

# II Encontro Estadual de Controle Interno

**Riscos Envolvidos com a  
Utilização de Sistemas e  
Tecnologia da Informação**

Cláudio Reginaldo Alexandre



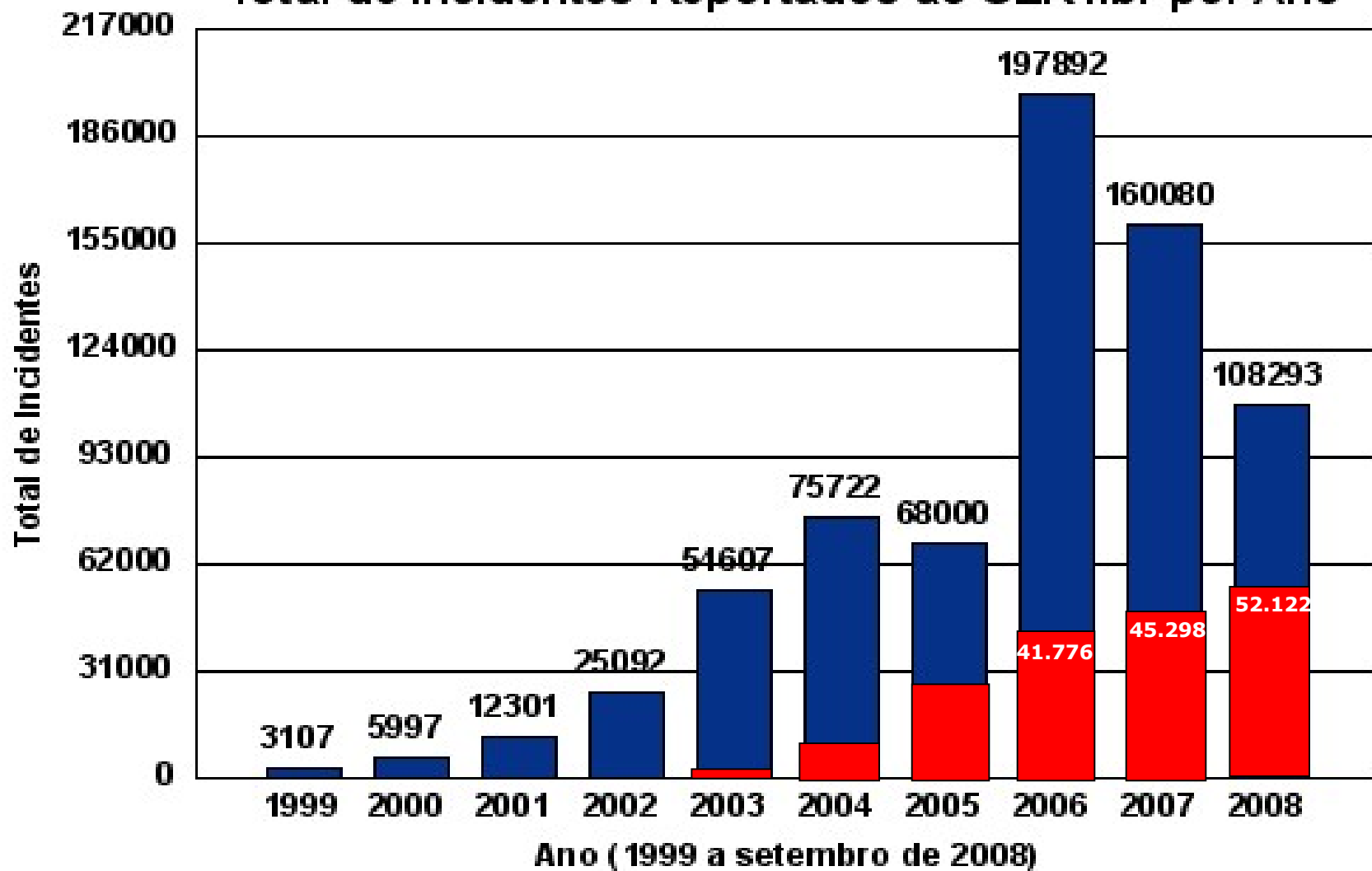
# Panorama Atual



Números e Informações



## Total de Incidentes Reportados ao CERT.br por Ano



Fonte: <http://www.cert.br>

■ **Fraudes**



# Ação repressora

## NOTÍCIAS

### **Polícia Federal prende quadrilha que desviava dinheiro pela internet**

(<http://pcworld.uol.com.br/noticias/2008/05/13/policia-federal-prende-quadrilha-que-desviava-dinheiro-pela-internet>)

Redação do IDG Now!

13-05-2008

#### **Crackers obtinham senhas bancárias a partir dos PCs dos correntistas; ação envolveu mandados de prisão em sete Estados.**

A Operação Cardume da Polícia Federal desarticulou, nesta terça-feira (13/05), uma quadrilha especializada em cibercrimes. A PF cumpriu 27 mandados de prisão, além de 42 mandados de busca e apreensão no Rio Grande do Sul, Santa Catarina, São Paulo, Rio de Janeiro, Minas Gerais, Bahia e Sergipe.

Os criminosos obtinham senhas bancárias por meio de phishings, que instalavam malwares na máquina do usuário. A partir dos dados obtidos, os crackers transferiam dinheiro para contas de laranjas, além de pagar contas e fazer compras online.

As investigações, iniciadas em 2007, foram conduzidas pela Delegacia de Repressão a Crimes Fazendários (DELEFAZ), da Polícia Federal do Rio Grande do Sul, e iniciaram em 2007. A ação foi um desdobramento da Operação Navegantes, quando foram presos 15 crackers e laranjas.

A PF estima que a quadrilha fez mais de 200 vítimas e que fraudes totalizaram em torno de 500 mil reais por mês.

Os integrantes da quadrilha serão indiciados por furto qualificado, formação de quadrilha, interceptação informática não autorizada e receptação - podendo ser condenados ao pagamento de multas e máximo de 8 anos de prisão.



Fonte: <http://pcworld.uol.com.br/>

# Contra-ataque

---



05/05/2008  
Seção: Overview -

---

## F-Secure identifica nova técnica para golpes na Internet

Risk Report

A F-Secure, fabricante finlandês de soluções de segurança, identificou cybercriminosos de phishing estão utilizando uma nova técnica para ataques à usuários na Internet. Agora eles enviam e-mails com cavalo-de-tróia espião, ao invés daqueles que pedem para a vítima digitar número de conta ou senha.

Os e-mails trazem mensagens oferecendo aos clientes uma ferramenta de segurança para acessarem suas contas pela Internet sem riscos. Para cair no golpe, basta que a vítima faça o download do suposto certificado digital e o instale no computador. Com a ferramenta de espionagem instalada, o criminoso poderá obter todas as informações do computador que desejar.

---

Copyright © 2007 Conteúdo Editorial

# Onde os Bandidos Atuam

---



Fonte: <http://www.antiphishing.org>

---





# Evidências

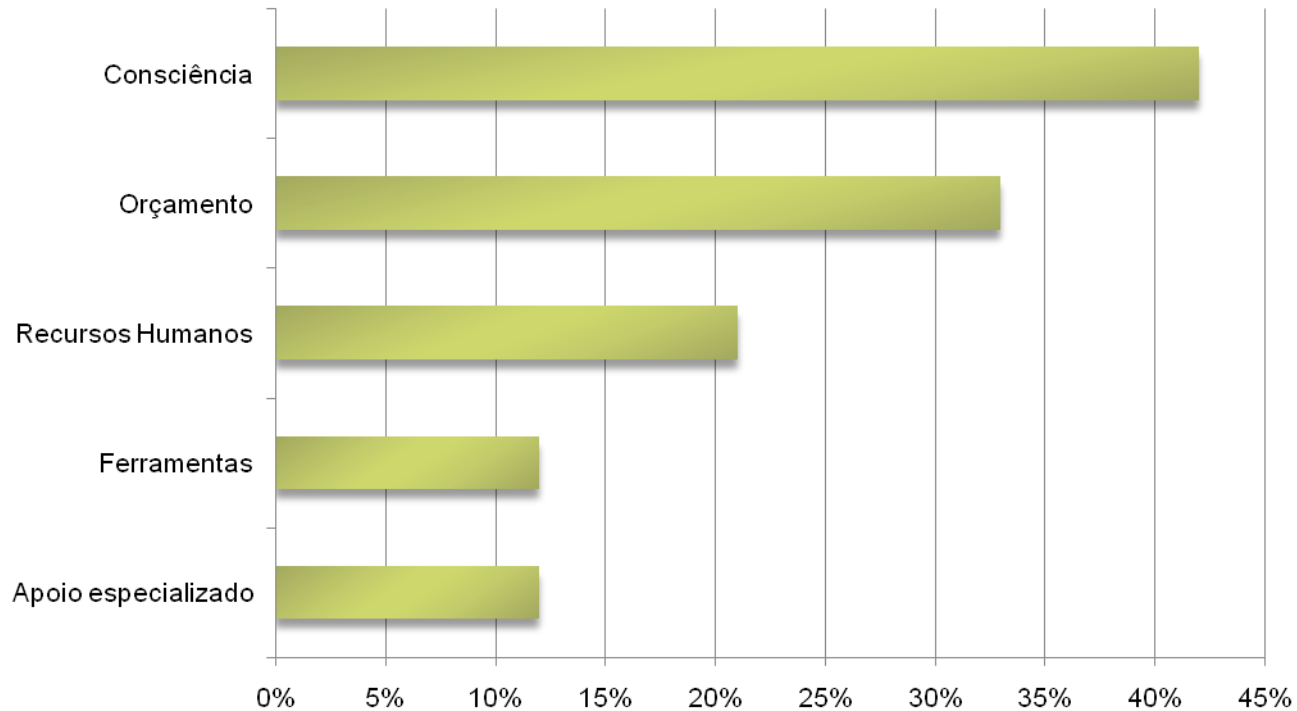
---

- ▶ Todas as estatísticas mostram grande queda no número de ataques diretos
  - ▶ Isso pode significar que as médias e grandes empresas melhoraram seu nível de segurança com *softwares* e *hardwares*
- ▶ Os bandidos passaram a investir no elo mais fraco – clientes e usuários
- ▶ As empresas continuam com dificuldades de implantar uma cultura de segurança com os funcionários
- ▶ Funcionários e clientes desconhecem os riscos existentes no ambiente de informática

# Ciclo Vicioso

---

## Obstáculos à Implementação da Segurança



Fonte: Academia Latino-Americana de Segurança da Informação – dez/2007



# Consciência dos Riscos Existentes



Árdua Tarefa

# Sobre Risco em Informática

---

## ▶ Verdades

- ▶ Todo sistema informatizado tem vulnerabilidades
- ▶ Não existe 100% de segurança
- ▶ Não existe risco zero

## ▶ As pessoas têm consciência dos riscos que correm?

# Risco vs Medidas de Segurança

---

## ▶ Risco (R)

- ▶ É a probabilidade de que agentes, que são ameaças (A), explorem vulnerabilidades (V), expondo os ativos a perdas de confidencialidade, integridade e disponibilidade, e causando impactos (I) nos negócios. Os impactos são limitados por medidas de segurança (M) = controle

$$R = \frac{A \times V \times I}{M}$$



# Profusão de Ameaças

---

- ▶ Ameaças Intencionais
- ▶ Ameaças Acidentais
- ▶ Ameaças Ativas
- ▶ Catástrofes
- ▶ Pane na comunicação e no suprimento de energia
- ▶ Pane na rede
- ▶ Problemas nos sistemas operacionais
- ▶ Problemas nos sistemas corporativos
- ▶ Comportamento anti-social – paralisações e greves; alcoolismo e drogas; rixas entre funcionários setores, gerências, diretorias; inveja profissional; etc.
- ▶ Ação criminosa – furtos e roubos, fraudes, sabotagem, terrorismo e atentados, seqüestros, espionagem industrial, engenharia social, etc.



# Diversidade de Medidas de Segurança

---

- ▶ Política de Segurança
- ▶ Criptografia forte
- ▶ Certificação Digital
- ▶ Controle de Acesso (físico e lógico)
- ▶ Segurança física
- ▶ Política de *backup*
- ▶ Plano de Continuidade de Negócios
- ▶ Monitoração
- ▶ *Firewall*
- ▶ Segurança de roteadores
- ▶ Filtros de conteúdo
- ▶ Política de senha
- ▶ Detecção de intrusos
- ▶ Teste de invasão
- ▶ Alertas
- ▶ Treinamento/Conscientização dos usuários
- ▶ Auditoria de sistemas
- ▶ Antivírus



# Segurança Lógica e Segurança Física

Disciplinas Complementares

# Segurança Lógica

---

## ▶ Problemas

- ▶ Ataques lógicos à rede de computadores
- ▶ Implantação de códigos maliciosos
- ▶ Captura de senhas
- ▶ Roubo de informações
- ▶ Manipulação de informações

## ▶ Soluções

- ▶ Equipamentos de análise e filtros de acesso
- ▶ Estrutura de Perfis de Acesso
- ▶ Controle de acesso lógico – Política de senha forte
- ▶ Uma única identificação por usuário
  - ▶ Sistemas não controlam acesso, sistemas controlam perfis

# Segurança Física

---

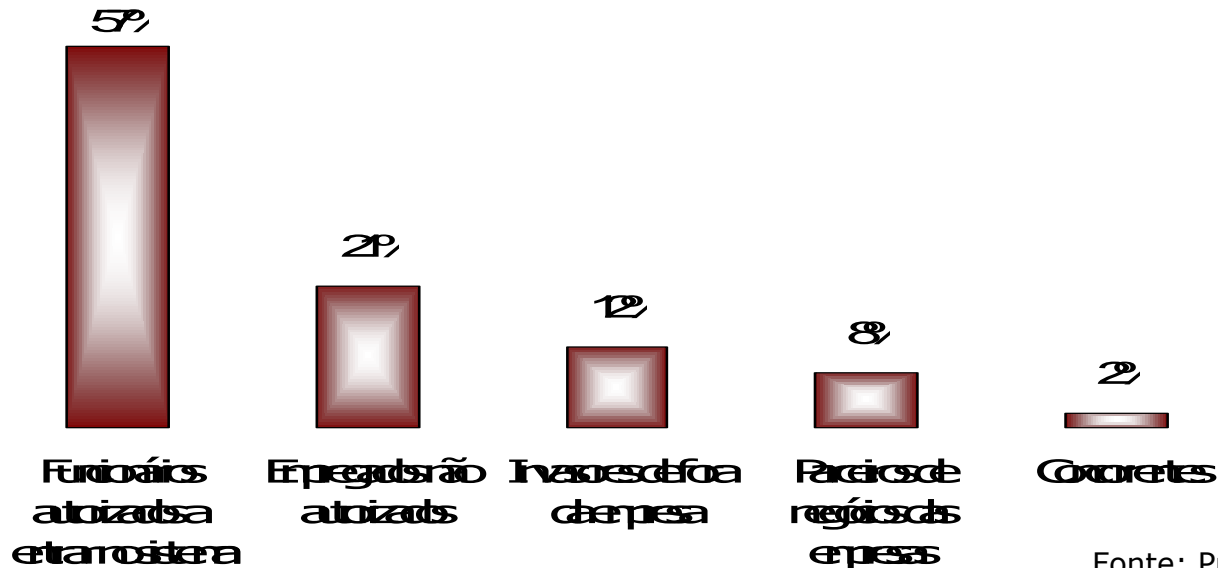
## ▶ Problemas

- ▶ Acesso indevido
- ▶ Roubos de equipamentos
- ▶ Ameaça à integridade física dos funcionários
- ▶ Ameaça ao patrimônio da empresa
- ▶ Engenharia Social

## ▶ Soluções

- ▶ Controle eficaz de identificação
- ▶ Acesso setorizado e controlado
- ▶ Sistema de controle e monitoramento de acesso físico
- ▶ Colaboradores treinados para cumprimento das normas

# Aspecto Especial da Segurança Lógica



Fonte: Pricewaterhouse Coopers

- ▶ Segurança no desenvolvimento de sistemas
- ▶ 62% das empresas usam dados reais nos testes
- ▶ Risco da transferência do conhecimento para os sistemas
- ▶ Sistemas sem trilhas de auditoria
- ▶ Terceirização baseada em alocação de mão-de-obra

# Arsenal de Defesa

Também é Preciso Rever Posturas

# Verdades

---

*“Se fizermos tudo que o pessoal de segurança quer, não fazemos negócio.*

*Se fizermos tudo como o pessoal de negócios deseja, não teremos segurança.”*

*Laércio Albino Cruz – VP do Bradesco*

- ▶ Eficiência em tecnologia da informação significa entrega e disponibilidade.
  - ▶ Entrega implica em rapidez com qualidade
- ▶ A arte está em encontrar o equilíbrio



# Arsenal de Defesa

---

- ▶ Política de Segurança
- ▶ Gestão de Identidade
- ▶ Metodologia de Desenvolvimento de Sistemas
- ▶ Conhecimento e aplicação das normas existentes
  - ▶ NBR ISO/IEC 27001 – Sistemas de Gestão de Segurança da Informação - Requisitos
  - ▶ NBR ISO/IEC 27002 – Código de Prática para a Gestão da Segurança da Informação
  - ▶ NBR ISO/IEC 27005 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Risco de Segurança da Informação
- ▶ Auditoria de Sistemas


# Posturas

---

- ▶ A prática comum da equipe de segurança
  - ▶ Avaliar propostas de implementação e apresentar pareceres, dificilmente entrando no mérito do “como”
- ▶ Qual deve ser o real objetivo da segurança
  - ▶ Definir a forma mais segura da empresa realizar seus negócios, aproveitando eficientemente as oportunidades e mantendo a competitividade
- ▶ Definir as melhores práticas de segurança (consultoria) e atestar sua aplicabilidade (avaliação)


# Preocupações atuais

---

- ▶ Poucas ações de orientação e educação de usuários e clientes
  - ▶ Os usuários apresentam baixo nível de conhecimento sobre as ferramentas e produtos utilizados 

# Preocupações atuais

---

- ▶ Poucas ações de orientação e educação de usuários e clientes
  - ▶ Os usuários apresentam baixo nível de conhecimento sobre as ferramentas e produtos utilizados 
- ▶ Mobilidade: contraste entre os serviços disponíveis
  - ▶ Internet Banking está perdendo a mobilidade
  - ▶ Serviços financeiros pelo celular



# Preocupações atuais

---

- ▶ Colocação de mecanismos/produtos de segurança nos computadores dos clientes
  - ▶ Novas responsabilidades
  - ▶ Profusão de mecanismos de segurança nem sempre conhecidos pelo usuário



# Resumo

---

- ▶ O perigo existe, é real e não pode ser ignorado
- ▶ Os bandidos mudaram seu objetivo, passando a atacar usuários e clientes
- ▶ As empresas e prestadores de serviços não estão investindo na orientação de usuários e clientes
- ▶ A segurança da informação precisa alinhar-se mais ao negócio
- ▶ Os usuários e clientes estão sendo bombardeados com mecanismos de segurança
- ▶ Do ponto de vista da segurança da informação não existe diferença entre serviço público e iniciativa privada

# Obrigado!

Cláudio Reginaldo Alexandre

[cralexandre@oi.com.br](mailto:cralexandre@oi.com.br)