nic.br

Núcleo de Informação e Coordenação do Ponto BR

cgi.br

Comitê Gestor da Internet no Brasil

registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

Práticas importantes para a segurança de seu provedor

Gilberto Zorello

IX Fórum Fortaleza, CE, 05/06/2025

nic.br

Boas práticas e padrões de Segurança

https://bcp.nic.br/i+seg/

Objetivos do Programa

- Reduzir ataques DDoS
- Melhorar a segurança de roteamento
- Reduzir vulnerabilidades e falhas de configuração
- Melhorar a segurança da resolução de nomes
- Divulgar melhores práticas de segurança
- Aumentar a cultura de segurança

https://bcp.nic.br/i+seg

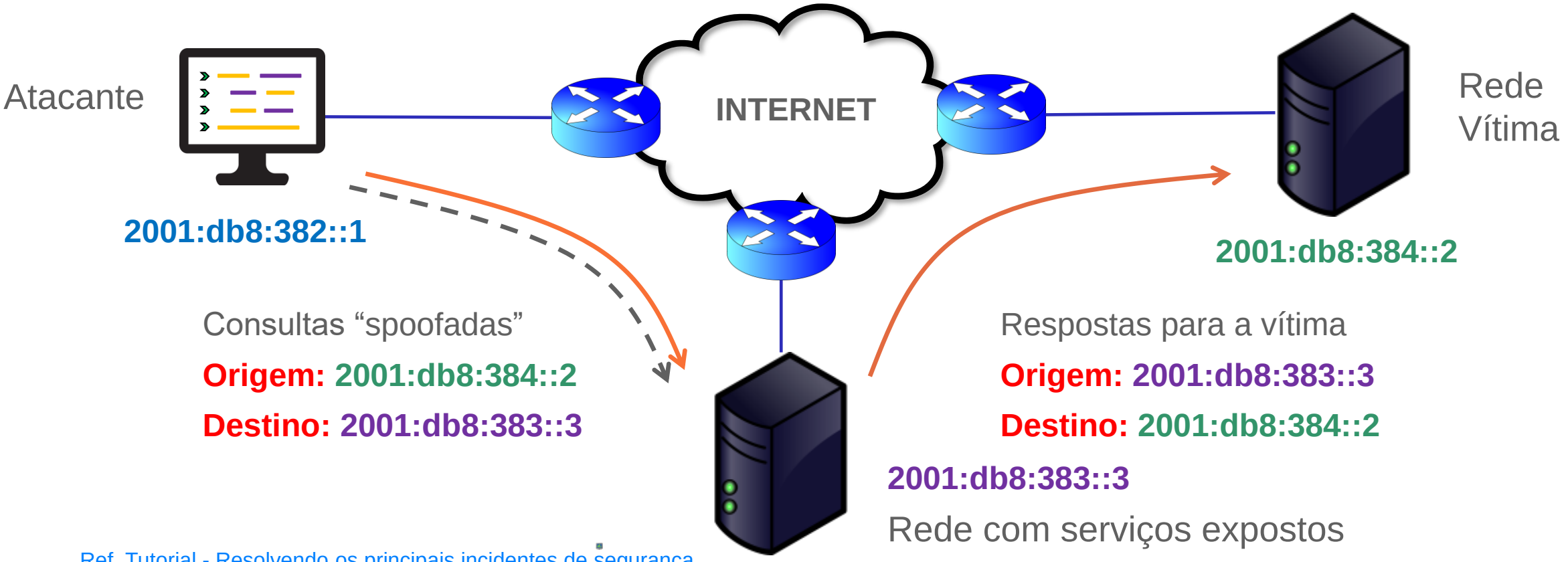
PROGRAMA INTERNET +SEGURA

https://bcp.nic.br/i+seg

Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Utiliza um terceiro para fazer o ataque

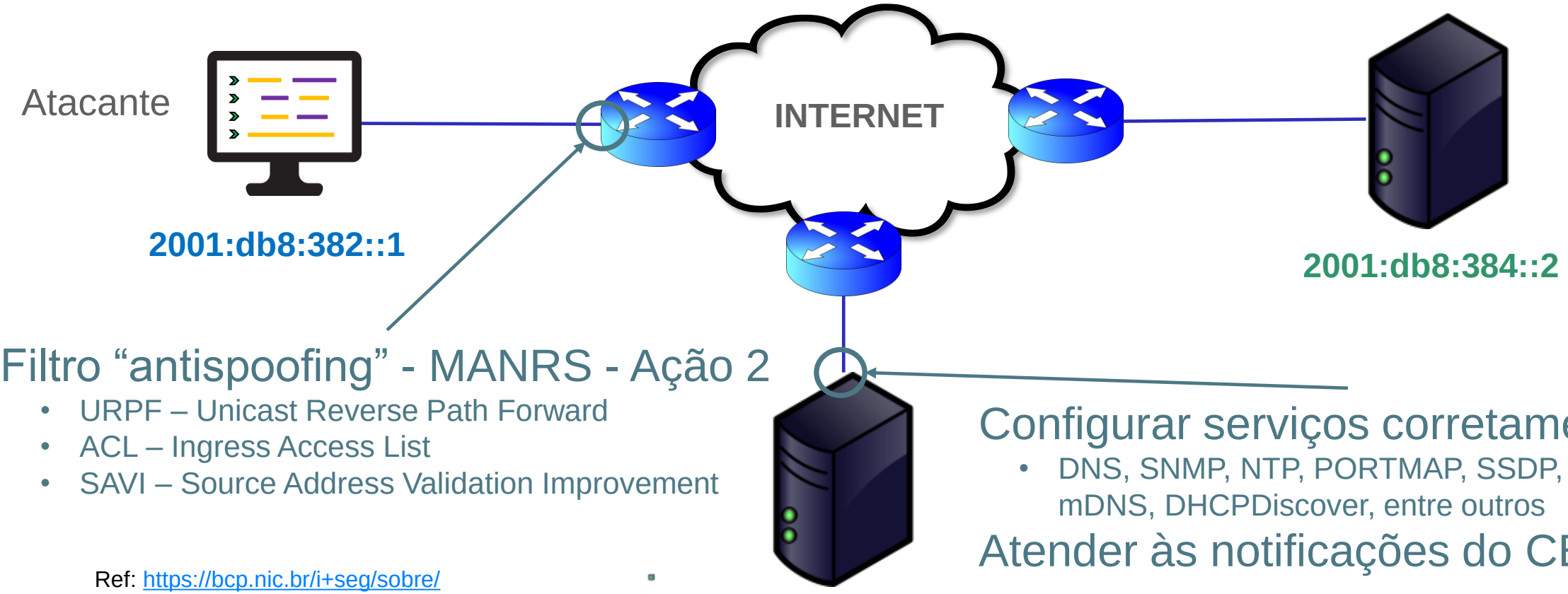


Ref. Tutorial - Resolvendo os principais incidentes de segurança

Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Como resolver o problema



Filtro “antispoofing” - MANRS - Ação 2

- URPF – Unicast Reverse Path Forward
- ACL – Ingress Access List
- SAVI – Source Address Validation Improvement

Configurar serviços corretamente

- DNS, SNMP, NTP, PORTMAP, SSDP, NETBIOS, mDNS, DHCPDiscover, entre outros

Atender às notificações do CERT.br

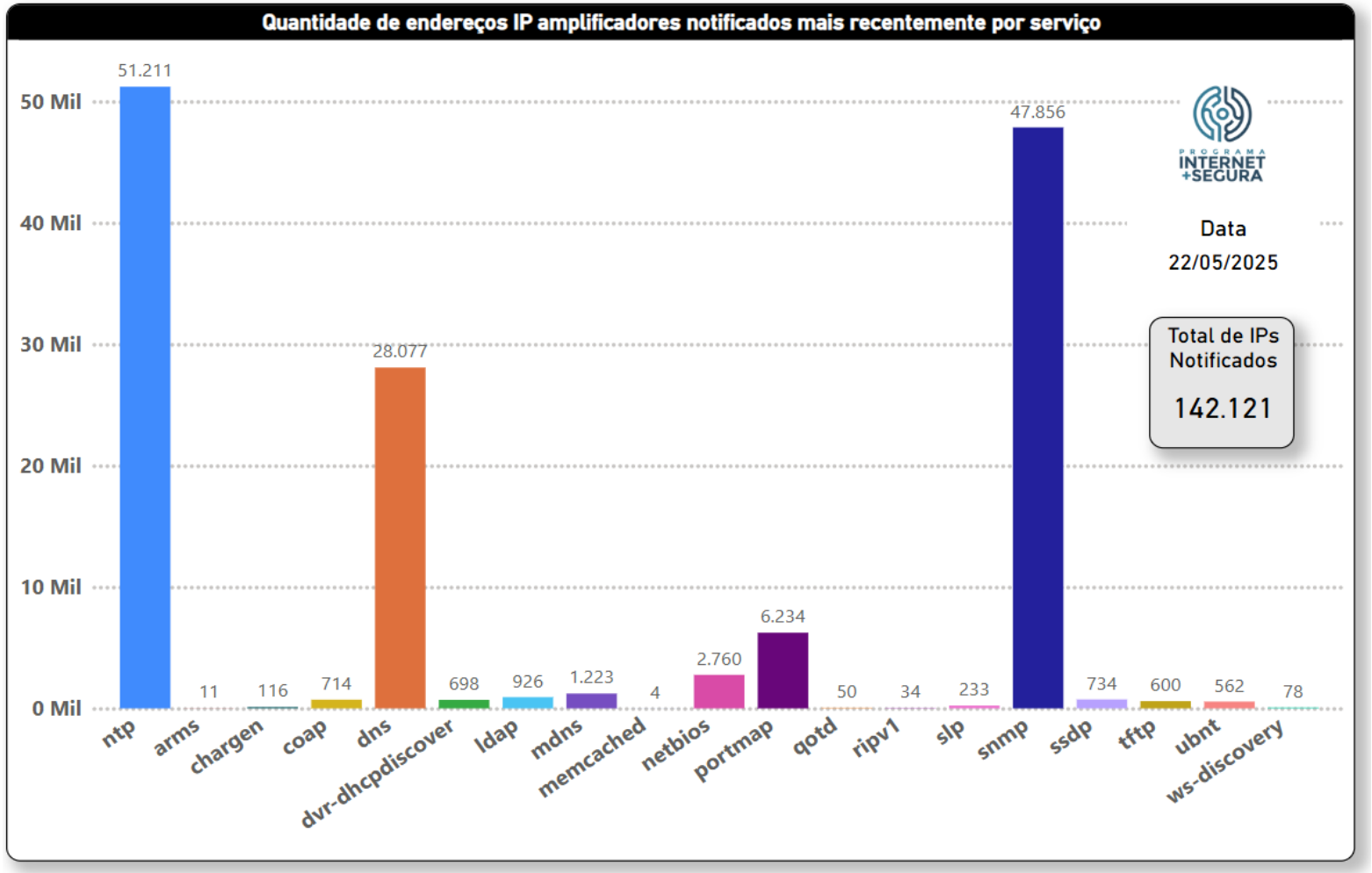
Ref: https://bcp.nic.br/i+seg/sobre/

Configuração de serviços expostos na Internet

- Usados para amplificação em DDoS
- Portas UDP: DNS (53), SNMP (161), NTP (123), e várias outras!
- Notificações do CERT.br

https://bcp.nic.br/i+seg/acoes/amplificacao/

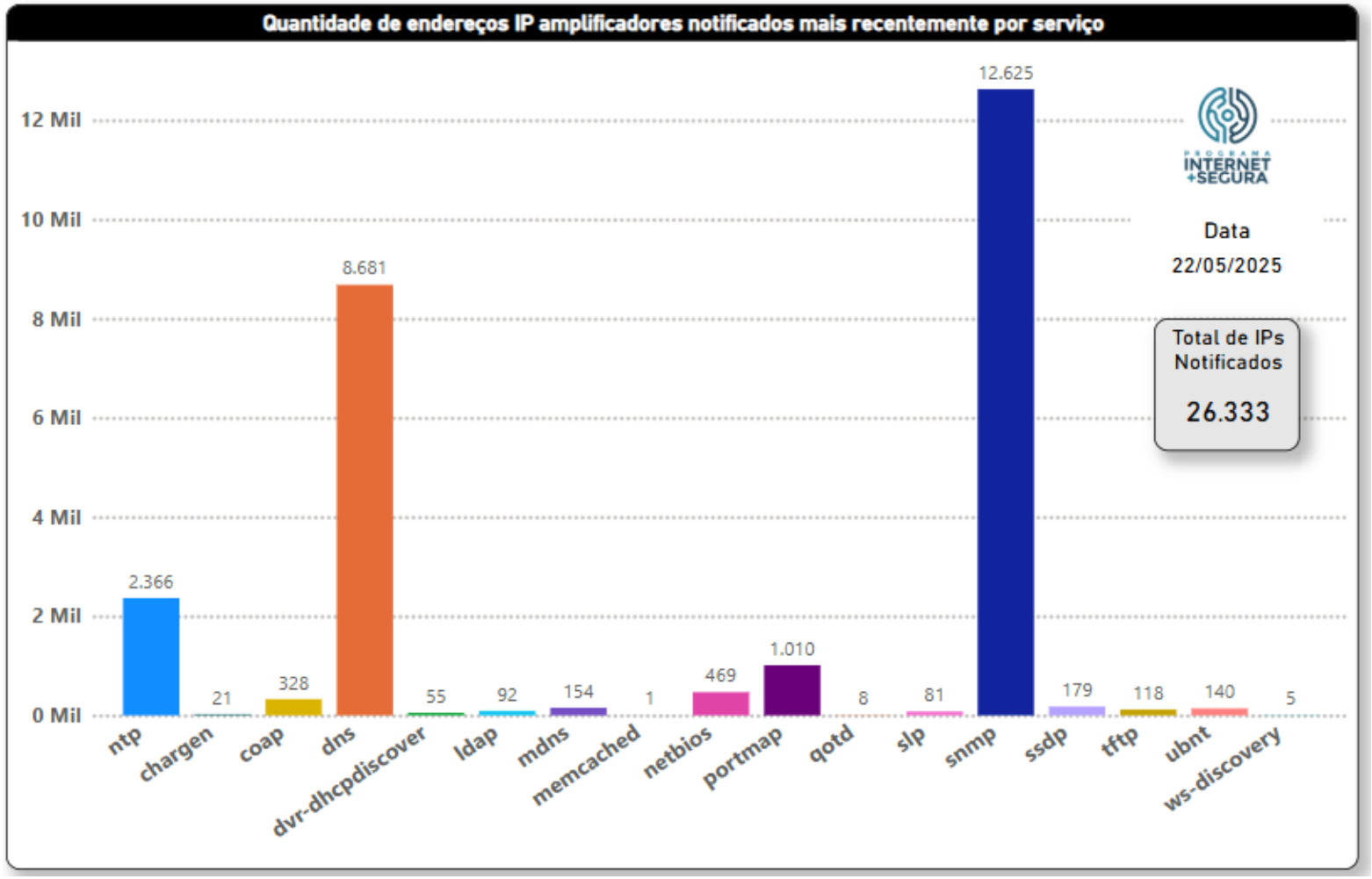
Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Brasil

- 5.077 AS notificados
- 142.121 endereços IP mal configurados
  - SNMP 47.856
  - NTP 51.211
  - DNS 28.077

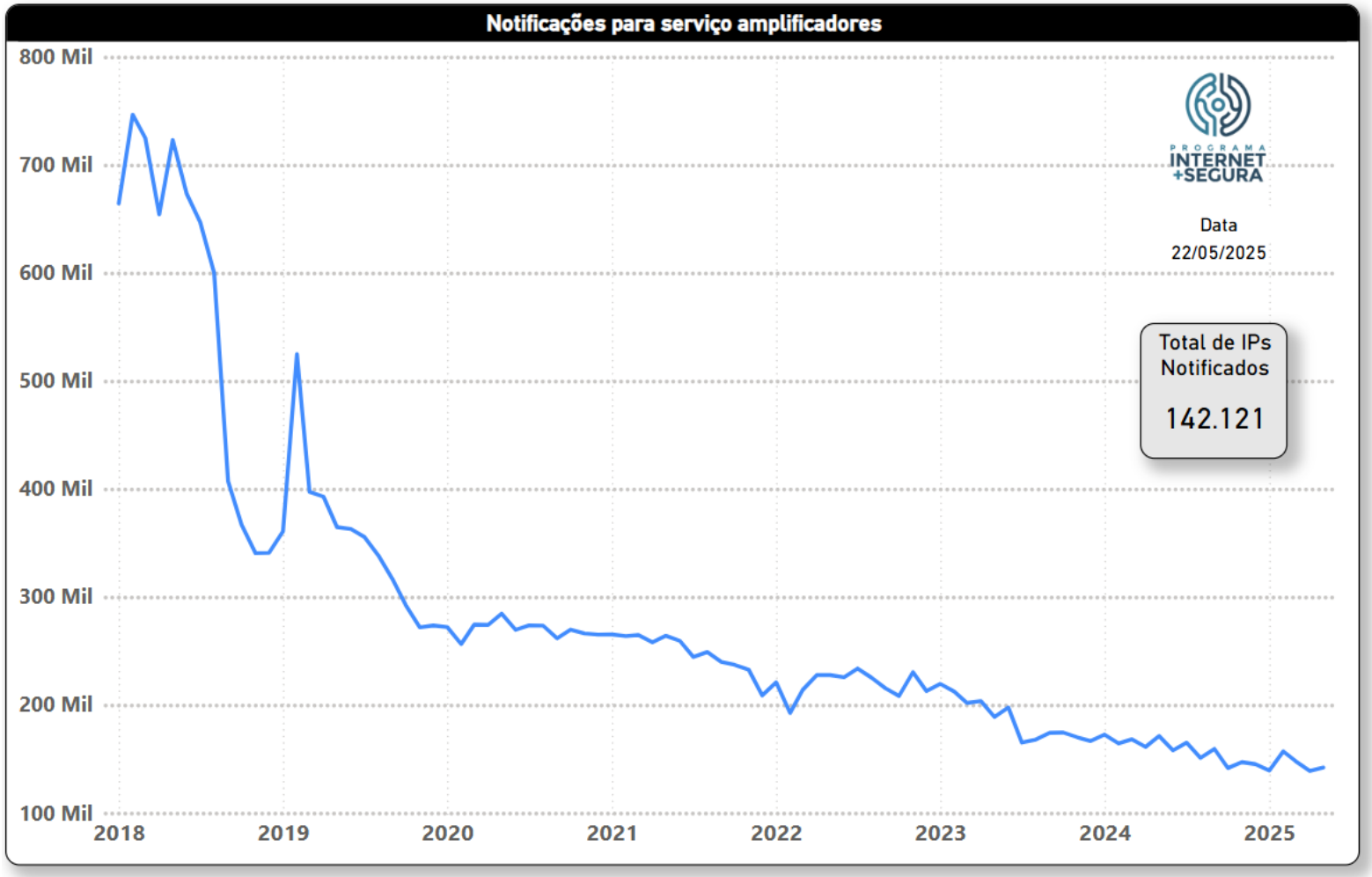
Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Região Nordeste

- 1.456 AS notificados
- 26.333 endereços IP mal configurados
  - SNMP 12.625
  - NTP 2.366
  - DNS 8.681

Programa por uma Internet mais Segura
Notificação de amplificadores - evolução



Brasil

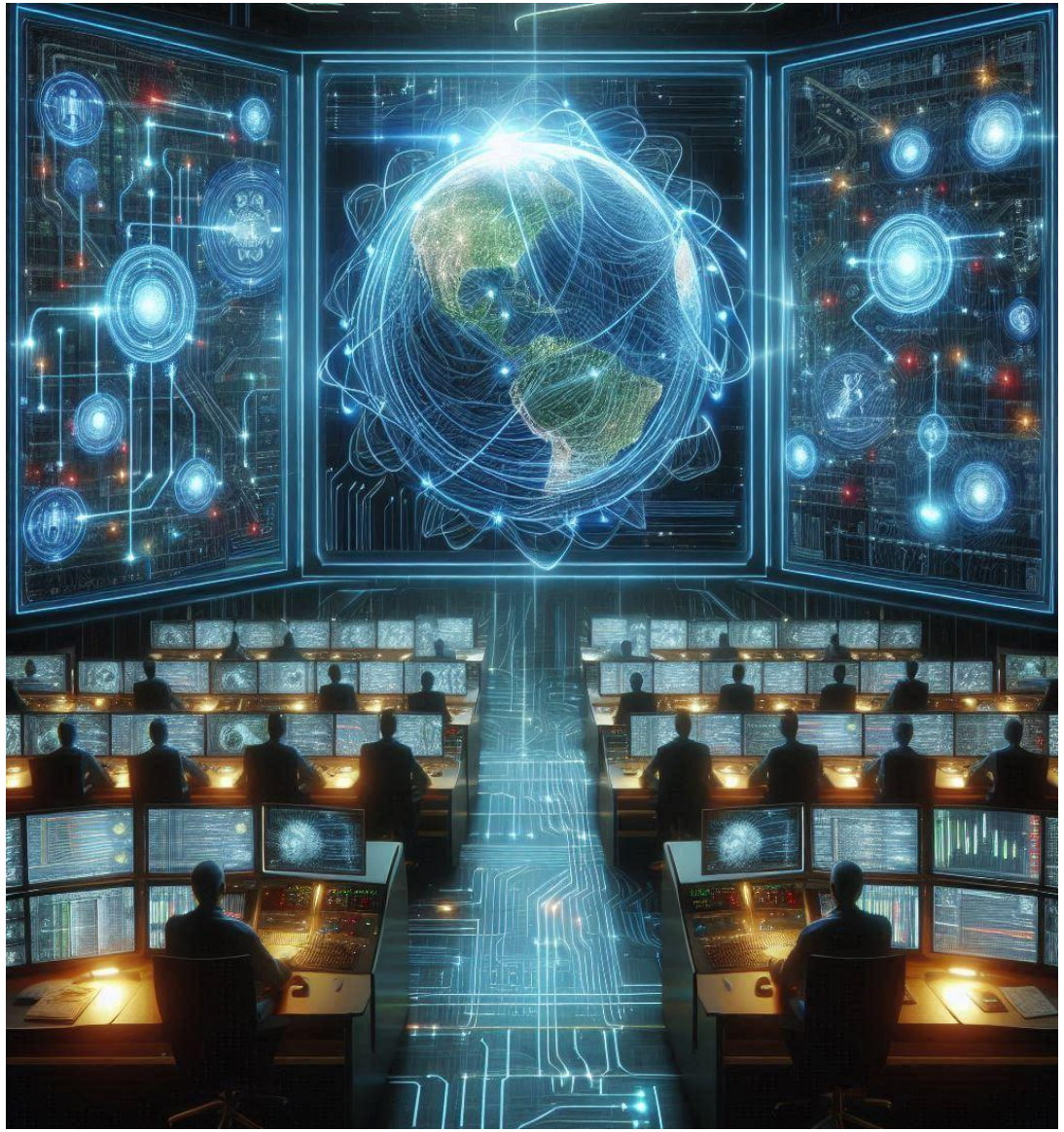
- Início (fev/2018)
  - Endereços IP: 746.508
  - Serviços: 5
- Atual:
  - Endereços IP: 142.121
  - Serviços: 19
  - **Redução de 80%**
  - Operadoras: 41%
  - ISP: 59%

Programa por uma Internet mais Segura

Boas práticas de gerenciamento

- **Autenticação**: senhas, duplo fator
- **Acesso**: protocolos seguros
- **Monitorar**: interfaces entrada e saída
- **Sistema**: hardening e sistemas atualizados
- **Registros**: gerar e armazenar logs
- **Configurações**: backup e scripts atualizados
- **Autorizaçã**o: permissão de usuários
- **Auditoria**: registrar e classificar usuários

Ref: Melhores Práticas de Hardening
Uso de *Netflows* para Segurança



MANRS

PROGRAMA INTERNET +SEGURA

Mutually Agreed Norms for Routing Security

http://manrs.org

https://bcp.nic.br/i+seg/acoes/manrs/

Programa por uma Internet mais Segura

Boas práticas de roteamento global

- MANRS - Internet Society (trocadilho em inglês)
- BGP é inseguro!
- Filtros BGP
- Filtro Anti Spoofing (endereço de origem)
- Pontos de contato de segurança no Peering DB, whois, IRR
- Cadastro da política de roteamento no IRR e RPKI

MANRS https://bcp.nic.br/i+seg/acoes/manrs/

Programa por uma Internet mais Segura

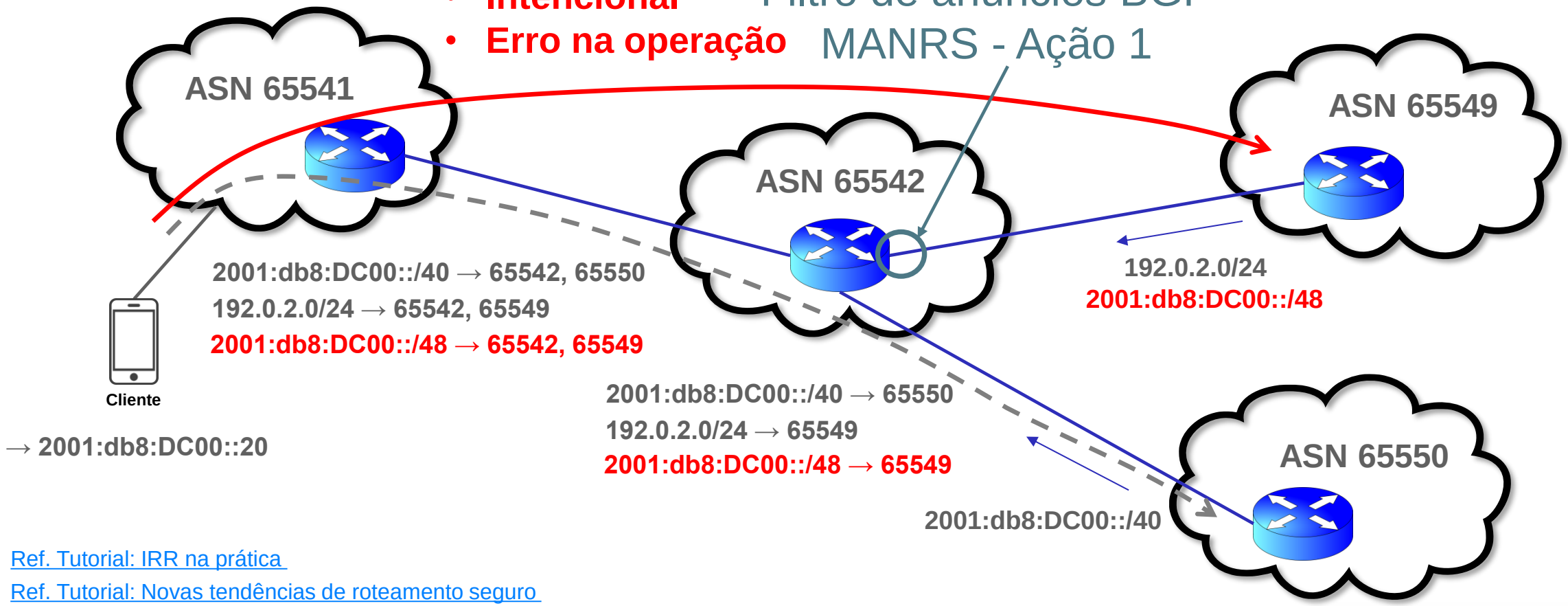
Sequestro de prefixos (Hijacking)

Anúncio de prefixos não autorizados:

- **Intencional**
- **Erro na operação**

Filtro de anúncios BGP

MANRS - Ação 1



Ref. Tutorial: IRR na prática

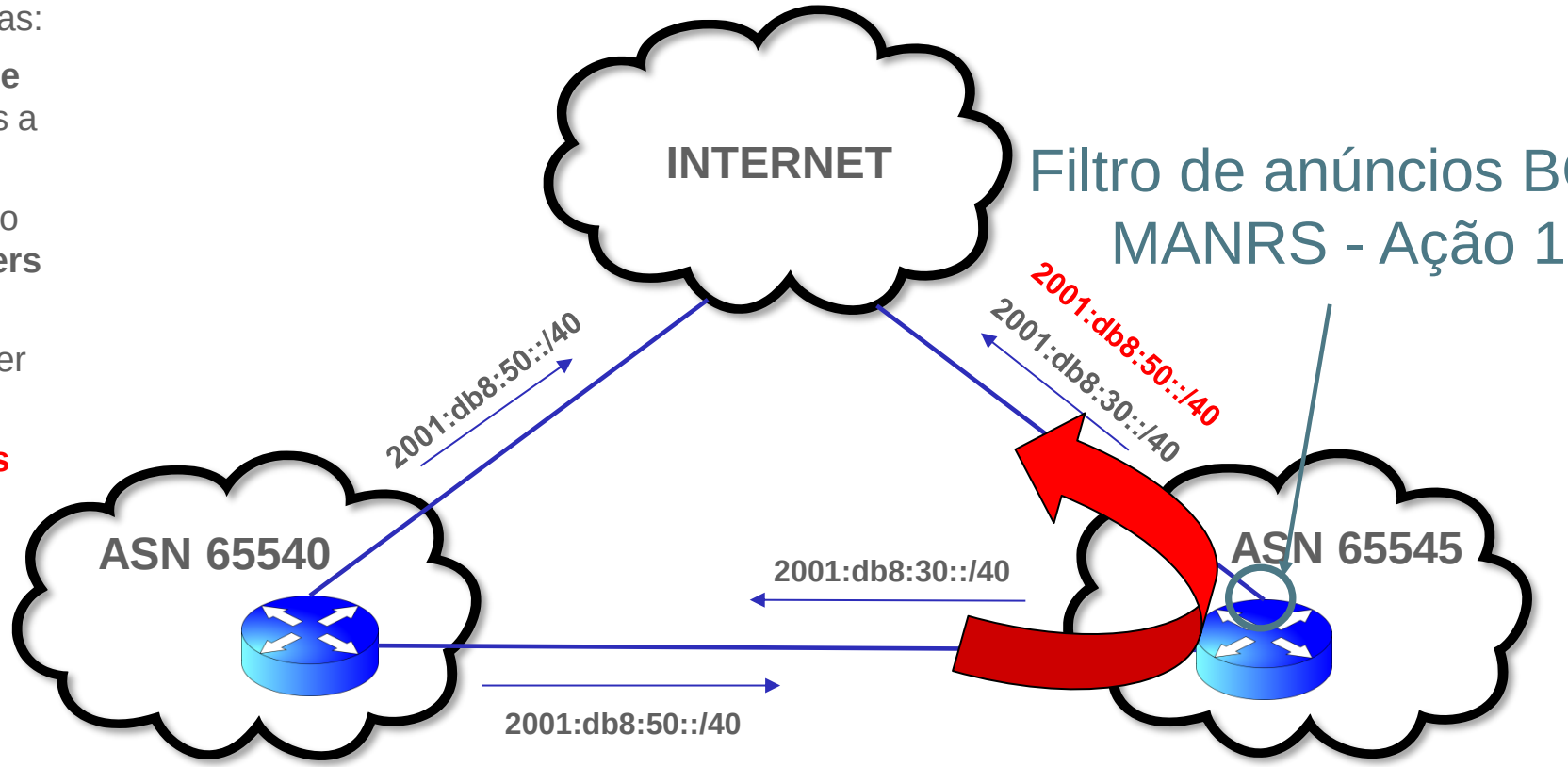
Ref. Tutorial: Novas tendências de roteamento seguro

Programa por uma Internet mais Segura

Vazamento de rotas (Route Leak)

- Algumas **regras** devem ser cumpridas:
  - Prefixos aprendidos do **provedor de trânsito** não devem ser anunciados a **outro provedor** ou a **peer** da rede
  - Prefixos aprendidos de um **peer** não devem ser anunciados a outros **peers** nem ao **provedor de trânsito**
  - Estes prefixos somente deveriam ser **anunciados a clientes**
- **Se as regras não forem cumpridas pode ocorrer vazamento de rotas**

Leak!
Normalmente são erros operacionais



Ref. Tutorial: IRR na prática

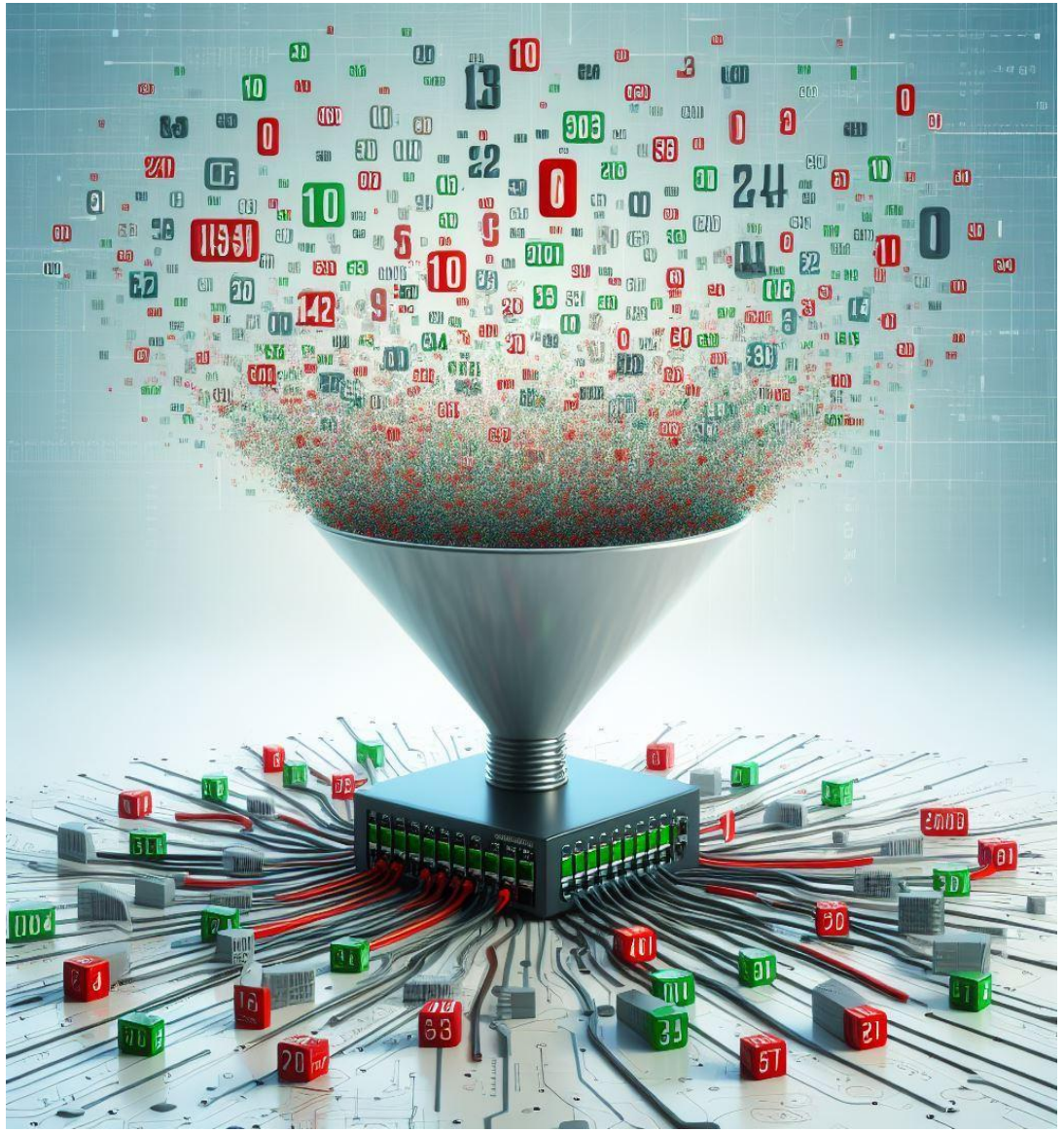
Ref. Tutorial: novas tendências de roteamento seguro

Programa por uma Internet mais Segura

MANRS - Ação 1 - Impedir a propagação de informações incorretas no BGP

- Implemente filtros no BGP para os seus prefixos e dos seus clientes

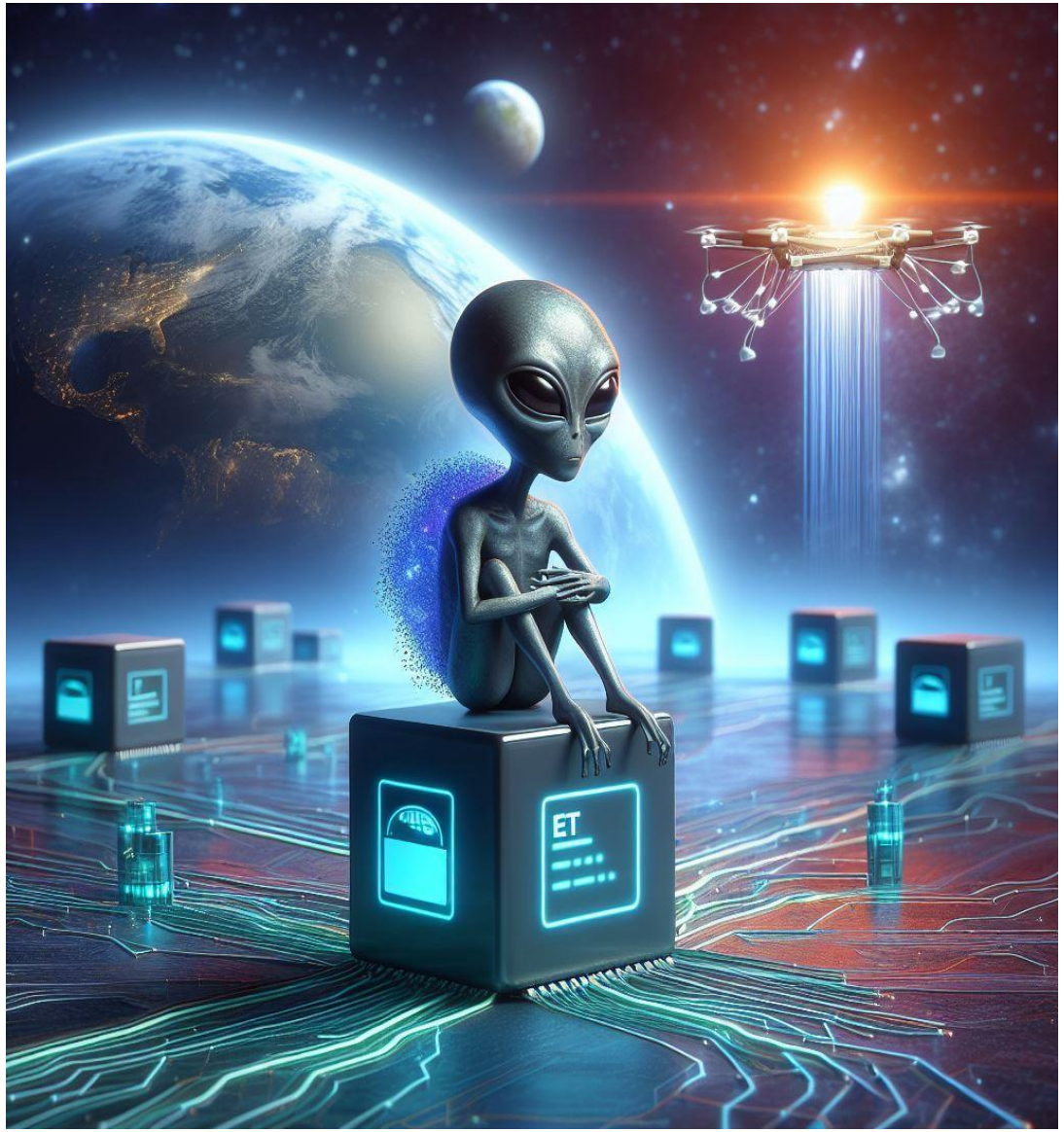
https://bcp.nic.br/i+seg/acoes/manrs/#filtragem-de-rotas



Programa por uma Internet mais Segura

MANRS - Ação 2 - Filtro Anti Spoofing

- Bloqueie pacotes com **origem** em IPs diferentes daqueles do seu bloco, eles **não podem sair de sua rede** (não podem ser originados na sua rede)!



MANRS

https://bcp.nic.br/antispoofing/

Programa por uma Internet mais Segura

MANRS - Ação 3 - Pontos de Contato

- **Contatos de roteamento e abuse no Registro.br** devem estar atualizados e serem de grupos de pessoas (RFC2142). Ex.: noc@seuprovedor.com.br
  - Registro.br está validando os e-mails de abuse e a não resposta pode causar a recuperação (perda) dos endereços IP
  - Mensagens do CERT.br estão indo para o SPAM em alguns casos!
- Atualizar contatos no **PeeringDB** e **IRR**

MANRS https://bcp.nic.br/i+seg/acoes/manrs/#coordenacao

Programa por uma Internet mais Segura

MANRS - Ação 4 - Cadastro da Política de Roteamento

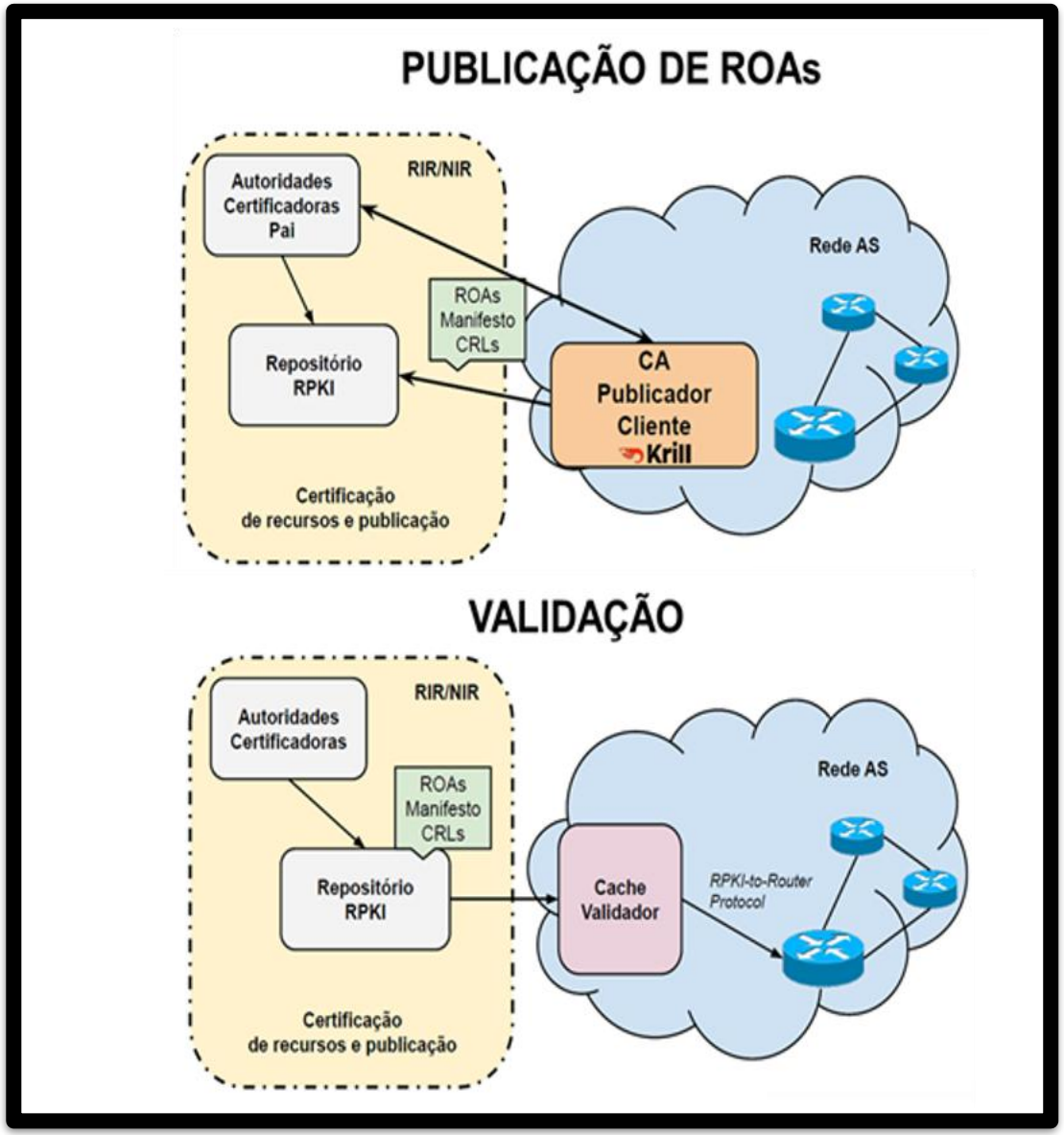
- **IRR** - Internet Routing Registry
  - RADB
  - TC (gratuito)

- **RPKI** - Resource Public Key Infrastructure

Artigo: War story: RPKI is working as intended

MANRS

https://bcp.nic.br/i+seg/acoes/



Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

MANRS Observatory - Brasil - 8647 AS

MANRS

Resumo 27-mai-25

MANRS - Status da Segurança de Roteamento

Incidentes

Sequestro de Rota	39
Vazamento de Rota	0
Anúncio inválido	16
Total	55

Responsáveis

AS responsáveis	44

Informação de Roteamento

IRR

Não registrado	4.022	4,4%
Registrado	88.070	95,6%

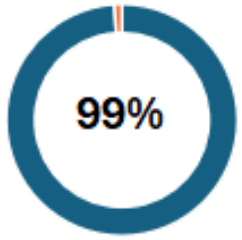
RPKI

Válido	43.896	47,7%
Desconhecido	48.018	52,1%
Inválido	178	0,2%

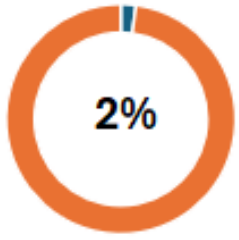
MANRS - Prontidão

Informação de Roteamento

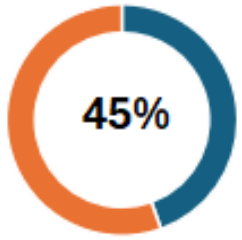
Filtros BGP



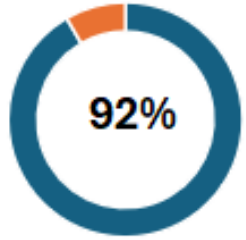
Anti-spoofing



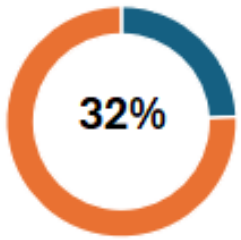
Coordenação



IRR



RPKI



Programa por uma Internet mais Segura

MANRS Observatory - Nordeste - 2314 AS

Resumo 27-mai-25

MANRS - Status da Segurança de Roteamento

Incidentes

Sequestro de Rota	11
Vazamento de Rota	0
Anúncio inválido	5
Total	16

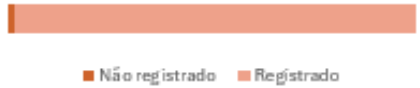
Responsáveis

AS responsáveis	10

Informação de Roteamento

IRR

Não registrado	375	1,9%
Registrado	19.584	98,1%



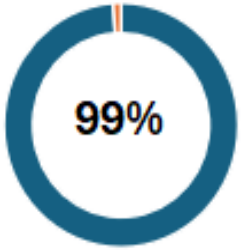
RPKI

Válido	9.376	47,1%
Desconhecido	10.458	52,6%
Inválido	56	0,3%

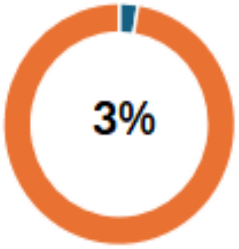
MANRS - Prontidão

Informação de Roteamento

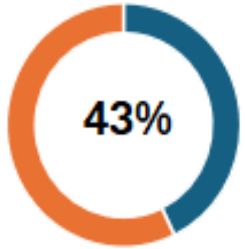
Filtros BGP



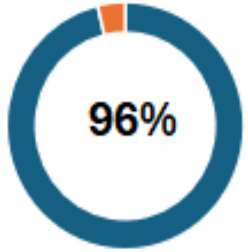
Anti-spoofing



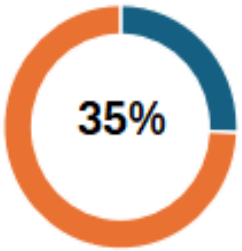
Coordenação



IRR



RPKI



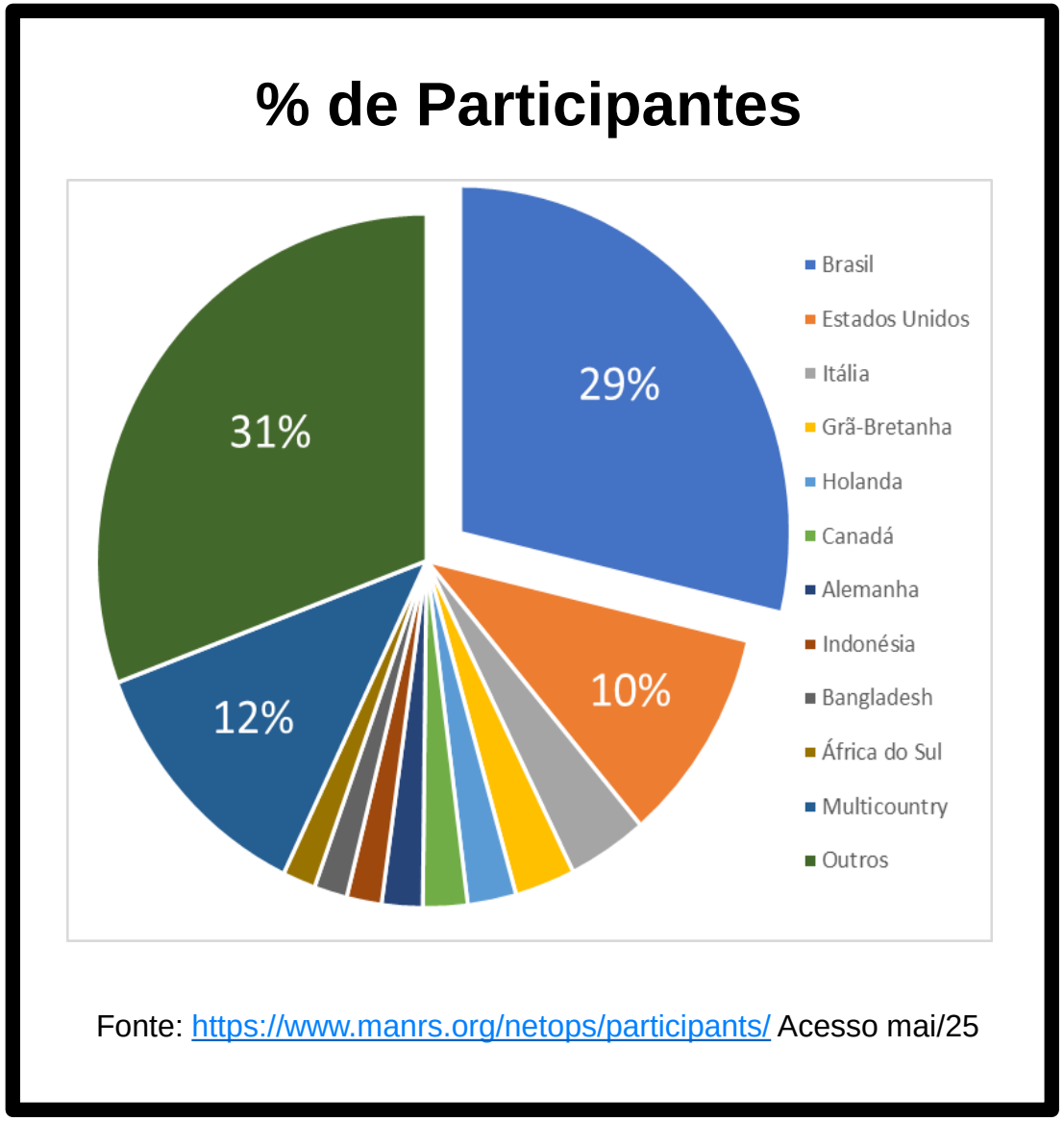
Programa por uma Internet mais Segura

Participantes por país

- Total: 1195
- Participantes no Brasil → 302

MANRS

2023 → 258
2022 → 206
2021 → 174
2020 → 140



Fonte: https://www.manrs.org/netops/participants/ Acesso mai/25

PROGRAMA INTERNET +SEGURA

Stands for **K**nowledge-Sharing and
Instantiating **N**orms for **DNS** and **N**aming
Security

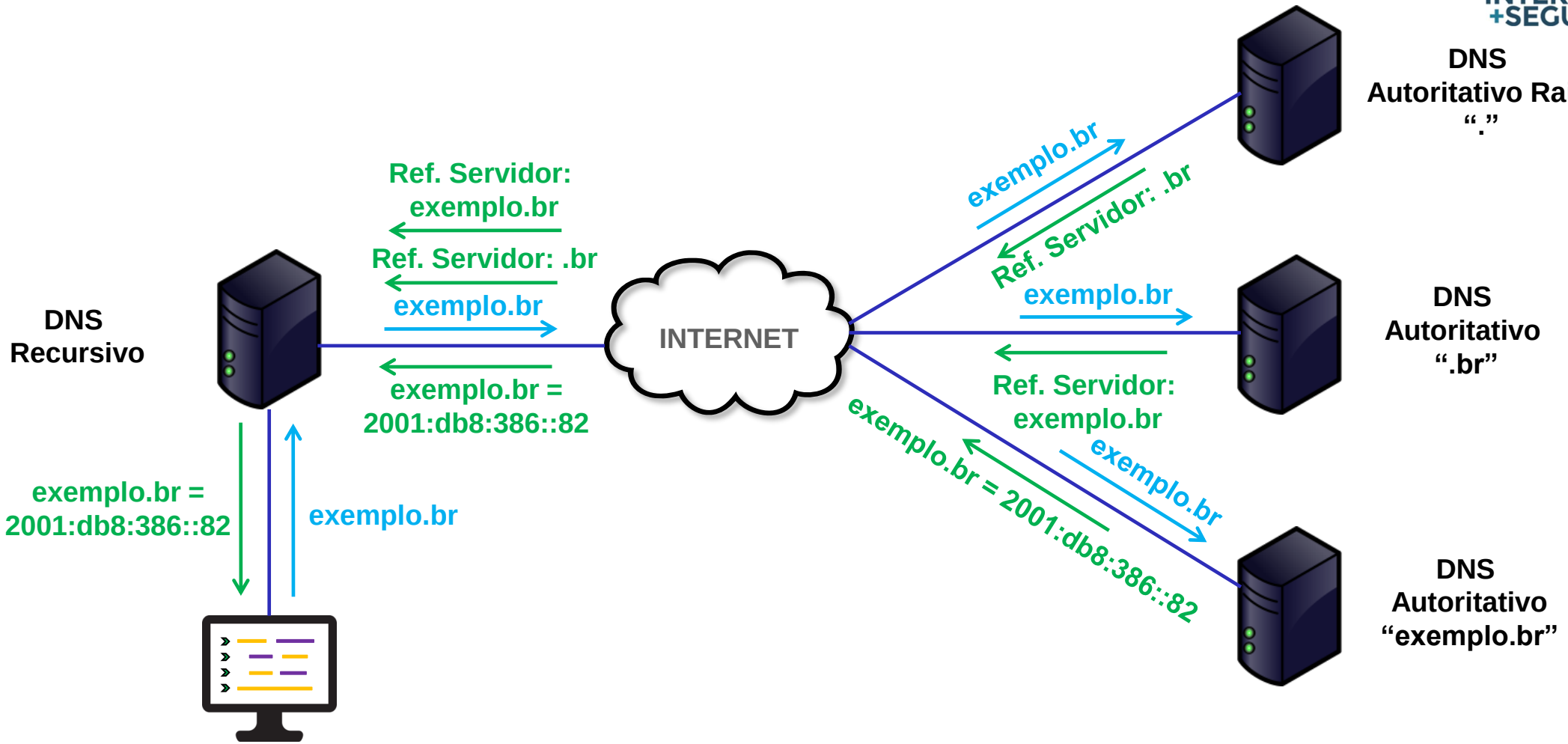
https://kindns.org/

An ICANN Initiative

ICANN

Programa por uma Internet mais Segura

Processo de Recursão DNS



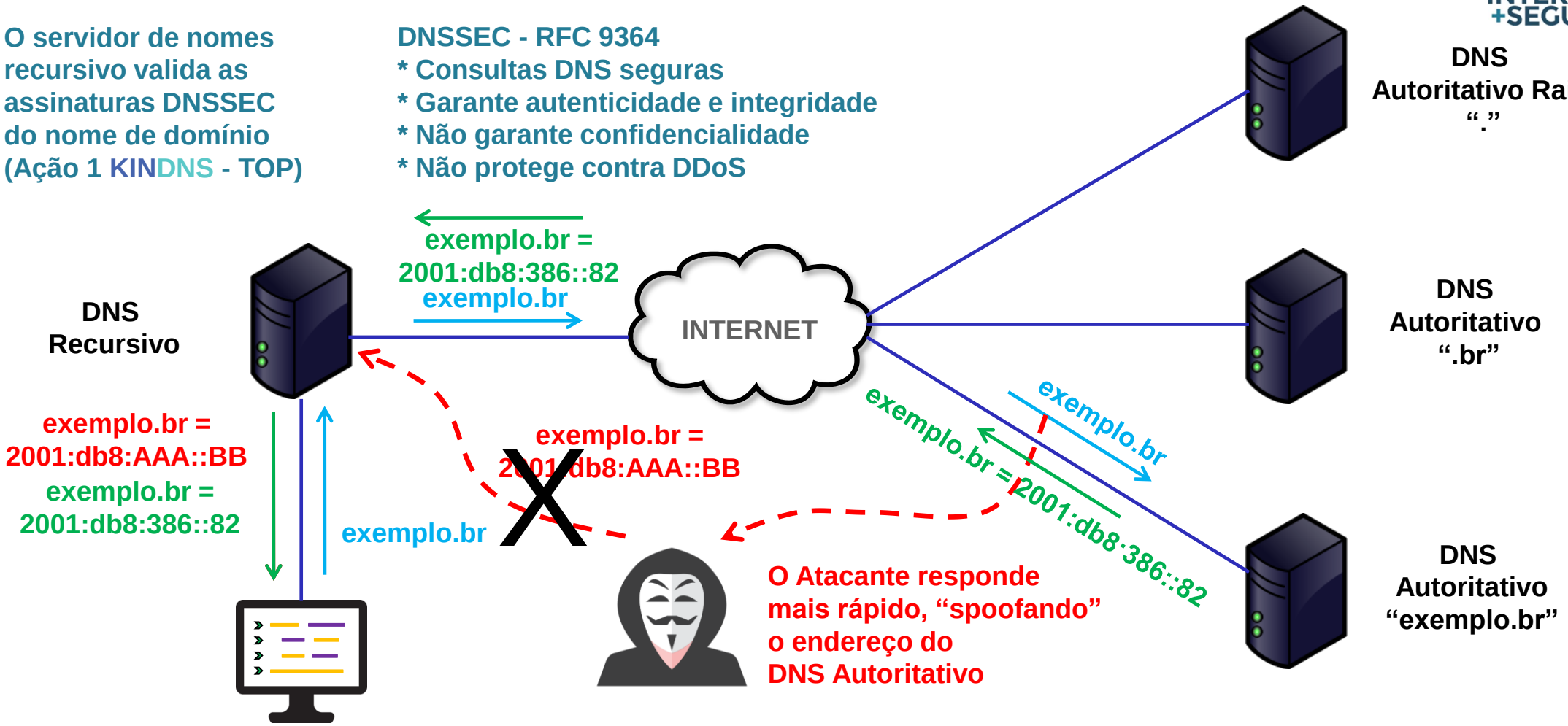
Fonte: [#SemanaCap 7] Curso - Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning

Programa por uma Internet mais Segura

Ataque DNS – Poisoning

O servidor de nomes recursivo valida as assinaturas DNSSEC do nome de domínio (Ação 1 KINDNS - TOP)

DNSSEC - RFC 9364
* Consultas DNS seguras
* Garante autenticidade e integridade
* Não garante confidencialidade
* Não protege contra DDoS



Fonte: [#SemanaCap 7] Curso - Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning

Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

Boas práticas para DNS

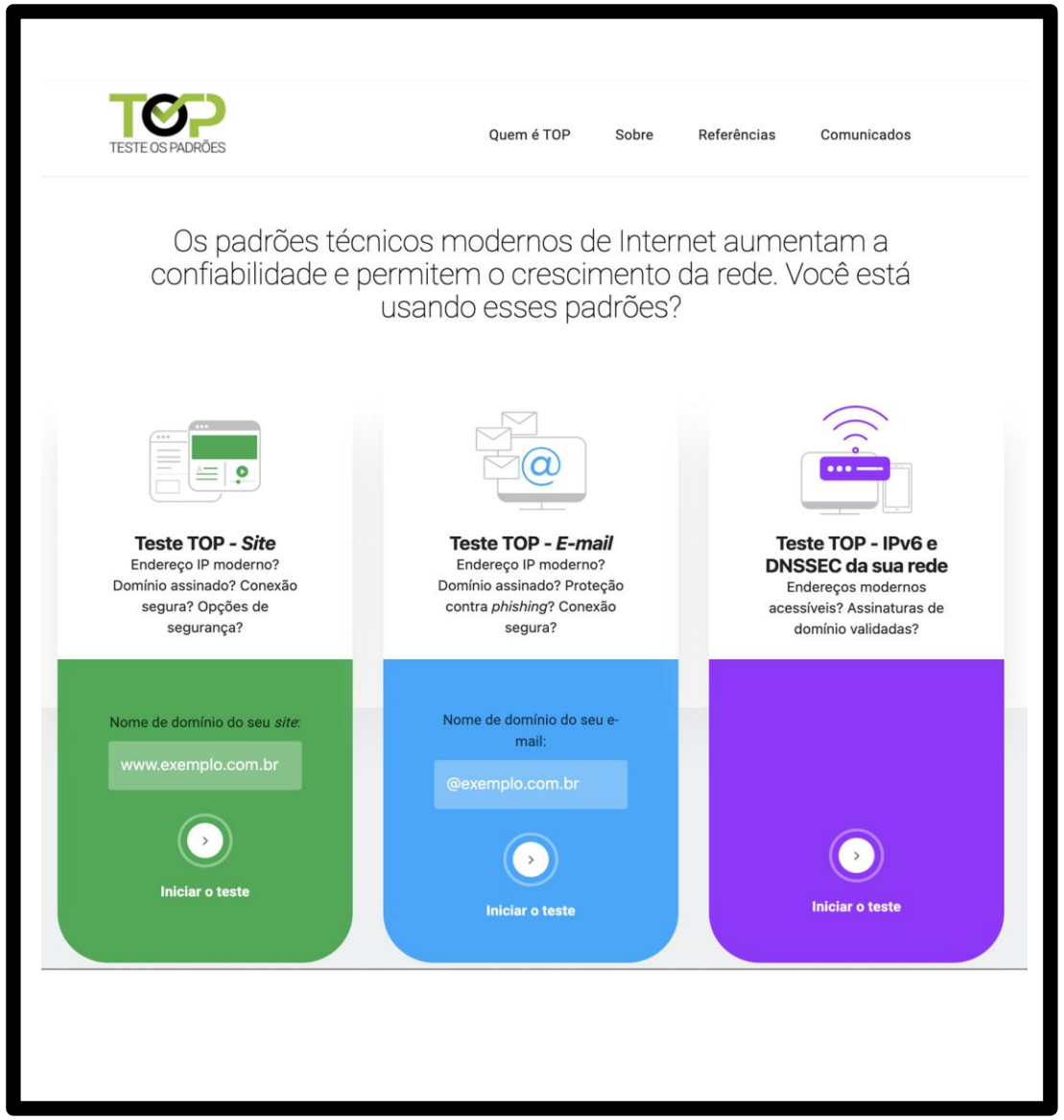
- KinDNS da ICANN (trocadilho em inglês)
- Configuração correta do recursivo somente para seus usuários
- Validação do DNSSEC no recursivo
- Configuração do autoritativo do seu nome de domínio com DNSSEC

BCP: Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos

https://kindns.org/ KINDNS

PROGRAMA INTERNET +SEGURA

https://top.nic.br



Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

TOP - Teste os padrões

- Teste do DNS recursivo na sua rede (DNSSEC)!
- Teste do IPv6 na sua rede!
- Teste do seu site!
- Teste do seu e-mail!
- Mostra o que está errado e links com informações para corrigir!

https://top.nic.br

Programa por uma Internet mais Segura
Implemente as melhores práticas

MANRS

KINDNS

Reuniões on-line com os responsáveis pelos AS (KPI)

- Serviços notificados mal configurados
- Adoção do MANRS
- Adoção do KINDNS
- Testes do TOP: conexão, site e e-mail

https://bcp.nic.br/i+seg
https://kindns.org/
https://top.nic.br

Camada 8 - NIC.br

- Podcast sobre a infraestrutura da Internet
- Edição Novembro/24

https://www.nic.br/podcasts/camada8/episodio-57

Programa por uma Internet mais Segura

APOIO

conexis brasil.digital

A CONECTIVIDADE AO SEU ALCANCE

abranet
Associação Brasileira de Internet

AbraCloud

REDETELESUL

abrint

TelComp
Competição para o Futuro Digital

abramulti
Associação brasileira dos operadores de telecomunicações e provedores de internet.

APRONET
Associação Catarinense dos Provedores de Internet

RNP
REDE NACIONAL DE ENSINO E PESQUISA

InternetSul

Obrigado

Gilberto Zorello

gzorello@nic.br

05 de junho de 2025

www.nic.br | www.cgi.br