

# Rede de sensores distribuídos do CAIS

Edilson Lima

5º Fórum brasileiro de CSIRTs

# Agenda



**Apresentação**



**O Projeto**



**Principais números**

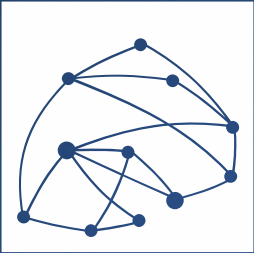


**Integração com o sistema SGIS**



**Encerramento**

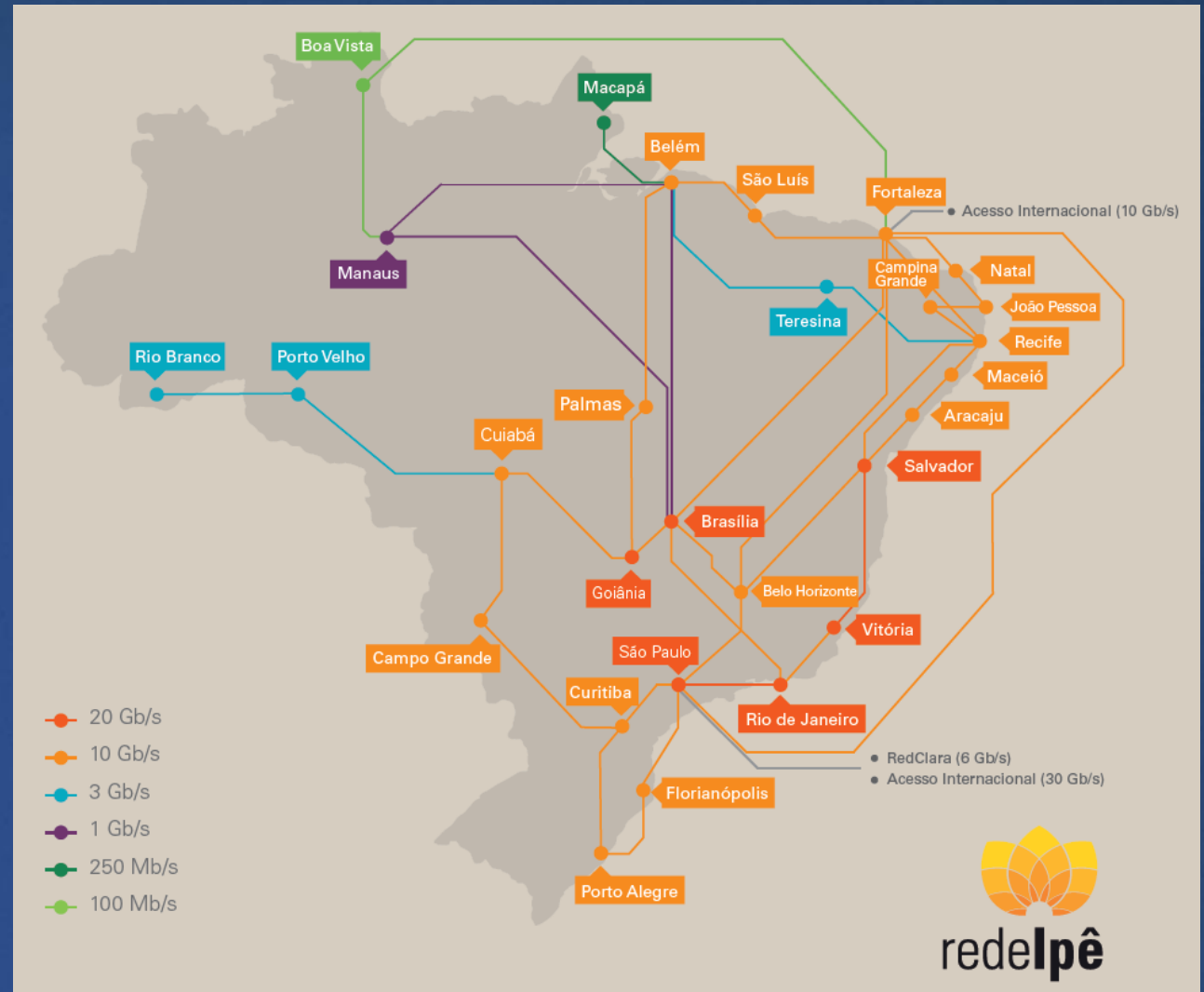
# Apresentação



# RNP

Rede Nacional de Ensino e Pesquisa (RNP), criada pelo MCTI em 1989, para construir uma infraestrutura de internet acadêmica.

Desde então, participa do desenvolvimento da internet no Brasil, com a introdução de novas tecnologias e a implantação da primeira rede óptica acadêmica da América Latina, em 2005, batizada de Ipê.



## Apresentação



CSIRT de coordenação da rede acadêmica brasileira, a Rede Ipê, desde 1997.

Atua na detecção, resolução e prevenção de incidentes de segurança de rede, além de elaborar, promover e disseminar práticas de segurança na RNP e instituições a ela vinculadas.

## Projeto - Contexto

**Rede Ipê, backbone da rede acadêmica.  
Capacidade integrada de 345,45 Gb/s.**

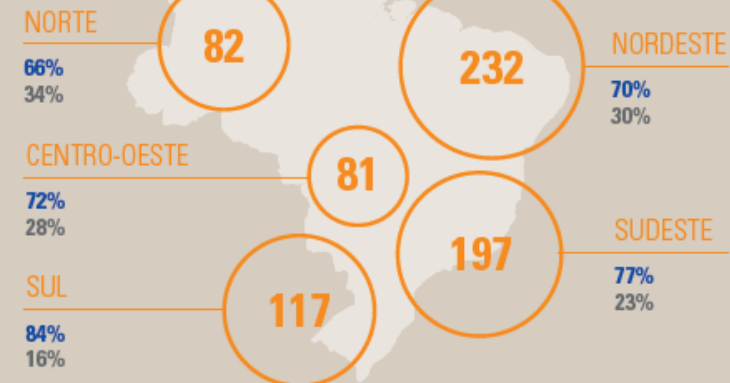
**Interliga 1.237 *campi* de Organizações Usuárias  
(IFs, IFEs, Unidades de Pesquisa).**

**Ambiente altamente diversificado em redes,  
tecnologias e maturidade das equipes de segurança.**

**Dificuldades para uma detecção eficiente.**

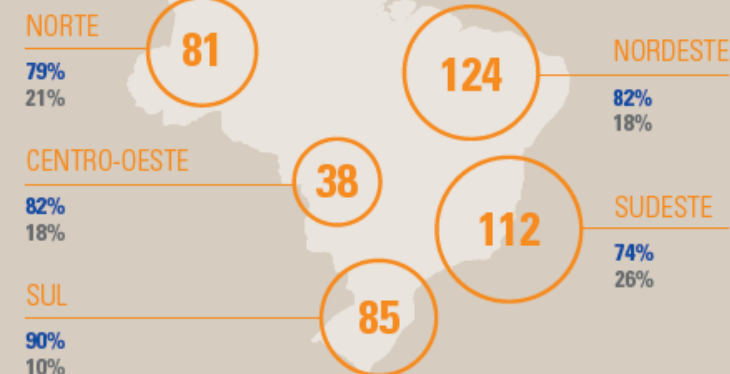
### **CAMPI** INSTITUTOS FEDERAIS

**Total: 709**



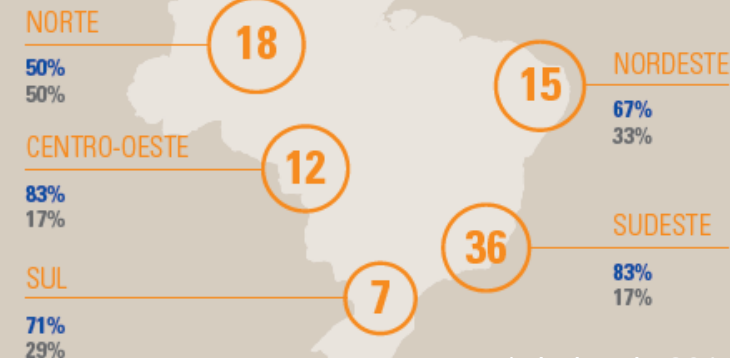
### **CAMPI** INSTITUTOS FEDERAIS DE ENSINO SUPERIOR

**Total: 440**



### **UNIDADES DE PESQUISA**

**Total: 88**



## Projeto - Objetivo

Criar uma rede se sensores na rede acadêmica.

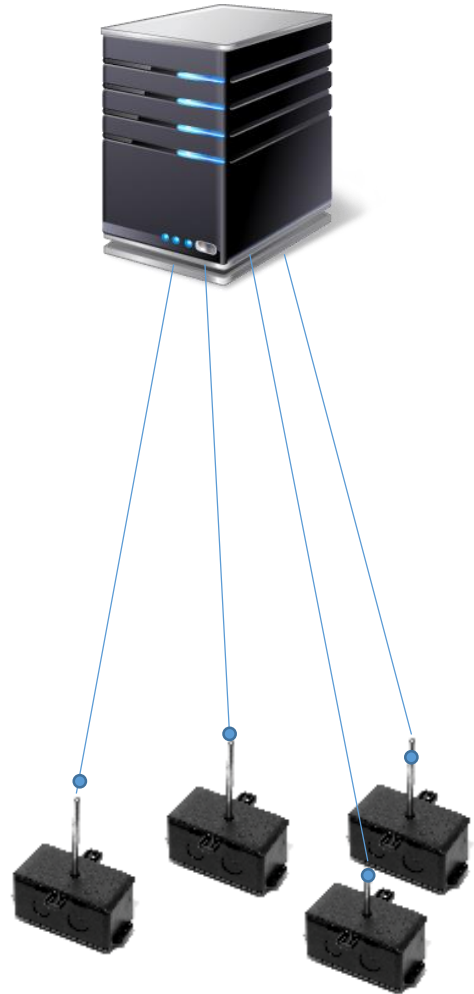


# Projeto - O sistema



# Projeto - O sistema

Master



Sensor

## Sensores Distribuídos CAIS/RNP

HOME INSTITUIÇÕES SENSORES ATUALIZAÇÕES RELATÓRIOS ADMINISTRAÇÃO LOGOUT

### Sensores distribuídos - MASTER

Bem vindo ao gerenciador de sensores distribuídos

Tarefas comuns:

- [Cadastrar novo sensor](#)
- [Inserir atualizações de regras](#)
- [Ver relatórios](#)
- [Mapa geral de incidentes](#)

#### TOP TALKERS

Instituição	Sensor	Qtde
[REDACTED]	200 [REDACTED]	2236075
[REDACTED]	200 [REDACTED]	1402551
[REDACTED]	200 [REDACTED]	1201383
[REDACTED]	200 [REDACTED]	1101994
[REDACTED]	200 [REDACTED]	775189

#### TOP INCIDENTES

Evento	Qtde	Porcentagem
2101867	8443279	29.0%
2017921	895943	7.55%
2001569	763299	6.43%
2017318	555843	4.68%

Sensor de atividade maliciosa - CAIS/RNP

Por favor, escolha uma opcao:

- 1 Configurar rede
- 2 Selecionar interface coletora
- 3 Configurar DNS
- 4 Inserir chave de registro
- 5 Gerenciar o servico IDS
- 6 Gerenciar o crond da ENGINE
- 7 Configurar o NTP da ENGINE
- 8 Checar update
- 9 Diagnostico
- 10 Sobre

< OK > <<Cancel>



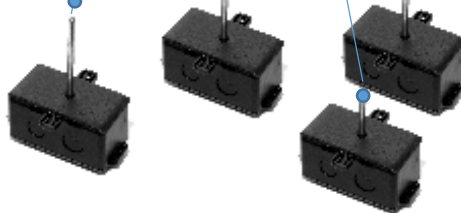
## Projeto - O sistema

Master



- Gerenciamento dos sensores e instituições
- Gerenciamento das atualizações
- Estatísticas do sistema geral e dos sensores
- Classificação das atividades maliciosas
- Administração geral do sistema

Sensor

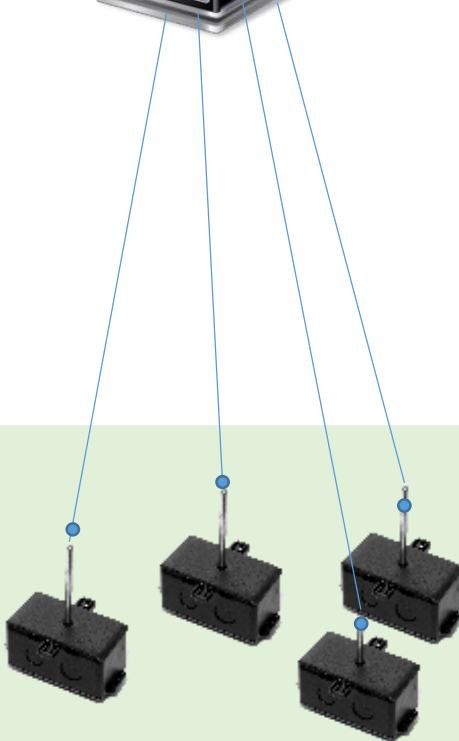


# Projeto - O sistema

Master



Sensor



- Interface friendly user
- Plug and play
- Exige pouco conhecimento técnico
- Pouca manutenção e suporte
  - Envio das detecções por e-mail
  - Envio de dados estatísticos e de status
  - Solicitação de atualizações

# Projeto - O sistema

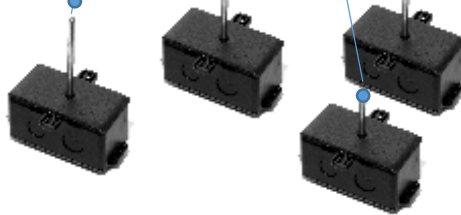
Master



Conexão

- HTTPS
- Autenticação

Sensor

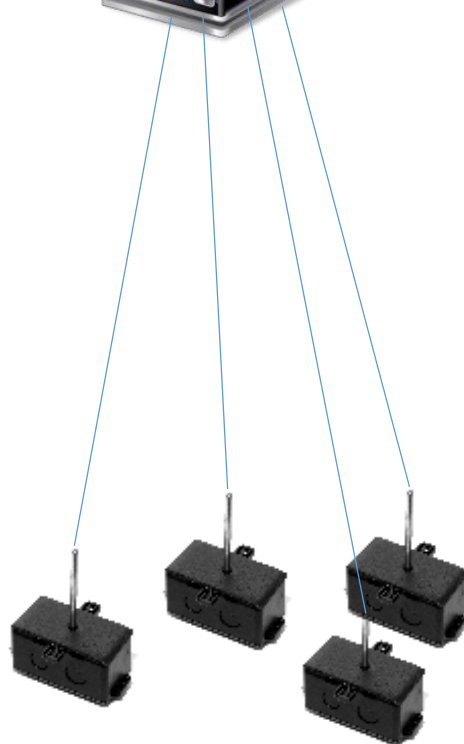


# Projeto - O sistema

Master



Sensor



## Tipos de atualizações

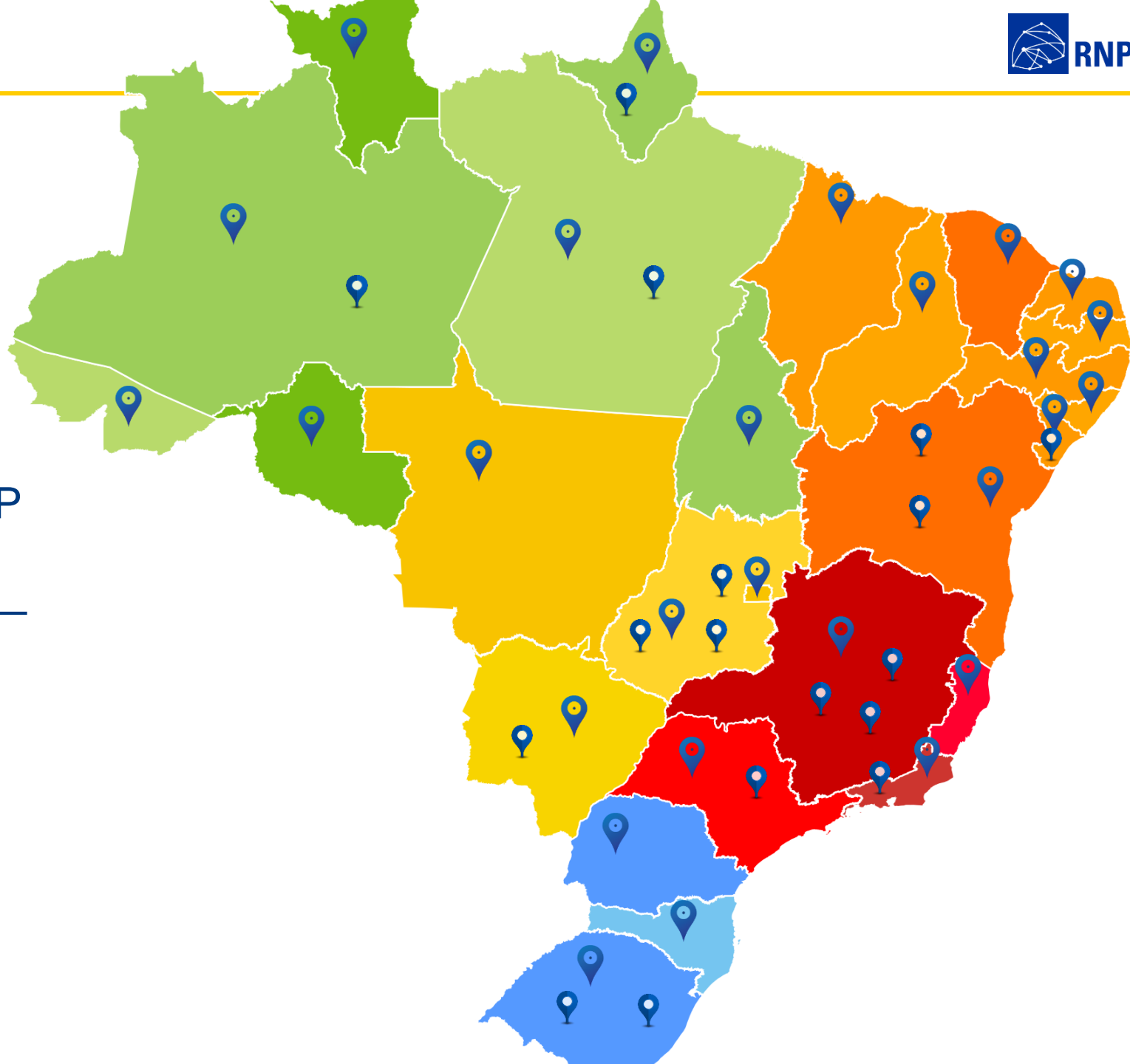
Tipo	Finalidade
Regras gerais	Prover as regras gerais.
Regras customizadas	Prover regras específicas, sob demanda.
Exceções de regras	Desativar regras, sem a necessidade de gerar nova release.
Blacklist URLs	Identificar acessos a URLs maliciosas
Blacklist de IPs	Identificar acessos a IPs maliciosos, como C&C.
Redes	Cada cliente possui sua própria rede, portanto a HOME_NET de cada um deve ser única, para maior assertividade.
Atualizações de Sistema	Novas versões do sensor, correções e features.

## Projeto - Implantação

- ✓ 27 Pontos de Presença da RNP
- ✓ 17 Organizações Usuárias

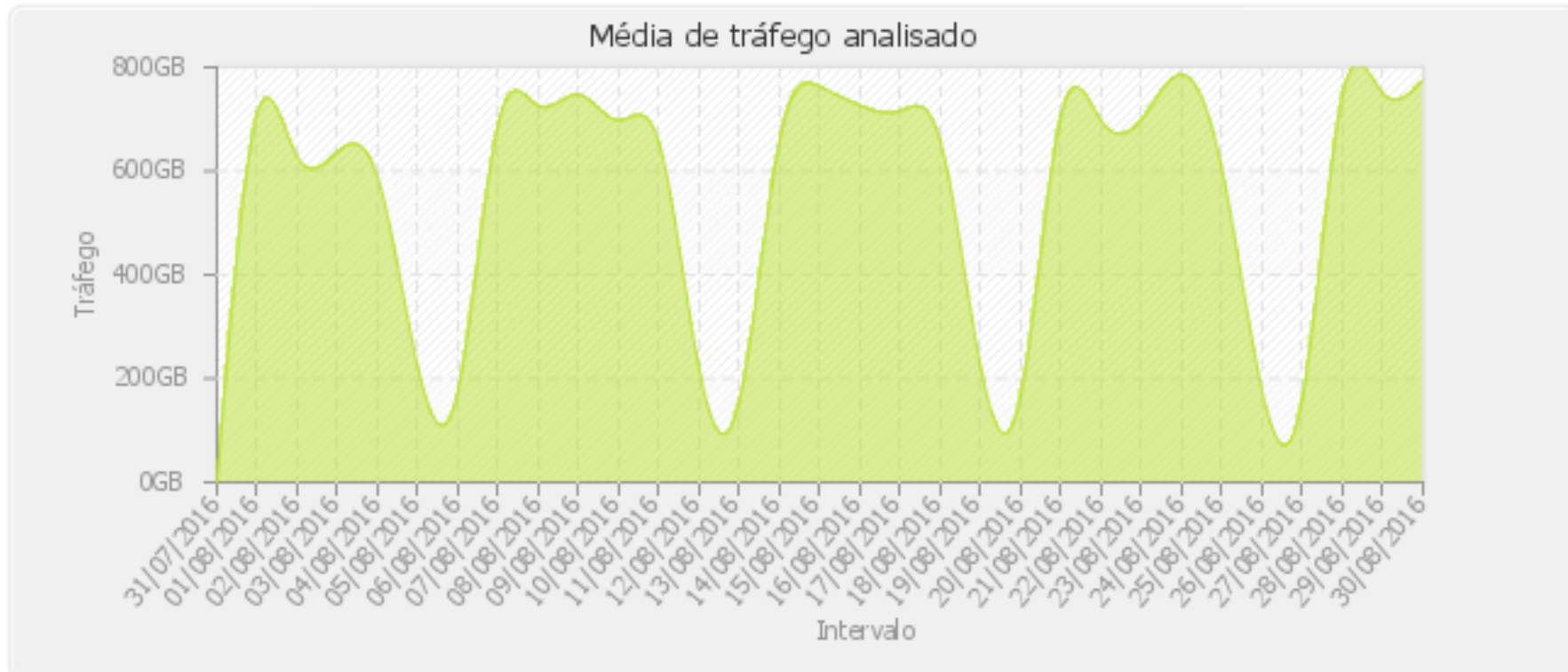
---

**44 Sensores Instalados**



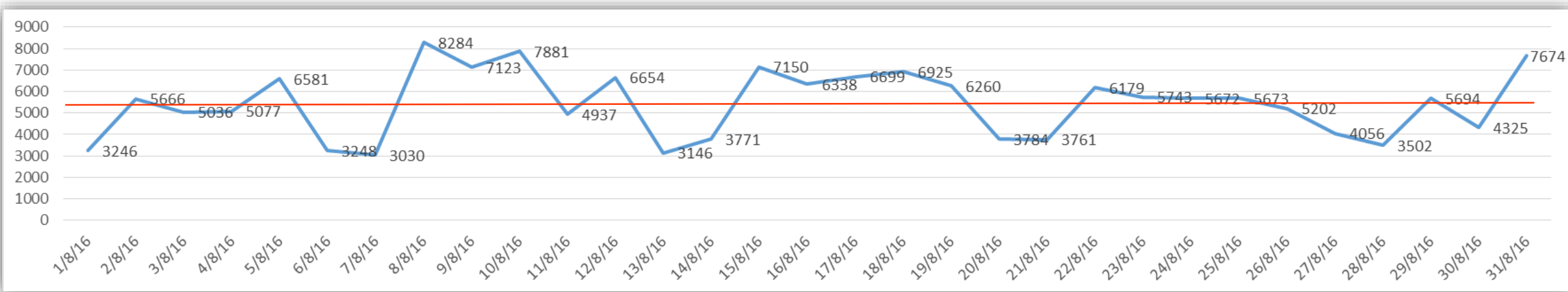
# Principais números

## Tráfego analisado



# Principais números

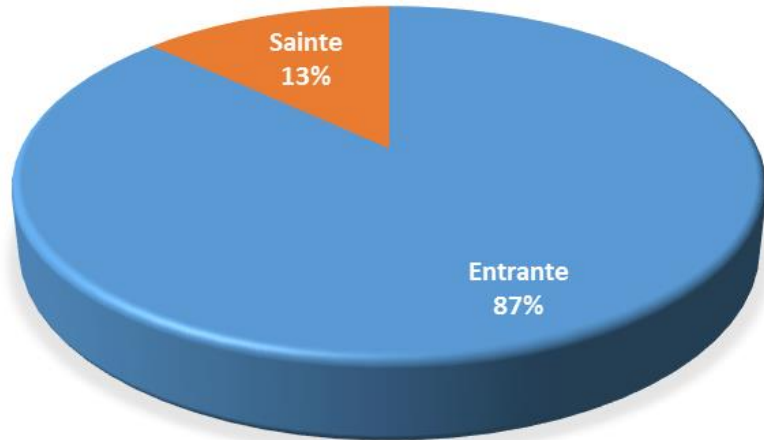
## Quantidade de detecções x dia



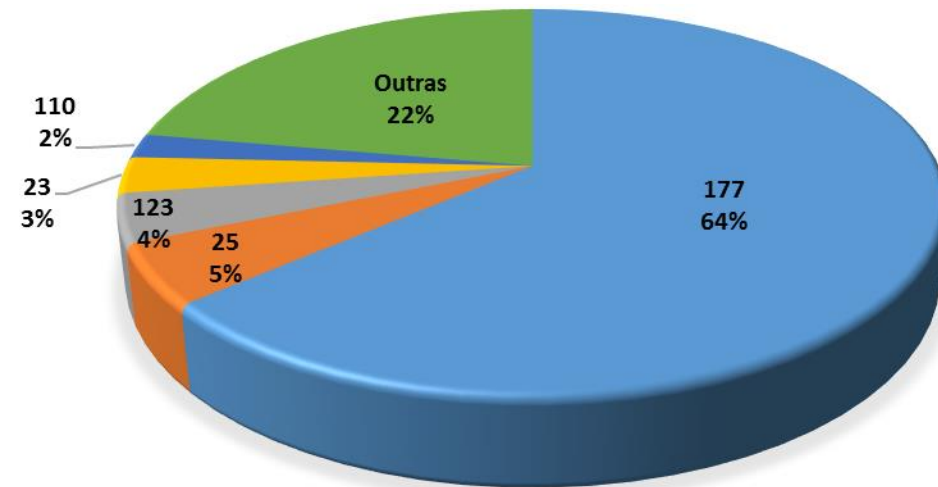
----- Média: 5.430

# Principais números

## Fluxo da atividade maliciosa



## Portas utilizadas





# Principais números

## Principais atividades maliciosas detectadas

```
[*] Generating module info table, hang on...
- Processing modules
- Done. Let's rock 'n roll.

Module info :
-----
Base      Top      Size     Rebase   SafeSEH  ASLR     NXCompat  OS Dll  Version, Modulename & Path
-----
0x77b20000 0x77b32000 0x00012000 False    True     False    True    5.1.2600.5512 [MSASNI.dll] (C:\WINDOWS\system32\MSASNI.dll)
0x00570000 0x005F0000 0x00080000 True     True     False    False   -1.0- [SDL.dll] (C:\Program Files\AudioCoder\SDL.dll)
0x77c10000 0x77c22000 0x00012000 False    True     False    True    5.00.2900.5512 [CONDL32.dll] (C:\WINDOWS\system32\CONDL32.dll)
0x77c50000 0x77c62000 0x00012000 False    True     False    True    5.1.2600.5512 [NETAPI32.dll] (C:\WINDOWS\system32\NETAPI32.dll)
0x77c90000 0x77ca1000 0x00011000 False    True     False    True    5.1.2600.5512 [urlmon.dll] (C:\WINDOWS\system32\urlmon.dll)
0x77cb0000 0x77cc2000 0x00012000 False    True     False    True    5.1.2600.5512 [image.dll] (C:\Program Files\AudioCoder\SDL\image.dll)
0x77ce0000 0x77cf4000 0x00014000 False    True     False    True    5.131.2600.5512 [CRVPT32.dll] (C:\WINDOWS\system32\CRVPT32.dll)
0x77d10000 0x77d25000 0x00015000 True     True     False    True    5.1.2600.5512 [xpsp2res.dll] (C:\WINDOWS\system32\xpsp2res.dll)
0x77d40000 0x77d56000 0x00016000 True     True     False    True    1.0.0.402 [SysInfo.dll] (C:\Program Files\AudioCoder\SysInfo.dll)
0x77d80000 0x77d96000 0x00016000 True     True     False    True    5.1.2600.5512 [nsviewr.dll] (C:\WINDOWS\system32\nsviewr.dll)
0x77db0000 0x77dc9000 0x00019000 False    True     False    False   0.9.22.5506 [AudioCoder.exe] (C:\Program Files\AudioCoder\AudioCoder.exe)
0x77df0000 0x77e04000 0x00014000 False    True     False    True    5.1.2600.5512 [RPCRT4.dll] (C:\WINDOWS\system32\RPCRT4.dll)
0x77e30000 0x77e44000 0x00014000 False    True     False    True    5.1.2600.5512 [ndr11.dll] (C:\WINDOWS\system32\ndr11.dll)
0x77e70000 0x77e84000 0x00014000 False    True     False    True    -1.0- [libxml2.dll] (C:\Program Files\AudioCoder\libxml2.dll)
0x77f10000 0x77f24000 0x00014000 True     True     False    True    5.1.2600.5512 [wshcrtcpip.dll] (C:\WINDOWS\system32\wshcrtcpip.dll)
0x77f40000 0x77f54000 0x00014000 True     True     False    True    8.00.6001.18702 [ieframe.dll] (C:\WINDOWS\system32\ieframe.dll)
0x77f80000 0x77f94000 0x00014000 False    True     False    True    5.1.2600.5512 [sensapi.dll] (C:\WINDOWS\system32\sensapi.dll)
0x77fb0000 0x77fc4000 0x00014000 True     True     False    True    5.1.2600.5512 [RASAPI32.dll] (C:\WINDOWS\system32\RASAPI32.dll)
0x77fd0000 0x77fe4000 0x00014000 False    True     False    True    8.00.6001.18702 [rtutils.dll] (C:\WINDOWS\system32\rtutils.dll)
0x77ff0000 0x78004000 0x00014000 True     True     False    True    5.1.2600.5512 [IMAGEHELP.dll] (C:\WINDOWS\system32\IMAGEHELP.dll)
0x78030000 0x78044000 0x00014000 True     True     False    True    5.1.2600.5512 [rasadhlp.dll] (C:\WINDOWS\system32\rasadhlp.dll)
0x78070000 0x78084000 0x00014000 False    True     False    True    5.1.2600.5512 [Secur32.dll] (C:\WINDOWS\system32\Secur32.dll)
0x780b0000 0x780c4000 0x00014000 True     True     False    True    5.1.2600.5512 [MSOCK32.dll] (C:\WINDOWS\system32\MSOCK32.dll)
0x780f0000 0x78104000 0x00014000 True     True     False    True    8.00.2900.5512 [shdocvw.dll] (C:\WINDOWS\system32\shdocvw.dll)
0x78130000 0x78144000 0x00014000 True     True     False    True    5.1.2600.5512 [MS2HELP.dll] (C:\WINDOWS\system32\MS2HELP.dll)
0x78170000 0x78184000 0x00014000 True     True     False    True    5.1.2600.5512 [ole32.dll] (C:\WINDOWS\system32\ole32.dll)
0x781b0000 0x781c4000 0x00014000 True     True     False    True    5.1.2600.5512 [IM32.DLL] (C:\WINDOWS\system32\IM32.DLL)
0x781f0000 0x78204000 0x00014000 True     True     False    True    5.1.2600.5512 [hnetcfg.dll] (C:\WINDOWS\system32\hnetcfg.dll)
0x78230000 0x78244000 0x00014000 True     True     False    True    5.1.2600.5512 [USER32.dll] (C:\WINDOWS\system32\USER32.dll)
0x78270000 0x78284000 0x00014000 True     True     False    True    1.13 [libiconv-2.dll] (C:\Program Files\AudioCoder\libiconv-2.dll)
0x782b0000 0x782c4000 0x00014000 True     True     False    True    5.131.2600.5512 [CRYPTUI.dll] (C:\WINDOWS\system32\CRYPTUI.dll)
0x782f0000 0x78304000 0x00014000 True     True     False    True    5.1.2600.5512 [rtutils.dll] (C:\WINDOWS\system32\rtutils.dll)
0x78330000 0x78344000 0x00014000 True     True     False    True    5.1.2600.5512 [IPHLPAPI.DLL] (C:\WINDOWS\system32\IPHLPAPI.DLL)
0x78370000 0x78384000 0x00014000 True     True     False    True    2001.12.4414.700 [CLBTRUST.dll] (C:\WINDOWS\system32\CLBTRUST.dll)
0x783b0000 0x783c4000 0x00014000 True     True     False    True    2001.12.4414.700 [COMRes.dll] (C:\WINDOWS\system32\COMRes.dll)
0x783f0000 0x78404000 0x00014000 True     True     False    True    5.1.2600.5512 [OLEAUT32.dll] (C:\WINDOWS\system32\OLEAUT32.dll)
0x78430000 0x78444000 0x00014000 True     True     False    True    5.1.2600.5512 [rasman.dll] (C:\WINDOWS\system32\rasman.dll)
0x78470000 0x78484000 0x00014000 True     True     False    True    8.00.2900.5512 [SHELL32.dll] (C:\WINDOWS\system32\SHELL32.dll)
0x784b0000 0x784c4000 0x00014000 True     True     False    True    -1.0- [nres.dll] (C:\Program Files\AudioCoder\nres.dll)
0x784f0000 0x78504000 0x00014000 True     True     False    True    5.1.2600.5512 [DNSAPI.dll] (C:\WINDOWS\system32\DNSAPI.dll)
0x78530000 0x78544000 0x00014000 True     True     False    True    2001.12.4414.700 [CLBCATQ.DLL] (C:\WINDOWS\system32\CLBCATQ.DLL)
0x78570000 0x78584000 0x00014000 True     True     False    True    (C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6095b641-8ccf-48c6-b941-ccf5d99e11d2\6.0.2600.5512_x-ww\sh32.dll] (C:\WINDOWS\system32\sh32.dll)
0x785b0000 0x785c4000 0x00014000 True     True     False    True    (C:\Program Files\AudioCoder\plugins\dsp_chmw.dll)
0x785f0000 0x78604000 0x00014000 True     True     False    True    (C:\WINDOWS\system32\WININET.dll] (C:\WINDOWS\system32\WININET.dll)
0x78630000 0x78644000 0x00014000 True     True     False    True    (C:\WINDOWS\system32\SHLWAPI.dll] (C:\WINDOWS\system32\SHLWAPI.dll)
0x78670000 0x78684000 0x00014000 True     True     False    True    5.1.2600.5512 [ATL7IL32.dll] (C:\WINDOWS\system32\ATL7IL32.dll)
0x786b0000 0x786c4000 0x00014000 True     True     False    True    5.1.2600.5512 [rasman.exe] (C:\WINDOWS\system32\rasman.exe)
0x786f0000 0x78704000 0x00014000 True     True     False    True    5.1.2600.5512 [MSCTF.dll] (C:\WINDOWS\system32\MSCTF.dll)
0x78730000 0x78744000 0x00014000 True     True     False    True    -1.0- [dsp_zsc.dll] (C:\Program Files\AudioCoder\plugins\dsp_zsc.dll)
0x78770000 0x78784000 0x00014000 True     True     False    True    5.1.2600.5512 [CONDL32.dll] (C:\WINDOWS\system32\CONDL32.dll)
0x787b0000 0x787c4000 0x00014000 True     True     False    True    5.1.2600.5512 [USERENV.dll] (C:\WINDOWS\system32\USERENV.dll)
0x787f0000 0x78804000 0x00014000 True     True     False    True    5.1.2600.5512 [WINMM.dll] (C:\WINDOWS\system32\WINMM.dll)
0x78830000 0x78844000 0x00014000 True     True     False    True    5.1.2600.5512 [kernel32.dll] (C:\WINDOWS\system32\kernel32.dll)
0x78870000 0x78884000 0x00014000 True     True     False    True    5.1.2600.5512 [GDI32.dll] (C:\WINDOWS\system32\GDI32.dll)
0x788b0000 0x788c4000 0x00014000 True     True     False    True    -1.0- [ncommon.dll] (C:\Program Files\AudioCoder\ncommon.dll)
0x788f0000 0x78904000 0x00014000 True     True     False    True    6.00.2900.5512 [watheme.dll] (C:\WINDOWS\system32\watheme.dll)
0x78930000 0x78944000 0x00014000 True     True     False    True    -1.0- [jres.dll] (C:\Program Files\AudioCoder\jres.dll)
0x78970000 0x78984000 0x00014000 True     True     False    True    5.1.2600.5512 [MLDAP32.dll] (C:\WINDOWS\system32\MLDAP32.dll)
0x789b0000 0x789c4000 0x00014000 True     True     False    True    5.1.2600.5512 [nsavl_0.dll] (C:\WINDOWS\system32\nsavl_0.dll)
0x789f0000 0x78a04000 0x00014000 True     True     False    True    5.1.2600.5512 [VERSION.dll] (C:\WINDOWS\system32\VERSION.dll)
0x78a30000 0x78a44000 0x00014000 True     True     False    True    5.1.2600.5512 [RASAPI32.dll] (C:\WINDOWS\system32\RASAPI32.dll)
0x78a70000 0x78a84000 0x00014000 True     True     False    True    5.1.2600.5512 [PSAPI.DLL] (C:\WINDOWS\system32\PSAPI.DLL)
0x78ab0000 0x78ac4000 0x00014000 True     True     False    True    5.1.2600.5512 [MS2_32.dll] (C:\WINDOWS\system32\MS2_32.dll)
0x78af0000 0x78b04000 0x00014000 True     True     False    True    5.1.2600.5512 [normaliz.dll] (C:\WINDOWS\system32\normaliz.dll)
0x78b30000 0x78b44000 0x00014000 True     True     False    True    6.0.5441.0 [Normaliz.dll] (C:\WINDOWS\system32\Normaliz.dll)
0x78b70000 0x78b84000 0x00014000 True     True     False    True    5.1.2600.5512 [TAPI32.dll] (C:\WINDOWS\system32\TAPI32.dll)

[*] This nona.py action took 0:00:00.500000
```

Intentativa de DDoS (xdmcp)

Shellshock

Brute force

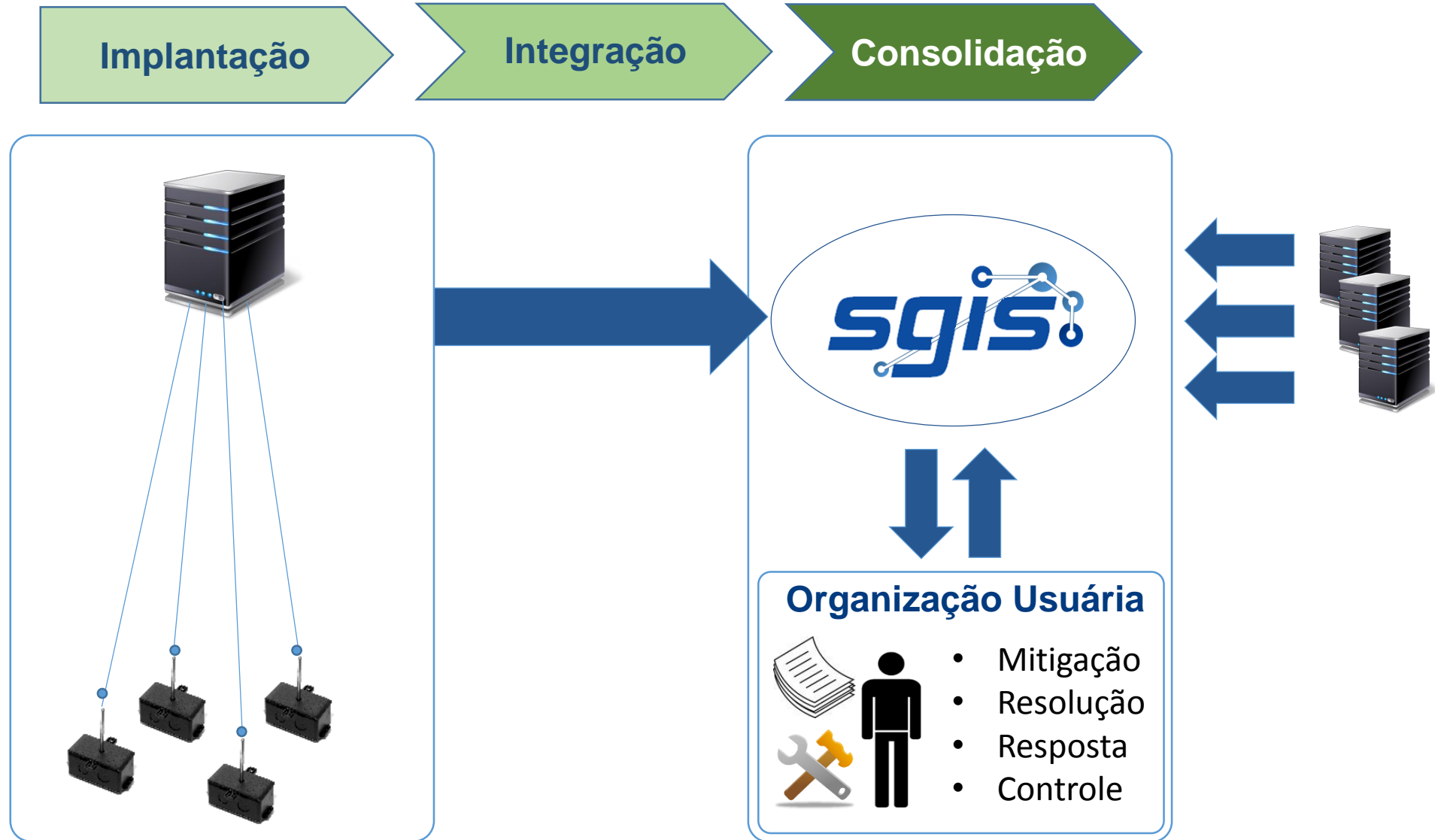
Malware

Transferência de zona (DNS)

Ataque a serviço IMAP

Poodle

# Integração com o SGIS



# Encerramento



## Encerramento

**Muito obrigado,**

**Edilson Lima**  
edilson.lima@rnp.br