CSIRT Unicamp

Tratamento de Incidentes de Segurança da Informação

CCUEC

setembro/2013

Histórico

- Criação: 1999 com o nome Equipe de Segurança
- Por que? Necessidade de ter uma equipe para centralizar os problemas de segurança da informação que envolviam a rede da Unicamp;
- A Equipe era formada por 1 analista em tempo integral e contava com o apoio de 2 analistas (1 da equipe de Suporte Unix e outro da equipe de Redes);
- Em 2004 o nome foi alterado para CSIRT (Computer Security Incident Response Team);

Histórico

Desafios:

- Conquistar a credibilidade dos técnicos de TIC nos Órgãos/Unidades da Unicamp (não existia uma Equipe que centralizava os incidentes de segurança da informação);
- Obter apoio da Direção para agir com rapidez e sem burocracia dentro da Unicamp;
- Relevância: Nosso trabalho faz alguma diferença? Ela é positiva?

Atualmente

- 14 anos de atuação;
- Alocada no Centro de Computação na Diretoria de Redes e Segurança;
- Ponto de contato e responsável pelo acompanhamento dos incidentes de segurança da informação da Unicamp;
- Atende as contas “security” e ”abuse” at unicamp.br e ccuec.unicamp.br (sem filtros);

Atualmente

- Atende em horário comercial - 8:30 às 17:30;
- 3 analistas de suporte computacional que trabalham em esquema de rodízio no atendimento aos incidentes;
- Principais parceiros: CERT.br e CAIS-RNP;
- Participante do projeto Honeynet do CERT.br.

Rotina de trabalho

1) Notificações de possíveis problemas de segurança:

- análise da solicitação;
- repasse para os técnicos de TIC dos Órgãos/ Unidades;
- cadastro/categorização do atendimento;
- histórico (todos os e-mails trocados sobre o atendimento são registrados);
- aguarda retorno para conclusão do atendimento;
- monitora da resolução do problema.

Rotina de trabalho

2) Análise diária dos firewalls administrados pela Equipe de Redes do Centro de Computação:

- análise dos logs com os *port scans* mais críticos;
- notifica os responsáveis pelos IPs que estão gerando o problema (Whois);
- cadastro/categorização do atendimento;
- histórico (todos os e-mails trocados sobre o atendimento são registrados);
- aguarda retorno para conclusão do atendimento (status “sem retorno”);
- 3 notificações “sem retorno” = bloqueio do IP

Rotina de trabalho

3) Análise diária dos logs gerados por 3 Honeypots (CERT.br):

- abrange os 3 ranges de IP da Unicamp;

- mesma dinâmica usada para os logs de firewall;

Ferramentas

- Conjunto de *shells* em *perl* que enviam as notificações tanto internas quanto externas.

- Até 12/2011: utilizava-se o *software* “**Jitterbug**” para cadastro e acompanhamento dos incidentes de segurança da informação. Os dados eram gravados em formato texto e extraídos por *scripts shells* desenvolvidas internamente.

Ferramentas

- A partir de 01/2012: utiliza-se o software "**Mantis**" para cadastro e acompanhamento dos incidentes de segurança da informação. A ferramenta é desenvolvida em *php* e os dados são gravados em um banco de dados *MySQL*.

- A própria ferramenta gera alguns gráficos e foram desenvolvidas internamente, em php, outras funcionalidades para extração dos dados e cobrança de retorno dos atendimentos pendentes.

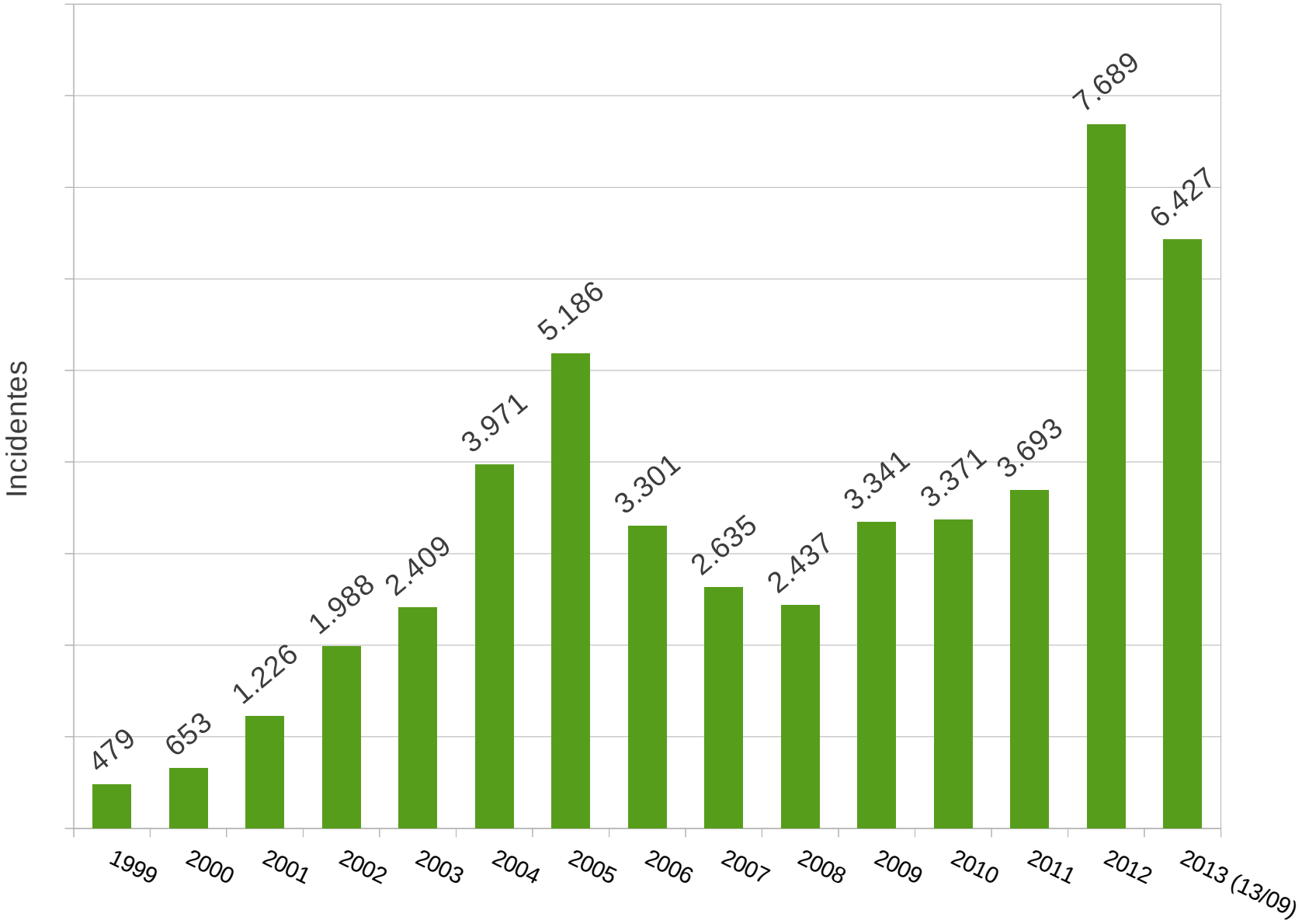
Ferramentas

- Segundo semestre/2013: Aprimorar ferramenta de gestão de incidentes:
  - Notificações;
  - Gerência de chamados;
  - Estatísticas;

- Mais detalhes: Próximo Fórum! ;)

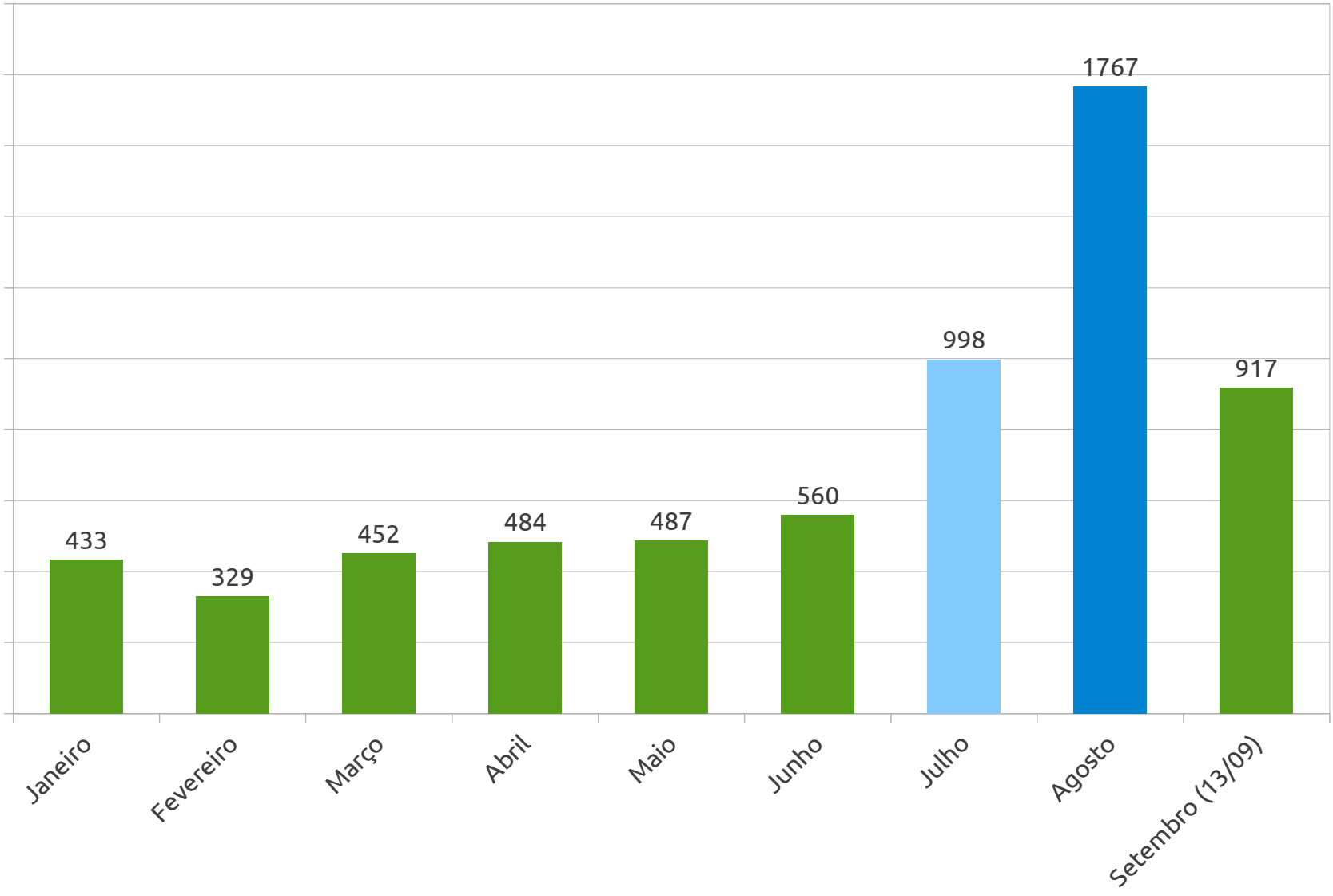
Estatísticas

Total de chamados: 1999 à 2013



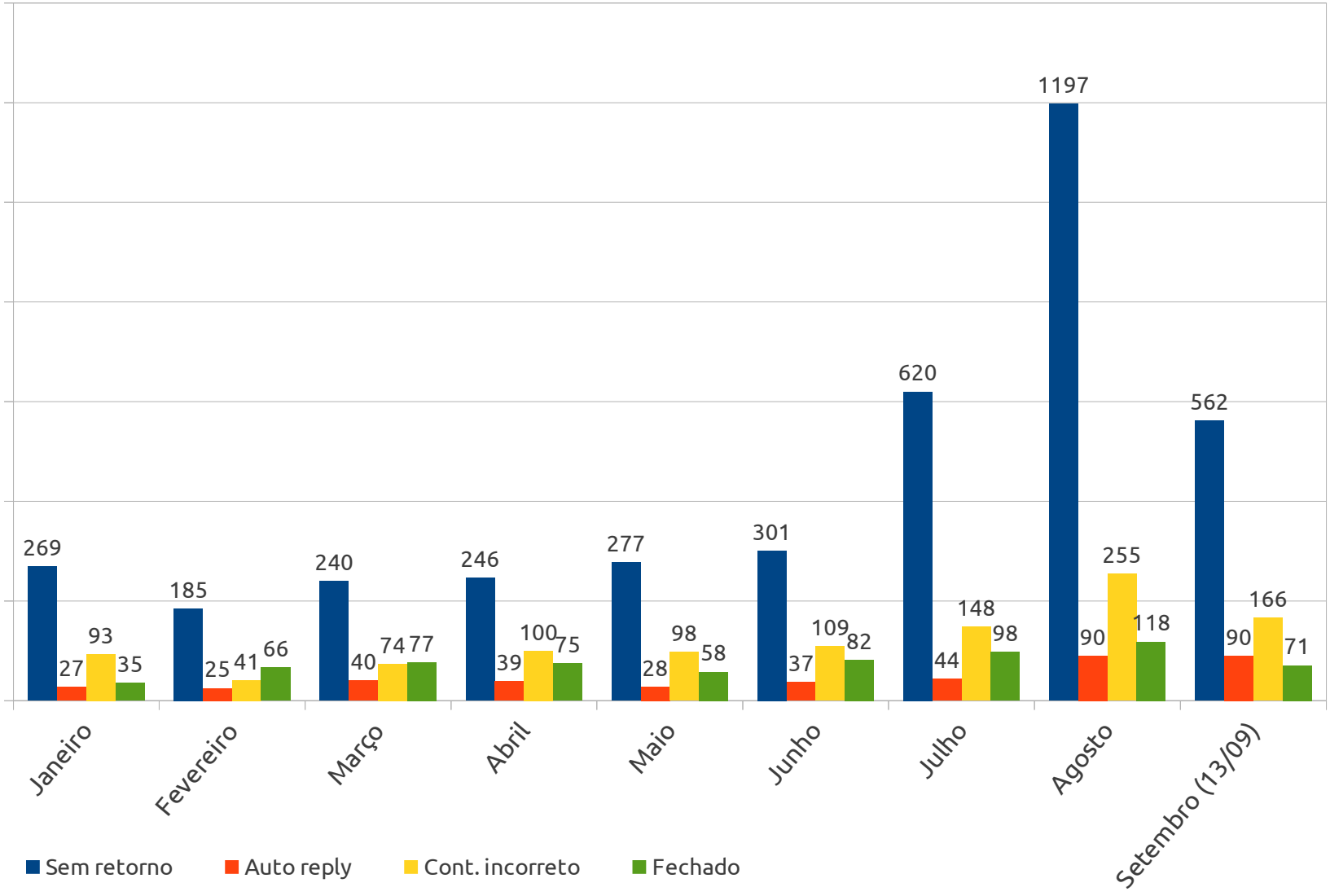
Estatísticas

Chamados por mês: 2013



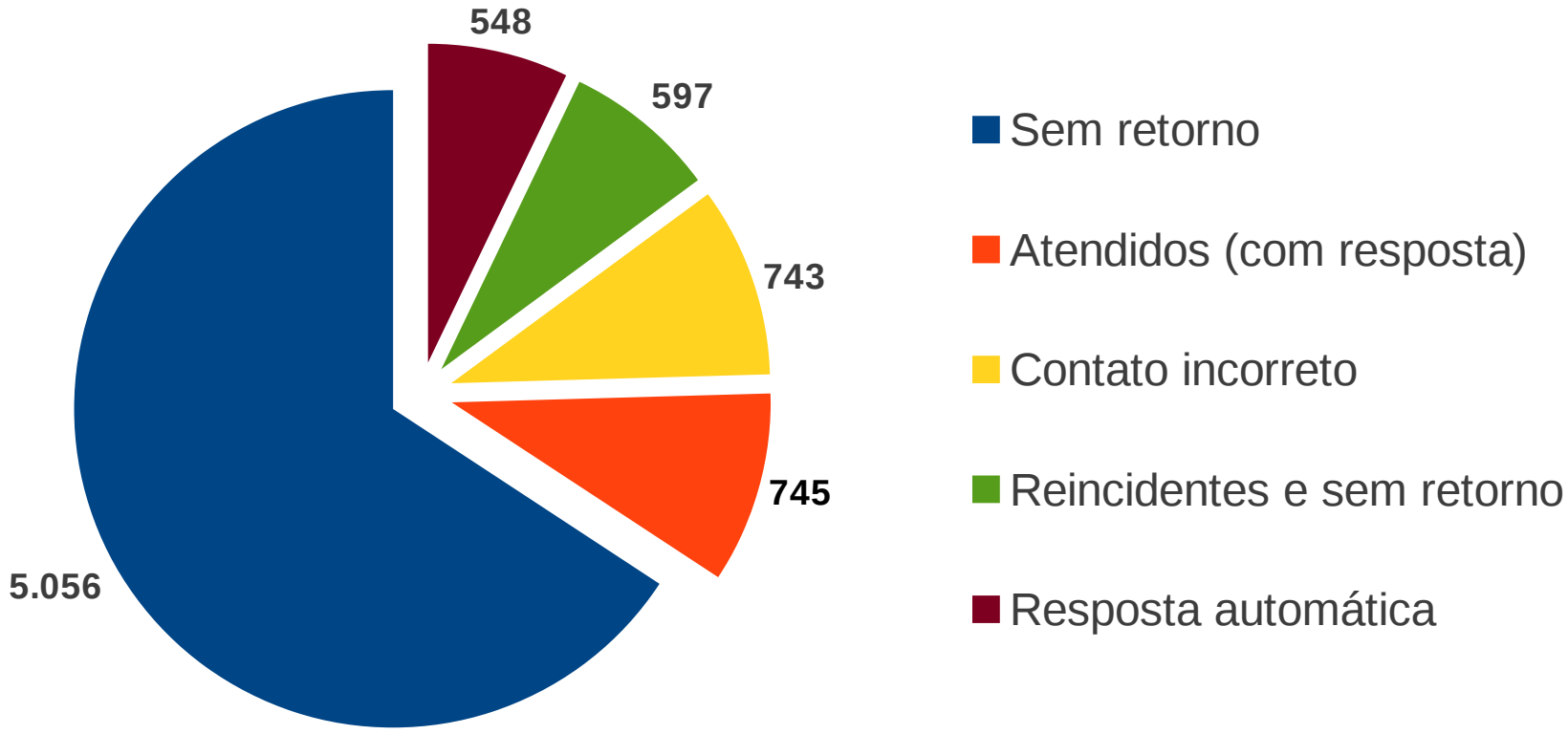
Estatísticas

Retorno dos Chamados 2013 (mensal)



Atendimentos em 2012

Retornos

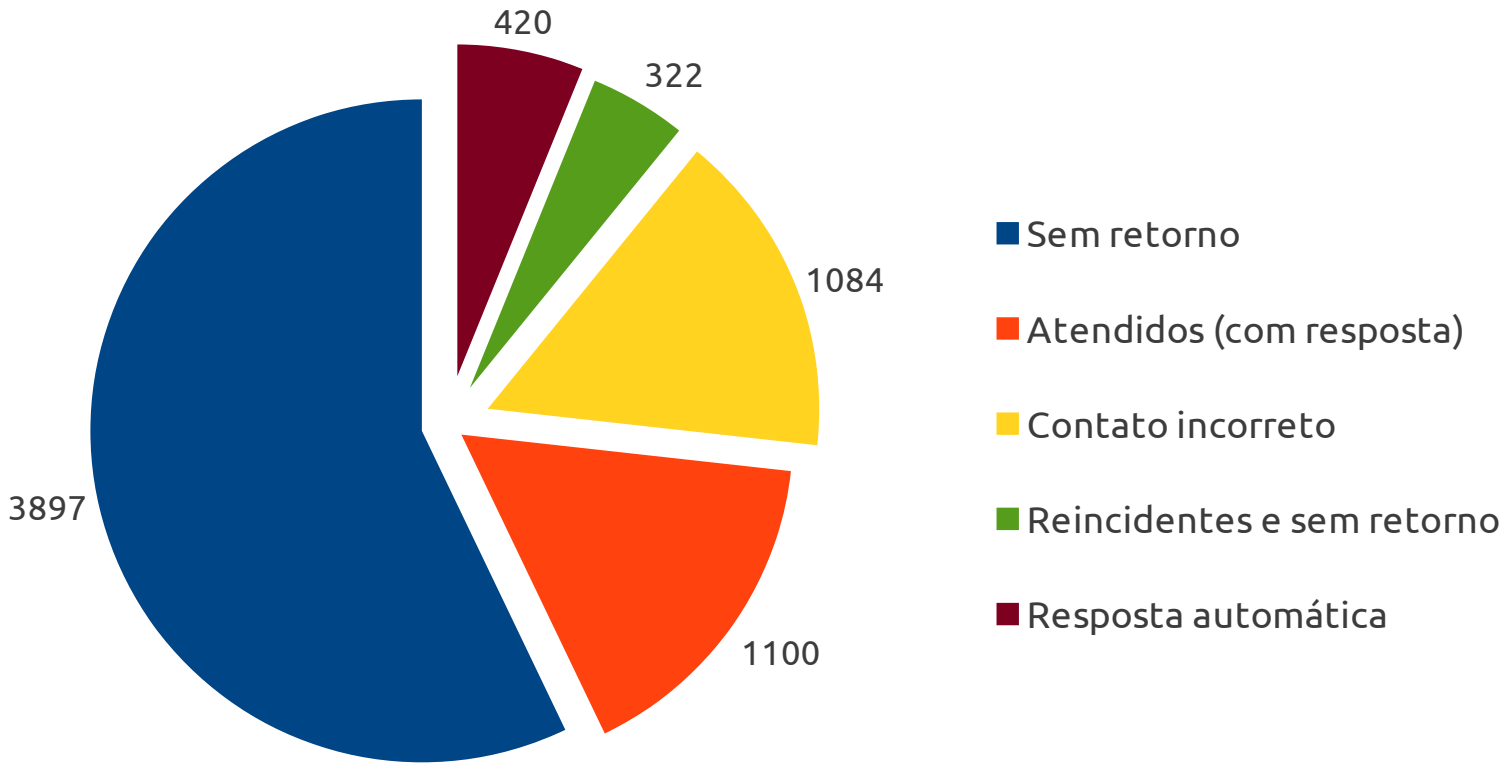


Total de atendimentos: **7.689**

O CSIRT solicitou o bloqueio de aproximadamente **198** IPs externos referentes a **597** chamados com reincidência e sem retorno.

Atendimentos em 2013

Retornos (até 13/09)

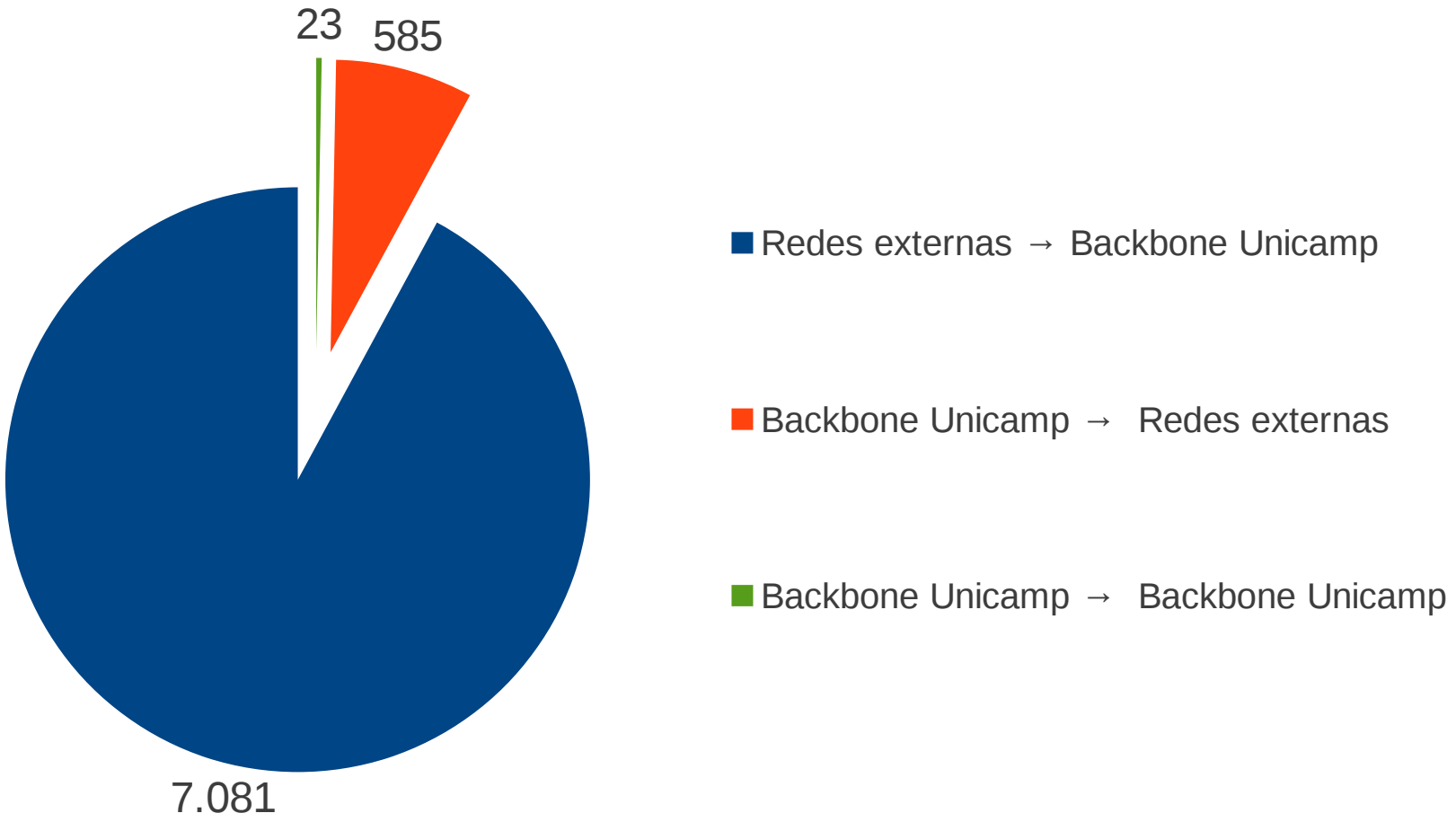


Total de atendimentos: **6.427**

O CSIRT solicitou o bloqueio de aproximadamente **130** IPs externos referentes a **322** chamados com reincidência e sem retorno.

Atendimentos em 2012

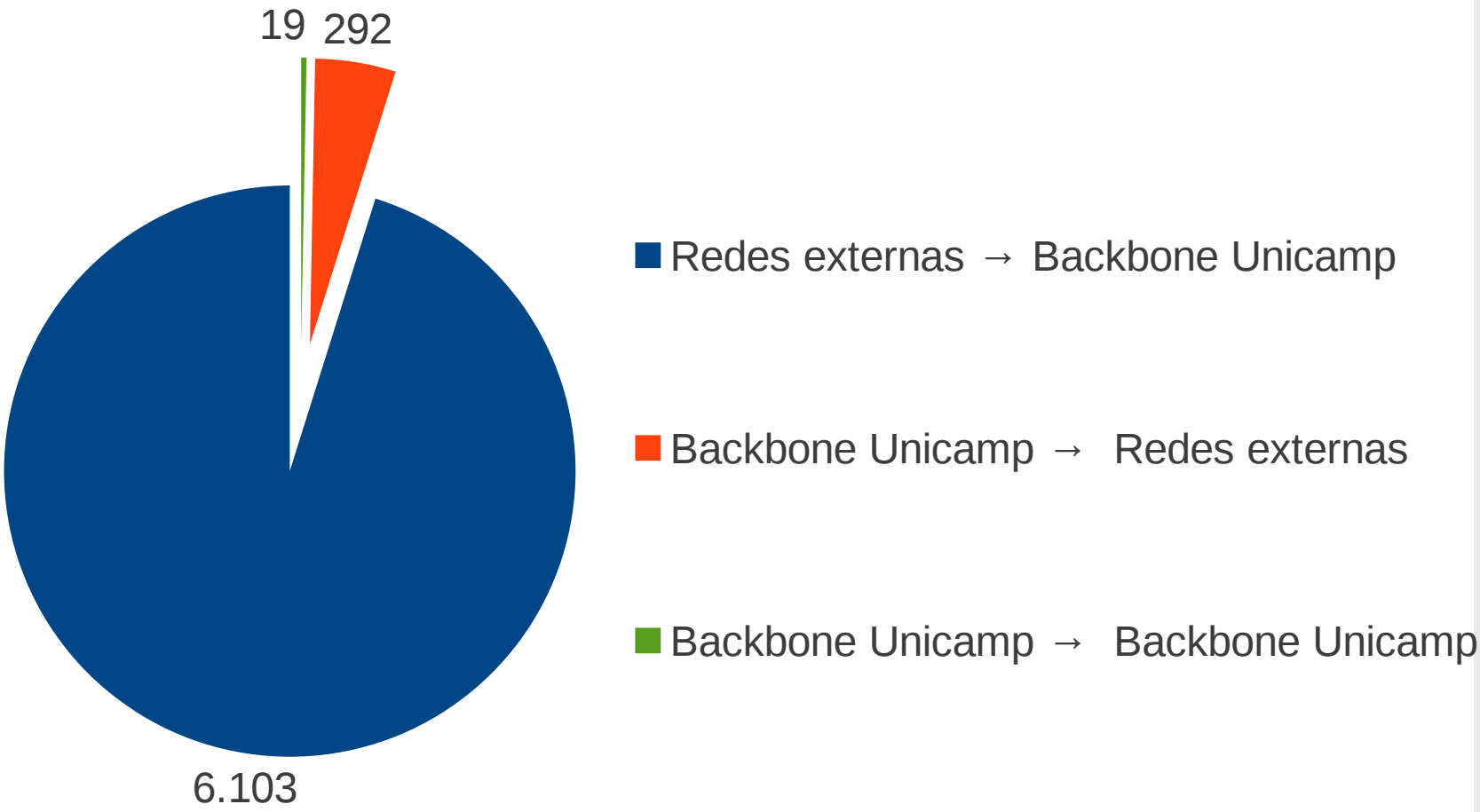
Origem x Destino



Total de atendimentos: 7.689

Atendimentos em 2013

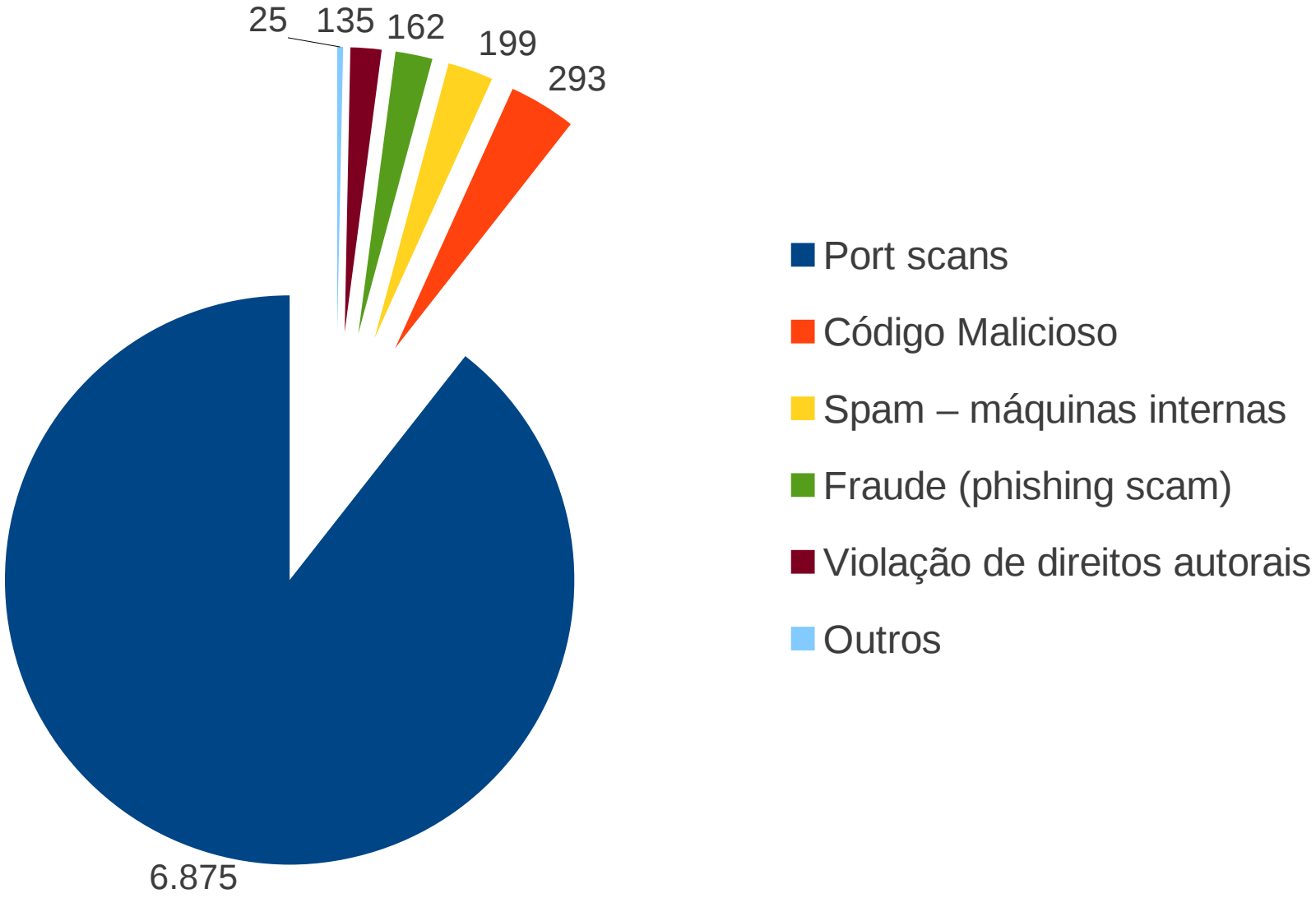
Origem x Destino



Total de atendimentos: 6.427

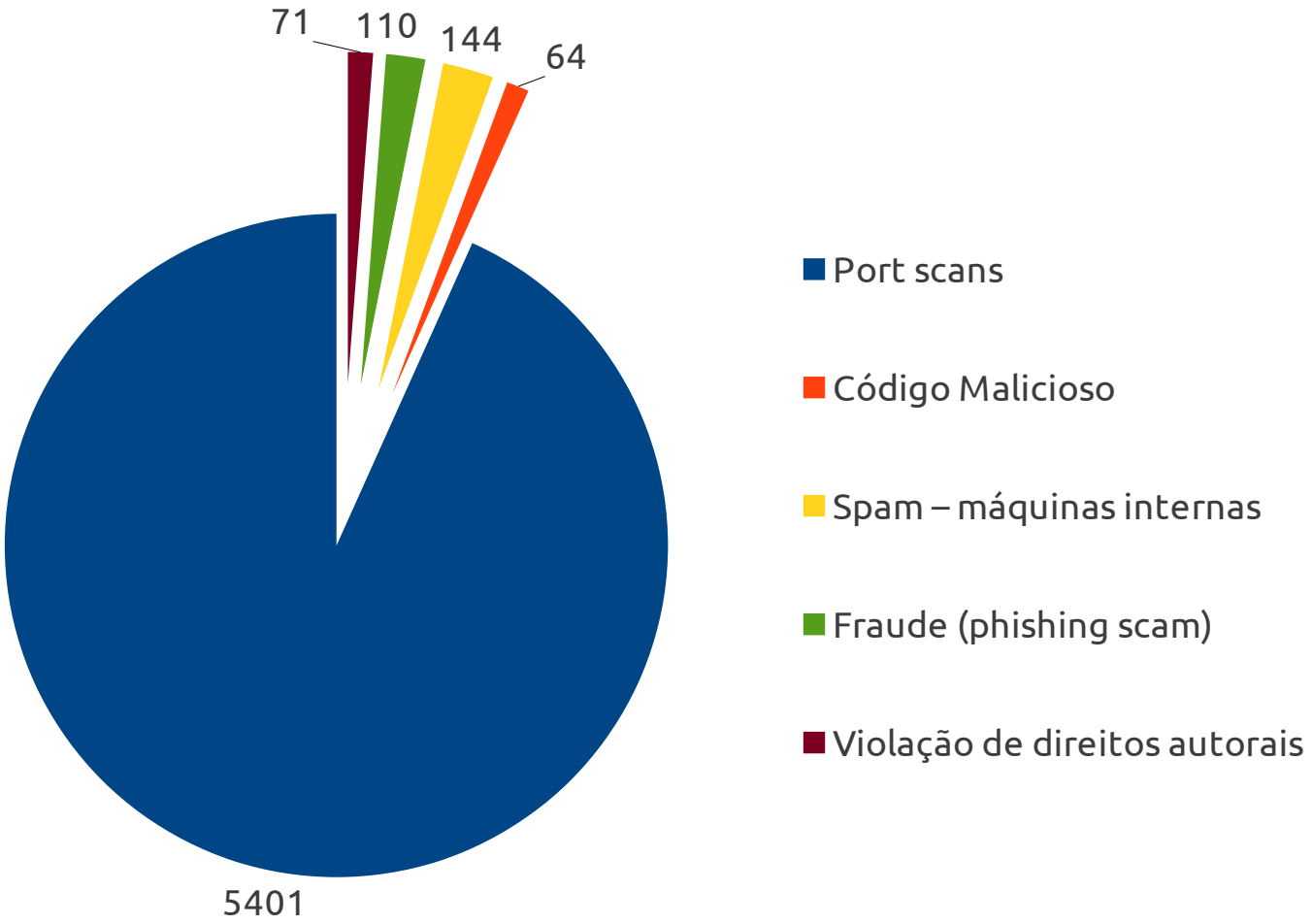
Atendimentos em 2012

Resumo dos atendimentos



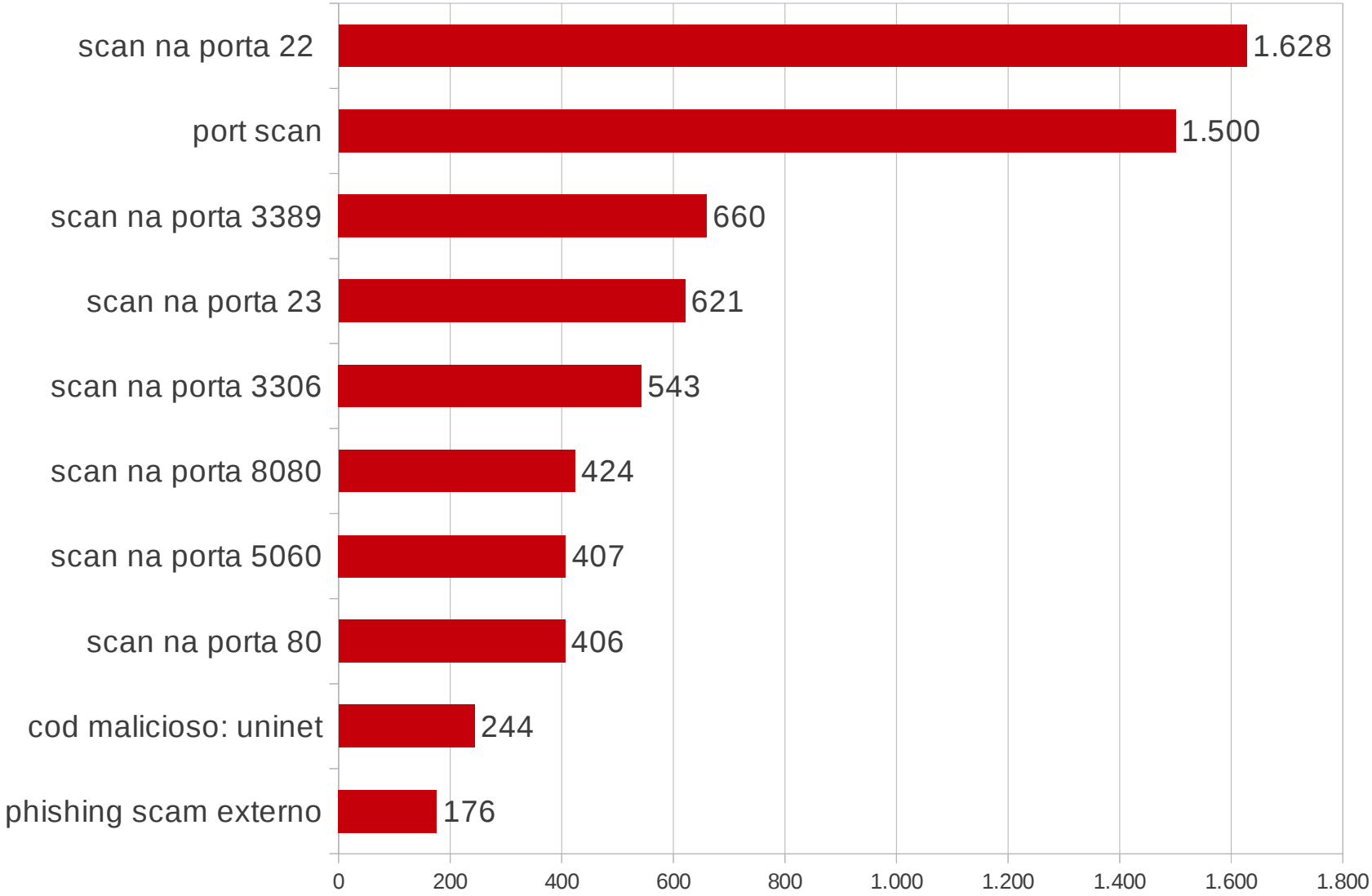
Atendimentos em 2013

Resumo dos atendimentos



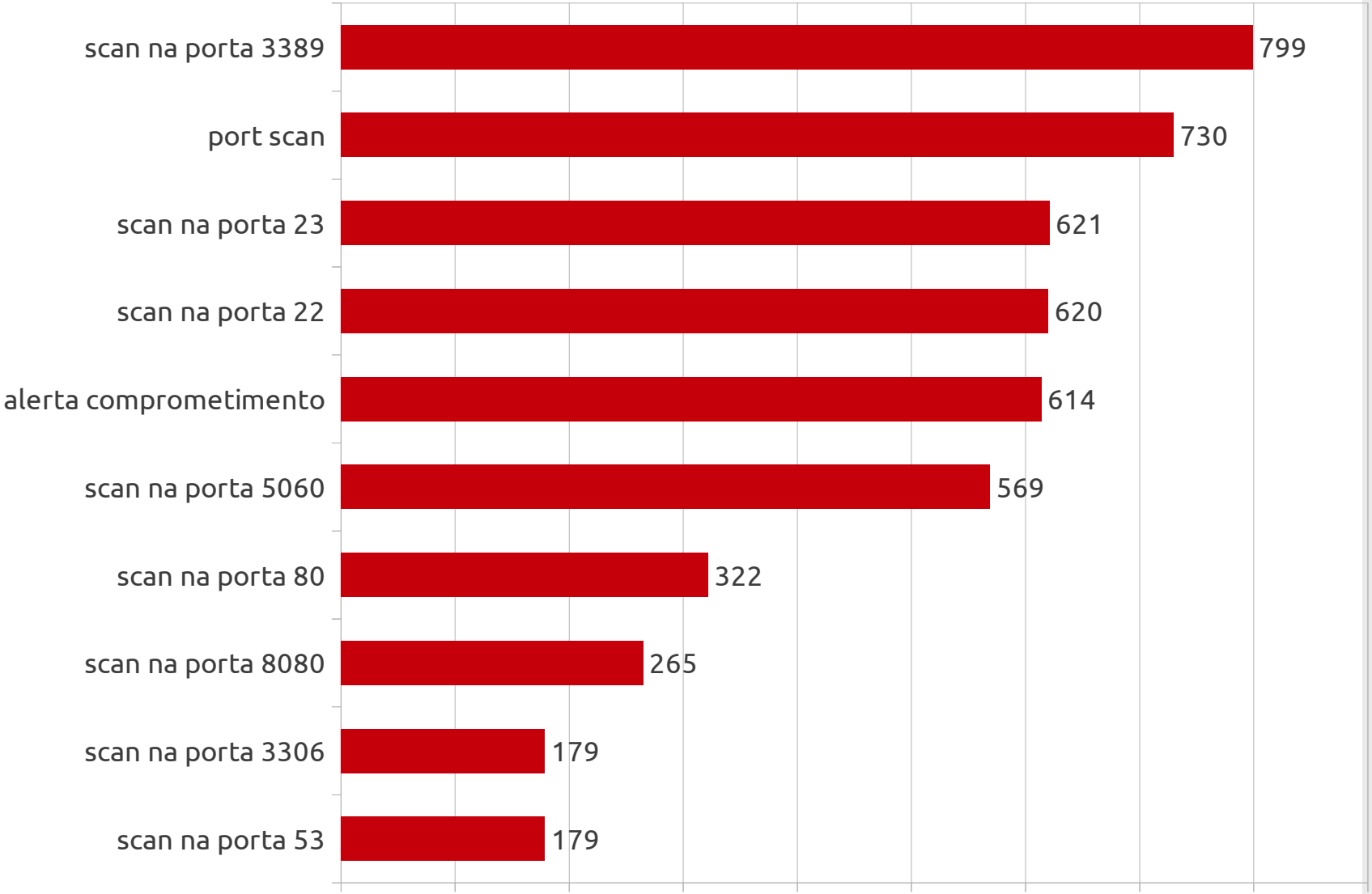
Atendimentos em 2012

Tipos de Ataque - Top 10



Atendimentos em 2013

Tipos de Ataque - Top 10



Sucesso...

- Preocupação dos técnicos de TIC com segurança da informação;
- Conscientização e crescimento das equipes de TIC nos Órgãos/Unidades;
- Investimento/evolução dos ativos de rede;
- Trabalho colaborativo entre o CSIRT e os técnicos de TI (agilidade na solução de problemas);
- Trabalho colaborativo entre o CSIRT Unicamp e outros CSIRTs do mundo;
- CSIRT possuir autonomia de trabalho e apoio da administração da Instituição

Outras atividades

- Divulgar boletins com *bugs* de segurança;

- Manter o ambiente computacional de trabalho da Equipe;

- Manter o ambiente da ICP Unicamp (certificados digitais);

- Elaborar em conjunto com alguns técnicos de TIC da Universidade uma Política de Segurança da Informação;

Próximos passos...

CCUEC

- Novo site da equipe;

- Atividades preventivas em Segurança da Informação;

- Tornar a segurança de TIC responsabilidade de todos:
  - Ingressantes;
  - Eventos internos.

- Consolidar as ferramentas de tratamento de incidentes;

Contatos

E-mail institucional: security@unicamp.br

Telefones: 3521-2289 ou 3521-2290

Analistas de TIC:

Daniela: daniela@ccuec.unicamp.br

Gesiel: gesielgb@ccuec.unicamp.br

Vanderlei: vando@ccuec.unicamp.br

Fim !