



TAURUS

Gestão de **Ativos Digitais** com Nível Bancário para Bancos Brasileiros

Hot e Cold Wallets da Taurus com HSMs da DINAMO Networks



Préfacio

Plataforma de Custódia Hot e Cold da Taurus com HSMs da DINAMO Networks

Saiba como a Taurus e a DINAMO Networks oferecem uma solução abrangente de custódia de ativos digitais com padrão bancário, voltada a casos de uso críticos.

A Taurus fornece infraestrutura corporativa para custódia de ativos digitais, tokenização e gestão do ciclo de vida de ativos, utilizada por instituições financeiras reguladas em todo o mundo.

Os HSMs da DINAMO Networks são amplamente implementados no setor financeiro brasileiro, inclusive para proteger o PIX, a infraestrutura de pagamentos instantâneos do Brasil.

Ao integrar diretamente os HSMs da DINAMO Networks à plataforma de custódia da Taurus, os bancos operam a custódia de ativos digitais com um modelo de confiança enraizado em hardware, alinhado às arquiteturas de segurança já existentes no sistema bancário.

Seja implantado on-premises, em ambientes híbridos ou em modelo SaaS, e operado em configurações hot ou cold, os clientes contam com o Taurus-PROTECT, construído sobre os HSMs DINAMO Networks certificados FIPS 140-2/3 Nível 3.

Elementos-chave do Nosso Modelo de Segurança Baseado em Hardware

Cada controle de segurança abaixo aborda uma limitação dos sistemas de custódia baseados exclusivamente em software.



Gestão de chaves controlada pelo cliente

HSMs implantados on-premises ou em data-centers gerenciados pela Taurus / Dinamo.

Os clientes mantêm o controle das chaves e dos backups.

Taurus ou Dinamo nunca têm acesso às chaves privadas nem a qualquer fração delas.



As chaves nunca deixam os HSMs

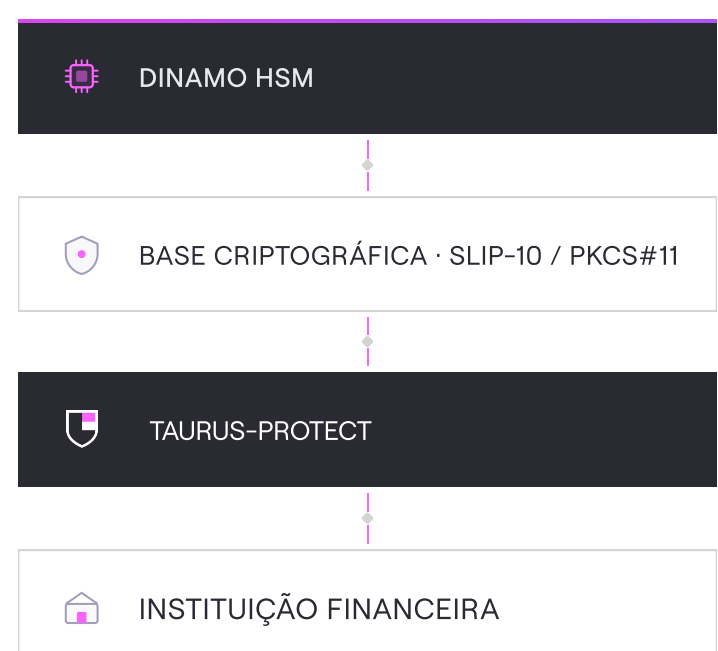
Chaves privadas são geradas, armazenadas e utilizadas exclusivamente dentro do HSM DINAMO, sem possibilidade de exposição ou exportação. A derivação SLIP-10 ocorre sob demanda no próprio HSM, com eliminação segura de materiais intermediários. Controles PKCS#11 garantem inexportabilidade, uso restrito e conformidade com padrões de segurança, reduzindo riscos e superfície de ataque.

O Jeito Taurus: Segurança Incomparável

A Taurus utiliza os HSMs da DINAMO Networks como raiz de confiança em hardware e base criptográfica.

As chaves privadas para assinatura de transações são utilizadas exclusivamente dentro dos HSMs e nunca são expostas a servidores, estações de trabalho ou dispositivos móveis.

O Taurus-PROTECT, integrado aos HSMs da DINAMO Networks, pode ser implantado em ambientes hot, warm e cold (air-gapped).



Implantação: **Hot, Cold e Air-Gapped**

As instituições operam diferentes modelos de custódia de acordo com seu perfil de risco. Os controles de segurança devem permanecer consistentes em todos eles.



Hot wallets

Assinatura automatizada de transações com aplicação de políticas dentro do HSM, garantindo eficiência operacional



Cold wallets

Fluxos de aprovação com participação humana para transações de alto valor.



Modo air-gapped

Implantação fisicamente isolada do HSM, com transferência de dados de transação por meio de canais offline seguros, eliminando completamente a superfície de ataque em rede.

Todos os modos **utilizam a mesma arquitetura baseada em HSM**, com controles de segurança aplicados no limite do hardware, independentemente do nível de exposição da wallet.

Desenvolvido para as Expectativas de Segurança e Regulação do Brasil

Os HSMs da DINAMO Networks já protegem infraestruturas financeiras críticas em todo o Brasil.

Ao utilizar essa base de segurança já estabelecida, a Taurus oferece uma solução de custódia que se integra naturalmente às estruturas de segurança existentes dos bancos brasileiros.

As instituições se beneficiam de:

- ✓ Governança robusta de chaves criptográficas.
- ✓ Clara segregação de funções.
- ✓ Alto nível de auditabilidade e controle.
- ✓ Alinhamento com requisitos brasileiros de segurança e proteção de dados.
- ✓ Expertise em ativos digitais da Taurus, com mais de 40 bancos, incluindo alguns dos maiores do mundo (State Street, Deutsche Bank, Credit Agricole).
- ✓ Expertise em segurança e hardware da DINAMO, backbone de segurança utilizado pelo PIX, a infraestrutura de pagamentos instantâneos do Brasil, com ampla adoção também no SPB e em projetos de custódia digital nos principais bancos do país.

Casos de Uso: Da Custódia à Tokenização

O modelo de validação baseado em HSM permite diversos casos de uso, mantendo controles de segurança consistentes:



Custódia de criptomoedas

Suporte multi-chain (redes blockchain diversas) com chaves-mestre por cadeia e derivação sob demanda. Escala para milhões de endereços sem preocupações com armazenamento de chaves.



Staking seguro

Ampla variedade de protocolos de staking disponíveis, com políticas de conformidade flexíveis. Os clientes podem utilizar provedores de staking selecionados pela Taurus ou qualquer provedor terceirizado.



Instrumentos financeiros tokenizados e RWAs

Políticas de transação granulares até o nível de smart contract, suportando fluxos complexos como liquidação definitiva, bloqueios regulatórios, restrições de transferência e eventos corporativos, todos aplicados criptograficamente, e não por lógica de software.



Operações com stablecoins (custódia e emissão)

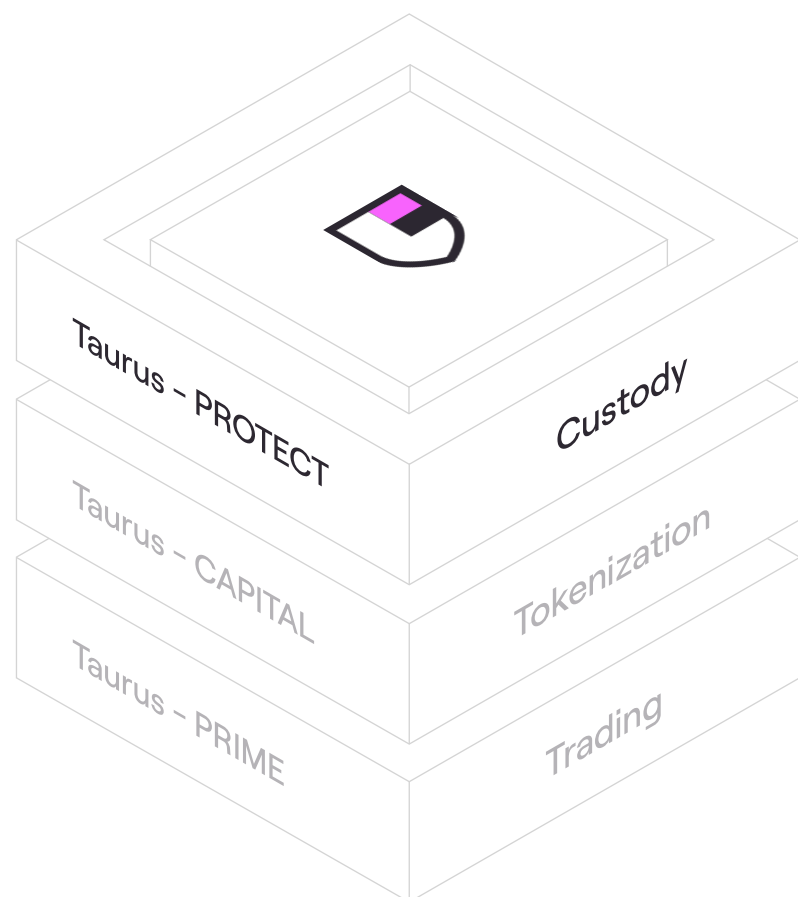
Emissores exigem tanto segurança de custódia (proteção das reservas) quanto controles de emissão (autorização de mint/burn). Políticas de transação granulares até o nível de função do smart contract garantem que as operações de emissão cumpram autorizações multipartite verificadas criptograficamente, sem depender de camadas de orquestração de software.

Esse design suporta implantações hot, cold e air-gapped. Escala entre blockchains. Permite custódia, tokenização e emissão de stablecoins sob um único modelo de segurança. Para instituições reguladas, o resultado é claro. As operações com ativos digitais funcionam com controles de segurança equivalentes aos padrões já existentes no sistema bancário.

DINAMO HSMs

O HSM DINAMO é a base da confiança digital em ambientes críticos, garantindo proteção criptográfica de alto desempenho, rastreabilidade e controle rigoroso de acessos a chaves e certificados. Com gestão centralizada via APIs, arquitetura inviolável, divisão de responsabilidades (split knowledge) e capacidade superior a 23 mil operações por segundo, entrega alta disponibilidade com geo-redundância e backup estruturado.

Certificado pelos principais padrões internacionais como FIPS 140-2, ISO 9001, PCI DSS e alinhado a NIST, ICP-Brasil e Inmetro, o HSM DINAMO assegura segurança, compliance e continuidade para instituições financeiras, governo e grandes empresas.



Sobre a Taurus SA

Fundada em 2018, a Taurus é uma empresa suíça de tecnologia financeira que oferece infraestrutura de ativos digitais em nível empresarial, com 13 escritórios ao redor do mundo.

A empresa disponibiliza serviços para emissão, custódia e negociação de todos os tipos de ativos digitais, incluindo criptomoedas, ativos tokenizados e stablecoins.

Além disso, a Taurus opera um marketplace para ativos privados e valores mobiliários tokenizados e é uma instituição financeira regulada e supervisionada pela Autoridade Supervisora do Mercado Financeiro Suíço (FINMA).

Para mais informações, acesse [WWW.TAURUSHQ.COM](https://www.taurushq.com)

Sobre a DINAMO Networks

A DINAMO Networks é referência em segurança digital, criptografia e identidade digital no Brasil, com mais de 20 anos de atuação no desenvolvimento de soluções para proteção de dados, identidades e transações críticas. Especialista em HSMs, gestão de chaves e autenticação segura, a empresa possui tecnologia própria, certificações internacionais como FIPS 140-2 e ISO 9001, e presença em projetos estratégicos do ecossistema financeiro, incluindo o PIX e o Sistema de Pagamentos Brasileiro (SPB).

A DINAMO atua no núcleo da confiança digital, garantindo sigilo, integridade, autenticidade e soberania para organizações que operam em ambientes de alta criticidade.