

CLAVIS

segurança da informação

οἰκονομική πληροφορία





Soluções de Segurança da Informação para o mundo corporativo

(para cada problema, algumas soluções!)

Rafael Soares Ferreira

Diretor de Resposta a Incidentes e Auditorias

rafael@clavis.com.br

>> Segurança da Informação

Disponibilidade

Confidencialidade

Integridade



>> Vulnerabilidades

- Falhas de projeto, implementação ou configuração de redes, sistemas ou aplicações
- Resultam em violação da segurança
- Algumas vezes são descobertas pelo próprio fabricante, outras não...



>> Vulnerabilidades

Onde encontrá-las?

- Listas de discussão
- Site do Fabricante
- Sites especializados
- Todas as anteriores...



www.seginfo.com.br



>> Incidentes de Segurança

- Comprometimento dos pilares da SI
- Violação da política de segurança



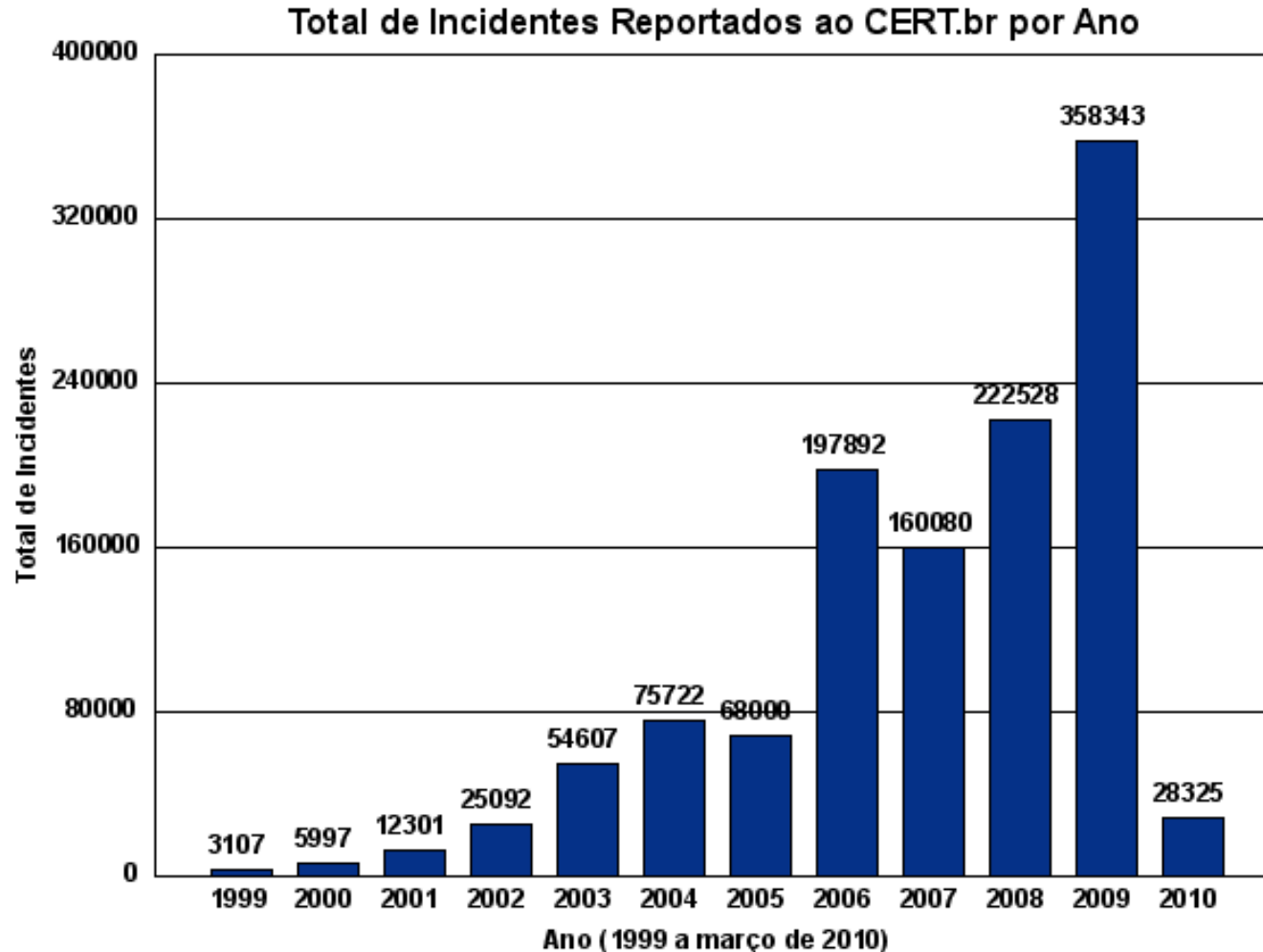
- Vírus, Worms, Cavalos de Tróia ...
- Acesso não Autorizado (Interno/Externo)
- Fraudes / Engenharia Social
- Furto de Equipamentos
- Negação de Serviço



- Pichação de Sites (Defacement)
- Injeção de Códigos
- Senhas Padrão / Força Bruta
- Captura de Tráfego
- Vulnerabilidades



Principais Ameaças

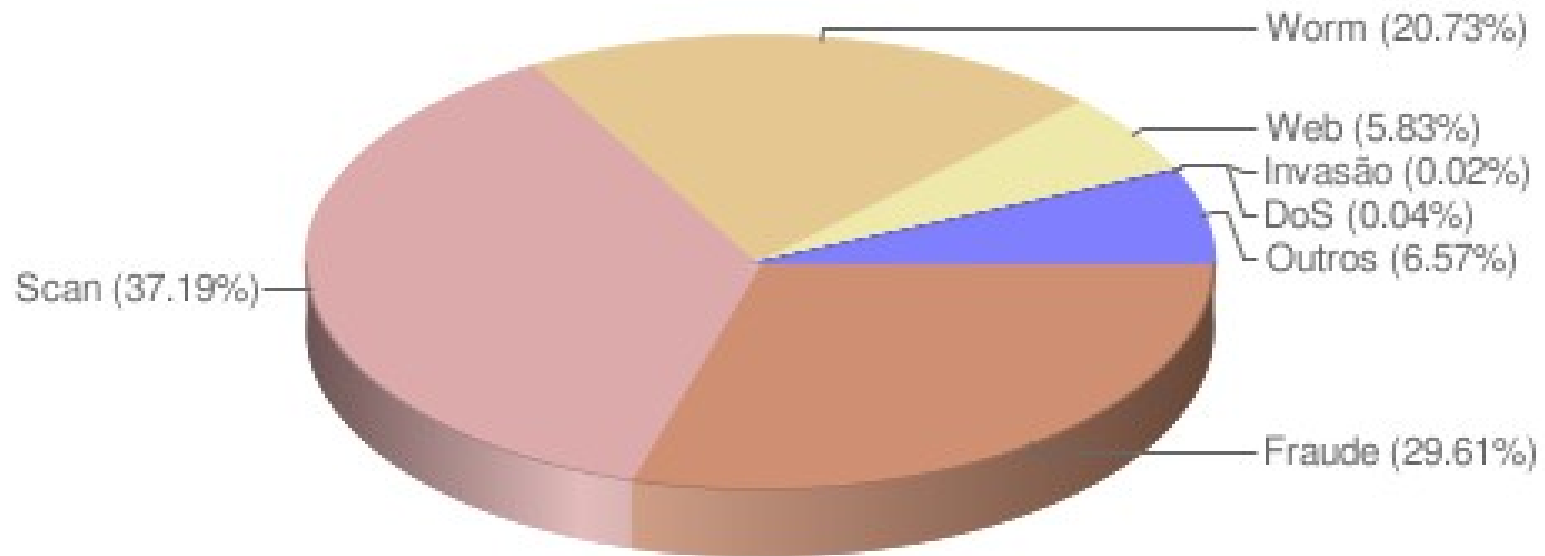


Fonte: Cert.br



Principais Ameaças

Incidentes reportados
(Tipos de ataque)

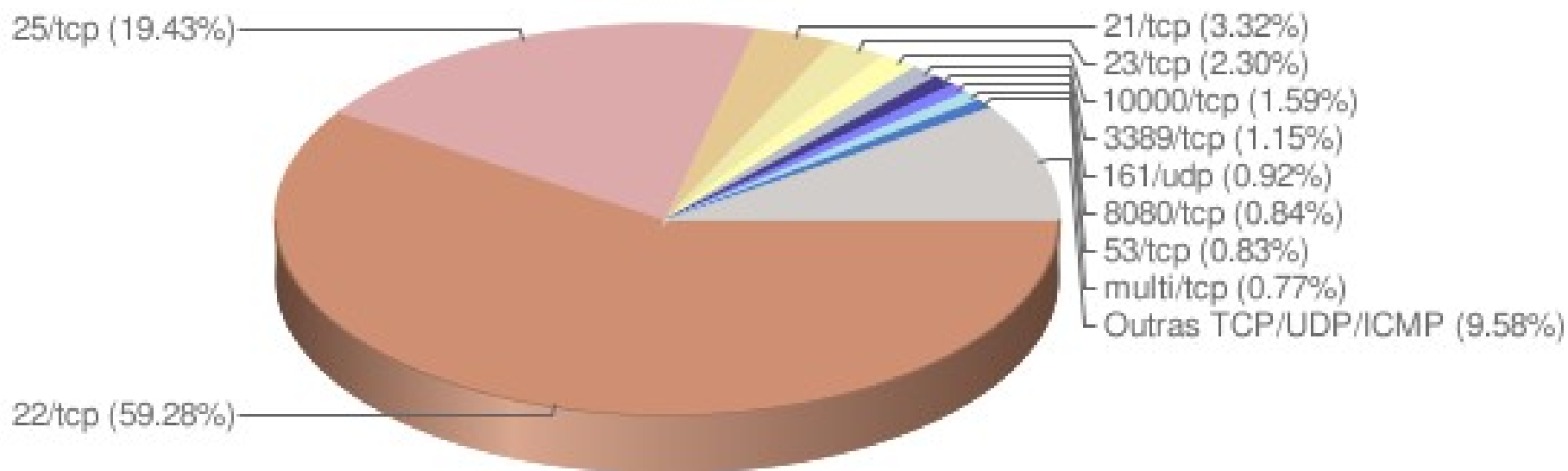


Fonte: Cert.br



Principais Ameaças

Scans reportados, por porta
(Não inclui scans realizados por worms)

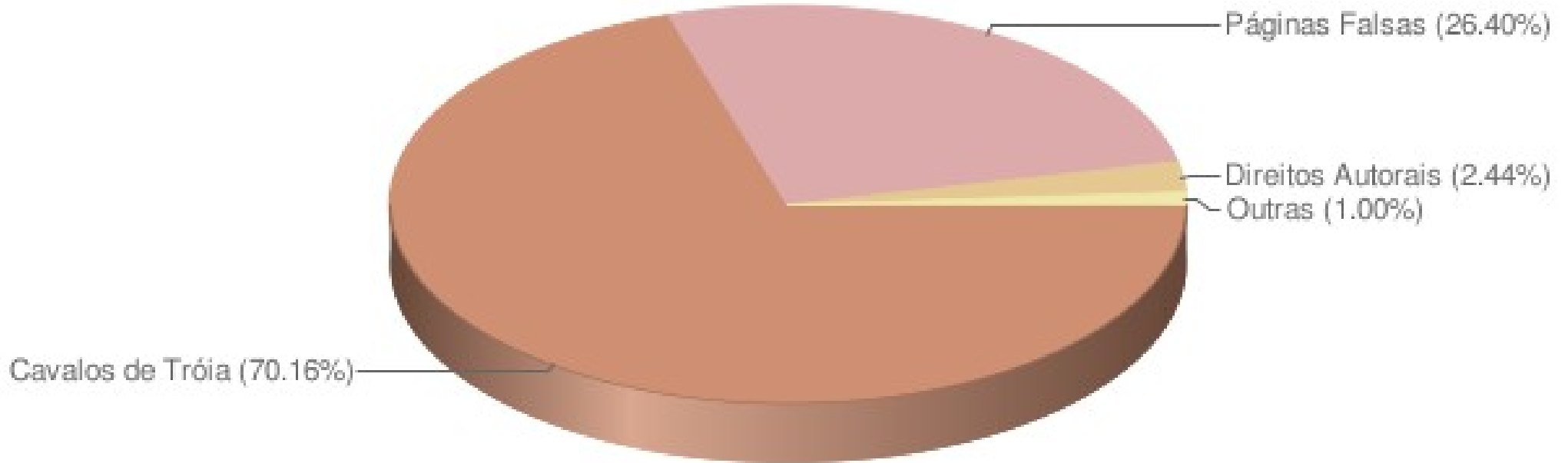


Fonte: Cert.br



Principais Ameaças

Tentativas de fraudes reportadas



Fonte: Cert.br



- Normas, Processos e Diretrizes
- Continuidade do Negócio
- Conscientização e Orientação
- Padronização nos processos organizacionais
- Definição de responsabilidades
- Conformidade



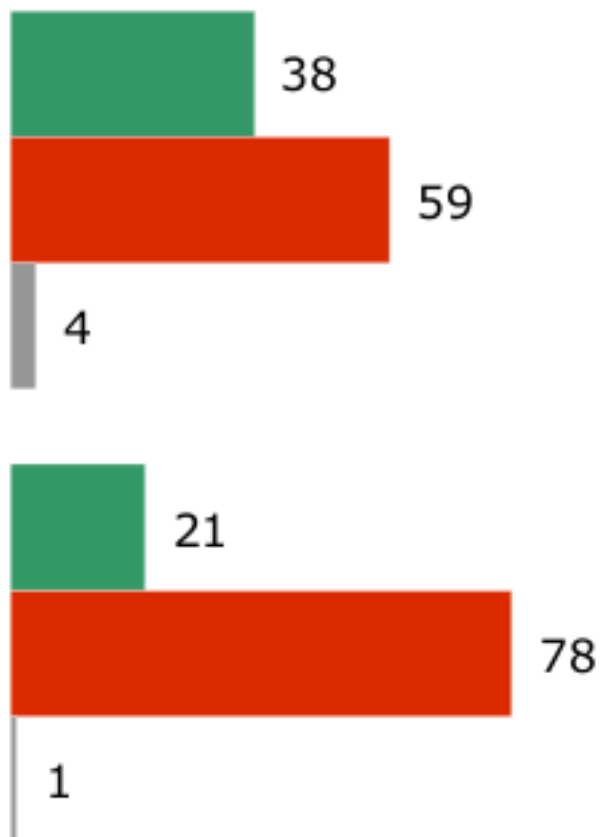
- Divulgação dos conceitos de segurança
- Melhor aceitação de controles de segurança
- Conscientização sobre os riscos
- Capacitação Técnica
- Prevenção contra ataques de Engenharia Social



Medidas de Apoio à SI

2009

■ Sim ■ Não ■ NS/ NOP



- **Política de Segurança ou de uso aceitável**

- **Programa de Treinamento em SI para funcionários**

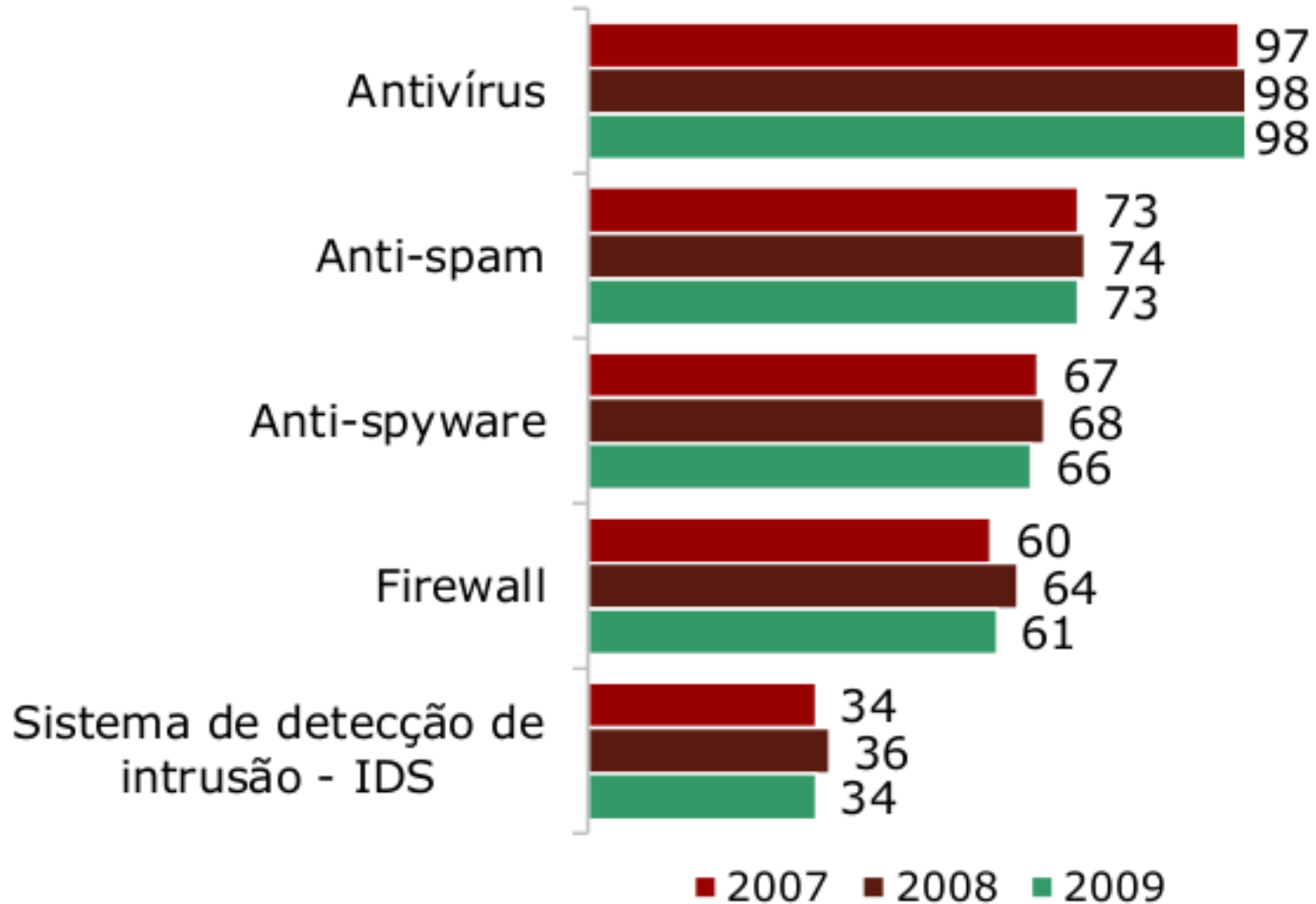
Fonte: Cetic.br



- Controles de Acesso
- Sistemas de Detecção/Prevenção de Intrusão
- Sistemas de Monitoramento
- Sistemas Anti-vírus e Anti-Spam
- Filtro de Conteúdo Web
- Soluções de Backup e Redundância
- Gerenciamento de Registros (Logs)



Tecnologias Adotadas



Fonte: Cetic.br



Tecnologias Adotadas



Fonte: Cetic.br

- Mapeamento de processos
- Análise de vulnerabilidades
- Avaliação do grau de exposição
- Conformidade com boas práticas



- Análise de desempenho e vulnerabilidades
- Constante fortalecimento dos servidores
- Controles de segurança
- Alta Disponibilidade



- Simulação de ataques reais
- Teste dos controles de segurança existentes
- Homologação e Conformidade
- Testa sistemas, equipes e processos
- *OSSTMM, ISSAF, NIST800-42, OWASP*





>> **OSSTMM**

Open Source Security Testing Methodology Manual



>> **NIST 800.42**

Guideline on Network Security Testing



>> **OWASP**

Open Web Application Security Project



>> **ISSAF**

Information Systems Security Assessment Framework



- Projeto e Implementação segura
- Cobertura e Exposição
- Controles de Acesso ao meio
- Políticas de Uso



- Encaminhamento de incidentes
- Recomendações de correção
- Isolamento e Contensão
- Recuperação
- Investigação das causas principais
- Implementação de Correções



- Coleta de dados
- Preservação das Evidências
- Correlação das Evidências
- Elaboração da linha do tempo
- Respaldo jurídico
- Laudo pericial



Fim...

Muito Obrigado!

Rafael Soares Ferreira

rafael@clavis.com.br

