Fale com o seu executivo de contas Kryptus ou acesse [kryptus.com](https://kryptus.com)

Material da série  
**Anatomia de uma violação**