Centro de Tratamento de Incidentes de Rede da Administração Pública Federal – CTIR Gov

Aperfeiçoamento de um CSIRT governamental
Lições aprendidas em 12 meses

1º Fórum Brasileiro de CSIRTs
São Paulo – SP
26/03/2012

Objetivo

Apresentar o conjunto de lições aprendidas ao longo do processo de aperfeiçoamento vivido pelo CTIR Gov no decorrer de um ano.

Sumário

- **Ambientação**
- ***Lições Aprendidas***
  1. **Desenhe sua estratégia**
  2. **Estabeleça suas premissas**
  3. **Crie sua metodologia**
  4. **Avalie seus resultados**
  5. **Melhore seu processo continuamente**
- **Conclusões e trabalhos futuros**

Ambientação

CTIR Gov

✓ Nome do CSIRT

- Centro de Tratamento de Incidentes de Redes de Computadores da Administração Pública Federal

✓ Subordinação

- Presidência da República (PR)
  - Gabinete de Segurança Institucional (GSI)
    - Departamento de Segurança da Informação e Comunicações (DSIC)

✓ Público-Alvo

- Redes de Computadores da Administração Pública Federal Brasileira

✓ Contatos

- ctir@ctir.gov.br
- http://www.ctir.gov.br

Por que 12 meses?

Período de implantação de um *Issue Tracking System* (ITS) no CTIR Gov

> ***"ITS's são sistemas destinados a controlar e registrar o andamento de cada atividade desenvolvida por uma dada equipe."***
>
> (VINCENT et al., 2005, p.1)

Issue Tracking Systems (ITS)

✓ Destinam-se principalmente a:

- Registrar um evento (notificação);
- Atribuir um responsável pela atividade;
- Determinar as partes envolvidas; e
- Rastrear as mudanças ocorridas.

✓ No contexto de um CSIRT podem:

- Automatizar etapas;
- Manipular Templates;
- Suportar diversos processos;
- Aumentar a produtividade; e
- Reduzir erros nas notificações.

Lições aprendidas

1. Desenhe sua estratégia

1.1 - Conheça seu público-alvo

- Defina quais serviços irá oferecer
- Conceito de valor para os “clientes”

1.2 - Conheça suas potencialidades e limitações

- Competências da equipe
- Número de atividades *vs* recursos disponíveis

1.3 - Conheça seu papel

- CSIRT de coordenação
- Limites de atuação

2. Estabeleça as suas premissas

2.1 - É compensatório o uso de um ITS?

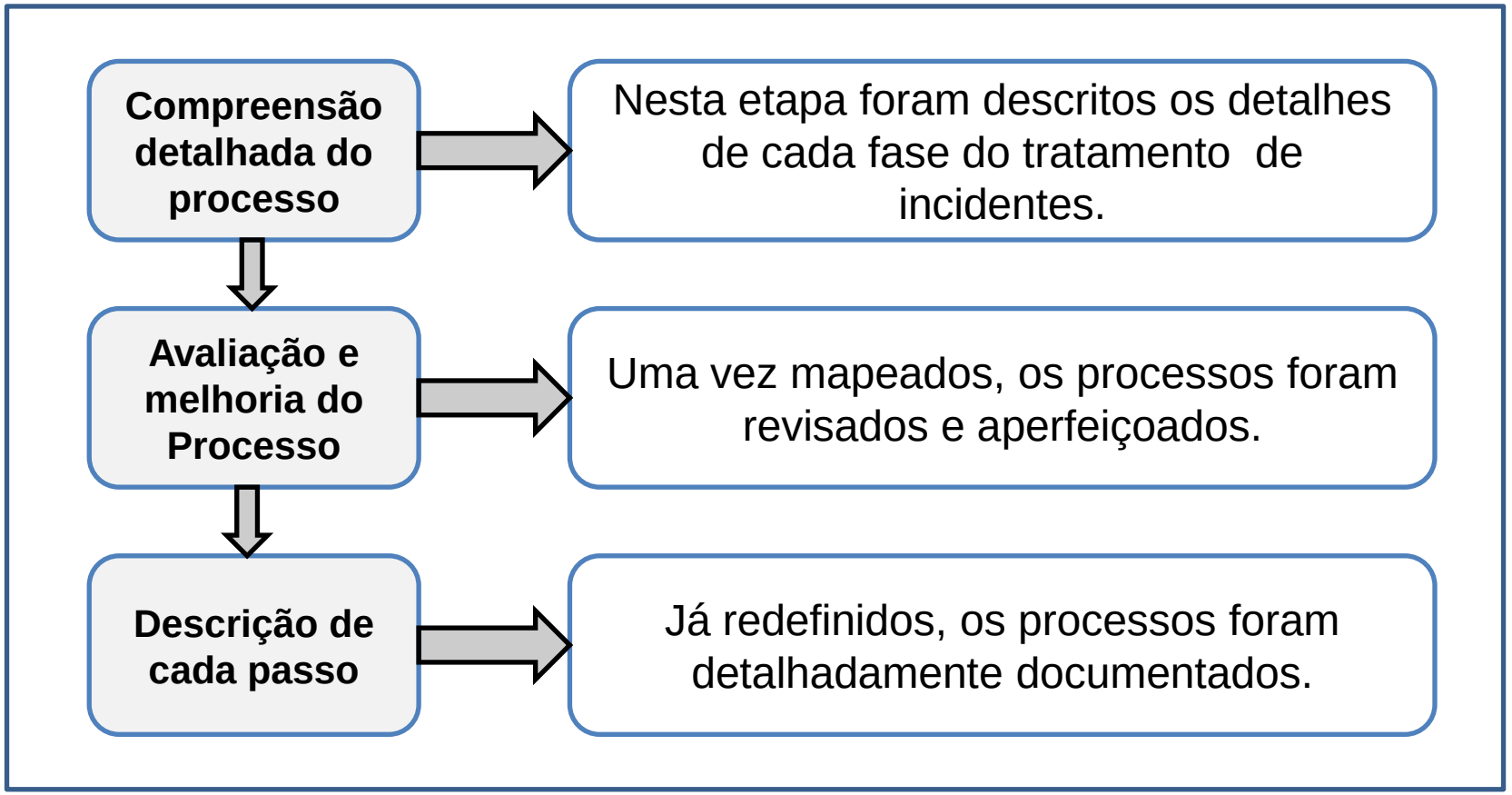
- Facilitar os processos
- Reduzir os erros mais comuns
- Possibilitar a rastreabilidade e o controle dos incidentes

2.2 - Avalie:

- Riscos
- Infraestrutura
- Continuidade dos negócio

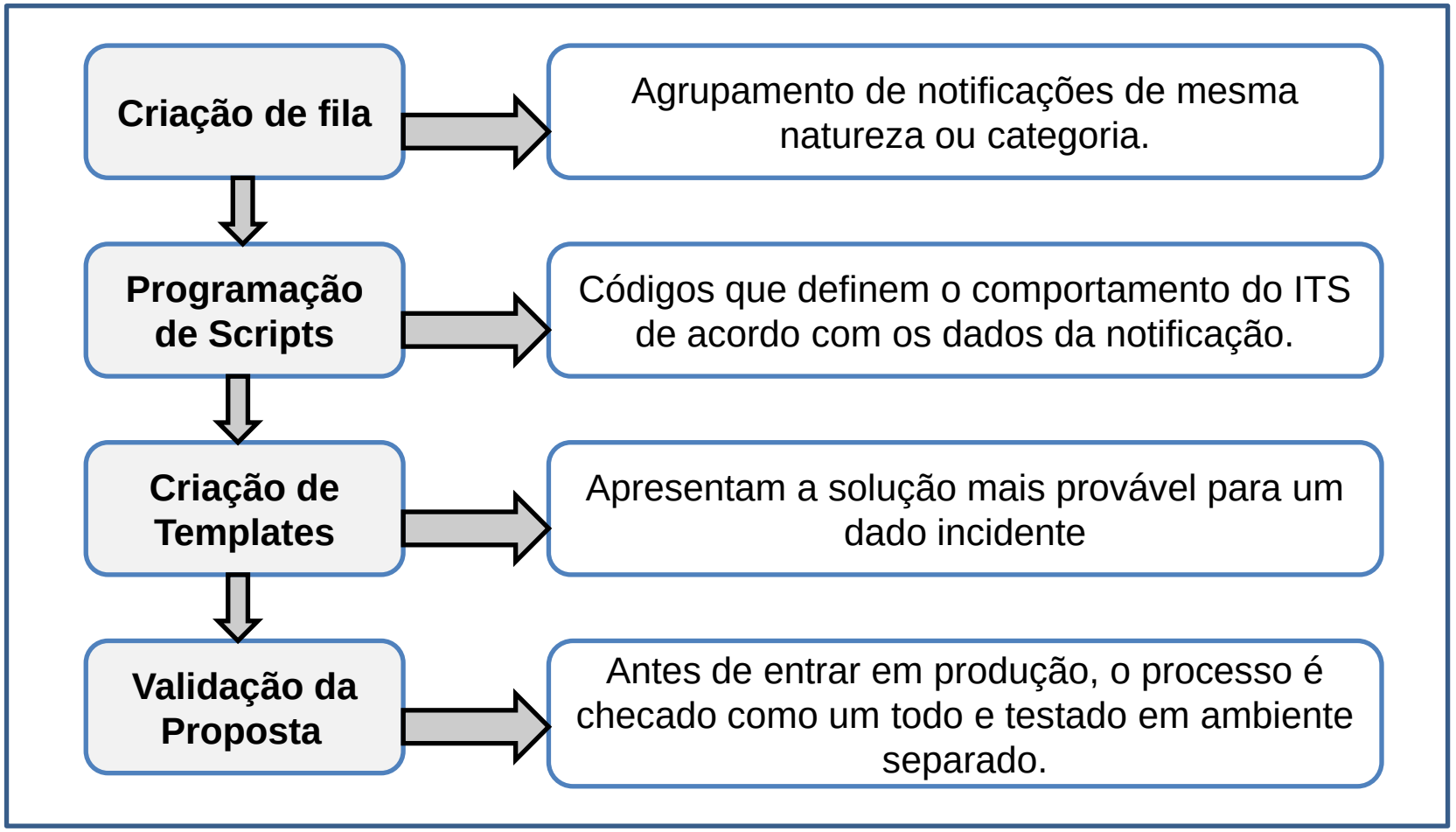
3. Crie sua Metodologia

3.1 - Ambiente Anterior



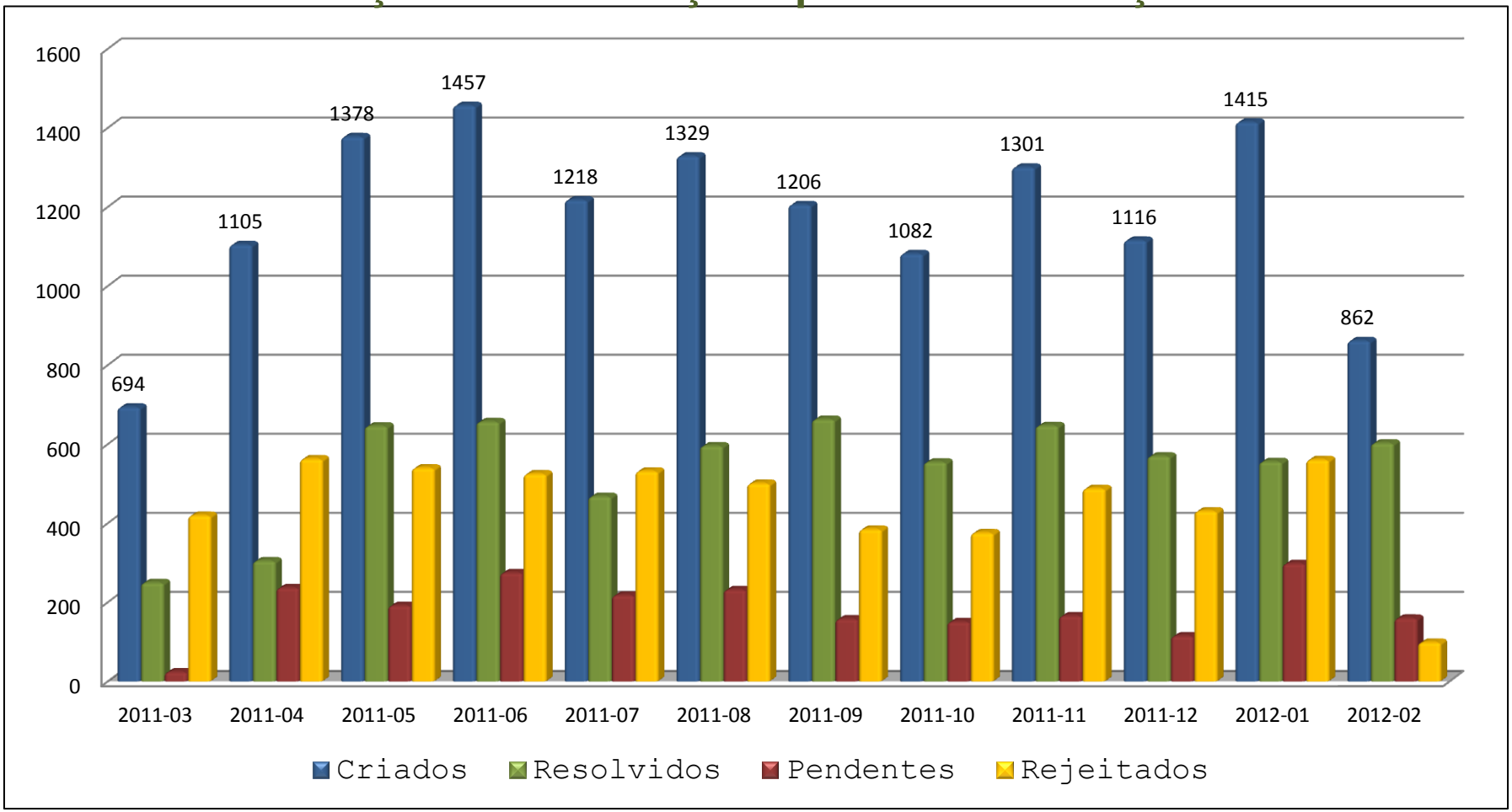
3. Crie sua Metodologia

3.2 - ITS



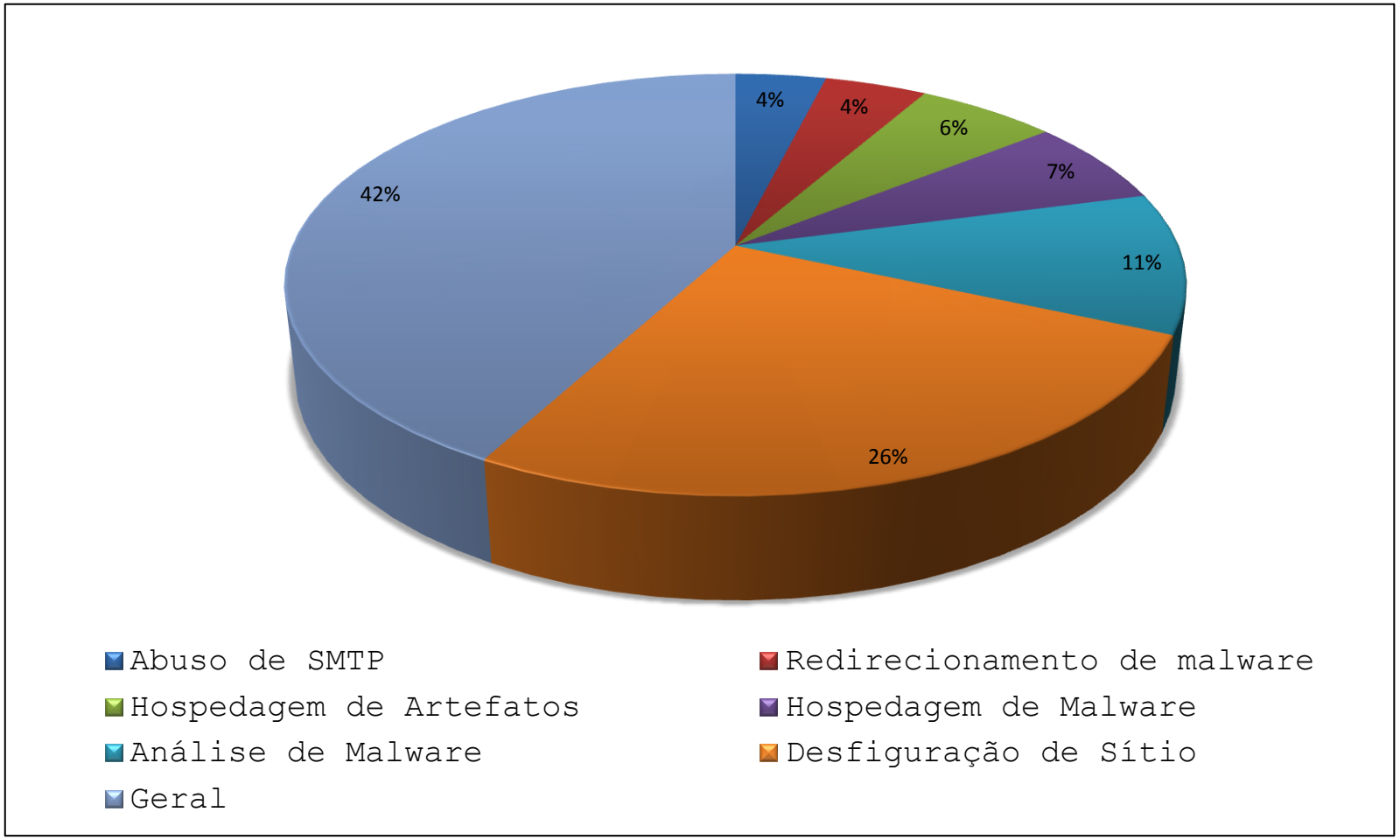
4. Avalie seus resultados

4.1 – Distribuição de notificações por mês de criação e *status*



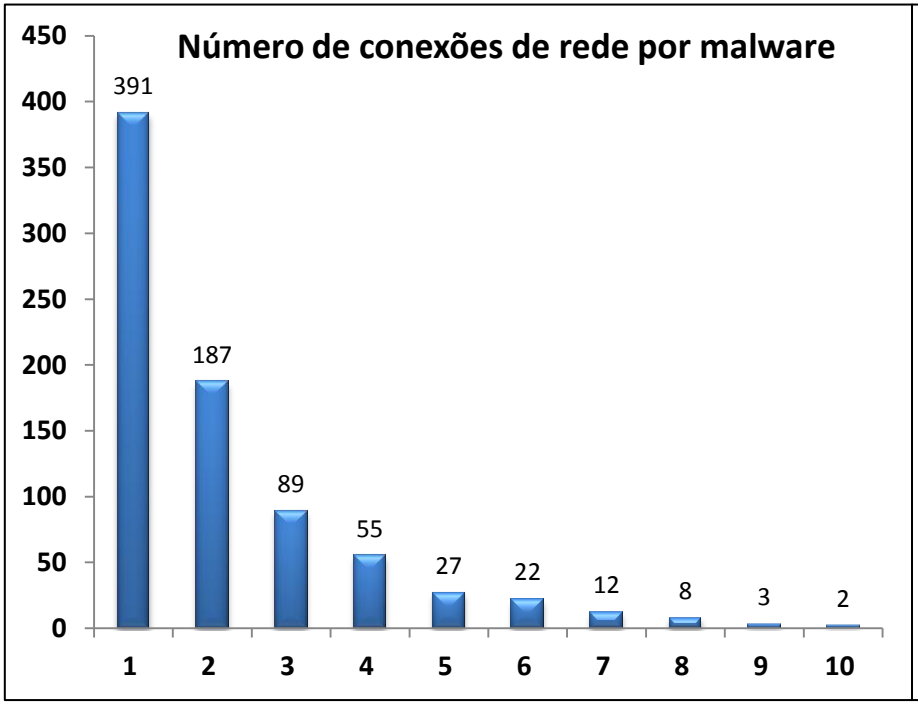
4. Avalie seus resultados

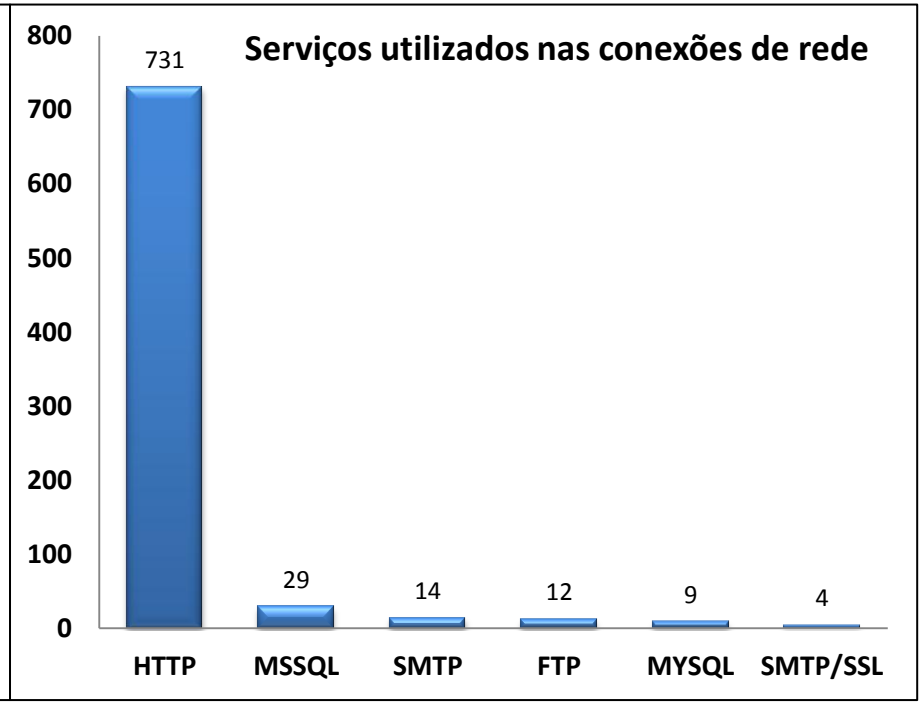
4.2 – Distribuição de notificações por categoria de incidente



4. Avalie seus resultados

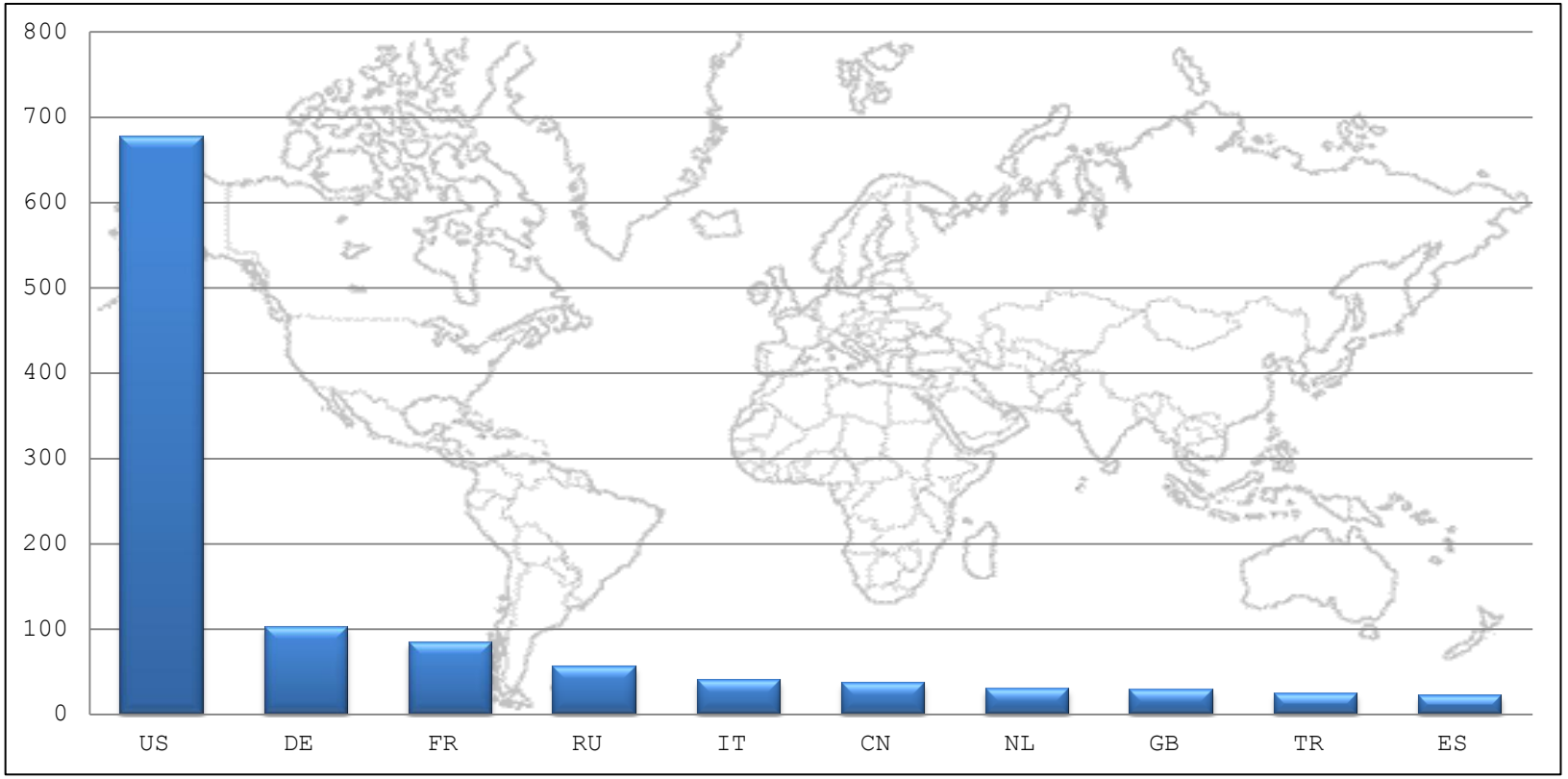
4.3 – Dados relativos à análise de malware





4. Avalie seus resultados

4.4 – Distribuição de notificações por destinatário estrangeiro



5. Melhore o processo continuamente

5.1 - Processos

- Análise das novas demandas
- Criação de novas filas
- Aperfeiçoamento dos processos já existentes

5.2 – Scripts

- Ajustes no grau de automatização
- Realização de tarefas repetitivas

5.3 – Templates

- Avaliação dos resultados conforme a mensagem
- Aperfeiçoamento / Correções

Conclusões

✓ Objetivos atingidos

- Aperfeiçoamento, compreensão e documentação dos processos

- Diminuição do número de erros nas notificações

- Facilidade no treinamento de novos integrantes

- Ganho de eficiência nas atividades rotineiras

- Concentração dos dados sobre incidentes

- Custo/Benefício compensatório

Trabalhos futuros

- ✓ Correlacionamento dos dados
- ✓ Interpretação das informações
- ✓ Georreferenciamento

Referências

- ✓ **Best Practical**

  http://www.bestpractical.com/rt/

- ✓ **RT Wiki**

  http://www.requesttracker.wikia.com/wiki/HomePage

Centro de Tratamento de Incidentes de Rede da Administração Pública Federal – CTIR Gov

OBRIGADO!

http://www.ctir.gov.br

ctir@ctir.gov.br

INOC-DBA: 10954*810