2025 WTR WORKSHOP TECNOLOGIAS DE REDE PoPRN

RPKI – UMA INFRAESTRUTURA PARA SEGURANÇA EM ROTEAMENTO

Wanderson Modesto

WTR PoP-RN, Natal, RN | 22/08/25

RNP

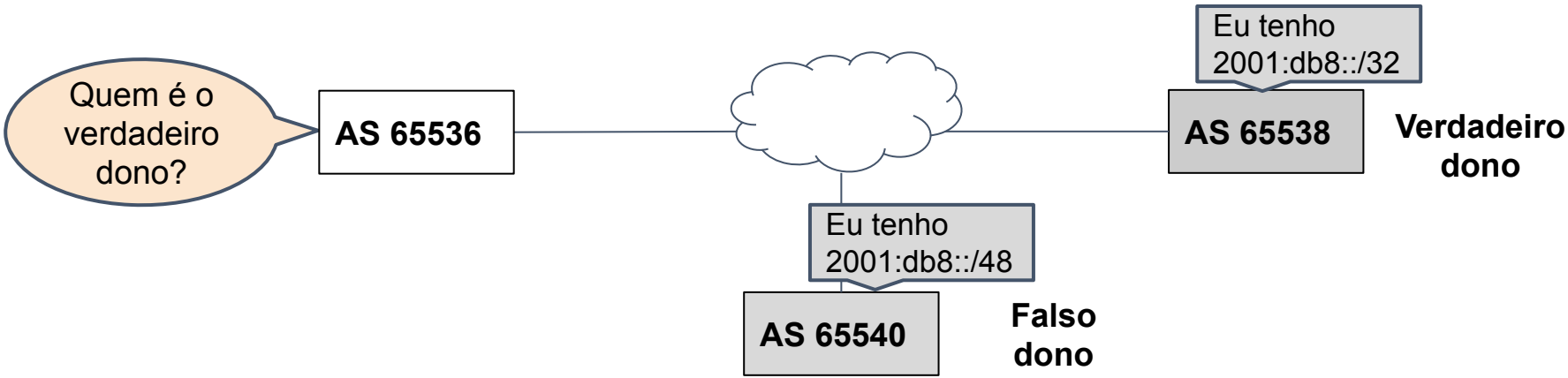
O que é RPKI?

- Estrutura desenvolvida para validar recursos de numeração
  - ASN e Prefixos IPs
    - Alocados
  - Utilizado no BGP

ROTAS:

2001:db8::/32 ... 65538 i

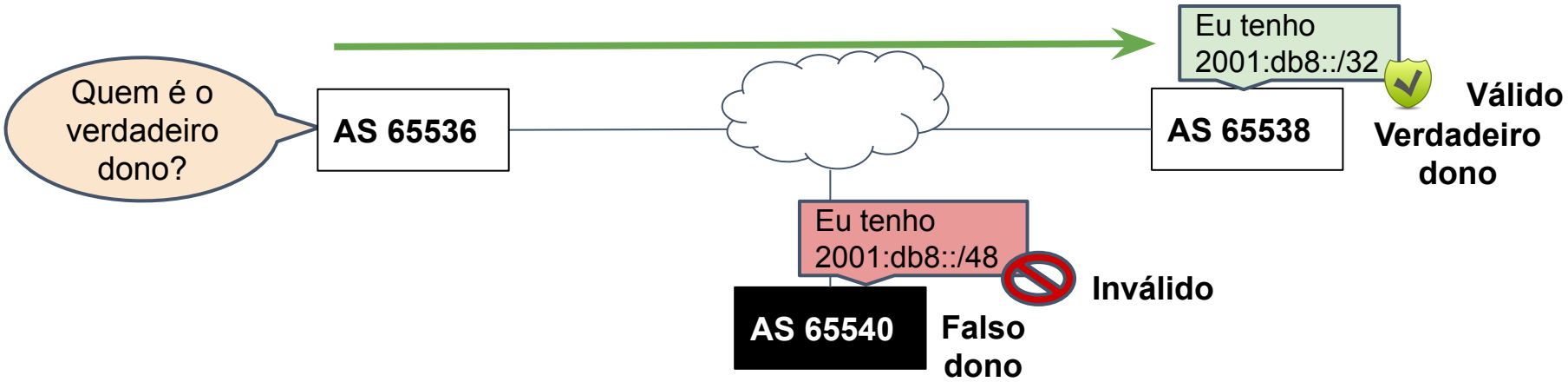
2001:db8::/48 ... 65540 i



ROTAS:

2001:db8::/32 ... 65538 i

2001:db8::/48 ... 65540 i



- Anúncio de prefixos não autorizados
  - "Sequestro do prefixo"

- Motivos:
  - Erro de configuração
  - Fat finger
  - Propositalㅤ

Por que isso acontece?

- A Internet funciona com base na cooperação entre Sistemas Autônomos (ASes):
- É uma *“rede de redes”;*
- São mais de **100.000** redes diferentes, sob gestões técnicas independentes;
- A estrutura de **roteamento BGP** funciona com base em cooperação e confiança;
- O BGP **não** tem validação dos dados.

Como resolver esses problemas???

MANRS

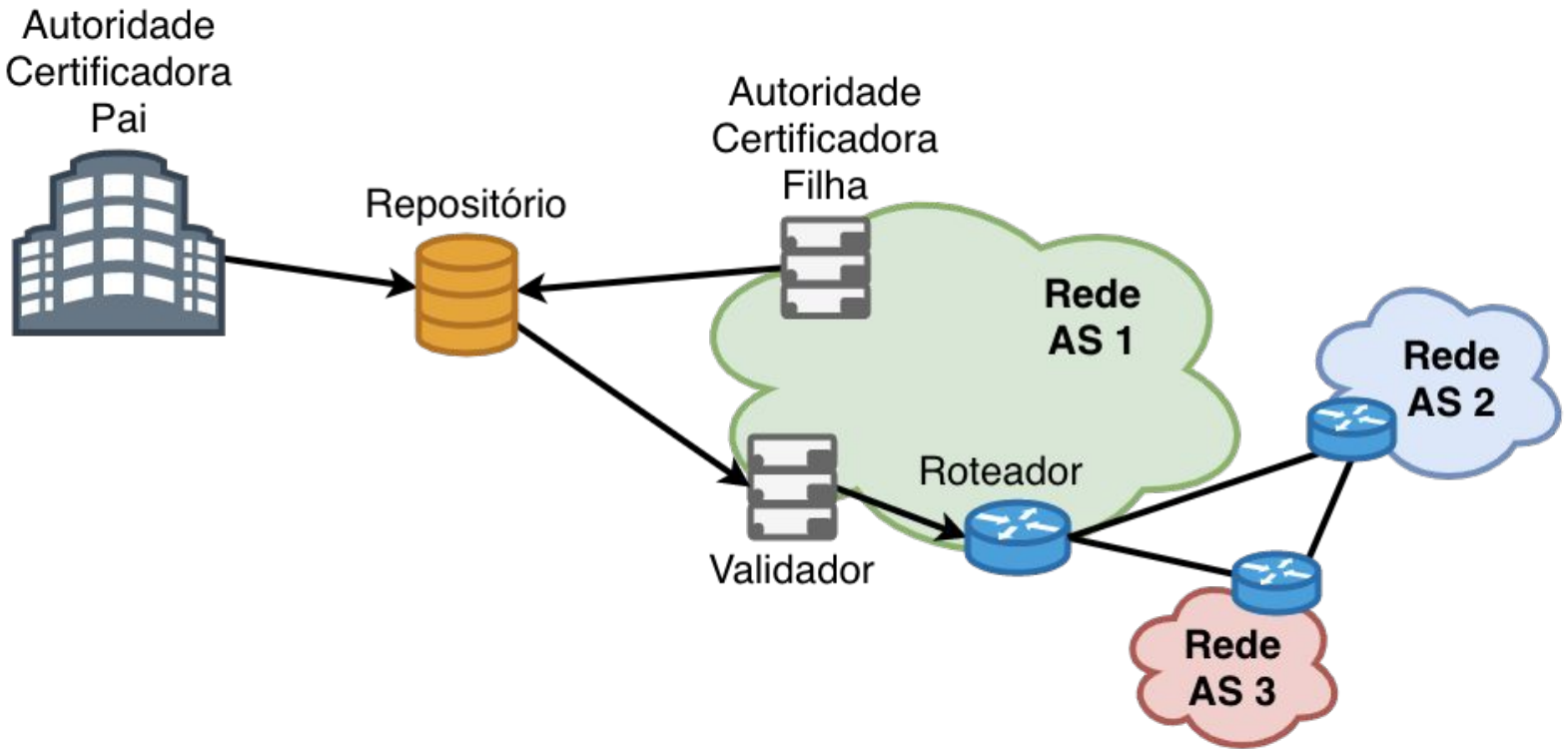
Resource Public Key Infrastructure (RPKI) faz parte do  MANRS!!!

O que é RPKI?

- Previne os problemas de BGP Hijacking
- A colaboração de todos os ASes é essencial!!!

MANRS

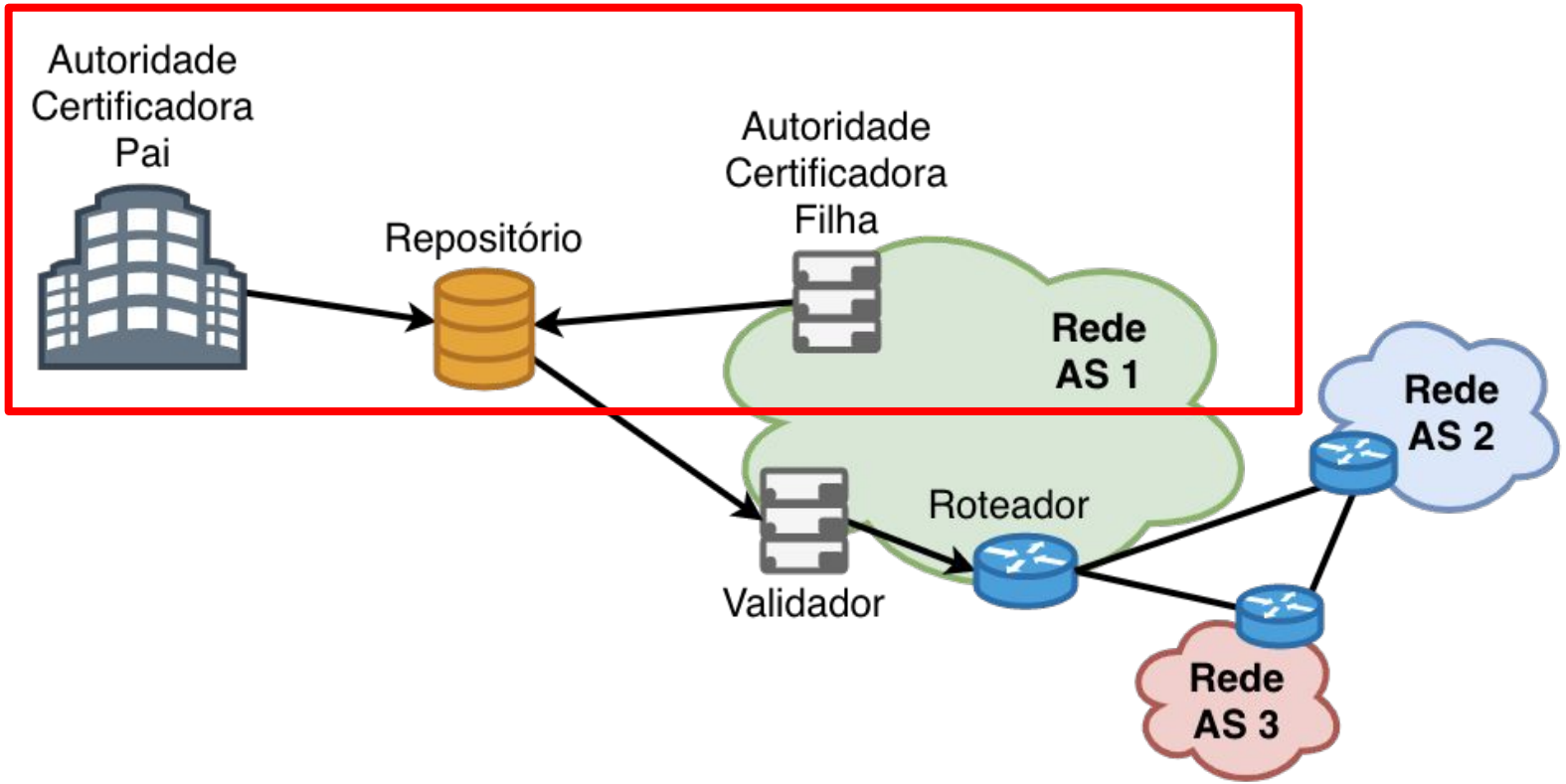
Estrutura do RPKI



Estrutura do RPKI

- Duas partes:
  - **Certificação de recursos**
    - Anunciar os prefixos no RPKI
    - Qualquer um que possuir recursos de IP pode aderir
  - **Validação da Origem**
    - Consultar prefixos anunciados no RPKI
    - Necessita uso de roteador compatível

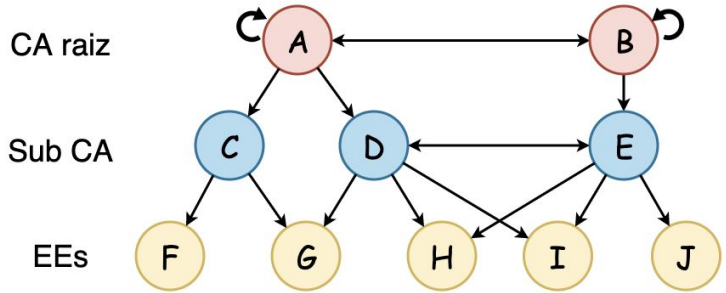
Certificação de Recursos



Certificação de Recursos

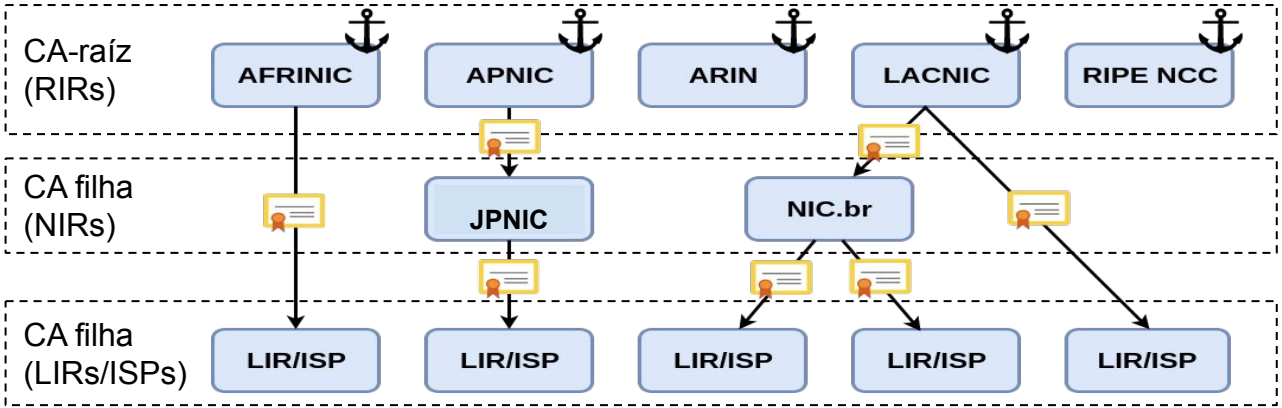
- Certificação digital
  - Associa a chave pública com o seu dono
- Modelo PKI (Public Key Infrastructure)
  - Certificado contém chave pública assinada por uma Autoridade Certificadora ou Certificate Authority (CA).
  - Ex.: ICP-Brasil
- RPKI
  - Certificação de recursos
  - Associa a chave pública com os recursos

- Cadeias de certificação
  - CA (Certificate Authority) são entidades confiáveis e sua chaves públicas são amplamente conhecidas!
  - Usa-se a chave da CA raiz (auto-assinado) para assinar outras chaves na cadeia até as entidades finais ou End Entities (EEs).
  - Importante a proteção das chaves mais críticas (mais próximas da raiz).



Cadeia de certificação do RPKI

- RIRs -Trust Anchor
  - Confiabilidade implícita
  - Certificados auto-assinados
  - Certificam somente os recursos de sua própria hierarquia



Autoridade Certificadora

- CAs Certificate
  - Organizações que distribuem recursos de numeração
  - Detentores de recursos de numeração
- Certificados das End Entities
  - Validam os documentos assinados contidos no repositório RPKI
  - Cada certificado assina um documento

Cadeia de certificação do RPKI

- Cada RIR pode ser uma fonte autoritativa para a alocação de recursos:
  - Delegação de endereços IPs (IPv4 e IPv6)
  - Delegação de ASNs

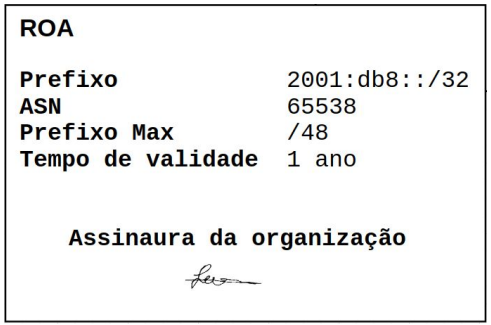
- Funcionam como CA do par IPs-ASN e da chave pública do AS

ROAs

- Route Origin Authorisation
  - Objeto assinado

  “Eu autorizo o ASN XXXX a originar esse prefixo”.

- Elementos principais:
  - Nome da ROA
  - Número do AS (ASN)
  - Prefixo alocado e máximo permitido
  - Tempo de validade
  - Assinatura da organização
  - Responsável pelos recursos



- Todos os prefixos anunciados devem estar cadastrados em um ou mais ROAs
- Assinados e guardados em um repositório RPKI
  - Certificado contendo recursos de numeração
  - Declarações da origem das rotas para esses recursos
- Cada ROA contém apenas um ASN
  - Prefixos podem possuir mais de um ROA

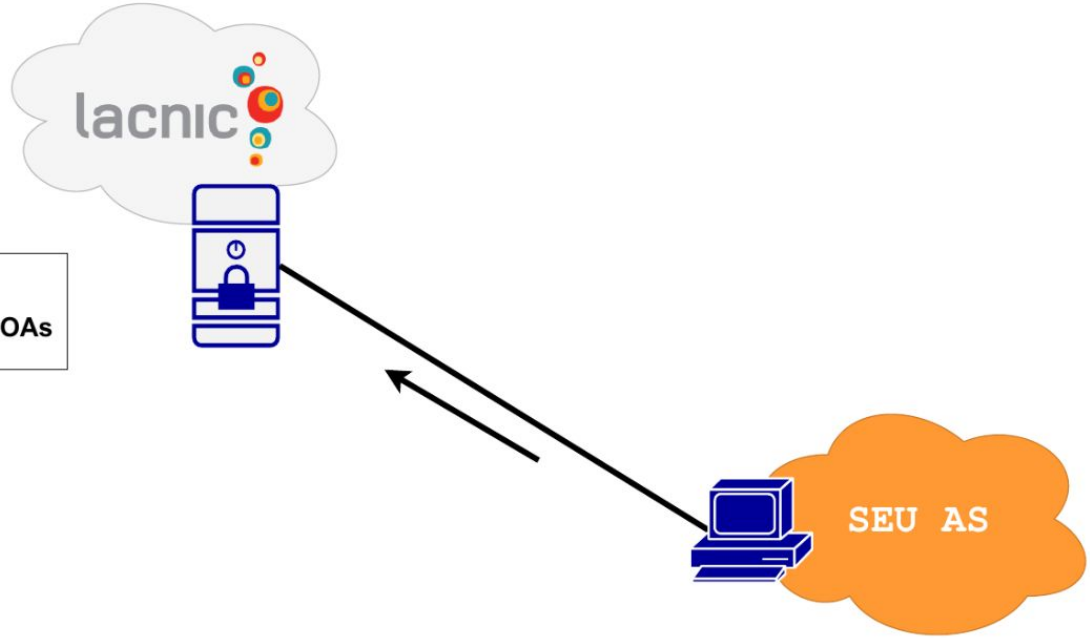
- E se uma organização quiser alocar seus recursos para outros ASes?
- **Duas opções:**
  1. Gerar a ROA para os próprios anúncios do seu ASN
  2. Gerar um certificado CA para outra organização (e.g. AS cliente), então essa gera a própria ROA
- Se existir ROA para o prefixo, a origem da rota é validada
- Publicar ROA incorreta é pior do que não publicar!

Modos de operação no RPKI

- Existem dois modos de operação no RPKI:
  - **Modo hospedado**
    - LACNIC
  - **Modo delegado**
    - NIC.br

Modo Hospedado

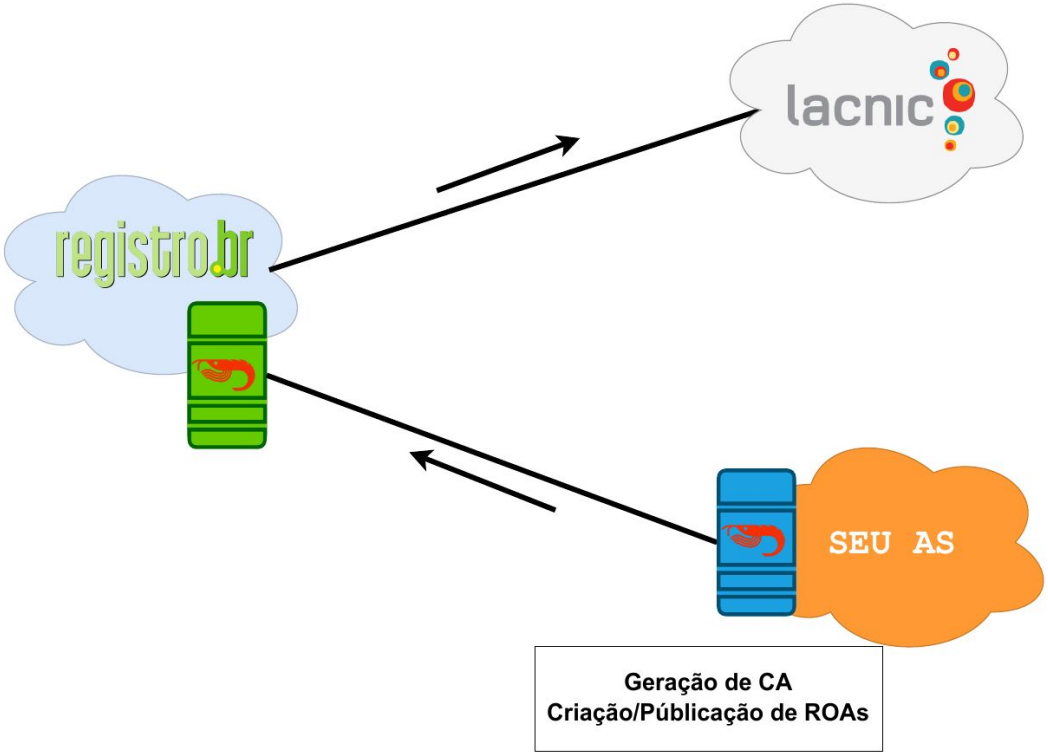
Geração de CA
Criação/Públicação de ROAs



Modo Hospedado

- Incentivar a adoção do RPKI
- **RIRs:**
  - Emitem e armazenam os certificados de recursos
  - Armazenam as chaves públicas e privadas
  - Oferecem interface web para os participantes
- AS depende do RIR para realizar suas ações no RPKI

Modo Delegado



Modo Delegado

- Sistema distribuído de CAs
  - Foi desenhado para ser assim
- Facilita a automatização
- Centraliza o gerenciamento das ROAs na organização dona dos recursos
- Controle da chave privada pelo AS
- Permite delegar CAs filhos para clientes
- AS têm mais autonomia no RPKI

- Protocolo UpDown
  - Geração e validação do repositório
  - Cada CA armazena a própria chave privada
  - Envia seus certificados para assinatura da CA pai
  - Publicação de certificados e ROAs
    - Repositório próprio ou de terceiros

- O que eu preciso?
  - **Software CA**
    - Krill - NLnet Labs
  - **Servidor de publicação**
    - Servidor proprio (alta disponibilidade)
    - Servidor de terceiros (NIC.br)

O que é o Krill ?

- Software open source
  - Criação, gerenciamento, publicação de CAs e ROAs
- Possui repositório próprio, mas permite a utilização de repositório de terceiros
- Funciona por linha de comando e por interface gráfica para usuário

Krill

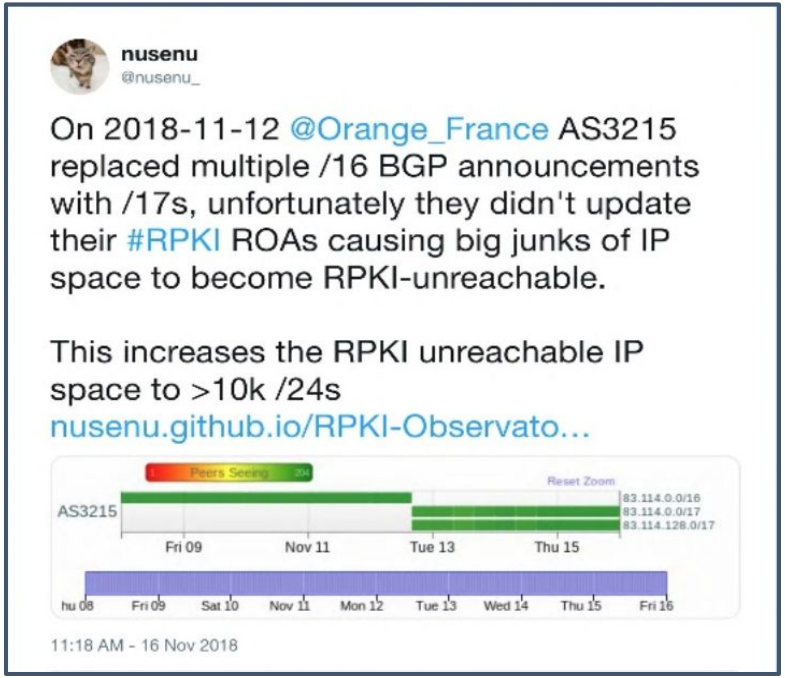
- **É de extrema importância manter seu servidor Krill sempre ativo!**
  - Documentos do RPKI possuem prazo de validade
  - Atualizações automáticas e periódicas desses documentos são feitas pelo protocolo UpDown
  - Se o servidor Krill ficar inacessível e os documentos expirarem, as rotas válidas podem passar a ser consideradas desconhecidas

Krill

Manutenção é essencial!

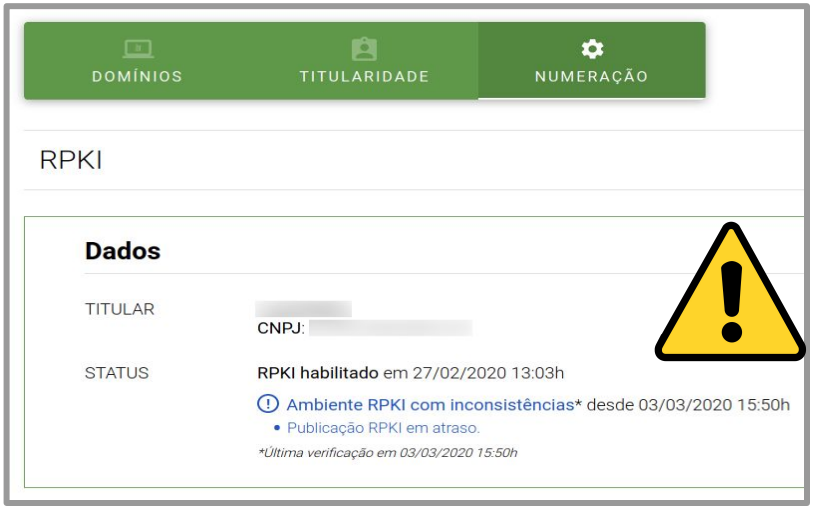
Não esqueça do RPKI!

Atualize as ROAs quando mudar os anúncios!

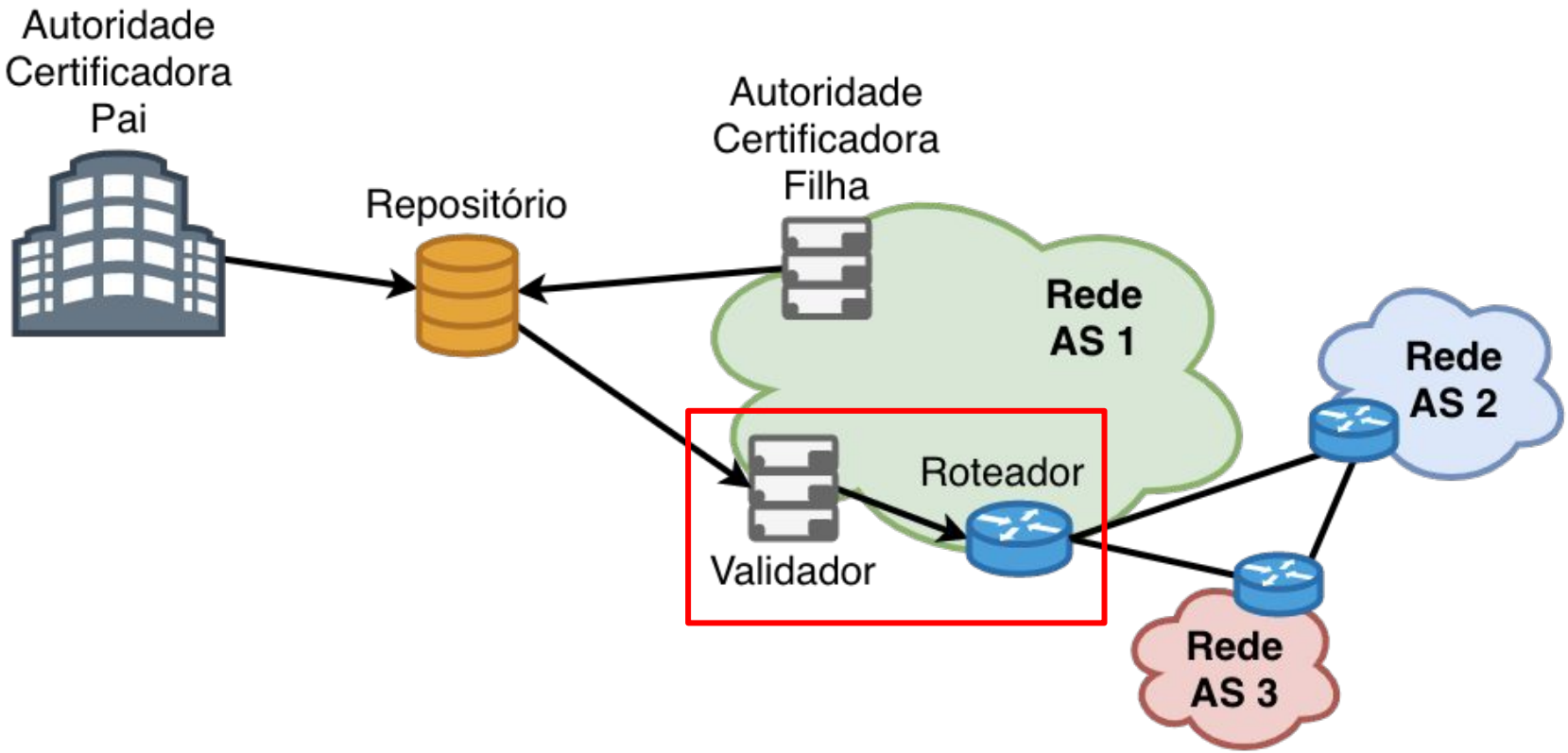


Monitoramento do RPKI pelo Registro.br

Para ajudar nessa fase inicial da implantação do RPKI, o Registro.br disponibilizou um serviço de monitoramento que informa se suas configurações de RPKI estão corretas.

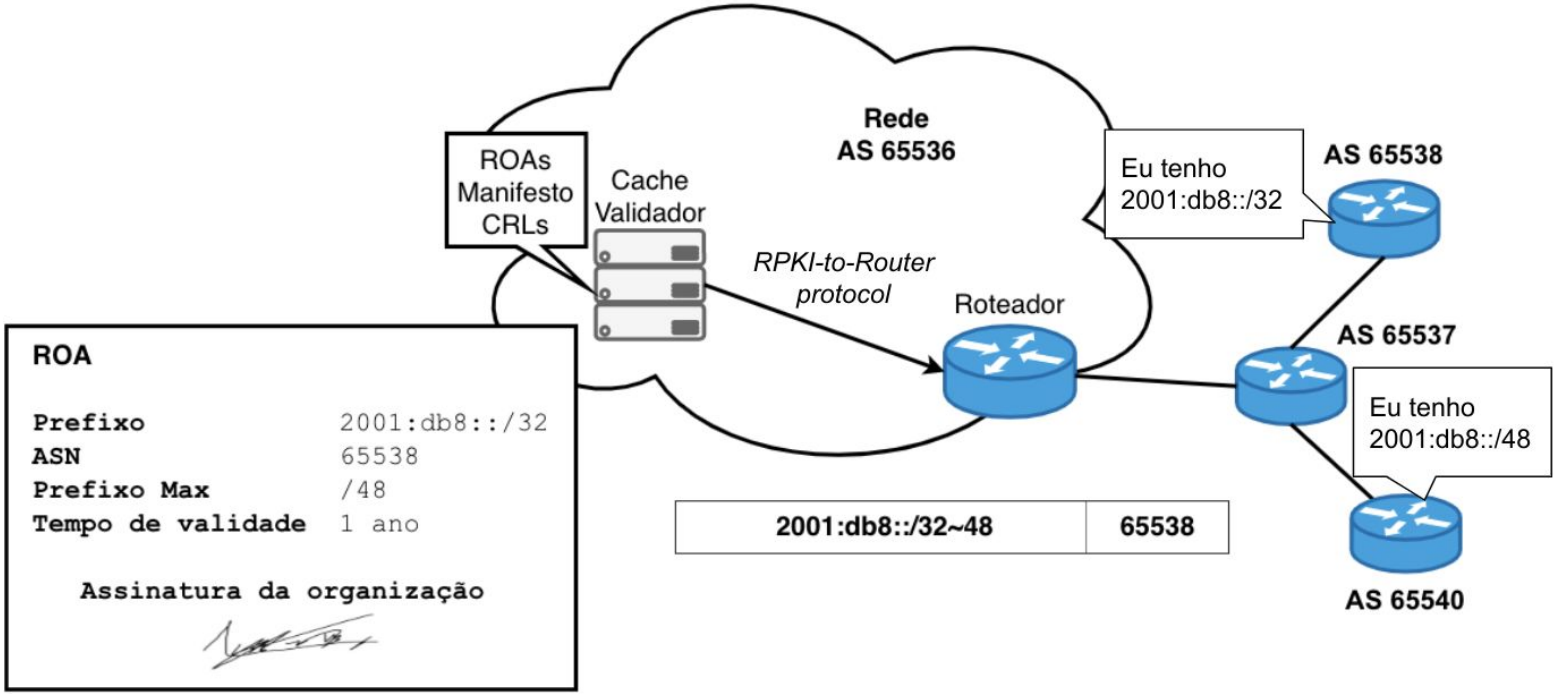


Validação da Origem

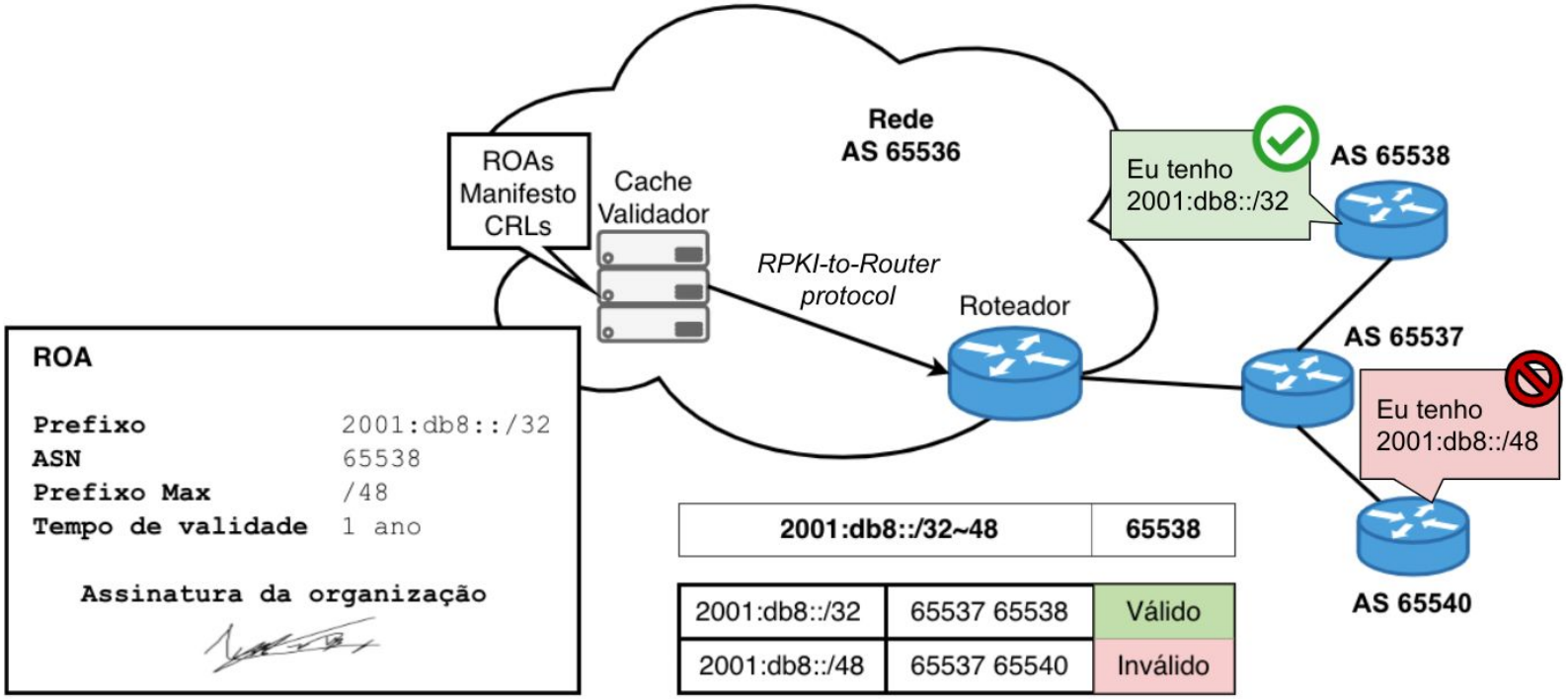


- **Validador**
  - Validação dos objetos certificados
  - Software que acessa fontes confiáveis e cria um cache da informação validada
- **Roteador**
  - Validação das rotas
  - BGP habilitado para usar o RPKI
  - Obtém informações do validador e utiliza para influenciar o roteamento

Validação da Origem



Validação da Origem



Exemplo:

	AS de Origem	Prefixo	Prefixo Max.
ROA	65536	10.0.0.0/16	/18

Válida	65536	10.0.128.0/17
Inválida	65536	10.0.0.0/24
Desconhecido	65540	10.0.0.0/8

Validador

- Existem vários softwares disponíveis:
  - ROUTINATOR
  - FORT (LACNIC)
  - RIPE validator
  - RTRlib (bird, FRR, Quagga...)
  - OctoRPKI & GoRTR (Cloudflare)
- Trust Anchor Locator (TAL) já vem incorporados
  - Localizador para os 5 RIRs

- Recebem VRPs do validador e utilizam para tomar decisões de roteamento
- Uma rota pode ser classificada como:
  - Válida: A origem e o prefixo máximo estão de acordo com a informação do ROA
  - Inválida: A informação não está de acordo com o ROA
  - Desconhecido: Não existe ROA para o prefixo verificado

- Suporte a validação na origem
- Hardware
  - Juniper
    - Junos versão 12.2 e superiores
  - Cisco
    - IOS release 15.2 e superiores
    - Cisco IOS/XR desde a 4.3.2
  - Nokia
    - Release R12.0R4 e superiores rodando no 7210 SAS, 7750 SR, 7950 XRS ou VSR.

- Suporte a validação na origem
- Hardware
  - Arista
    - EOS 4.24.0F e superiores
  - MikroTik
    - Versão 7.1 e superiores
  - Huawei
    - VRP 8.150 e superiores

Roteador – Software

- **Existem vários softwares com suporte a RPKI:**
  - BIRD
  - OpenBGPD
  - FRRouting
  - GoBGP
  - VyOS

Fonte: https://rpki.readthedocs.io/en/latest/rpki/router-support.html

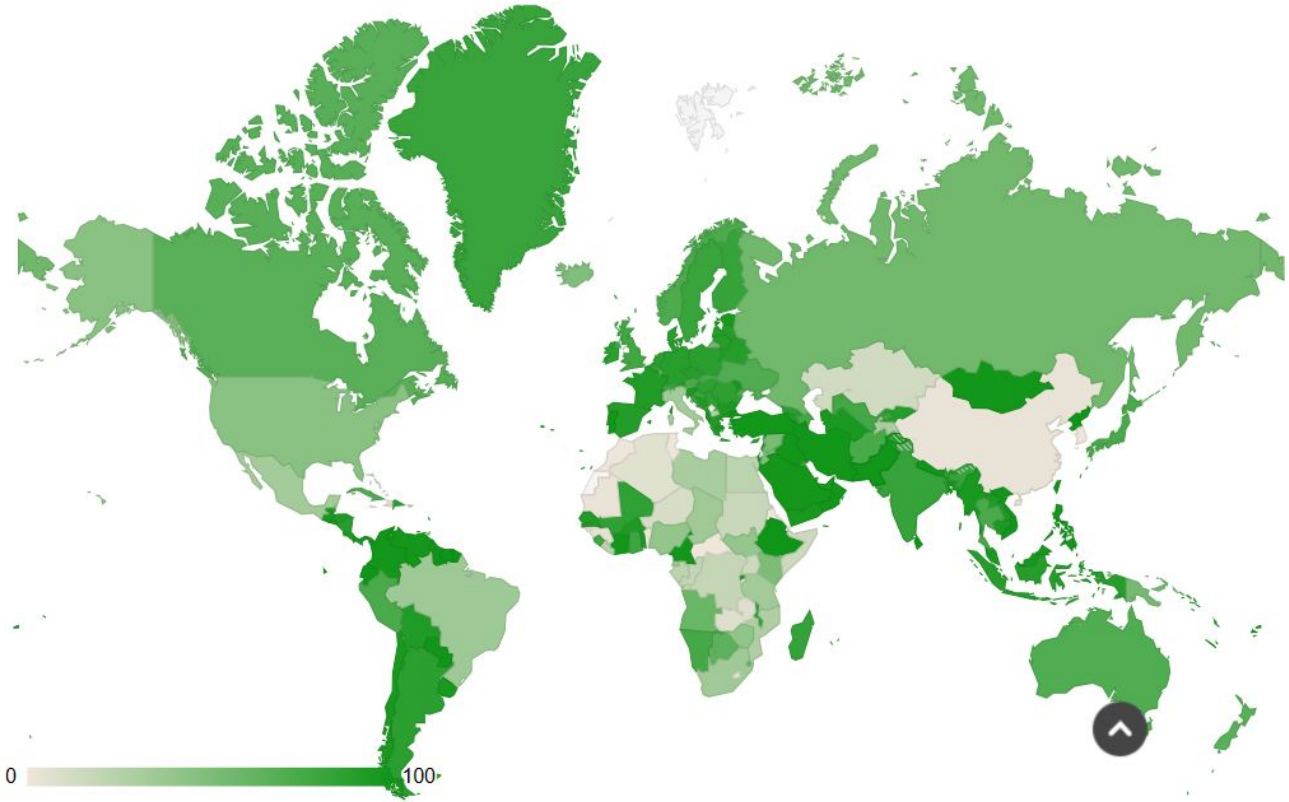
Recomendações

- Políticas de roteamento podem ser estabelecidas em cima da validação das rotas
  - Alterar preferências
  - Atribuir communities
  - Aplicar filtros

Colaboração é essencial: Adoção do RPKI

Fonte: https://monitor.fortproject.net/en/rpki_map

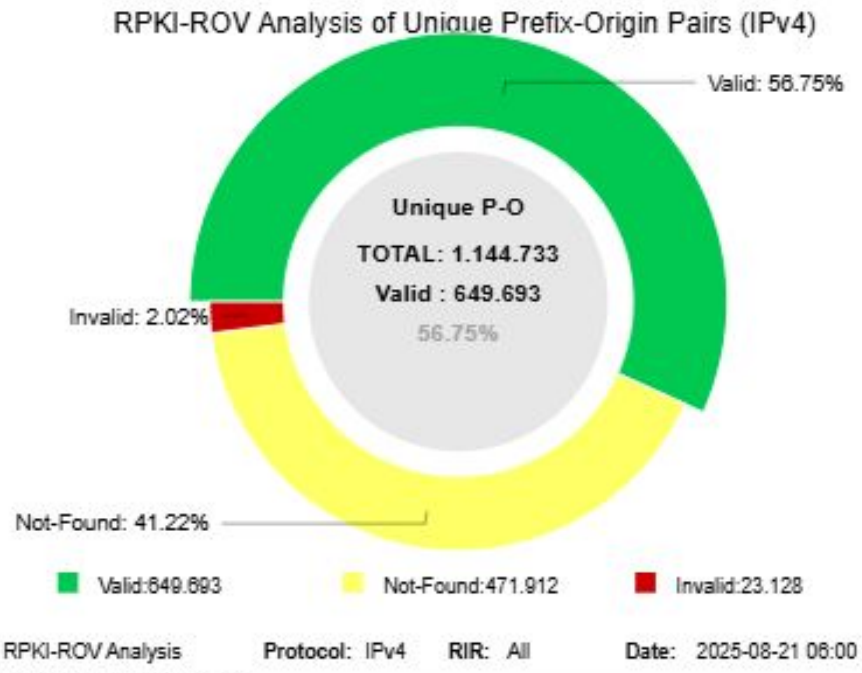
Colaboração é essencial: Adoção do RPKI



Fonte: https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html

Validação de Rotas

Análise da tabela completa do BGP em relação aos prefixos anunciados nos RPKIs



Fonte: https://rpki-monitor.antd.nist.gov/?p=0&s=0

Equipe de cursos do CEPTRO.br

wanderson@nic.br

PATROCÍNIO

ARPSIST FORTINET scansource Funpec GRUPO INTERJATO

APOIO

metrópole DIGITAL UFRN

REALIZAÇÃO

NÚCLEO DE REDES AVANÇADAS - UFRN

ESCOLA SUPERIOR DE REDES cais PoP RN RNP

MINISTÉRIO DA CULTURA MINISTÉRIO DA DEFESA MINISTÉRIO DA SAÚDE MINISTÉRIO DAS COMUNICAÇÕES MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO