MPF
Ministério Público Federal

Caso de Sucesso

Marcelo Caiado, M.Sc., CISSP, GCFA, GCIH, EnCE
Analista de Informática / Perito
Chefe da Divisão de Segurança da Informação
Procuradoria-Geral da República

2017

Esclarecimentos

- As opiniões do apresentador não refletem necessariamente as posições do MPF ou da PGR
- O apresentador não é remunerado pela organização do evento ou qualquer patrocinador
- Os slides dessa apresentação estão disponíveis para download no site http://dfir.com.br

Introdução ao MPF

- O MPU e o MPF são chefiados pelo Procurador-Geral da República e a sede administrativa do MPF é a Procuradoria-Geral da República

  MPF: PGR, Procuradorias Regionais da República, Procuradorias da República e Procuradorias da República nos Municípios

Introdução ao MPF

Introdução ao MPF

Mapa da atuação do MPF

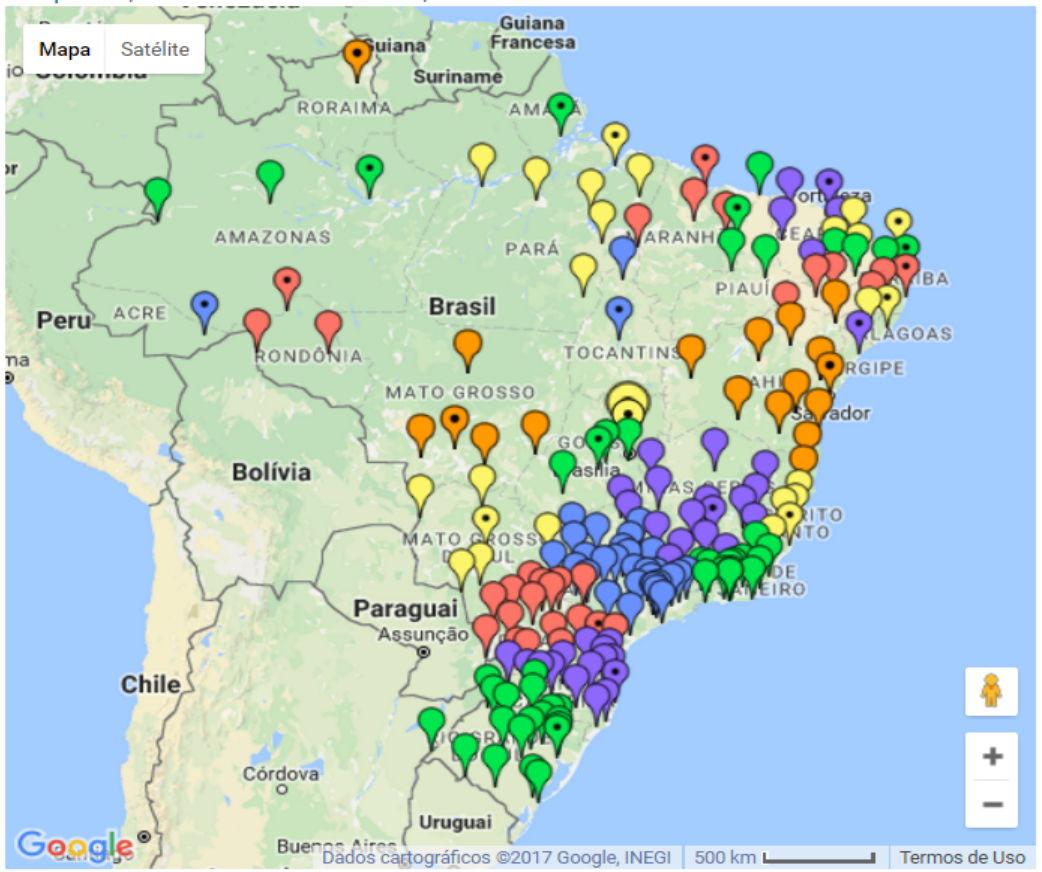
Informações sobre o conteúdo deste mapa Instruções de utilização

Exibindo procedimentos extrajudiciais

Selecione no menu abaixo os itens para exibição

QUANTIDADE DE PROCESSOS	167.332
ADMINISTRATIVO DO MP (ÁREA-MEIO)	269
DIREITO ADMINISTRATIVO E OUTRAS MATÉRIAS DE DIREITO PÚBLICO	102.214
DIREITO CIVIL	7.604
DIREITO DA CRIANÇA E DO ADOLESCENTE	4.034
DIREITO DO CONSUMIDOR	3.524
DIREITO DO TRABALHO	837
DIREITO ELEITORAL	2.015
DIREITO ELEITORAL E PROCESSO ELEITORAL DO STF	466
DIREITO INTERNACIONAL	341
DIREITO MARÍTIMO	18
DIREITO PENAL	44.028
DIREITO PENAL MILITAR	134
DIREITO PREVIDENCIÁRIO	1.372
DIREITO PROCESSUAL CIVIL E DO TRABALHO	323
DIREITO PROCESSUAL PENAL	496
DIREITO PROCESSUAL PENAL MILITAR	1
DIREITO TRIBUTÁRIO	1.021
A CLASSIFICAR	5.743
PROCURADORIA GERAL DA REPÚBLICA	46
REGISTROS PÚBLICOS	32

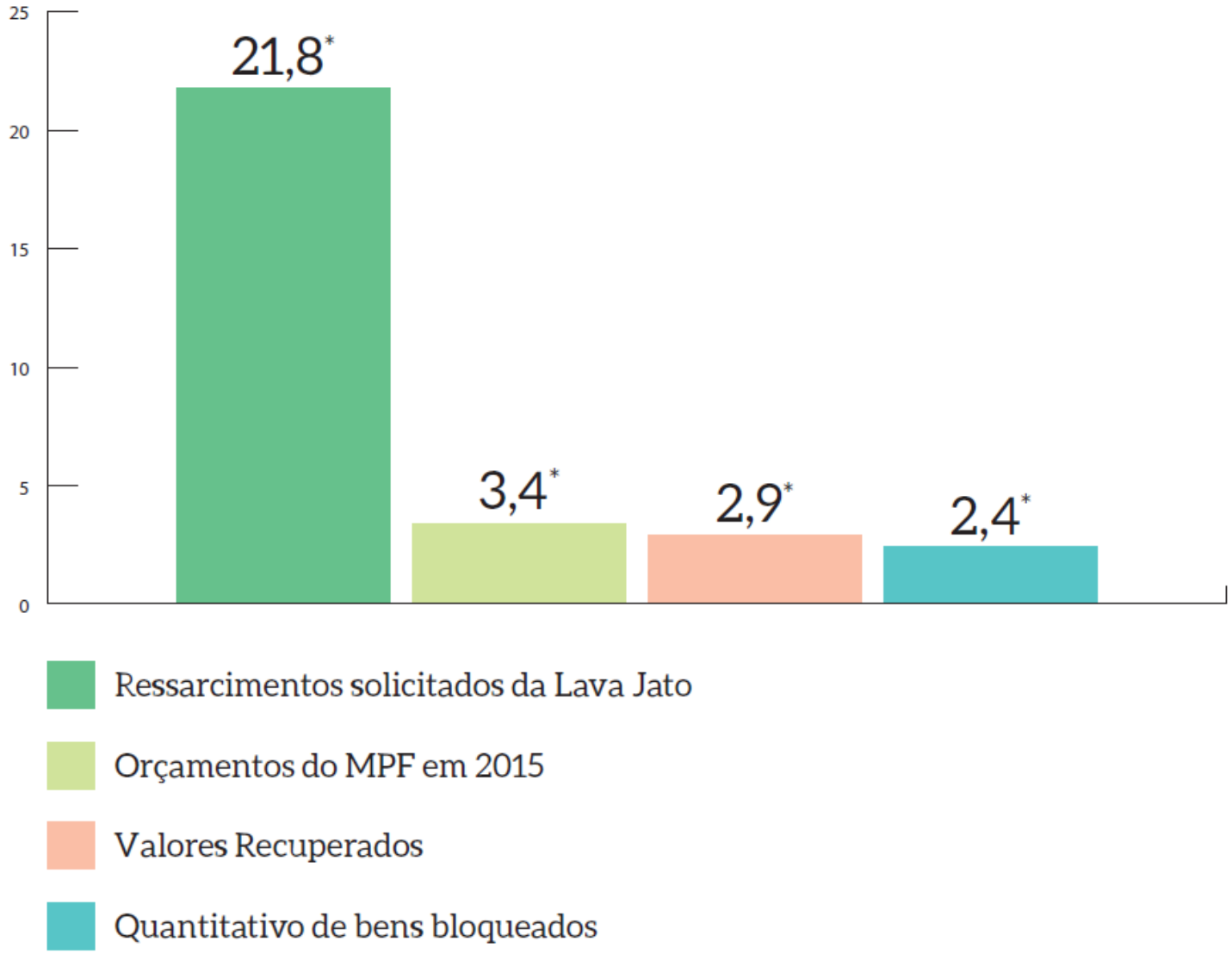
« Expandir / recolher » » Ocultar / exibir » » Centralizar «



É possível refinar a pesquisa segundo as seguintes classificações:

- » Áreas Temáticas
- » Classes
- » Unidades do MPF: 1ª Instância
- » Unidades do MPF: 2ª e 3ª Instâncias

Introdução ao MPF



Comparativos do Orçamento do MPF e com valores da Lava Jato (*valores em bilhões)

Fonte: Relatório de Resultados do PGR 2015/2016

Situação anterior ao contrato

- **Rede Nacional do MPF interconectada por MPLS**

- **Segurança existente somente no Data Center principal**

✔Firewall e IPS

- **Nenhuma proteção contra ataques internos**

✗Máquinas infectadas em uma unidade causaram problemas em outras localidades

✗Nenhuma visibilidade de tráfego entre as PRs

- **Uso não controlado dos links internos para tráfego web**

PE Nº 121/2014 - Objetivo

Contratação de empresa especializada para:

- Segurança de perímetro
  - Instalação
  - Manutenção
  - Gerenciamento e Monitoração
    - ✓ *Serviços de Firewall*
    - ✓ *Prevenção de Intrusão*
    - ✓ *Filtro de Conteúdo*
    - ✓ *Antivírus de Rede*
    - ✓ *VPN(Virtual Private Network) entre firewalls*
    - ✓ *Acesso Remoto para Usuários*
    - ✓ *Balanceamento de Aplicações*
    - ✓ *Otimização WAN*
- Para todas as unidades do Ministério Público Federal

Definição das Categorias

Mais de 220 localidades divididas em 8 categorias

Categoria	Parâmetros de Rede	Vazão Mínima	Ativações Realizadas
1	Links de até 5 Mbits/s e conexões para até 100 usuários.	100 Mbits/s	176
2	Links de até 9 Mbits/s e conexões para até 250 usuários.	200 Mbits/s	10
3	Links de até 17 Mbits/s e conexões para até 500 usuários.	400 Mbits/s	1
4	Links de até 35 Mbits/s e conexões para até 700 usuários.	800 Mbits/s	34
5	Links de até 65 Mbits/s e conexões para até 1.000 usuários.	1 Gbits/s	1
6	Links de até 200 Mbits/s e conexões para até 3.000 usuários.	1,5 Gbits/s	1
7	Links de até 500 Mbits/s e conexões para até 4.000 usuários.	2 Gbits/s	-
8	Links de até 1 Gbits/s e conexões para até 5.000 usuários.	5 Gbits/s	-

Contrato Atual

Contrato na Modalidade de Serviço

Gestão do contrato

Equipe PGR

Gerenciamento e Monitoração

Compartilhado entre equipe PGR e NCT

Acesso somente de leitura para demais coordenadorias

Relatórios semanais emitidos pela NCT

Equipamentos de Segurança

Fortinet Modelos FortiGate 80D até FortiGate 1500D

FortiManager e FortiAnalyzer

Benefícios

Solução Fortinet

- *Reformulação da TI com foco na arquitetura de segurança de rede*
- *Atendimento as necessidades de segurança*
- *Implementação rápida*

Aumento no nível de segurança

- *Aproximadamente 260 equipamentos distribuídos em 220 localidades*
- *Dependendo do tamanho da localidade, atribuída uma categoria de equipamento*
- *Funcionalidades de FW, IPS, AV, App Control, Filtro Web*
- *Visibilidade do tráfego de rede e de ataques*
- *Utilização dos links de Internet*

Benefícios

Redundância e acesso seguro

- *Alta disponibilidade da solução em algumas localidades*
- *Contingência de link (MPLS) em todas as localidades através de VPN IPSec*
- *Acesso remoto para Procuradores e Funcionários através de VPN SSL com certificado*

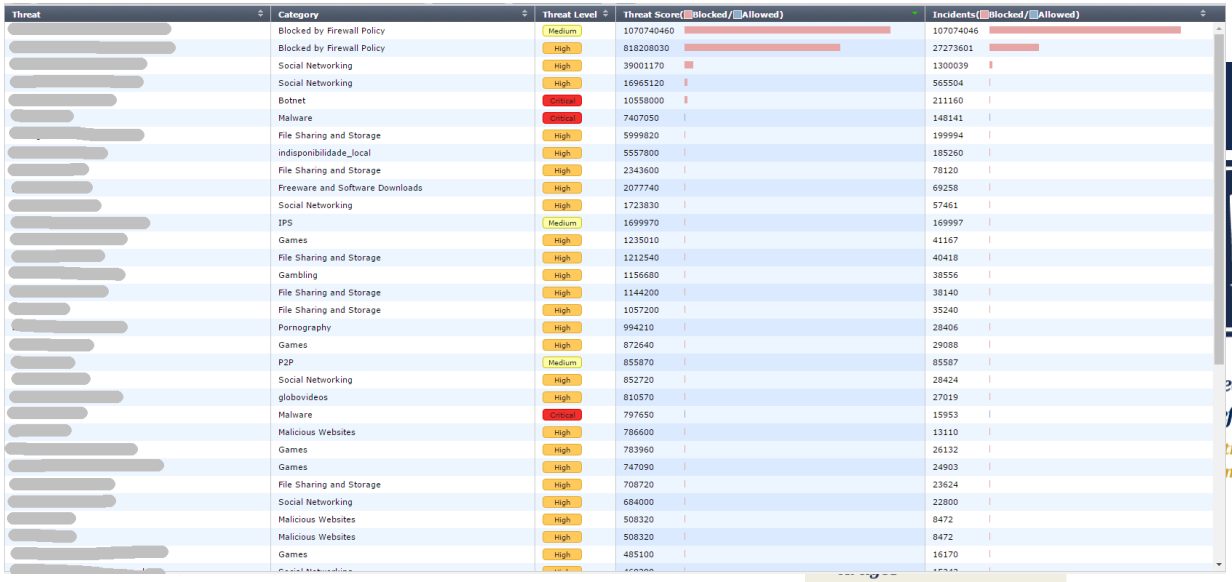
Gerenciamento e Monitoramento

- *Centralização de regras de acesso e logs*
- *Monitoração de disponibilidade dos equipamentos*
- *Monitoração de utilização de CPU e Memória (upgrade de equipamento caso necessário)*
- *Rápida mudança de categoria para as localidades*

Lava Jato

Maior exposição do Ministério Público Federal na mídia

Instituição mais suscetível a ataques cibernéticos



Threat	Category	Threat Level	Threat Score(Blocked/Allowed)	Incidents(Blocked/Allowed)
	Blocked by Firewall Policy	Medium	1070740460	107074046
	Blocked by Firewall Policy	High	818208030	27273601
	Social Networking	High	39001170	1300039
	Social Networking	High	16965120	565504
	Botnet	Critical	10558000	211160
	Malware	Critical	7407050	148141
	File Sharing and Storage	High	5999820	199994
	indisponibilidade_local	High	5557800	185260
	File Sharing and Storage	High	2343600	78120
	Freeware and Software Downloads	High	2077740	69258
	Social Networking	High	1723830	57461
	IPS	Medium	1699970	169997
	Games	High	1235010	41167
	File Sharing and Storage	High	1212540	40418
	Gambling	High	1156680	38556
	File Sharing and Storage	High	1144200	38140
	File Sharing and Storage	High	1057200	35240
	Pornography	High	994210	28406
	Games	High	872640	29088
	P2P	Medium	855870	85587
	Social Networking	High	852720	28424
	globovideos	High	810570	27019
	Malware	Critical	797650	15953
	Malicious Websites	High	786600	13110
	Games	High	783960	26132
	Games	High	747090	24903
	File Sharing and Storage	High	708720	23624
	Social Networking	High	684000	22800
	Malicious Websites	High	508320	8472
	Malicious Websites	High	508320	8472
	Games	High	485100	16170

Orientação Técnica 11 do Ministério Publico Federal

Relatórios semanais para as Coordenadorias de Informática

- *Saúde do link;*
- *Utilização de banda por aplicação e por usuário;*
- *Websites mais acessados;*
- *Ataques ocorridos;*

- *Relatórios gerados a partir dos dados coletados pela solução de Segurança – FortiAnalyzer*

- *Cada coordenador responsável por tomada de ações para sanar os possíveis desvios detectados*

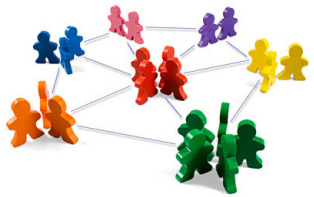
DFT

Dimensionamento de Força de Trabalho

- *Atualmente, a equipe de segurança da informação da PGR conta com 2 técnicos e 6 analistas*
- *Exigência de mais de 30 atividades de demandas de Segurança da Informação*
- *Pelo DFT Atual, necessários mais 6 técnicos e 13 analistas*

Contrato de segurança em modalidade de serviço

- *Gestão através de equipe local*
- *Gerenciamento e monitoração terceirizado*
- *Essencial para permitir nível de segurança adequado*



Otimização WAN

Contrato atual prevê a adição de Serviço de Otimização WAN

- ✔Divisão em 10 categorias diferenciadas por velocidade dos links e número de usuários
- ✔Serviço oferece melhoria na utilização de banda entre os links e também a realização de cache web nas localidades
- ✔Serviço ainda não foi ativado por falta de recursos financeiros

Parceria

MPF
Ministério Público Federal

Marcelo Caiado, M.Sc., CISSP, GCFA, GCIH, EnCE
Analista de Informática / Perito
Chefe da Divisão de Segurança da Informação
Procuradoria-Geral da República

Contato
MarceloBC@mpf.mp.br
http://dfir.com.br

"A ciência foi construída contra um monte de disparates"
Albert J. Libchaber (Nobel de Física, 1986)
"Por sua brilhante demonstração experimental da transição para a turbulência e o caos em sistemas dinâmicos"

2017