Combatendo Crimes Cibernéticos
Proteção Legal no Brasil

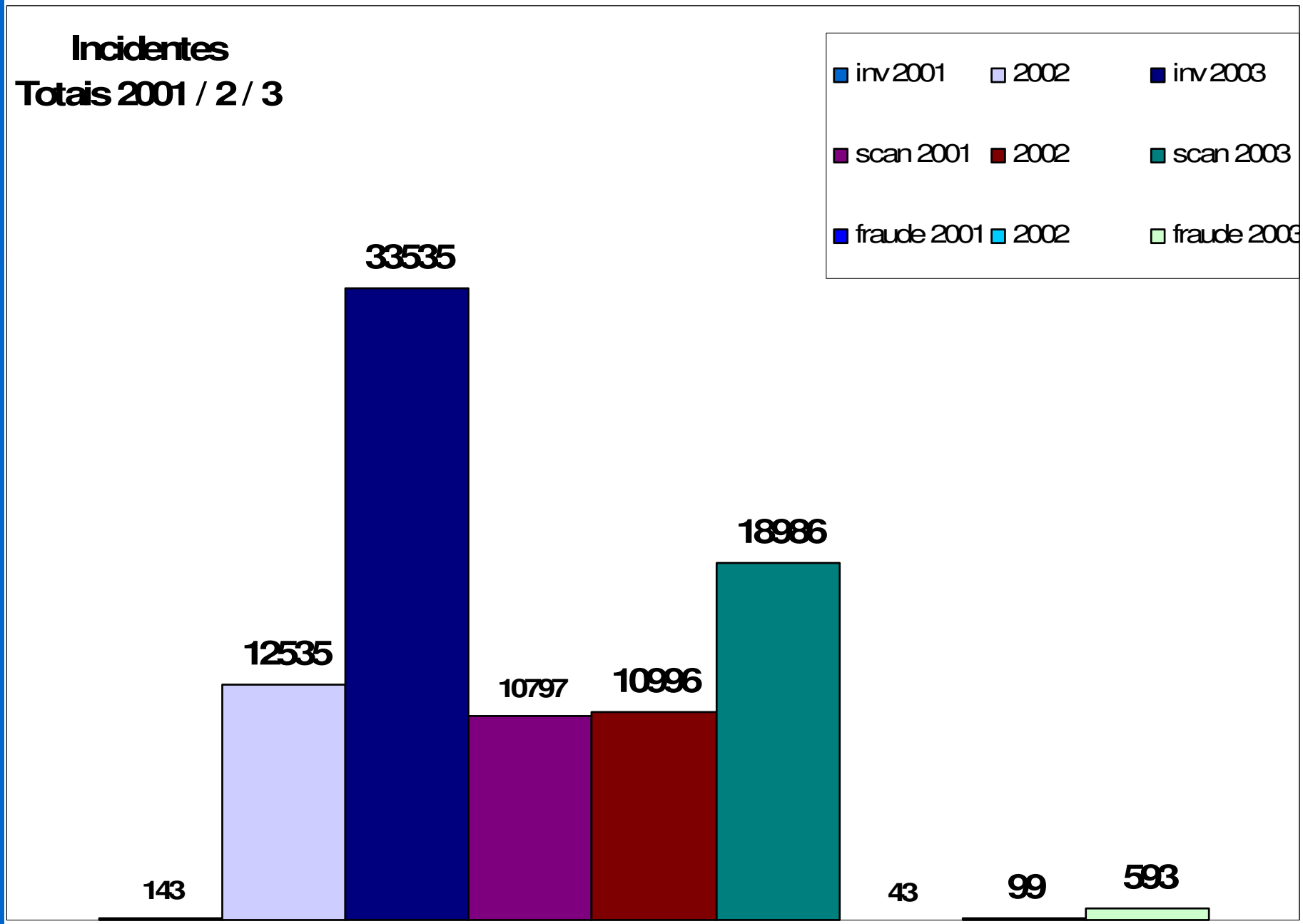
André Machado Caricatti

Jorilson da Silva Rodrigues

Objetivo do Trabalho

Utilizar um modelo de referência aceito internacionalmente para compreender o alcance das medidas legais disponíveis no Brasil para combater ilícitos vinculados à tecnologia da informação.

Empregou-se a *Convenção sobre Crimes Cibernéticos,* do Conselho da Europa, editada em 23/11/2001, enumerada como *European Treaty Series* – ETS 185

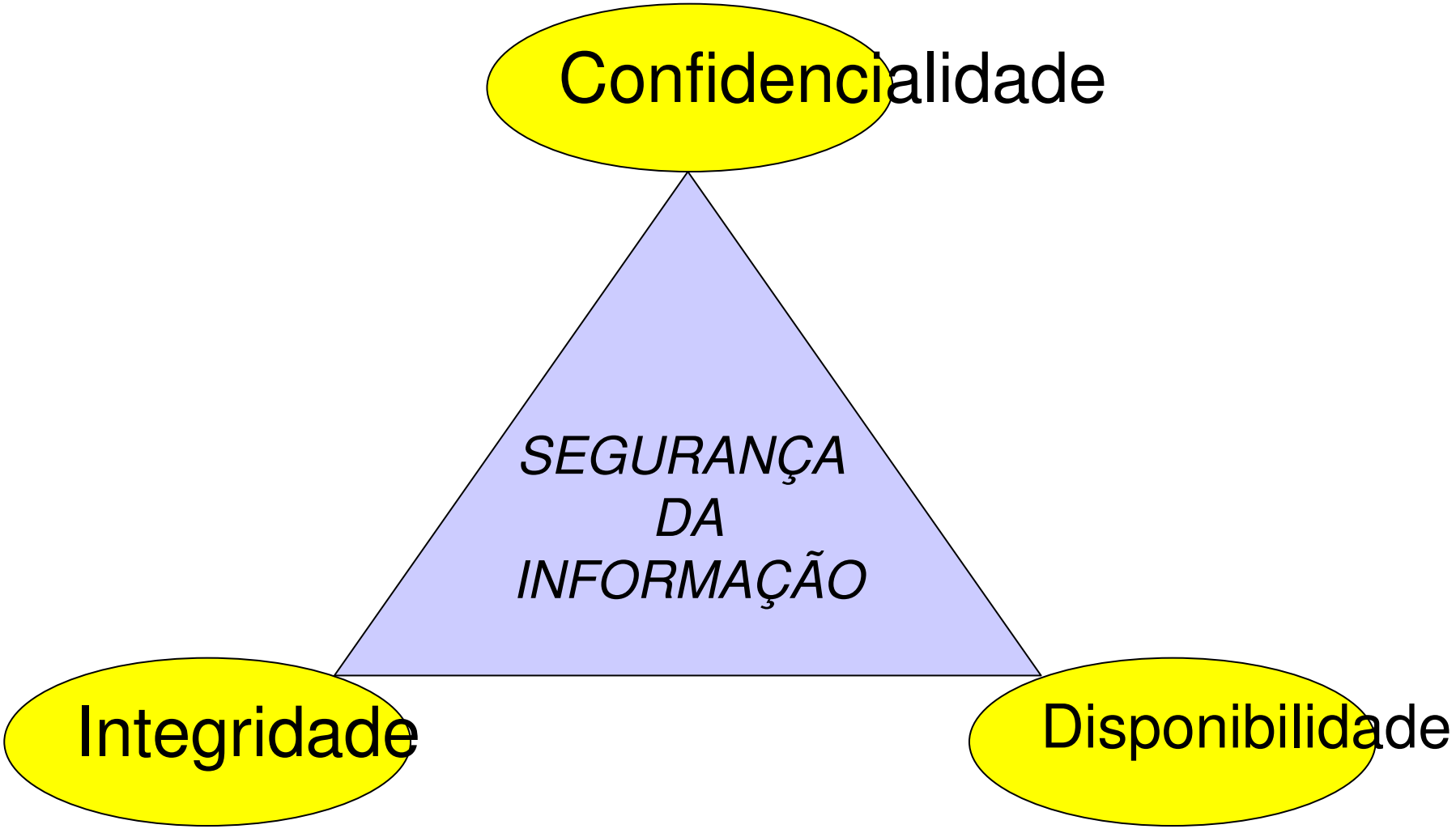


andrecaricatti@apcf.org.br

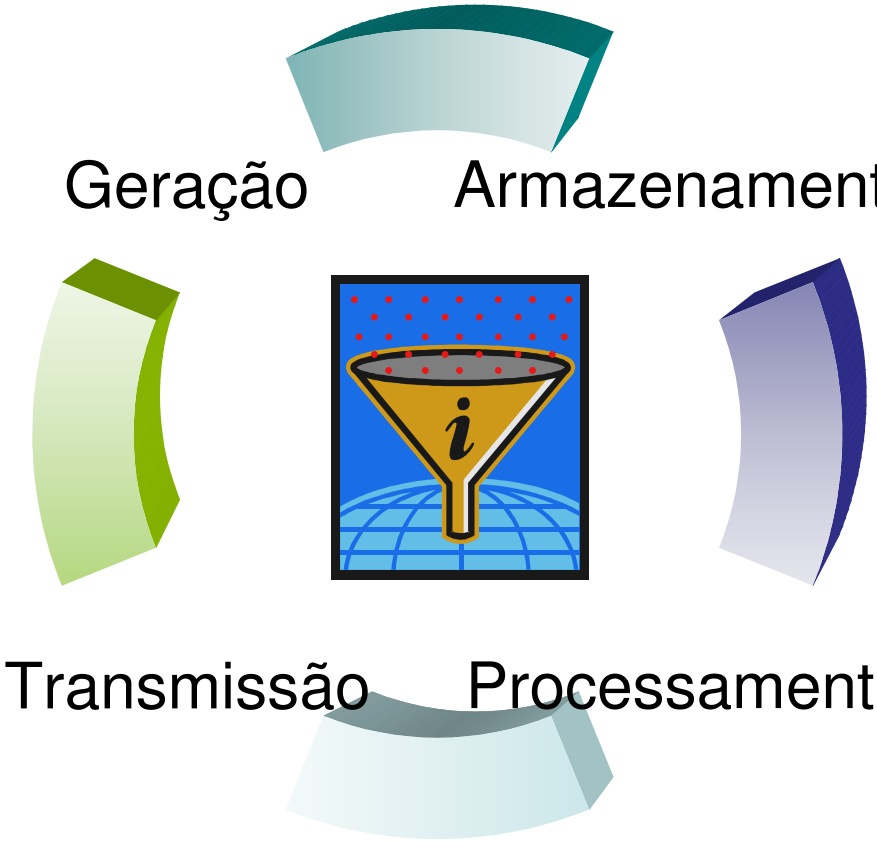
ISO 17799 - Informação

"**Informação** é um ativo que como qualquer outro, é importante para o negócio, tem valor para a organização e necessita ser protegido adequadamente.

A **segurança da informação** protege a informação de uma grande quantidade de ameaças, assegurando assim a continuidade do negócio, minimizando os danos, e maximizando o retorno sobre os investimentos e oportunidades de negócios."


Confidencialidade
SEGURANÇA
DA
INFORMAÇÃO
Integridade
Disponibilidade

Momentos da Informação



Convenção sobre Crimes Cibernéticos ETS 185

Capítulo I – Definições

Capítulo II – Medidas a serem Tomadas pelos Estados Membros

Capítulo III - Cooperação Internacional

Capítulo IV – Provisionamento Final

Cap. II , Seção 1 - Matéria Penal

Título 1 - Crimes contra a *Confidencialidade, Integridade e Disponibilidade* de Sistemas e Dados em Computadores

Artigo 2 - Acesso Ilegal
Artigo 4 - Interferência em Dados
Artigo 5 - Interferência em Sistemas

Lei 9.983/2000 - sistemas da administração pública + funcionário público

Artigo 3 - Interceptação Ilegal

Lei 9.296/1996 e CF

Artigo 6 - Uso Indevido de Dispositivos

(clonagem, virus, etc)

Matéria Penal

Título 2 - Crimes Vinculados ao Uso de Computadores

Artigo 7 - Falsificações Realizadas com Computadores
Artigo 8 - Fraudes Cometidas com Computadores

Código Penal, artigos 171 e 307

Título 3 - Crimes Vinculados aos Conteúdos

Artigo 9 - Crimes Relacionados à Pornografia com Crianças

Lei 8.069/1990 e Lei 10.764/2003
condutas de apresentar, produzir, vender, divulgar e publicar

Matéria Penal

Título 4 - Infrações aos Direitos de Autor

Artigo 10 - Crimes Relacionados à Violação de Direitos de Autor

Lei 9.610/1998 – direitos do autor
Lei 9.609/1998 – programas de computador

Título 5 - Culpabilidade e Penalidades Assessórias

Artigo 11 - Tentativa e cumplicidade
Artigo 12 - Culpabilidade da Pessoa Jurídica
Artigo 13 - Penalidades e Demais Medidas

Código Civil e responsabilidade objetiva

Cap. II , Seção 2
Matéria Processual

Título 1 – Provisões Gerais

Título 2 – Preservação Antecipada de Dados Armazenados

Título 3 – Autoridade para Solicitar Informações

Título 4 – Busca e Apreensão de Dados Armazenados

Título 5 – Obtenção de Dados em Tempo Real

andrecaricatti@apcf.org.br

Cap. II , Seção 2
Matéria Processual

Considerando as previsões básicas da Constituição Federal e do Código de Processo Penal do Brasil, o Poder Público goza de privilégios suficientes para combater os crimes cibernéticos, sendo resguardados ao cidadão sua intimidade e vida privada.

Sobre a antecipação de medidas que visem a preservação de evidências, nada impede que o detentor de dados privativos e voláteis cuide para que sejam mantidos protegidos até a expedição dos devidos mandados de afastamento de sigilo.

Uma premissa básica diretamente relacionada à privacidade estabelece a necessidade de obtenção de ordem judicial quando se fizer necessário investigar dados privativos, ou realizar buscas e apreensões de materiais de informática.

Cap. II , Seção 3 – Jurisdição

Princípio da Ubiqüidade

Todos os locais onde foram realizados atos constitutivos de um crime devem ser considerados locais do crime. Caso quaisquer destes estejam dentro do território nacional, será a Justiça Brasileira competente para processar os culpados.

Capítulo III
Cooperação Internacional

Acordos de Assistência Jurídica Mútua entre Estados Membros do MERCOSUL (2000)

Estados Unidos da América e Peru (2001)

Encontram-se em estudo acordos com países de outros continentes

Grupos de Trabalho do Comitê Gestor de Segurança da Informação - 2003

- Normas técnicas e regulamentos para a segurança da informação;
- Programa de proteção do conhecimento;
- Criação do *Centro de Tratamento de Incidentes em Redes de Computadores* do Executivo Federal;
- Uso comercial de criptografia;
- Normas para uso e disponibilização da Internet;
- Sistemas operacionais de fonte aberta;
- Política Nacional de Telecomunicações;
- Pesquisa sobre segurança da informação.

Conclusão

O objetivo maior é o de prover instrumentos para que favoreçam o combate aos crimes cibernéticos, compatibilizando as iniciativas de Estados Nacionais e formando uma cultura de segurança da informação internacional.

André Machado Caricatti
Perito Criminal Federal
andrecaricatti@apcf.org.br