



**nic.br**

Núcleo de Informação  
e Coordenação do  
Ponto BR

**egi.br**

Comitê Gestor da  
Internet no Brasil

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

nic.br egi.br

registro.br

IX FÓRUM 12  
São Paulo, SP | 11/12/18

# ATUALIZAÇÕES SOBRE A INICIATIVA POR UMA INTERNET MAIS SEGURA

Gilberto Zorello

gzorello@nic.br

registro.br nic.br cgi.br

# Agenda

- Programa por uma Internet mais segura – Gilberto Zorello
  - Iniciativa e Plano de Ação
  - Desenvolvimento do Programa
  - Outras ações importantes
- MANRS - Christian O'Flaherty
  - Por que? como? ISPs?
  - MANRS IXPP ( IX Partnership Program)
  - Próximos passos: MANRS Observatory, MANRS LAB
- Requisitos Mínimos para Aquisição de CPEs - Lucimara Desiderá
- Ações no IX – Júlio Sirota
- Status das Associações de Operadoras e ISPs sobre o Programa:
  - SindiTeleBrasil - Alex Castro
  - ABRANET - Eduardo Parajo
  - ABRINT - Basílio Perez

# **Ações para resolver os problemas de segurança e estabilidade na infraestrutura da Internet**

# Programa por uma Internet mais Segura Iniciativa

Lançado pelo CGI.br e NIC.br

## Painel do IX Fórum 11 em dez/17



Apoio: Internet Society, ABRANET, SindiTelebrasil, ABRINT

**Objetivo** - atuar em apoio à comunidade técnica da Internet para:



- **Redução de ataques de Negação de Serviço originados nas redes brasileiras**
- Reduzir **Sequestro de Prefixos, Vazamento de Rotas e Falsificação de IP de Origem**
- **Redução das vulnerabilidades e falhas de configuração presentes nos elementos da rede**
- Aproximar as diferentes equipes responsáveis pela segurança e estabilidade da rede
- **Criar uma cultura de segurança**

# Programa por uma Internet mais Segura

## Plano de Ação

Para solucionar os problemas de segurança, as ações devem ser realizadas pelos operadores dos Sistemas Autônomos, com apoio no NIC.br

### Ações coordenadas a serem executadas pelo NIC.br:

- Conscientização por meio de palestras, cursos e treinamentos
- **Criação de materiais didáticos e boas práticas**
- Interação com **Associações de Provedores** e seus afiliados para disseminação da **Cultura de Segurança**, adoção de **Melhores Práticas** e **mitigação** de problemas existentes:
  - **especificação, configuração e operação de CPEs em suas respectivas redes**
  - implantação das ações básicas para melhorar a Segurança de Roteamento, preconizadas pelo **MANRS**
- **Implementação de filtros de rotas no IX.br, que contribui para a melhora do cenário geral**
- Estabelecimento de métricas e acompanhamento da efetividade das ações



# Programa por uma Internet mais Segura

## **Desenvolvimento do Programa**

# Programa por uma Internet mais Segura

## Desenvolvimento do Programa - Cursos

- **Curso de Boas Práticas Operacionais p/ Sistemas Autônomos – BCOP**
  - Funcionamento da Internet, papel dos ASs, uso do endereçamento IP, boas práticas de roteamento e **segurança**, engenharia de tráfego, **hardening de equipamentos e prática em laboratório**
  - Este curso foi reestruturado de acordo com as premissas do Programa e do MANRS
  - Oferecido na semana do IX Fórum: dez cidades ao ano em todo o Brasil
  - Cursos já oferecidos: São Paulo, Teresina, Belo Horizonte, Goiânia, Aracaju, Salvador, Florianópolis, Porto Alegre: **251** alunos certificados
- **Tutorial LACNIC 30 – Rosário / Argentina - 9/18**
- Tutorial GTER 45 Florianópolis - 5/18

# Programa por uma Internet mais Segura

## Desenvolvimento do Programa - Palestras

- **Palestras sobre o Programa e MANRS:**
  - GTER 45 Florianópolis – 5/18
  - **ABRINT 2018 - 5/18**
  - Encontro Nacional ABRINT 2018 - 6/18
  - **Congresso da Sociedade Brasileira de Computação - 7/18**
  - Congresso RTI - Ribeirão Preto - 8/18
  - **Eventos Regionais REDETELESUL 2018 – Londrina – 8/18**
  - ABRINT na Estrada – Cascavel – 9/18
  - **Futurecom 2018 – 10/18**
  - Evento com Associações de ISP – 10/18
  - **VIII Fórum da Internet Brasil – 11/18**
  - Eventos Regionais REDETELESUL 2018 – Curitiba – 11/18
  - ABRINT na Estrada – Rio de Janeiro – 6/12

# Programa por uma Internet mais Segura

## Desenvolvimento do Programa - Operadoras

### Ações diretas do Programa por uma Internet mais Segura:

- **Reuniões técnicas com grandes operadoras (VIVO, CLARO, OI, TIM, ALGAR, SERCOMTEL):**
  - **Alinhamento com as Ações do MANRS**
    - Filtro de anúncios de entrada e saída
    - **Antispoofing**
    - Pontos de contato
    - **Cadastro de políticas de Roteamento em bases externa.**
  - **Fechamento de endereços IPs abertos para a Internet e abusáveis:**
    - **Em mar/18 – 725k IPs abertos // Hoje – 340k IPs abertos (- 53%)**
    - **Hoje: 206k grandes operadoras // 134k ISP e AS corporativos**
- **Melhora nos processos para atender às notificações do CERT.br e reduzir os Ips abertos e abusáveis...**

# Panorama Atual

## Endereços IP e ASN notificados pelo CERT.br

month	DNS		SNMP		NTP		SSDP	
	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
2018-01	2.412	61.875	2.130	479.247	823	97.075	888	25.982
2018-02	2.438	72.185	2.324	559.784	849	93.801	778	20.210
2018-03	2.476	63.811	2.278	515.345	844	84.483	544	11.431
2018-04	2.509	66.371	2.280	436.702	850	85.549	794	21.686
2018-05	2.343	65.270	2.390	502.861	870	88.788	846	23.174
2018-06	2.629	70.188	2.284	447.411	805	87.408	817	23.340
2018-07	2.721	68.415	2.436	431.907	881	89.484	787	17.255
2018-08	2.459	56.555	2.411	397.622	895	89.353	613	11.855
2018-09	2.767	62.942	2.366	193.432	772	87.378	836	21.836
2018-10	2.806	64.912	2.383	163.987	856	85.911	789	20.233
2018-11	2.604	60.937	2.376	137.331	851	87.155	814	20.124

O Brasil está em **terceiro** lugar entre os endereços IPs abertos para abuso utilizando o protocolo SNMP

Fonte: <https://snmpscan.shadowserver.org/>

# Programa por uma Internet mais Segura

## Desenvolvimento do Programa – ISPs e Indústria

### Ações diretas do Programa por uma Internet mais Segura:

- **Ação com as maiores Associações de Provedores de Internet**
  - ABRANET, ABRINT, Telcomp, InternetSul, RedeTeleSul, AbraHosting, Abramulti
  - Ações de disseminação da **Cultura de Segurança**, adoção de **Melhores Práticas e mitigação** de problemas existentes
  - Desenvolvimento de site do Programa
  - Primeira reunião em 10/18.
- **Ação com a indústria**
  - Incorporação do SIMET com medições de qualidade e BCP 38 em produtos CPEs da indústria nacional e multinacional
  - Aderência dos produtos à recomendação de **Requisitos Mínimos para Aquisição de CPEs** – draft 4 em revisão final

# Programa por uma Internet mais Segura

## **Outras ações importantes divulgadas pelo Programa**

# Programa por uma Internet mais Segura

## Recomendações Adicionais

### Receber e tratar notificações que são enviadas:

- Além de manter os e-mails de contato de **Abuso** e **Roteamento** do ASN no Whois atualizados
- Ajustar os procedimentos internos para tratamento das notificações de abuso e segurança e notificações de roteamento pelas respectivas equipes responsáveis
- **Ação 3 do MANRS**



### Reduzir ataques DDoS saindo de sua rede:

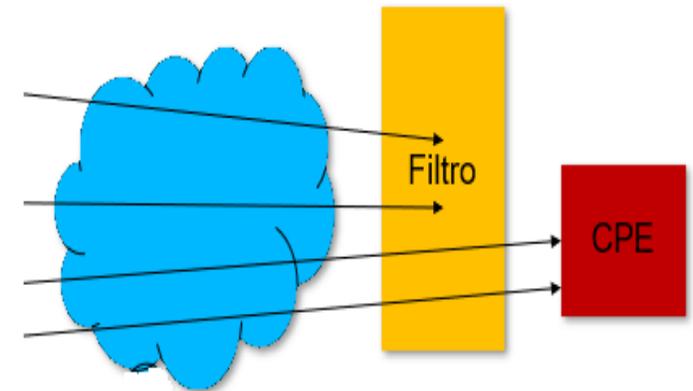
- Análise proativa do tráfego que sai da rede utilizando netflows
- Configurar os CPEs para não ter serviços abertos que permitam amplificação e ter política de senhas seguras (hardening)

# Programa por uma Internet mais Segura

## Recomendações Adicionais

Filtrar **tráfego de entrada** **tráfego de entrada** ou **bloquear comandos** com destino a serviços que permitam amplificação:

- DNS (53/UDP), SNMP (161/UDP), NTP (123/UDP), SSDP (1900/UDP)
- Para gerência de rede, permitir apenas blocos de redes de gerência da própria operadora
- Seguir as ações recomendadas pelo CERT.br nas notificações de ASNs e IPs com serviços abertos, passíveis de serem abusados para gerar ataques de amplificação
- Cuidado com o NTP porque muitos clientes usam a porta 123 UDP também como porta de origem, recebendo respostas nessa porta



# Programa por uma Internet mais Segura

## **SIMET - Sistema de Medição de Qualidade da Internet**

- **SIMET WEB**

- Widget para ISP
- Lista de Provedores

- **SIMET Mobile**

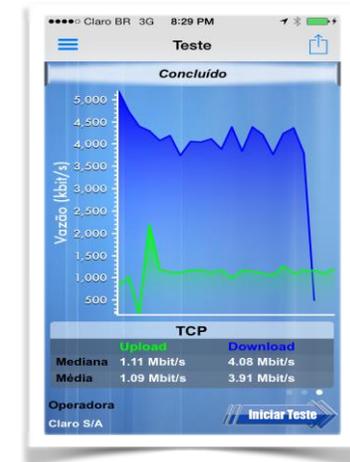
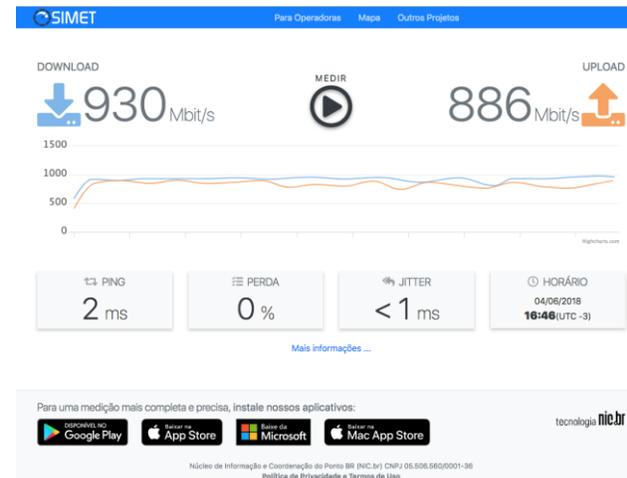
- Android, IOS

- **SIMETBox**

- Testes de Qualidade
- Testes Porta 25
- Teste BCP 38
  - Mesmo IP
  - Mesma rede
  - Outra rede
  - Endereço privado

- **Medições com IPv4 e IPv6**

- **Testes realizados do usuário até um dos PTTs do IX.br, fora da rede medida**



**Obrigado**  
[www.site.br](http://www.site.br)

@ gzorello@nic.br

11 de dezembro de 2018

**nic.br egi.br**

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)