

# *live* Segurança, Troca de Tráfego, Recursos de Numeração e OpenCDN

**Programa por uma Internet mais segura**

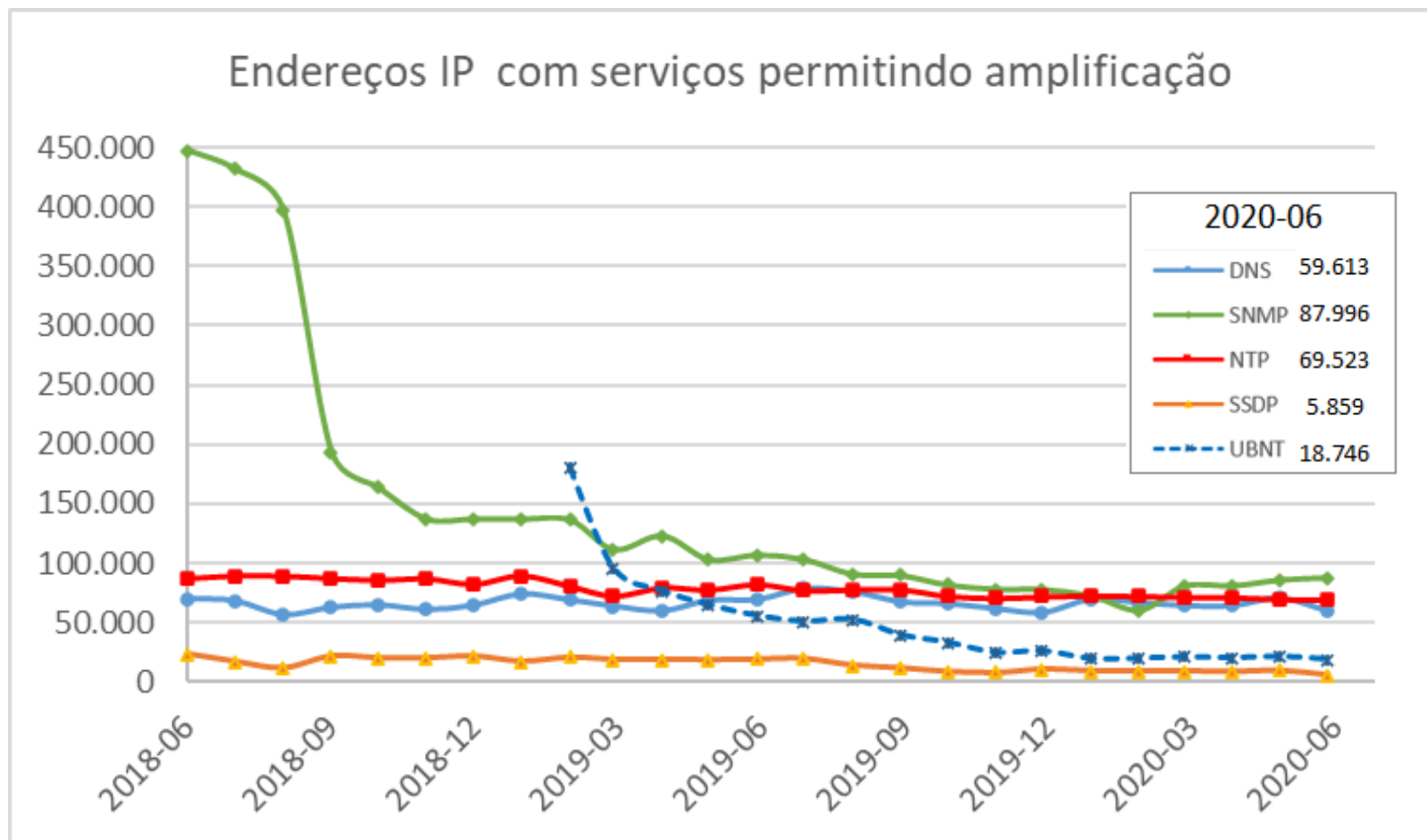
Gilberto Zorello | Júlio Sirota | Ricardo Patara

nic.br cgi.br



# Notificações encaminhadas pelo CERT.br

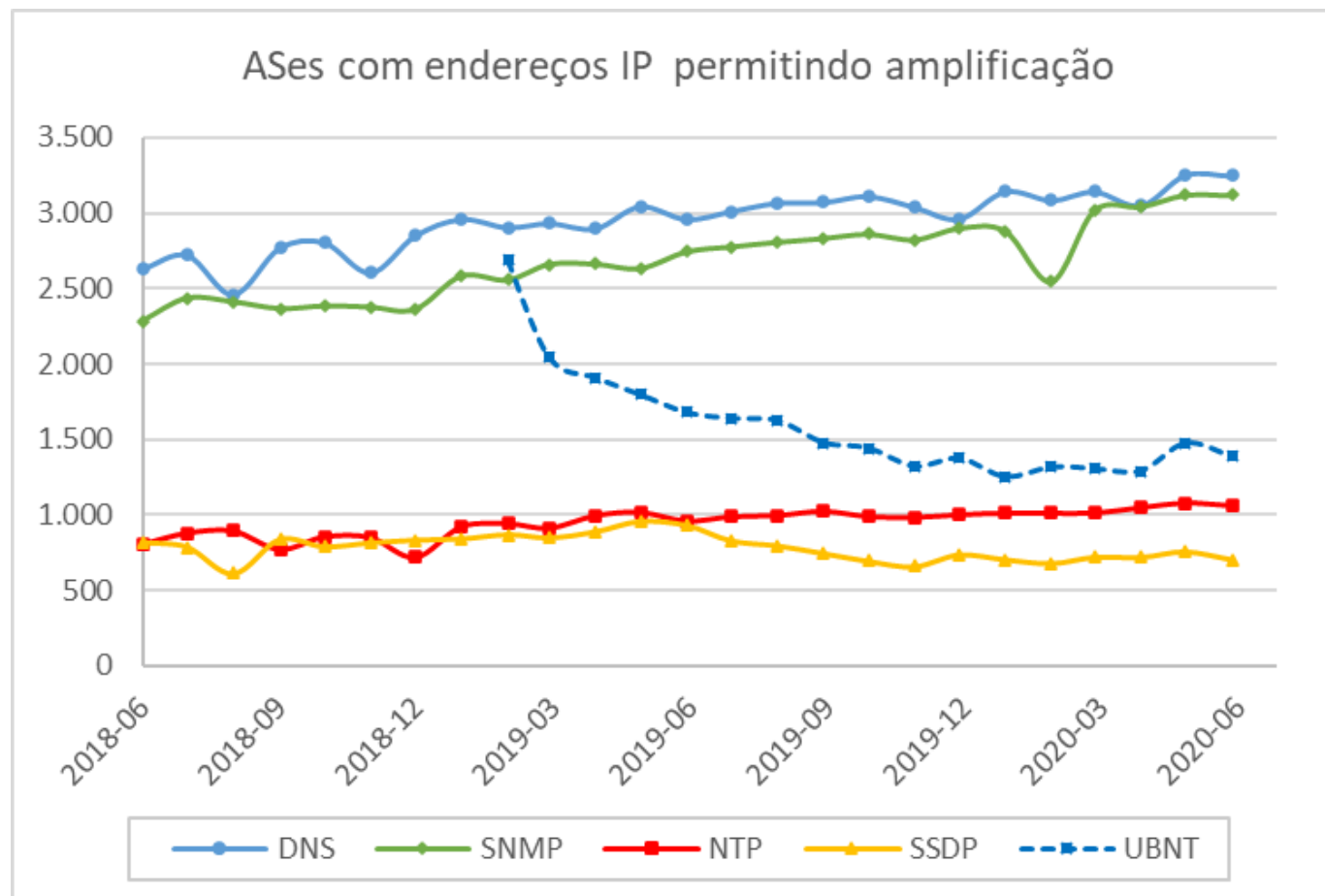
Endereços IP com serviços permitindo amplificação



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

# Notificações encaminhadas pelo CERT.br

Endereços IP com serviços permitindo amplificação

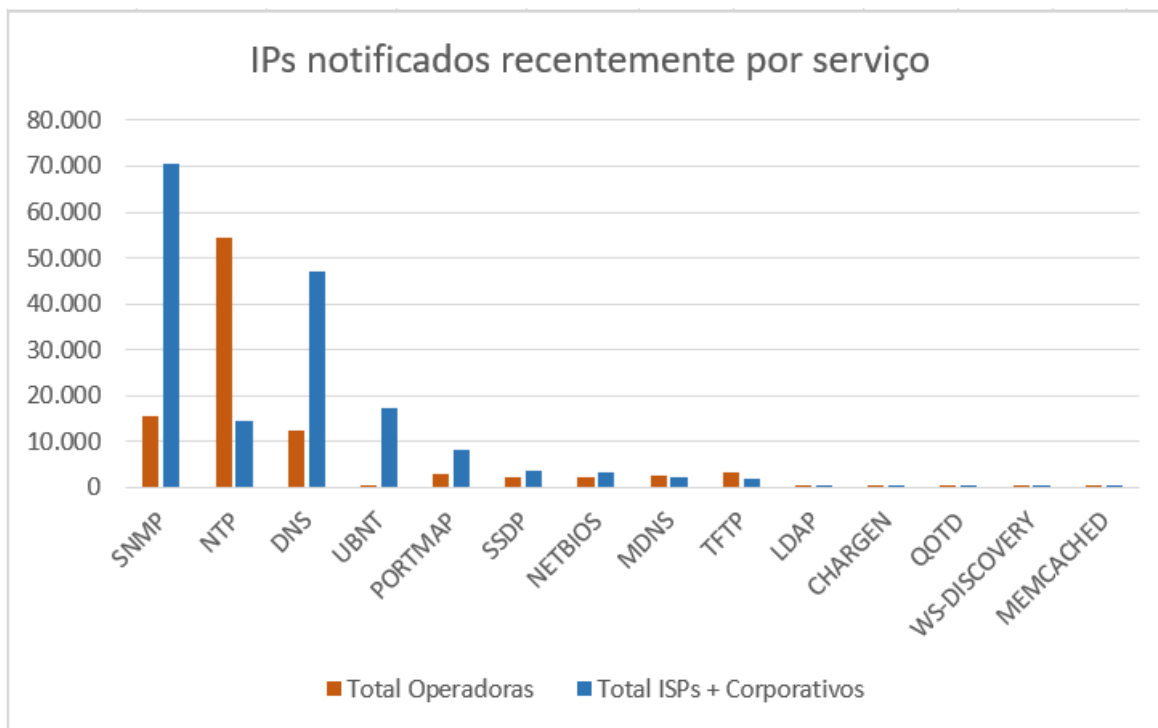


<https://bcp.nic.br/i+seg/acoes/amplificacao/>



# Notificações encaminhadas pelo CERT.br

Endereços IP notificados com serviços mal configurados



**Principais ofensores:**

**ISPs e ASes corporativos →  
SNMP, DNS, UBNT e NTP**

**Grandes operadoras →  
NTP, SNMP e DNS**

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



# MANRS

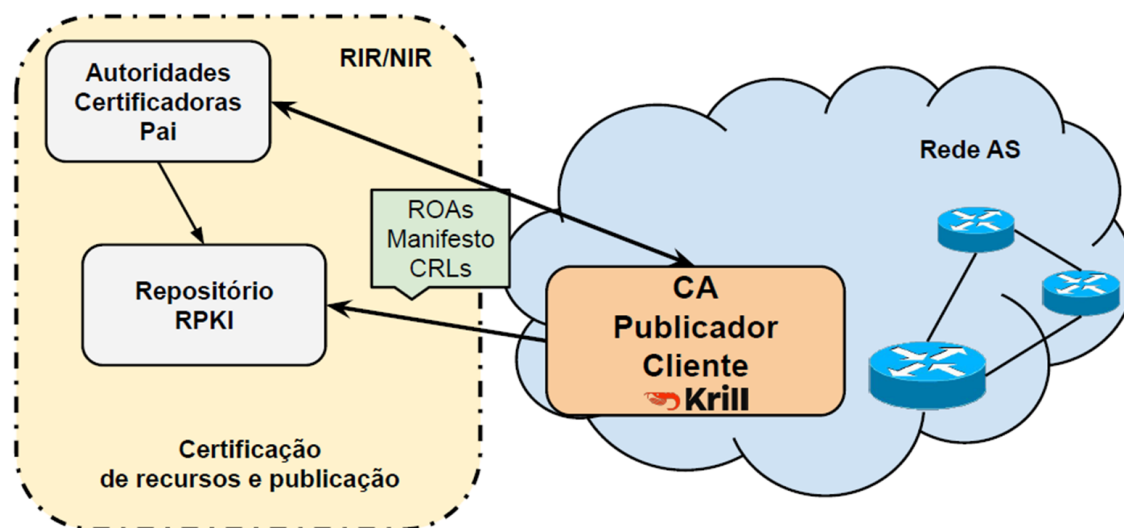
## Mutually Agreed Norms for Routing Security

<http://manrs.org>

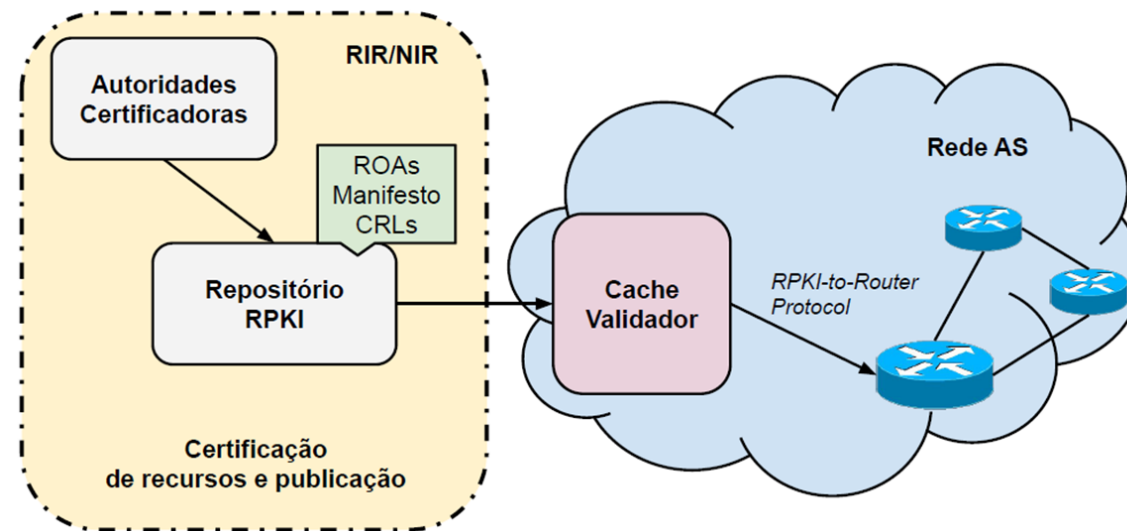
<https://bcp.nic.br/i+seg/acoes/manrs/>

# RPKI - Resource Public Key Infrastructure

## PUBLICAÇÃO DE ROAs



## VALIDAÇÃO



<https://bcp.nic.br/rpki>

<https://registro.br/tecnologia/numeracao/rpki/>

# Hardening

**Analisar vulnerabilidades, mapear as ameaças, mitigar e minimizar riscos e aplicar medidas corretivas**

- Autenticação
- Autorização
- Acesso
- Auditoria
- Sistema
- Registros
- Configurações

<https://bcp.nic.br/i+seg/acoes/hardening/>



# Minimum security requirements for CPEs acquisition

Publicação conjunta:

- M<sup>3</sup>AAWG - Messaging, Malware and Mobile Anti-Abuse Working Group
- LACNOG - Latin American and Caribbean Network Operators Group
- Editora: Lucimara, LAC-AAWG Chair / CERT.br

Um *checklist* de referência para aquisição de equipamentos que permitam atualização e gerenciamento remoto, e que sejam nativamente mais seguros, visando:

- Redução dos riscos de comprometimento da rede do provedor e da Internet como um todo
- Redução dos custos e perdas resultantes do abuso dos equipamentos por invasores: degradação ou indisponibilidade de serviços, suporte técnico e trabalho de reparo

<https://www.m3aawg.org/CPESecurityBP>

<https://www.m3aawg.org/CPESecurityBP-Portuguese>



**Documento conjunto LACNOG-M3AAWG:**  
**Melhores Práticas Operacionais Atuais**  
**sobre Requisitos Mínimos de Segurança para**  
**Aquisição de Equipamentos para Conexão de Assinante (CPE)**  
**LAC-BCOP-1**  
**Maio 2019**

Este documento está disponível no site do LACNOG em [www.lacnog.net/docs/lac-bcop-1](http://www.lacnog.net/docs/lac-bcop-1)

Este documento está disponível no site do M3AAWG em [www.m3aawg.org/CPESecurityBP-Portuguese](http://www.m3aawg.org/CPESecurityBP-Portuguese)

A versão original em Inglês está disponível no site do M3AAWG em [www.m3aawg.org/CPESecurityBP](http://www.m3aawg.org/CPESecurityBP)

Este é um documento conjunto de Melhores Práticas Operacionais Atuais (*Best Current Operational Practices*, BCOP) desenvolvido pelo LACNOG; (Grupo de Operadores de Redes da América Latina e o Caribe) e pelo M3AAWG; (Messaging, Malware and Mobile Anti-Abuse Working Group). É o produto das versões originais do LACNOG por seus grupos de trabalho LAC-AAWG; (Grupo de Trabalho Antiabuso da América Latina e o Caribe) e Grupo de Trabalho BCOP, em cooperação com membros do M3AAWG, Assessores Técnicos Sêniores e o Comitê Técnico do M3AAWG.

## Índice

|                                                                                                       |    |
|-------------------------------------------------------------------------------------------------------|----|
| Sumário Executivo .....                                                                               | 2  |
| 1. Terminologia .....                                                                                 | 2  |
| 2. Requisitos Gerais ( <i>General Requirements – GR</i> ) .....                                       | 3  |
| 3. Requisitos de Segurança de Software ( <i>Software Security Requirements – SSR</i> ) .....          | 4  |
| 4. Requisitos de Atualização e Gerenciamento ( <i>Update and Management Requirements – MR</i> ) ..... | 4  |
| 5. Requisitos Funcionais ( <i>Functional Requirements – FR</i> ) .....                                | 5  |
| 6. Requisitos de Configuração Inicial ( <i>Initial Configuration Requirements – IR</i> ) .....        | 7  |
| 7. Requisitos do Fornecedor ( <i>Vendor Requirements – VR</i> ) .....                                 | 8  |
| 8. Lista de Acrônimos .....                                                                           | 8  |
| 9. Agradecimentos .....                                                                               | 9  |
| 10. Referências Informativas .....                                                                    | 9  |
| Anexo 1 – Tabela de Requisitos .....                                                                  | 11 |

<sup>1</sup> Grupo de Operadores de Redes da América Latina e o Caribe (LACNOG), <https://www.lacnog.net/>

<sup>2</sup> Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), <https://www.m3aawg.org/>

<sup>3</sup> Grupo de Trabalho Antiabuso da América Latina e o Caribe (LAC-AAWG), <https://www.lacnog.net/lac-aawg/>

<sup>4</sup> Grupo de trabalho BCOP, <https://www.lacnog.net/vg-bcop/>

**LACNOG**

Grupo de Operadores de Redes da América Latina e o Caribe  
Departamento de Montevideo, República Oriental do Uruguai  
[www.lacnog.net](http://www.lacnog.net)

**M3AAWG**

Messaging, Malware and Mobile Anti-Abuse Working Group  
781 Beach Street, Suite 302  
San Francisco, California 94109 U.S.A. – [www.m3aawg.org](http://www.m3aawg.org)