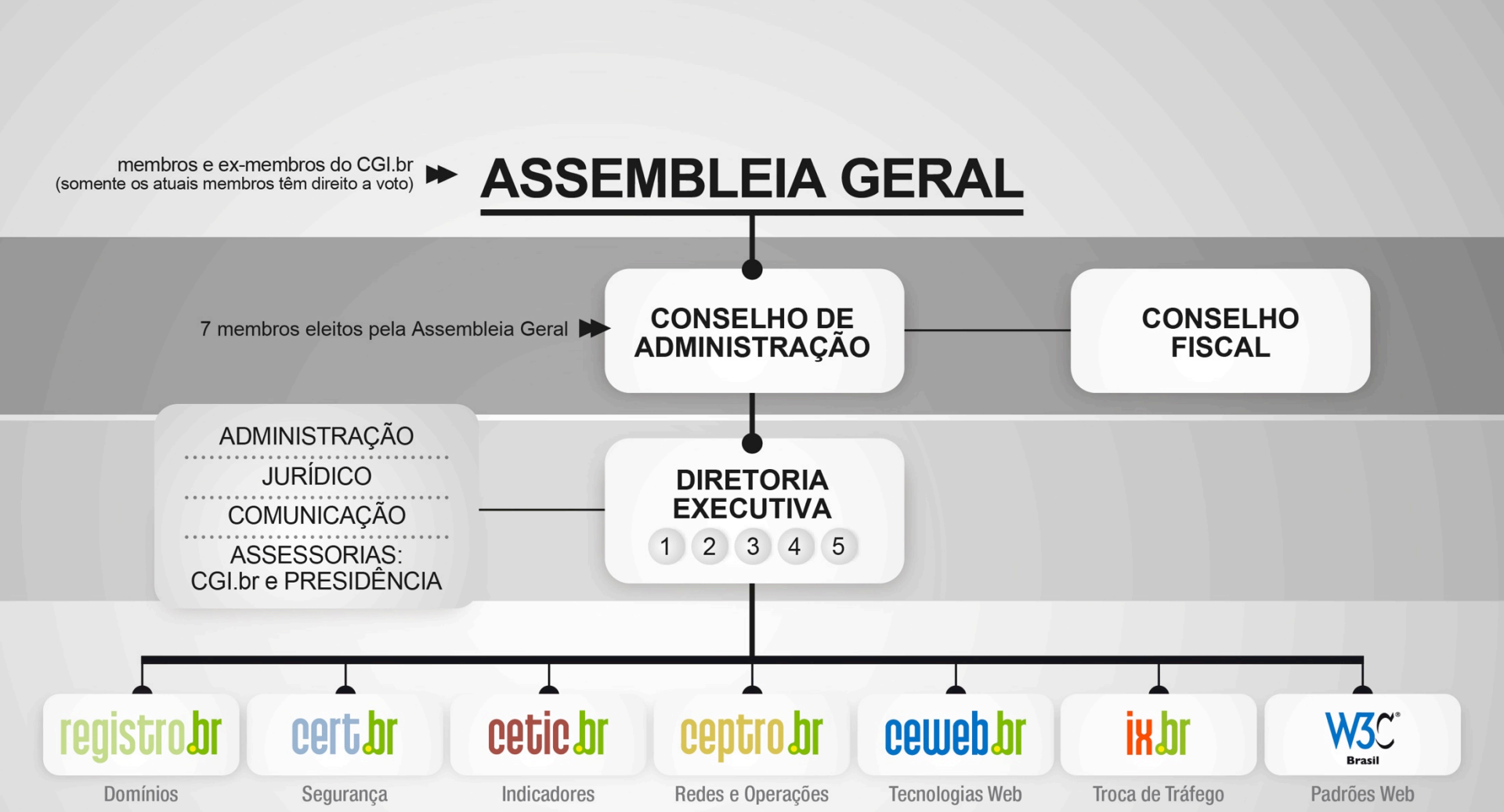
nic.br

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



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

cgi.br

1 2 3 4 5 6 7 8 9 — GOVERNO e 10 11 12 13 14 15 16 17 18 19 20 21 — SOCIEDADE CIVIL

Representantes do Governo:

1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
2 Casa Civil da Presidência da República
3 Ministério das Comunicações
4 Ministério da Defesa
5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 Ministério do Planejamento, Orçamento e Gestão
7 Agência Nacional de Telecomunicações
8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

Representantes da Sociedade Civil:

10 Notório saber em assunto da Internet
11 a 14 Representantes do setor empresarial
- provedores de acesso e conteúdo da Internet
- provedores de infra-estrutura de telecomunicações
- indústria de bens de informática, de bens de telecomunicações e de software
- setor empresarial usuário

15 a 18 Representantes do terceiro setor
19 a 21 Representantes da comunidade científica e tecnológica

nic.br cgi.br | ix.br

Nome do Evento
São Paulo, SP | 12/01/15

Programa por uma Internet Segura
Ações no IX.br

Julio Sirota

ix.br nic.br cgi.br

Ambiente do IX.br

Compartilhado

- ✓ Participantes presentes nas VLANs do ATMv4 e ATMv6
- ✓ Com sessões BGP com os Route Servers (RS)

Privado

- ✓ Acordo Bilateral com troca de tráfego direta em VLAN dedicada
- ✓ Troca de tráfego direta através das VLANs do ATMv4 e ATMv6 com o estabelecimento de sessões BGP entre os roteadores dos dois Ass

As ações propostas devem ser consideradas e aplicadas pelos gestores do ASs envolvidos em relações de peering dentro e fora IX.br

Aumento da Segurança nos Route Servers do IX.br

Classificação das ações propostas quanto ao tempo previsto para sua implementação:

EM USO

CURTO (45 dias)

MÉDIO (120 dias)

LONGO (12 a 18 meses)

Ação 1: Filtro de Prefixos BOGONs

Rejeição de anúncios que contenham prefixos indevidos (BOGONs):

IPv4

```
0.0.0.0/8 prefixlen >= 8                 # 'this' network [RFC1122]
10.0.0.0/8 prefixlen >= 8                # private space [RFC1918]
100.64.0.0/10 prefixlen >= 10            # CGN Shared [RFC6598]
127.0.0.0/8 prefixlen >= 8               # localhost [RFC1122]
169.254.0.0/16 prefixlen >= 16           # link local [RFC3927]
172.16.0.0/12 prefixlen >= 12            # private space [RFC1918]
192.0.2.0/24 prefixlen >= 24             # TEST-NET-1 [RFC5737]
192.168.0.0/16 prefixlen >= 16           # private space [RFC1918]
198.18.0.0/15 prefixlen >= 15            # benchmarking [RFC2544]
198.51.100.0/24 prefixlen >= 24          # TEST-NET-2 [RFC5737]
203.0.113.0/24 prefixlen >= 24           # TEST-NET-3 [RFC5737]
224.0.0.0/4 prefixlen >= 4               # multicast
240.0.0.0/4 prefixlen >= 4               # reserved for future use
```

IPv6

```
::/8 prefixlen >= 8
0100::/64 prefixlen >= 64                # Discard-Only [RFC6666]
2001:2::/48 prefixlen >= 48              # BMWG [RFC5180]
2001:10::/28 prefixlen >= 28             # ORCHID [RFC4843]
2001:db8::/32 prefixlen >= 32            # docu range [RFC3849]
3ffe::/16 prefixlen >= 16                # old 6bone
fc00::/7 prefixlen >= 7                  # unique local unicast
fe80::/10 prefixlen >= 10                # link local unicast
fec0::/10 prefixlen >= 10                # old site local unicast
ff00::/8 prefixlen >= 8                  # multicast
```

Status: **EM USO**

Ação 2: Filtro dos prefixos do IX.br

Rejeição de anúncios que contenham o espaço de endereçamento do AS26162 do IX.br, que deve ser utilizado apenas entre os roteadores de cada localidade.

Mesmo sendo endereços válidos, a rede do IX.br NÃO DEVE ser anunciada. Endereços válidos são utilizados para facilitar o trabalho de investigação de problemas de conectividade e/ou roteamento (*troubleshooting*).

Status: **EM USO**

Ação 3: Filtro de ASNs BOGONs

Rejeição de anúncios que contenham ASNs reservados (BOGONs) em qualquer parte do AS-PTH:

16 bits

0	# RFC 7607
23456	# RFC 4893 AS_TRANS
64496 a 64511	# RFC 5398 and documentation/example ASNs
64512 a 65534	# RFC 6996 Private ASNs
65535	# RFC 6996 Last 16 bit ASN
65536 a 65551	# RFC 5398 and documentation/example ASNs
65552 a 131071	# IANA reserved ASNs

32 bits

4200000000 a 4294967294	# RFC 6996 Private ASNs
4294967295	# RFC 6996 Last 32 bit ASN

Tempo para implementação: **CURTO**

Ação 4: Filtro de TIER-1 no AS-PTH

Rejeição de anúncios que contenham ASNs de redes conhecidas como tendo trânsito livre, tipicamente os TIER-1:

174 - Cogent
209 - Centurylink
701 - Verizon
702 - Verizon
1239 - Sprint
1299 - Telia
2914 - NTT
3257 - GTT Communications
3320 - Deutsche Telekom
3356 - Level 3
3549 - Level 3
3561 - Centurylink
4134 - China Telecom
5511 - Orange
6453 - Tata Communications
6461 - Zayo
6762 - Telecom Italia Sparkle
7018 - AT&T
12956 - TIWS

Tempo para implementação: **CURTO**

Ação 5: Proteção aos ASs stubs

ASN stub: ASN brasileiro, participante do ATM do IX.br, anunciando apenas seus próprios prefixos, não existindo outro ASN no AS-PATH

ASN trânsito: participa do ATM do IX.br, anunciando prefixos de outros ASNs, além dos seus. O AS-PATH pode conter múltiplos ASNs.

- ✓ Durante a Quarentena do processo de ativação, serão analisados os anúncios recebidos e feita a classificação do ASN.
- ✓ Para os ASNs em produção, a classificação será baseada na tabela de rotas em vigor na data.
- ✓ A classificação poderá ser alterada através do Portal do Participante do IX.br.
- ✓ Para os ASNs stubs, será aplicado filtro que aceitará apenas os blocos de endereço IP alocados para o ASN (até /24 em IPv4 e /48 em IPv6). Filtro atualizado uma vez ao dia.

Tempo para implementação: **MÉDIO**

Ação 6: Validação via bases de dados externas

Na proposta de política de tratamento de communities BGP no IX.br já havíamos definido marcações (Válidos, Inválidos ou Desconhecidos) aplicadas aos anúncios recebidos de acordo com presquisas realizadas em três tipos de serviços/bases de dados:

RDAP (Registration Data Access Protocol)

- ✓ API para acesso à base de dados do Whois do Registro.br
- ✓ Fundamental que as informações estejam atualizadas, tais como delegações, transferência de blocos, contatos, etc.

Tempo para implementação: **CURTO**

Ação 6: Validação via bases de dados externas

IRR (Internet Routing Registers)

- ✓ Bases de dados que armazenam políticas de roteamento
- ✓ RPSL (Routing Police Specification Language)
- ✓ São bases de dados distribuidas, operadas por organizações como RIR (Regional Internet Registry), empresas de telecom, etc.
- ✓ Algumas bases tem cópias (espelhos) de outras bases, oferecendo um conjunto de informações mais abrangente
- ✓ Exemplos de IRRs: RADB, ARIN, RIPE, APNIC, TC
- ✓ Fundamental manter as informações atualizadas

! Ponto de atenção: bases IRR podem eventualmente aceitar o registro de informações de outros que não o detentor dos recursos

Ação 6: Validação via bases de dados externas

IRR (Internet Routing Registers)

Proposta de procedimento para geração de filtros (Prefix-list)

- ✓ Obter das bases IRR informações dos ASs que informaram base/ usuário (*mnt-by*) no Portal do Participante do IX.br (Base Prioritária)
- ✓ Manutenção de cache que será utilizado como base local, formado através da sintetização dos dados obtidos de uma lista de bases IRRs espelhadas pelo IX.br
- ✓ Uma vez ao dia a configuração dos filtros a serem aplicados nos route servers será atualizada

RPKI (resource Public Key Infrastructure)

Tempo para implementação: **CURTO**

Ação 6: Validação via bases de dados externas

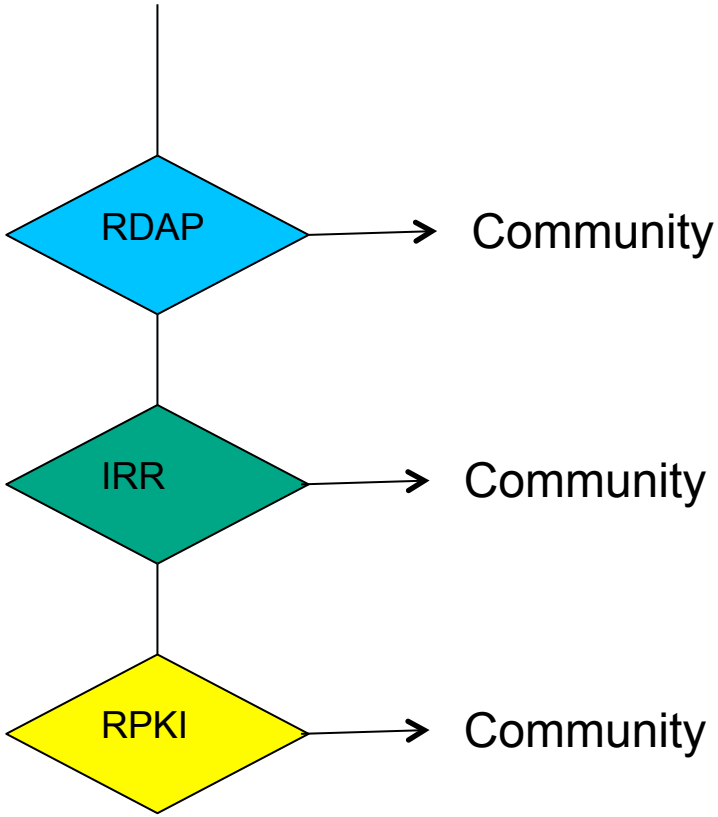
RPKI (resource Public Key Infrastructure)

- ✓ Utiliza infraestrutura de certificados de chaves públicas para dar segurança ao roteamento na Internet
- ✓ Geração de ROAs (Route Origination Authorization) que informa AS está autorizado a originar determinados prefixos, bem como o tamanho máximo do prefixo anunciado

Tempo para implementação: **LONGO**

Ação 6: Validação via bases de dados externas

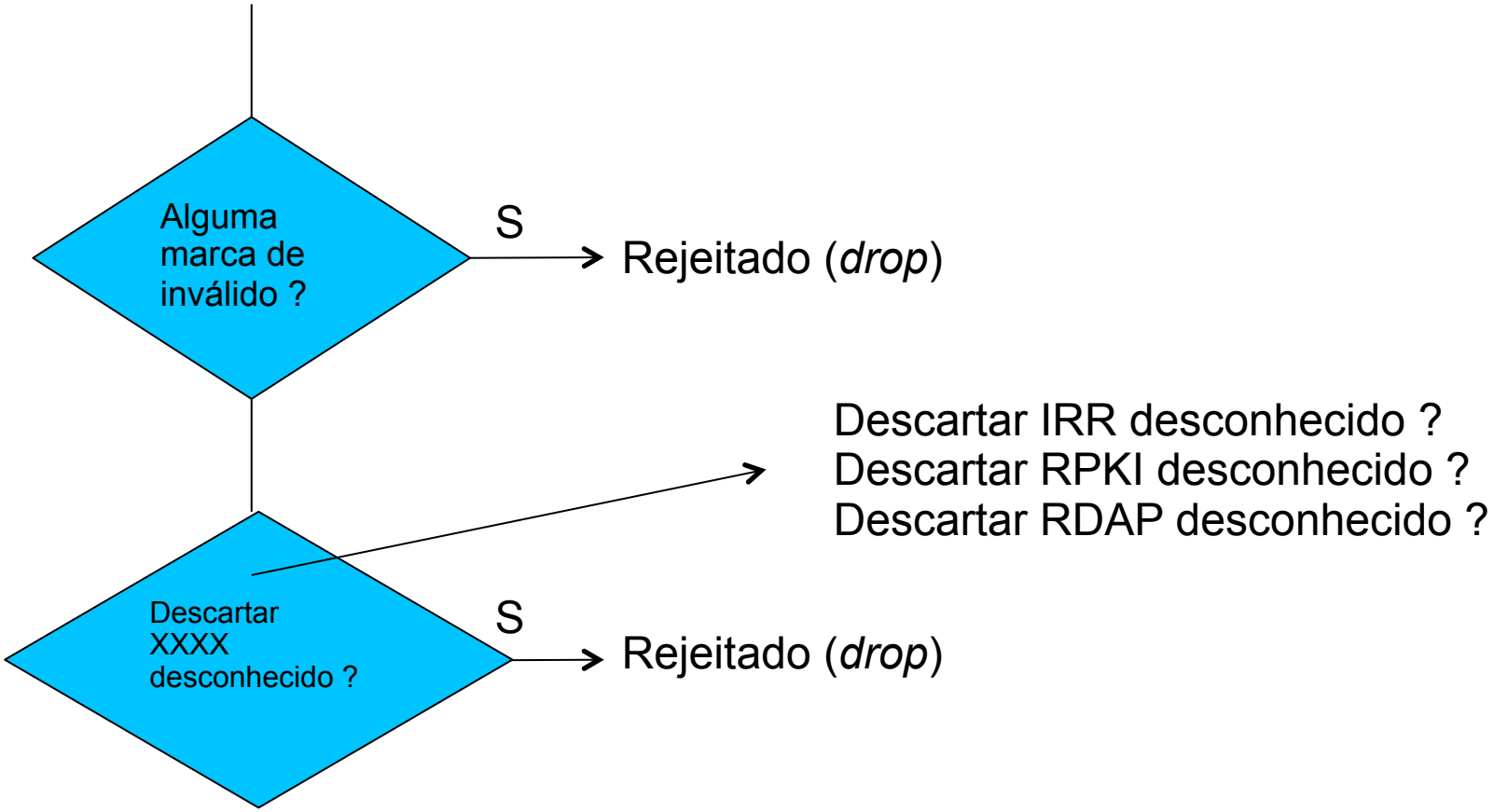
Processo de marcação do anúncio



Tempo para implementação: **LONGO**

Ação 6: Validação via bases de dados externas

Filtragem pelo Route Server



Tempo para implementação: **CURTO**

Ação 7: Visibilidade do processo de filtragem de anúncios

- ✓ Serviço de Looking Glass Web, hoje acessível através do Portal do Participante, irá mostrar o resultado do processo de marcação por communities descrito na Ação 6
- ✓ O que será visualizado é a tabela de rotas antes do processo e filtragem do Route Server.

Tempo para implementação: **CURTO**

Ação 8: Análise do AS-SET

- ✓ Uma lista de ASNs que podem anunciar os prefixos de um AS podem ser cadastrada em um IRR utilizando-se a linguagem RPSL
- ✓ O AS deverá informar no Portal do Participante se o AS-SET deverá ou não ser consultado, bem como qual a política a ser adotada para o descarte de anúncios
- ✓ Durante a importação dos anúncios, o Route Server consulta o AS-SET definido pelo AS, otendo como resultado Válido, Inválido ou Desconhecido
- ✓ Uma community será inserida no anúncio, refletindo o resultado da consulta, nos moldes do utilizado na Ação 6
- ✓ No PeeringDB existe um campo denominado IRR Record, onde pode ser informado o AS-SET ou sua designação.

Tempo para implementação: **LONGO**

Cronograma de atividades da Solicitação de Comentários

1) Publicação no site do IX.br da primeira versão do documento: 04/05/18.
2) Apresentação à comunidade: no IX Fórum Regional de São Paulo, no dia 17/05/2018, e na reunião GTER 45, em 22/05/2018.
3) Recepção de comentários através da lista de e-mails da GTER: até 04/06/18.
4) Análise, preparação e publicação no site do IX.br da segunda versão do documento, com a inclusão de sugestões da comunidade: 11/06/18.
5) Recepção de comentários através da lista de e-mails da GTER: até 25/06/18.
6) Publicação da versão final do documento com as ações a serem implementadas: 02/07/18.

Obrigado(a)

www.site.br

jsirota@nic.br @ComuNICbr Facebook.com/nic.br/

22 de maio de 2018

nic.br cgi.br

www.nic.br | www.cgi.br