



**SUÍTE ANTISPAM GERENCIÁVEL**

## **Bruno de Loyola Herides**

Analista de Sistemas e especialista em segurança e redes.

Entusiasta em tecnologias e fã de software livre, vem se dedicando ao mundo linux a mais de 10 anos. Sócio fundador da Omnikron Soluções Inteligentes, empresa especializada em soluções corporativas em software livre. Atualmente é responsável pelo serviço de e-mails do Estado do Paraná - CELEPAR, onde trabalha há mais de 9 anos.

**Palestrante**

Podemos considerar como SPAM toda e qualquer comunicação on-line indesejada. Os tipos mais comuns de SPAM são divulgação de produtos e promoções.



# O que é SPAM?

- **Captura de dados**
- **Validação de e-mail**
- **Golpes e fraudes**

# Perigos

- Customização
- Adaptatividade ao Cenário do Cliente
  - Baixo Custo
  - Implantação Rápida

# Vantagens do Software Livre

- **RBL – Realtime Black List**
  - **Expressão Regular**
  - **White / Black List**
  - **Controle de Taxa**
  - **Análise Eurística**

**Tipos de regras**

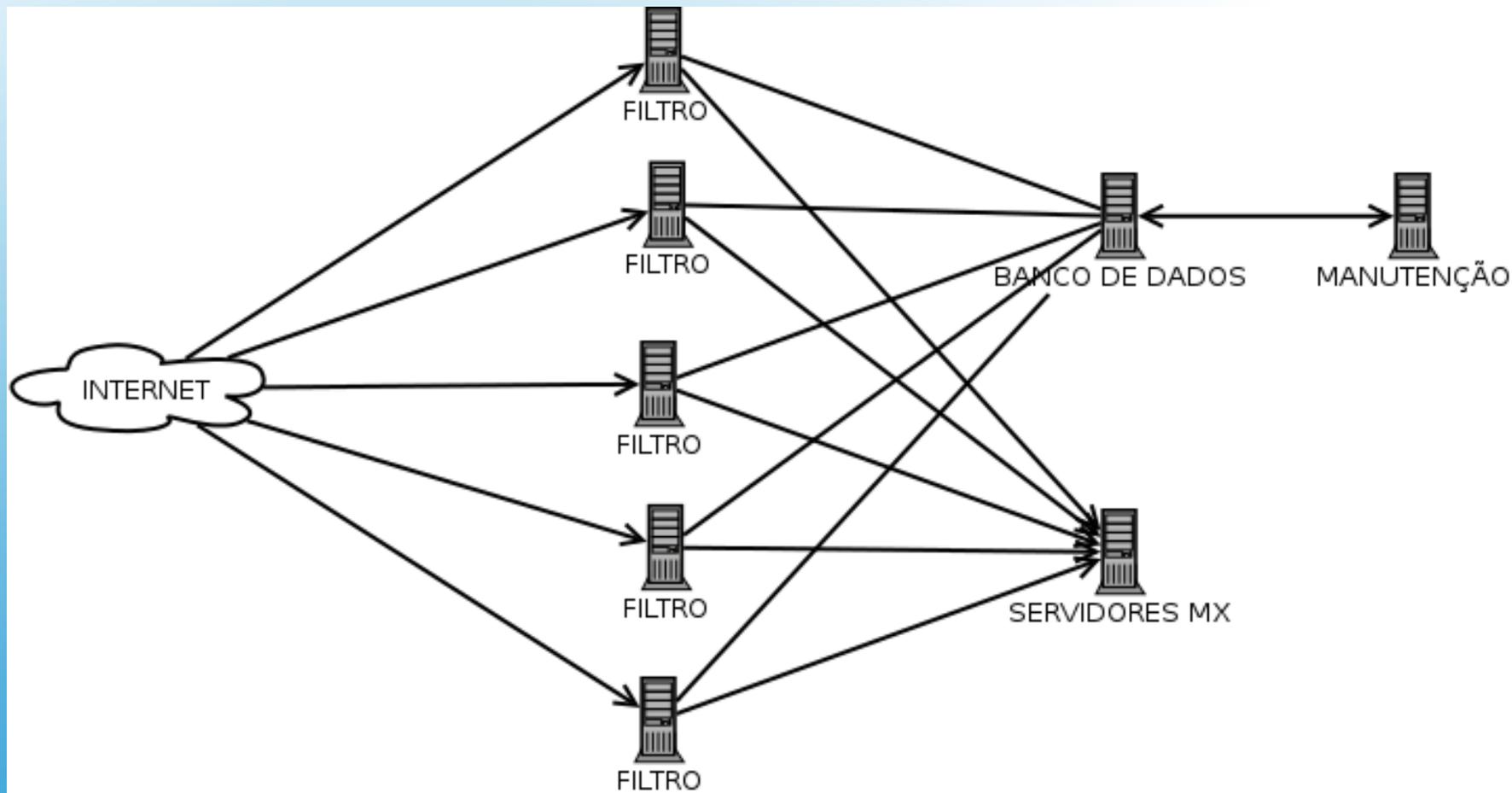
## **Ex.: Atualização Cadastral Banco Itaú Urgente**

- Totem 1: Atualização Cadastral Banco Itaú Urgente**
  - Totem 2: Atualização Cadastral Banco**
  - Totem 3: Atualização Cadastral**
  - Totem 4: Atualização Urgente**
  - Totem N: ....**

# **Análise Eurística**

- **Postfix (SMTP)**
- **Policyd (RBL)**
  - **Postfwd**
  - **Dspam**
  - **Clamav**
  - **Postgres**
  - **PgBouncer**

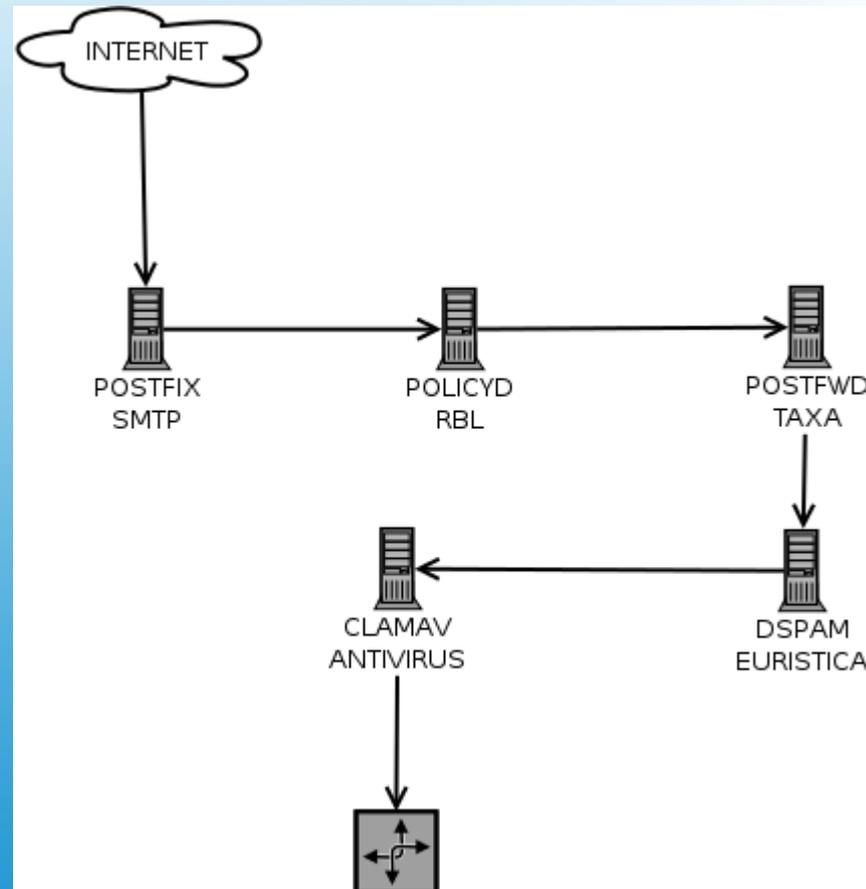
**Serviços da Solução**



# Topologia Aplicada na CELEPAR

- **Cron executa script de verificação de versão**
- **Script verifica se a versão do BD é mais nova que a versão aplicada ao servidor**
- **Script atualiza versão aplicada e também atualiza tabela de versão do BD.**

# Aplicação de Regras Estáticas



# Lógica de Funcionamento

- **Mailmarketing**
  - **Mala Direta**
  - **Redes Sociais**
- **Compras On-line**

# Desafios do E-mail Corporativo

## → Controle de Versão:



Informações



Redes



Domínios



Filtros



By\_Pass



Teste de Regras



Relatórios



Usuários



Sair do Sistema

Usuário : Bruno de Loyola Herides

### Informações Importantes

Servidor	Redes	Domínios	Filtros	By Pass
Versão do sistema	8	21	447	199
SPARANA10215	8	21	447	199
SPARANA10216	8	21	447	199
SPARANA10217	8	21	447	199
SPARANA10218	8	21	447	199
SPARANA10226	8	21	447	199

# Nossa Ferramenta de Gestão

# → Lista de Redes



Informações



Redes



Domínios



Filtros



By\_Pass



Teste de Regras



Relatórios



Usuários



Sair do Sistema

Usuário : Bruno de Loyola Herides

## Lista de Redes

Q Digite um filtro

Buscar

Nova Regra

ID	Rede	Ação	Descrição	Status	Opções
405	177.136.14.0/25	REJECT	Rede de Spam SDTEC	ATIVO	
404	201.157.248.0/21	REJECT	Rede de Spam SDTEC	ATIVO	
402	200.189.112.40/32	FILTER smtp:[200.189.123.31]:25	BARRACUDA ENTRADA	ATIVO	
401	200.189.112.39/32	FILTER smtp:[200.189.123.31]:25	BARRACUDA ENTRADA	ATIVO	
400	200.189.112.38/32	FILTER smtp:[200.189.123.31]:25	BARRACUDA ENTRADA	ATIVO	
399	200.189.112.37/32	FILTER smtp:[200.189.123.31]:25	BARRACUDA ENTRADA	ATIVO	
398	200.189.112.36/32	FILTER smtp:[200.189.123.31]:25	BARRACUDA ENTRADA	ATIVO	
394	200.189.113.29/32	FILTER smtp:[200.189.123.31]:25	relaycelepar4.pr.gov.br - p/ centraldeviagens - 2015	ATIVO	
393	186.293.222.154/32	FILTER smtp:[200.189.123.31]:25	mail.regispel.com - p/ Celepar - 2015	ATIVO	
392	200.189.112.44/32	FILTER smtp:[200.189.123.31]:25	ssmtp008.pr.gov.br - 2014	ATIVO	

Anterior

Próximo

Página - 0 / 24 :: Total - 249

# Nossa Ferramenta de Gestão

# → Lista de Domínios



Informações



Redes



Domínios



Filtros



By\_Pass



Teste de Regras



Relatórios



Usuários



Sair do Sistema

Usuário : Bruno de Loyola Herides

## Lista de Domínios

Q Digite um filtro

Buscar

Nova Regra

ID	Domínio	Destino	Descrição	Status	Opções
452	tecpa.br	smtp:200.189.113.249:25	MX04	ATIVO	
451	trabalho.pr.gov.br	smtp:200.189.113.247:25	MX03	ATIVO	
450	gestainteligente.pr.gov.br	smtp:200.189.113.249:25	MX04	ATIVO	
449	egi.pr.gov.br	smtp:200.189.113.249:25	MX04	ATIVO	
448	paranaeducacao.pr.gov.br	smtp:200.189.113.94:25	SEEDMX	ATIVO	
447	pm-fi.pr.gov.br	smtp:200.189.113.210:25	OS 700945	ATIVO	
446	defesacivil.pr.gov.br	smtp:200.189.113.232:25	MX02	ATIVO	
445	funeas.pr.gov.br	smtp:200.189.113.232:25	MX02	ATIVO	
444	defensoria.pr.def.br	smtp:200.189.113.249:25	MX04	ATIVO	
443	fmsfi.pr.gov.br	smtp:[200.189.113.210]:25	Loja	ATIVO	

Anterior

Próximo

Página - 0 / 44 :: Total - 448

# Nossa Ferramenta de Gestão

# → Expressão Regular



Informações



Redes



Domínios



Filtros



By\_Pass



Teste de Regras



Relatórios



Usuários



Sair do Sistema

Usuário : Bruno de Loyola Herides

## Lista de Expressões Regulares

Q Digite um filtro

Buscar

Nova Regra

ID	Expressão Regular	Descrição	Ação	Aplicações	Opções
1471	\\@ofertinhas\.cf	SPAM	HOLD	HEADER	
1470	\\@sua\-oferta\.com	SPAM	HOLD	HEADER	
1469	\\@.*leadsbr\.com	SPAM	HOLD	HEADER	
1468	\\@FreeLotto\.com	SPAM	HOLD	HEADER	
1467	\\@.*email\.club	SPAM	HOLD	HEADER	
1466	\\@.*adbrasil\.net\.br	SPAM	HOLD	HEADER	
1465	\\@.*dedic100\.com\.br	SPAM	HOLD	HEADER	
1464	amanda\_silveira\@terra\.com\.br	SPAM	HOLD	HEADER	
1463	\\@newsmailmarketing\.com\.br	SPAM	HOLD	HEADER	
1462	\\@(grow\sas)(central village engine)\.com\.br	SPAM	HOLD	HEADER	

Anterior

Próximo

Página - 0 / 145 :: Total - 1452

# Nossa Ferramenta de Gestão

# → White / Black List



Informações



Redes



Domínios



Filtros



By\_Pass



Teste de Regras



Relatórios



Usuários



Sair do Sistema

Usuário : Bruno de Loyola Herides

## Lista de By-Pass

Buscar

Nova Regra

ID	Endereço	Descrição	Ação	Status	Opções
3306	matfin\,com\,br	SPAM	HOLD	ATIVO	
3305	rpc.com.br	P-718298	FILTER smtp:[200.189.123.31]:25	ATIVO	
3304	pereirajair@fadeaway.com.br	Liberado solicitação JAIR	FILTER smtp:[200.189.123.31]:25	ATIVO	
3303	rastreio@correios.org.br	SPAM/FRAUDE	HOLD	ATIVO	
3299	cliquedefertas.com.br	P-534361-1	HOLD	ATIVO	
3298	locaenvios@gmail.com	P-533793-1	HOLD	ATIVO	
3297	stj.push	Liberado conforme SOC P-680723	FILTER smtp:[200.189.123.31]:25	ATIVO	
3296	mailexpresso.tk	SPAM/FRAUDE	HOLD	ATIVO	
3295	hospitaljoaodefraitas.com.br	SOC P-676296	FILTER smtp:[200.189.123.31]:25	ATIVO	
3294	contabilidadefazenda.com.br	OS 678481	FILTER smtp:[200.189.123.31]:25	INATIVO	

Anterior

Próximo

Página - 0 / 177 :: Total - 1771

# Nossa Ferramenta de Gestão

# → Smart Sugestion



Informações



Redes



Domínios



Filtros



By\_Pass



Teste de Regras



Relatórios



Usuários



Sair do Sistema

Usuário : Bruno de Loyola Herides

## Remetentes Mais Marcados

Data de Início:  Data de Término:    Somente DSPAM

Remetente	Quantidade
MAILER-DAEMON@smtpfilter.pr.gov.br (Mail Delivery System)	222
P/1 20º BPM <p120bpm@yahoo.com.br>	100
Aprimora Treinamentos <info@aprimoratreinamentos.com.br>	53
Oráculo Ching <ching@oraculoching.com>	49
Horoscopo Free <horoscopo@horoscopofree.com>	43
"Walmart.com   PFind" <nicole@sascentral.com.br>	35
"Extra.com.br   PFind" <nicole@sascentral.com.br>	30
"Pontofrio.com.br   PFind" <nicole@sascentral.com.br>	30
"CasasBahia.com.br   PFind" <nicole@sascentral.com.br>	29
"Netshoes Parceiro Afiliado" <contato@afiliadobr.com.br>	26
Atos Treinamentos <info@atostreinamentos.com.br>	26
auditoria <contato@mailto.com.br>	25

# Nossa Ferramenta de Gestão

# → Estatísticas

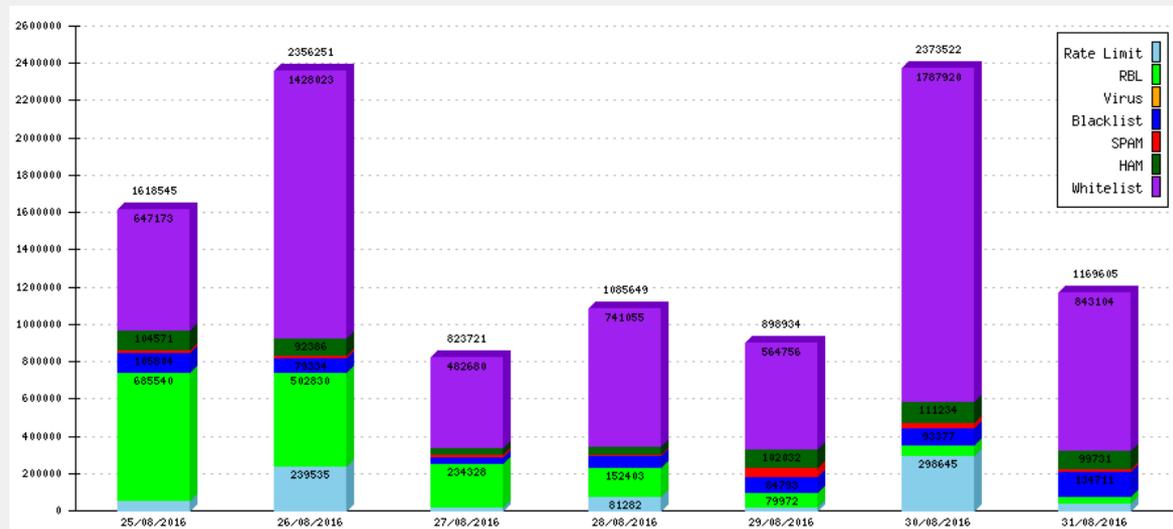


-   
Informações
-   
Redes
-   
Domínios
-   
Filtros
-   
By\_Pass
-   
Teste de Regras
-   
Relatórios
-   
Usuários
-   
Sair do Sistema

Usuário : Bruno de Loyola Herides

## Estatísticas de Uso Diário

Data de Início:  Data de Término:    Rate Limit  RBL  Vírus  Blacklist  SPAM  HAM  Whitelist



# Nossa Ferramenta de Gestão

**Dúvidas ou Sugestões?**

**Dúvidas ou Sugestões**

**<http://antispam.pr.gov.br>**

**[bherides@celepar.pr.gov.br](mailto:bherides@celepar.pr.gov.br)**

**Contato**