Supremo Tribunal Federal

1º Seminário de Gestão da Informação Jurídica em Espaços digitais

O Problema

- A Internet e a Globalização - um mundo conectado e interoperável
- Vou ao banco ou o banco é que vem? Banco feito de bits, “Nicholas Negroponte”
- O aumento nas transações mediadas pelas TIC, (informações sigilosas, compras, pagamentos)
- Mudanças culturais... – celular 100 mi! (inclusão?), computador x tv, Lost

O Problema

- A nova web - mais interativa, construída a cada vez mais mãos... e cliques... e comandos cerebrais

- O mundo todo está logo ali, ao alcance de um clique - “o mundo é plano?” “Thomas Friedman” – ainda existem antípodas?

O Problema

- E o papel? Bibliotecas digitais e e-Diário da Justiça
- Volume monstruoso nos Tribunais
- Certificação Digital - MP 2.200/2001
- Juizados Especiais Federais - Lei 10.259/2001
- Comunicação dos atos - Lei 11.280/2006
- Processo eletrônico - 11.419/2006
    - Sites são repositórios oficiais
    - e-Proc, e-DJ, peticionamento eletrônico

Tendências para nossas instituições

- Convergência!
- Consolidação!
- Acesso único + Certificação Digital: simplicidade, rapidez e segurança
- Integração com Aplicativos Web
- Acesso a tudo, de qualquer lugar
- A Biblioteca em qualquer lugar

Rede de Computadores

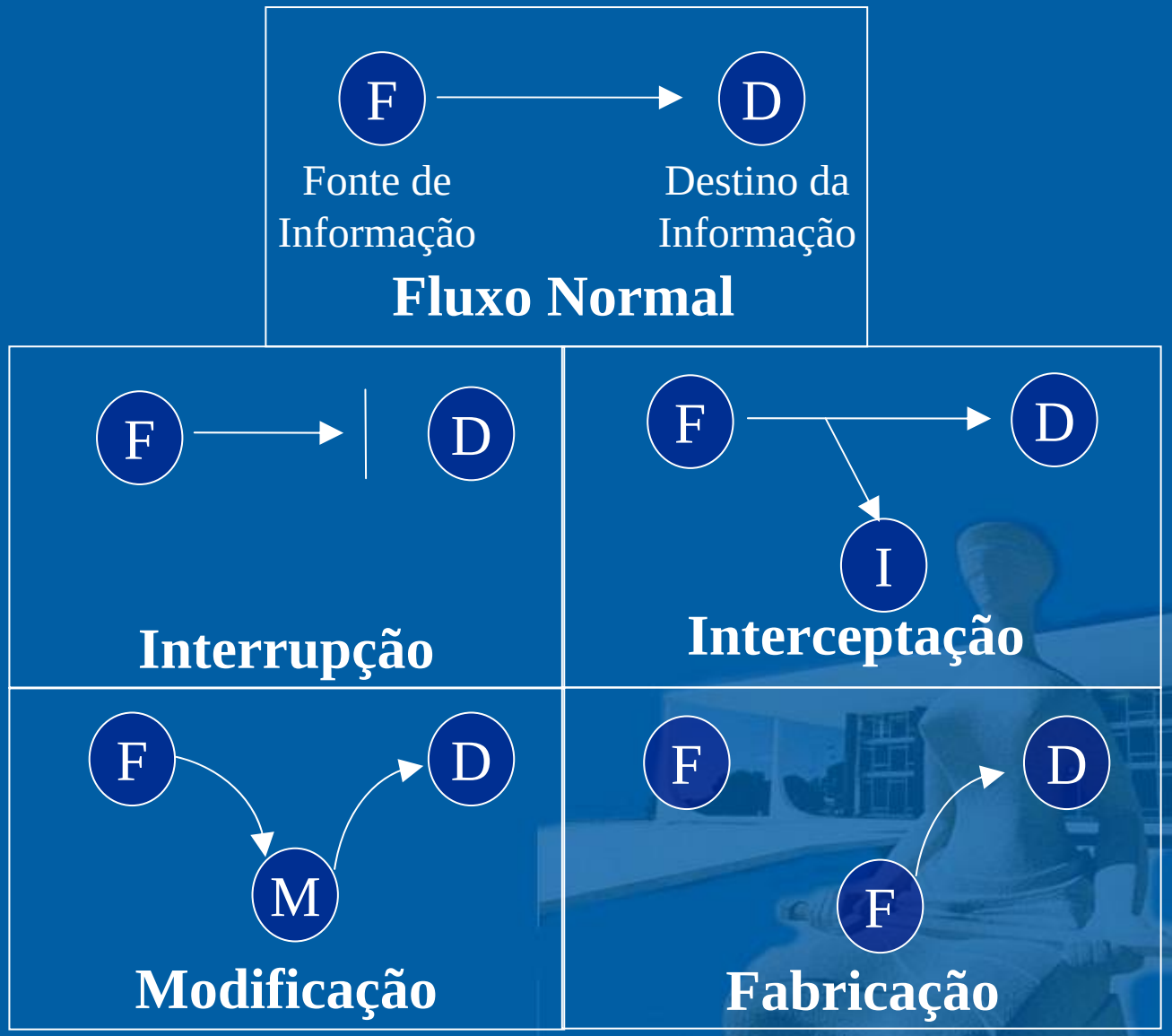
- Mainframe não se comunicava
- Meio de compartilhar recursos e serviços computacionais (descentralização)
- Conjunto de elementos físicos e lógicos através dos quais é possível compartilhar recursos (Albuquerque, 2001)

Segurança

- Segundo o Aurélio, estar seguro é estar livre de perigo
- Também: prudente, ponderado, comedido, cauteloso

Segurança em TI

- A continuidade o negócio - ameaças
- A segurança em TI se preocupa em garantir que pessoas mal-intencionadas (externas à empresa,) não acessem, ou pior ainda, não modifiquem ou danifiquem dados e informações (ou pessoas internas não autorizadas)
- O objetivo do intruso é obter algum benefício ou prejudicar alguém (não é o curioso)


F
D
Fonte de Informação
Destino da Informação
Fluxo Normal
F
D
Interrupção
F
D
I
Interceptação
F
D
M
Modificação
F
D
F
Fabricação

A Solução

- **Rede 100% segura?**

Segurança em TI

- Boas práticas na configuração, administração e operação segura de redes conectadas (à Internet)
- Minimizar as chances de ocorrerem problemas de segurança
- Facilitar a administração das redes e recursos de forma segura

http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html

Introdução

Elementos Físicos:

- **Cabos**
- **Placas de comunicação - fax/modem, placas de rede, adaptadores de rede sem fio**
- **Equipamentos de interconexão de redes - repetidores, pontes, roteadores, servidores de acesso (gateways)**
- **Elementos acessórios - painéis de cabeamento, conectores, tomadas de conexão**

Introdução

Elementos Lógicos:

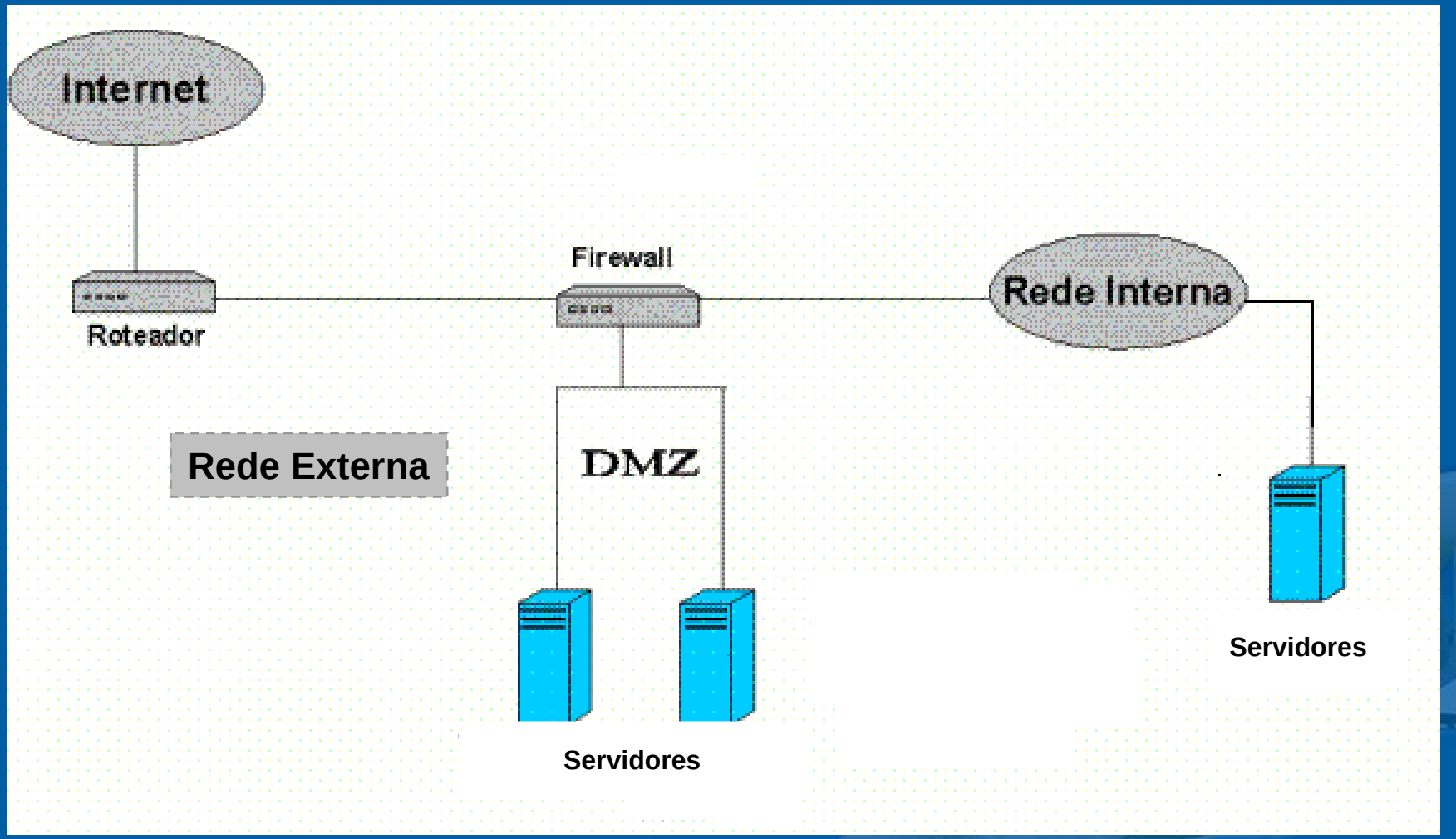
- Protocolos de comunicação – padrões e regras a serem seguidas
- Sistemas operacionais
- Softwares diversos

Ferramentas

Filtros

- **E-mail - remoção de ameaças que estejam sendo enviadas através de mensagens de e-mail: spam, vírus, anexos perigosos**
- **Conteúdo - permite/bloqueia o acesso a sites com determinado conteúdo (white / black lists, imagens, palavras-chave, tipo de arquivos)**
- **Pacotes – analisam cabeçalhos, tomam decisões**

Segurança de Redes



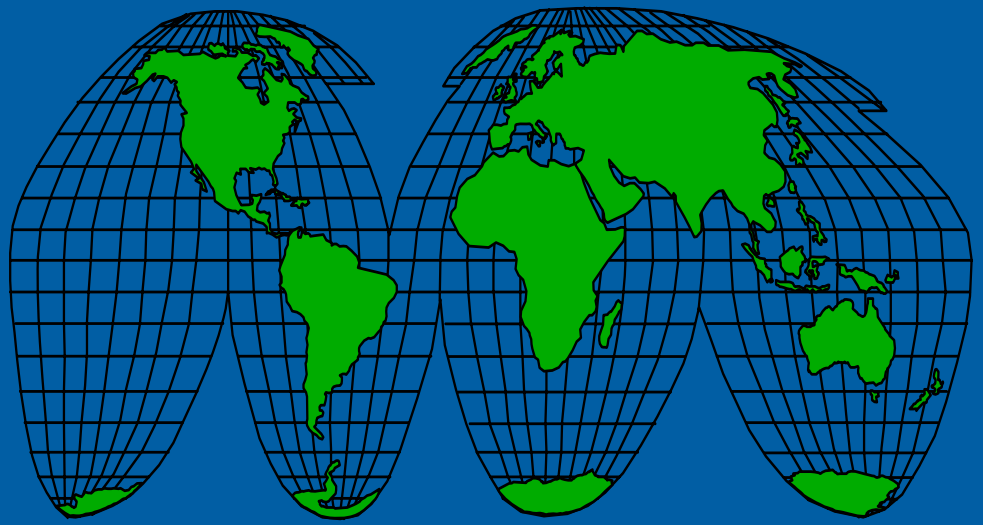
Ferramentas

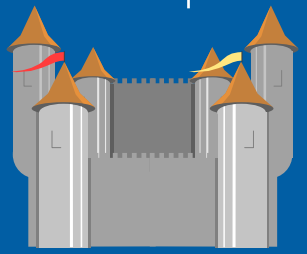
- Antivírus
- Proxys - procuradores
- Sistemas de detecção de intrusão IDS - coleta e analisa eventos, buscando sinais de intrusão ou de mau uso, gerando “alertas” quando estes sinais são encontrados

Firewall

- Combinação de um ou mais elementos, tais como filtros de pacotes, NAT, proxys de aplicação, antispams, IDS, etc para proteger as fronteiras de uma rede
- Normalmente situam-se na fronteira entre a Internet e a rede interna
- Sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes

Conexão Segura





Incidentes

- **Ocorrência de eventos de segurança da informação indesejados ou inesperados, que possam comprometer a confidencialidade, a integridade ou a disponibilidade das informações**

Ameaças

- Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (enchente, raios, invasão por um Hacker)

Ameaças Ambientais

- Correspondem a eventos indesejados causados por agentes de ordem natural ou de instalações que possam comprometer as informações de determinada organização.

Segurança de Redes

AGENTE	AMEAÇA	CONTRAMEDIDA
Raios	Pane Elétrica	Para-Raios, estabilizadores...
Raios	Falha de Hardware	Para-Raios, estabilizadores, contrato de manutenção...
Enchentes	Falha de Hardware	Planejamento arquitetônico, contrato de manutenção, seguros...
Sistema de Climatização	Superaquecimento dos servidores	Sistema backup, monitoramento do ambiente...
Estrutura predial	Desabamento	Reforço estrutural, Salas sofre, sites backup...

Ameaças Humanas

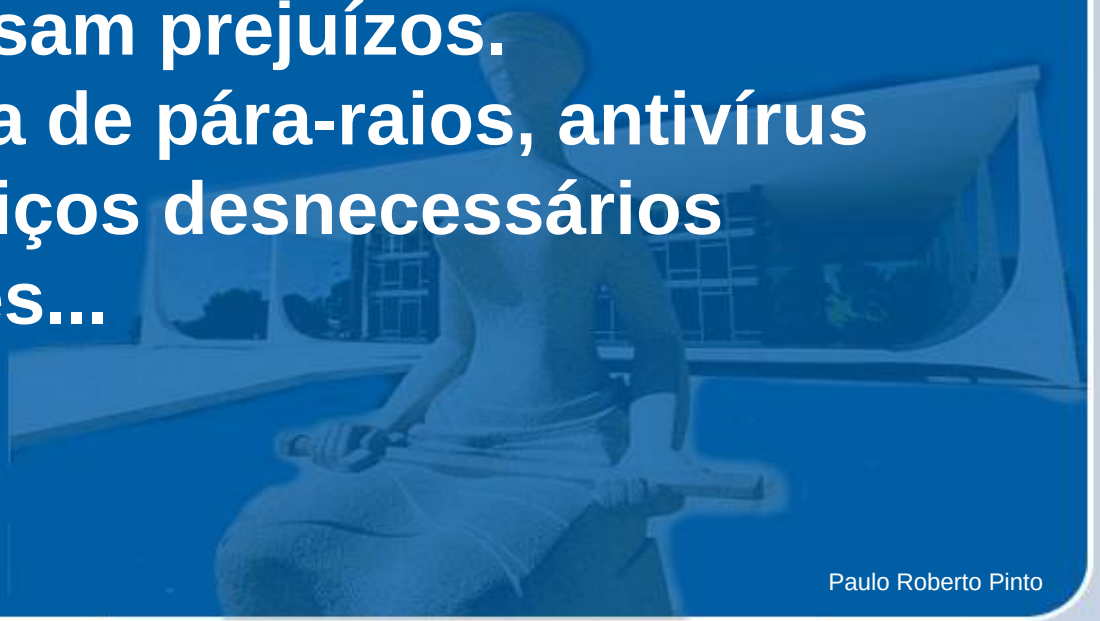
- Correspondem a eventos indesejados gerados pela atuação proposital ou acidental do homem.
- Contramedidas: Políticas de Segurança, treinamento, segurança física, ferramentas de proteção, etc.

Ameaças Humanas

AGENTE	AMEAÇA	CONTRAMEDIDA
Funcionário Insatisfeito	Sabotagem	Treinamento, Fiscalização, contrato de manutenção...
Filhos de Funcionários	Danos Patrimoniais	Política organizacional
“Faxineira Hacker”	Desligamento Acidental de Equipamentos	Proteção do ambiente de CPD, Treinamento...
“Faxineira Hacker”	Vazamento de Informações	Criação de Salas de Reunião...

Vulnerabilidade

- Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças
- Por si só, não causam prejuízos.
- Exemplo: ausência de pára-raios, antivírus desatualizado, serviços desnecessários ativos em servidores...



Ataques

- Tipo de ameaça humana cuja finalidade é explorar vulnerabilidades

Ataques não técnicos

- Engenharia social
- Ameaças físicas (arrombamentos, furtos)

Ataques

Ataques técnicos

- Varreduras
- Cavalos de Tróia
- Back-doors
- Negação de Serviço (DoS, DDoS - denial of service)
- Analisadores de Trafego (sniffers)
- Vírus
- SPAMs
- Logs de Teclado

Engenharia social

- Consiste em explorar aspectos psicológicos (medo, insegurança, carência, boa-fé, despreparo) das pessoas para conseguir informações e acessos privilegiados
  - Intimidação: "*Você sabe com quem está falando?*"
  - Ingenuidade: Passar-se por um técnico e solicitar a senha para efetuar testes
- Contramedidas: Resguardar dados pessoais dos funcionários, políticas de conscientização, etc

Evolução do cenário

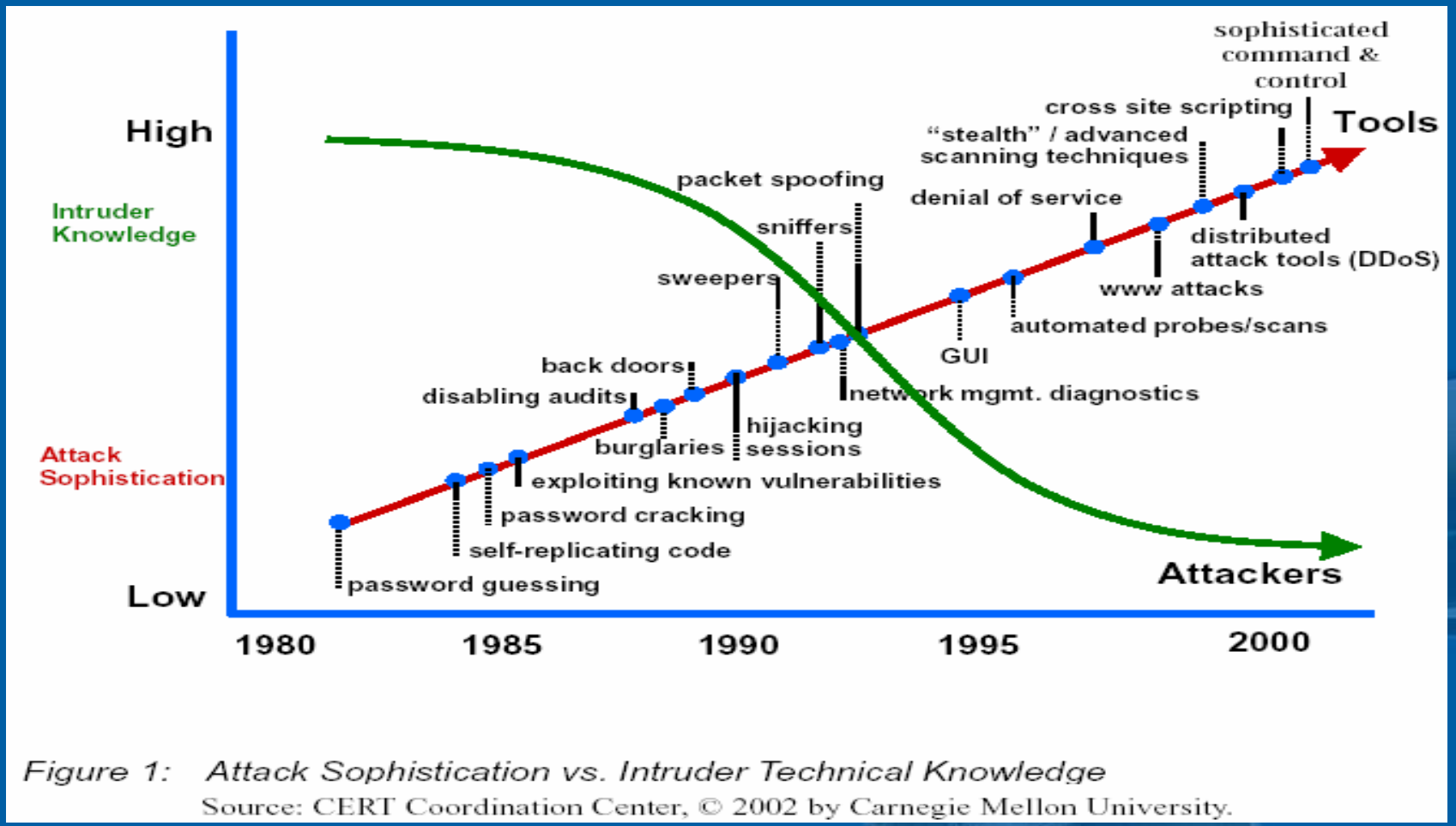
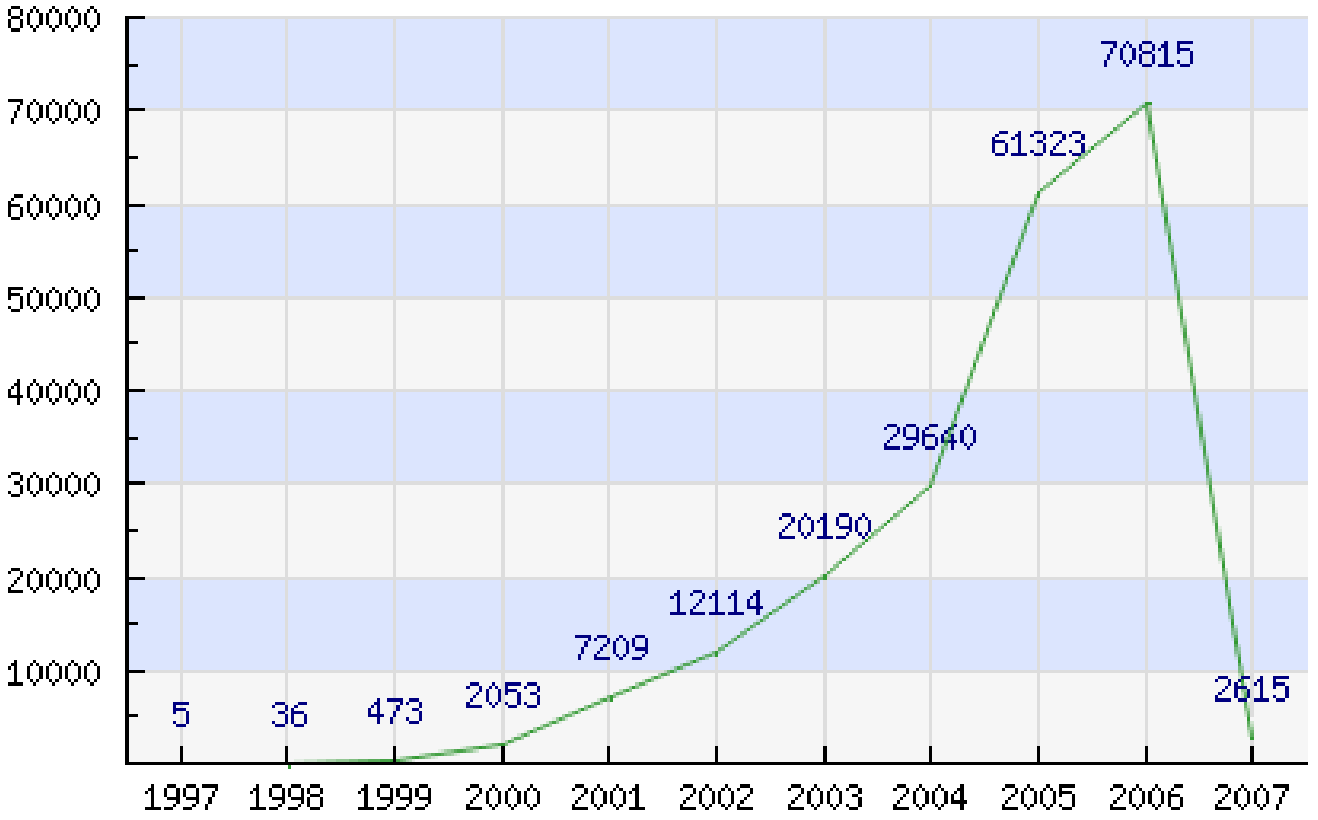


Figure 1: Attack Sophistication vs. Intruder Technical Knowledge

Source: CERT Coordination Center, © 2002 by Carnegie Mellon University.

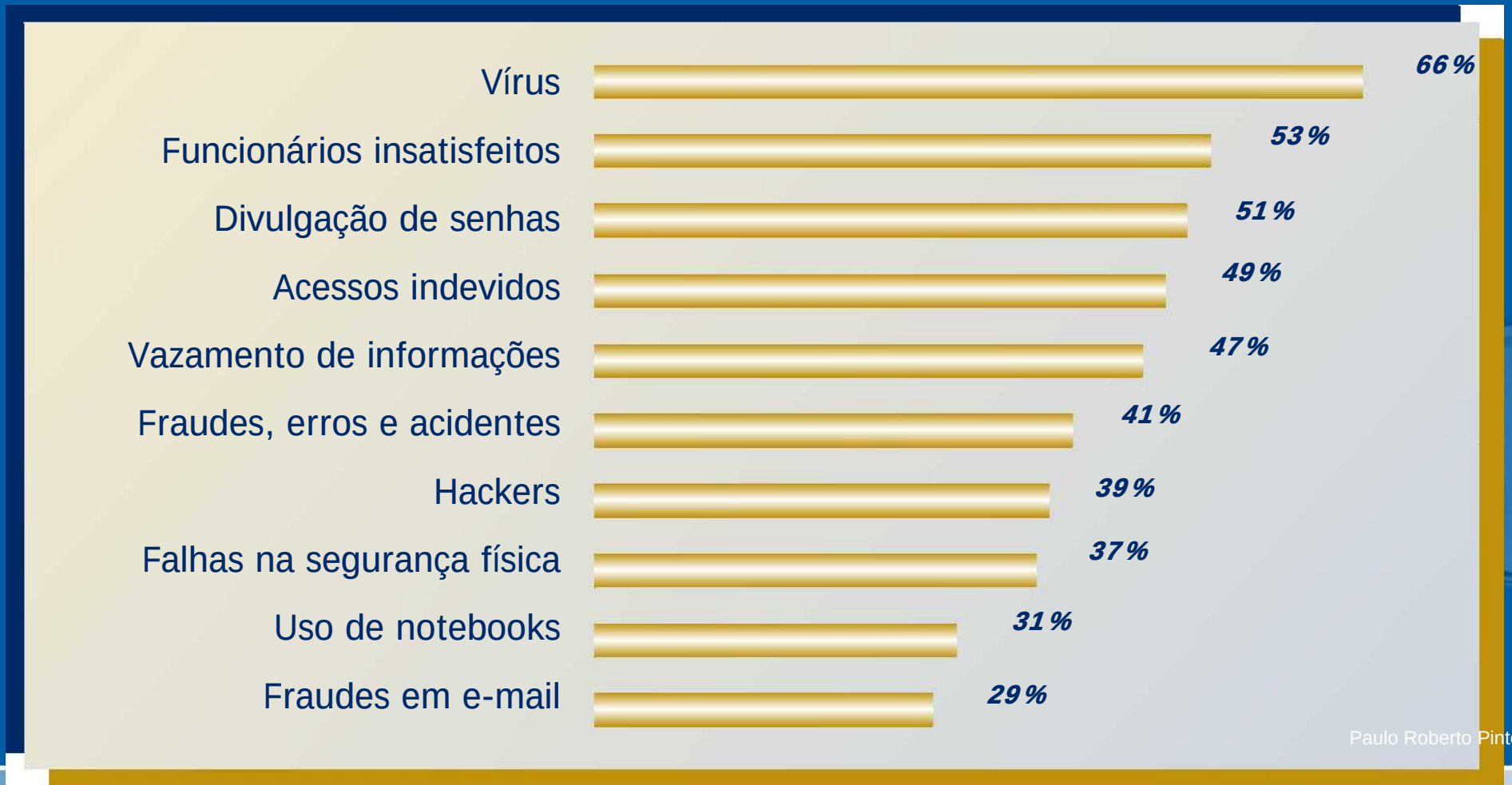
Evolução do cenário



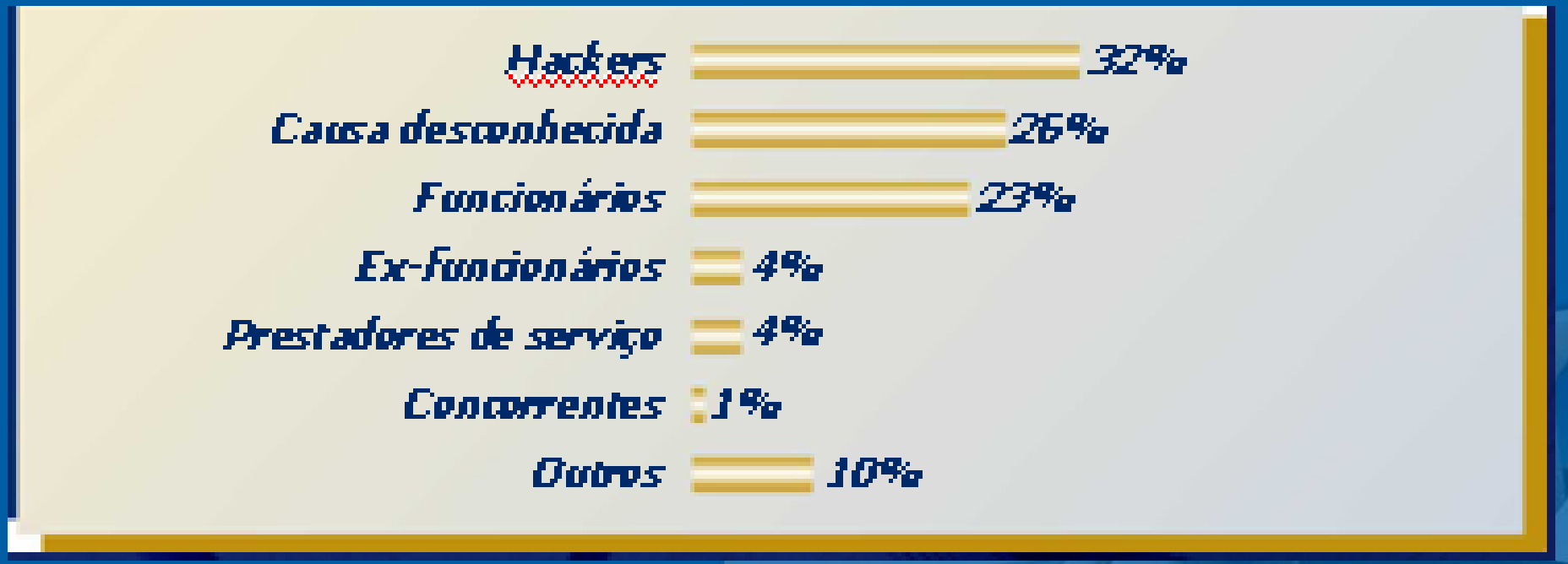
Quantidade de incidentes. Fonte RNP

Estatísticas - Ameaças

Fonte: MÓDULO SECURITY - Pesquisa Módulo de Segurança da Informação - 2003



Estatísticas - Responsáveis

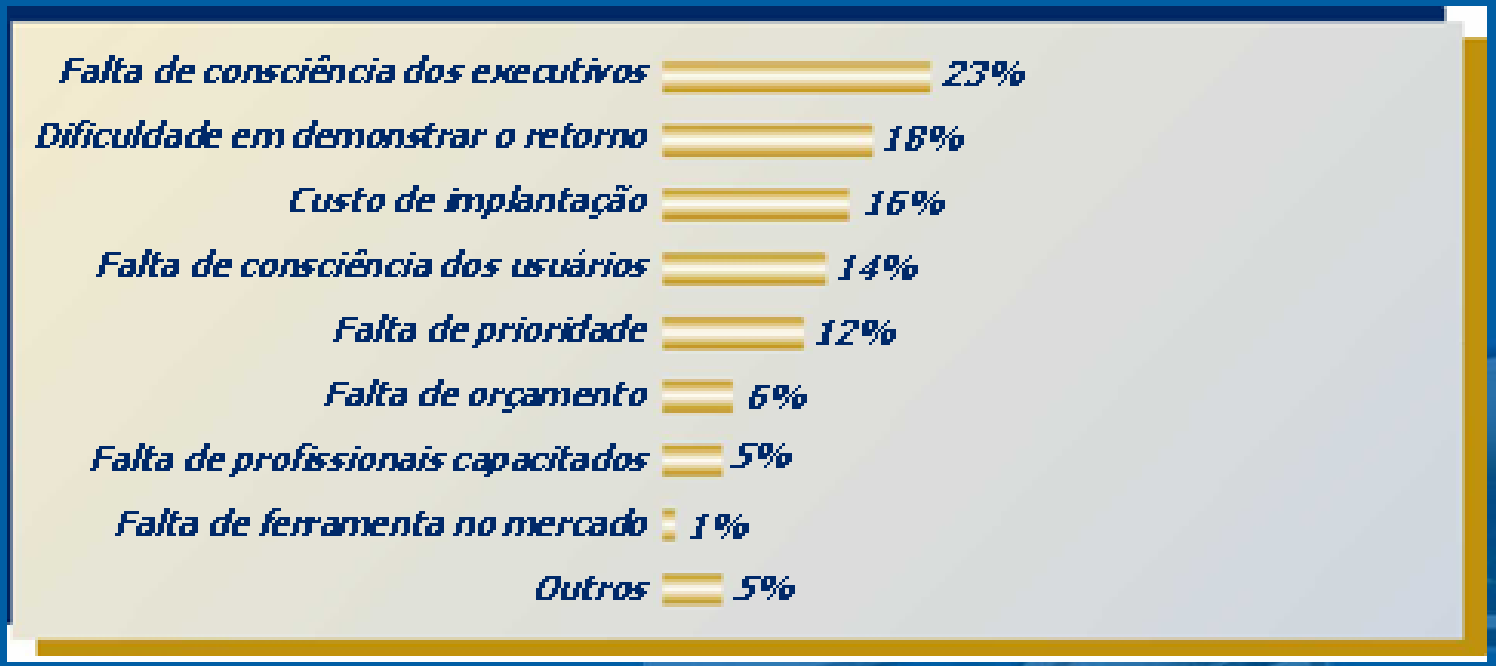


Fonte: MÓDULO SECURITY - Pesquisa Módulo de Segurança da Informação - 2003

Política de Segurança

- Tem por objetivo promover orientação e apoio da direção da organização para a segurança da informação, de acordo com os requisitos de negócio e com as leis e regulamentações relevantes.
- ABNT NBR ISO/IEC 17799:2005

Política de Segurança: desafios



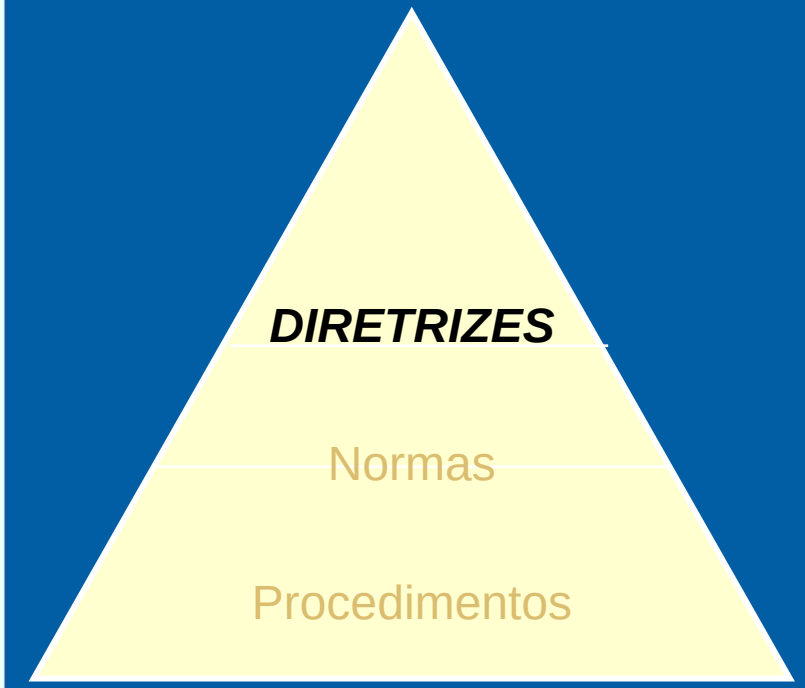
Fonte: **9ª PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO - Modulo**

Política de Segurança: divulgação

- **A política de segurança da informação deve ser comunicada em toda a organização, para todos os usuários, de forma que fique clara a sua relevância, acessível e compreensivelmente**

ABNT NBR ISO / IEC 17799:2005

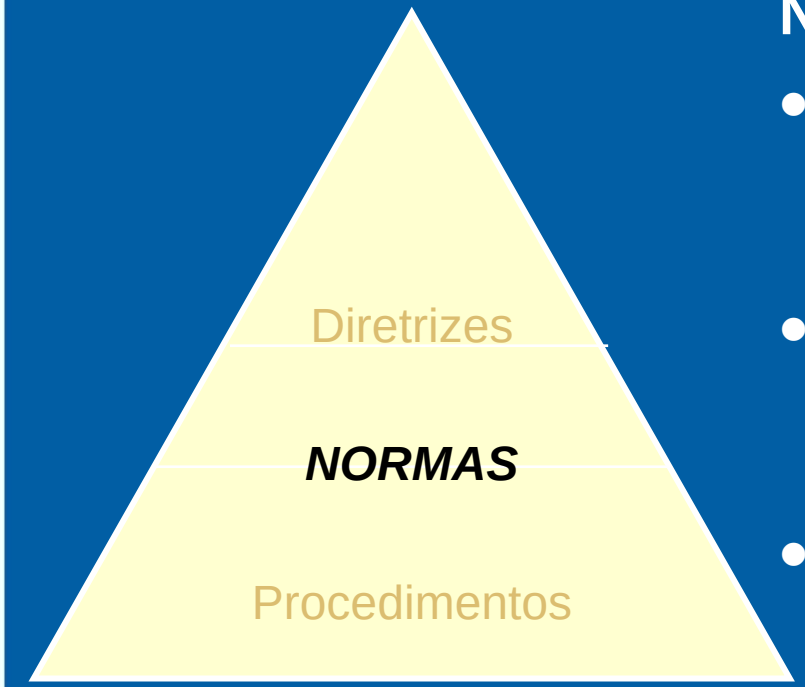
Política de Segurança



Nível Estratégico: Alta Direção

- **São valores que devem ser seguidos para que a informação tenha o nível de segurança pretendido.**
- **Não devem conter termos técnicos já que serão da responsabilidade de pessoas não qualificadas em TI**
- **Exemplo: O correio eletrônico destina-se exclusivamente a mensagens e transmissão de arquivos relacionados à atividade fim deste órgão**

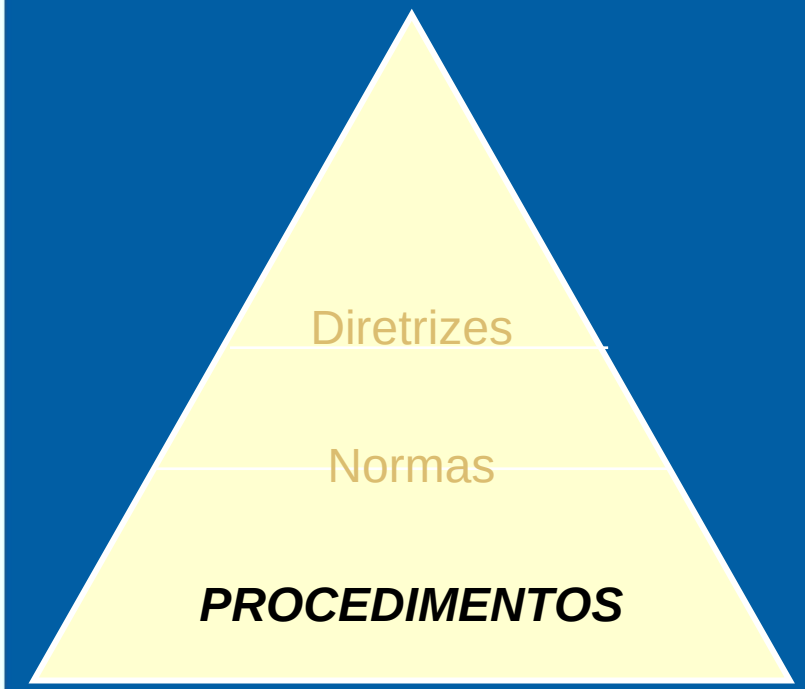
Política de Segurança



Nível Tático: Gerentes

- São regras e modelos de segurança que permitem o desempenho das atividades com segurança
- Devem ser destinados a dois públicos: Quem administra e quem usa (normas de administração e de uso de senhas)
- Exemplo: Cabe à área de Segurança de Redes a remoção de todos os anexos das mensagens de correio eletrônico, exceto arquivos do tipo .doc, .pdf e .xls

Política de Segurança

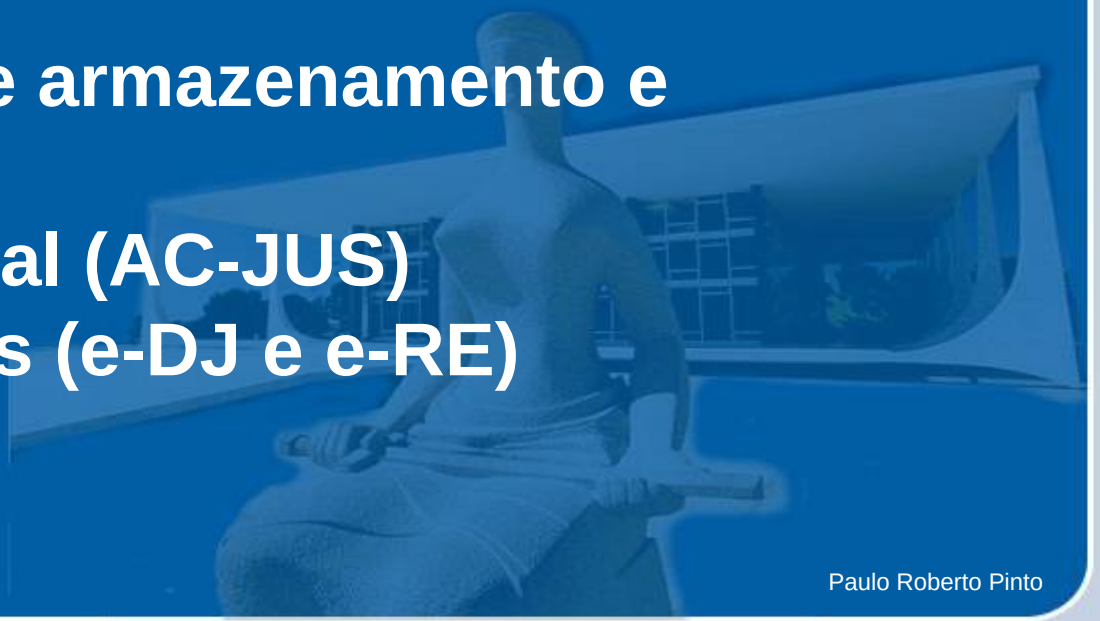


Nível Operacional: Técnicos

- **Tem como objetivo tornar a execução operacional de tarefas homogênea.**
- **Devem ser clara o suficiente para garantir a precisão, mas sem exageros de detalhes para não se tornarem de impossível utilização.**

Supremo Tribunal Federal

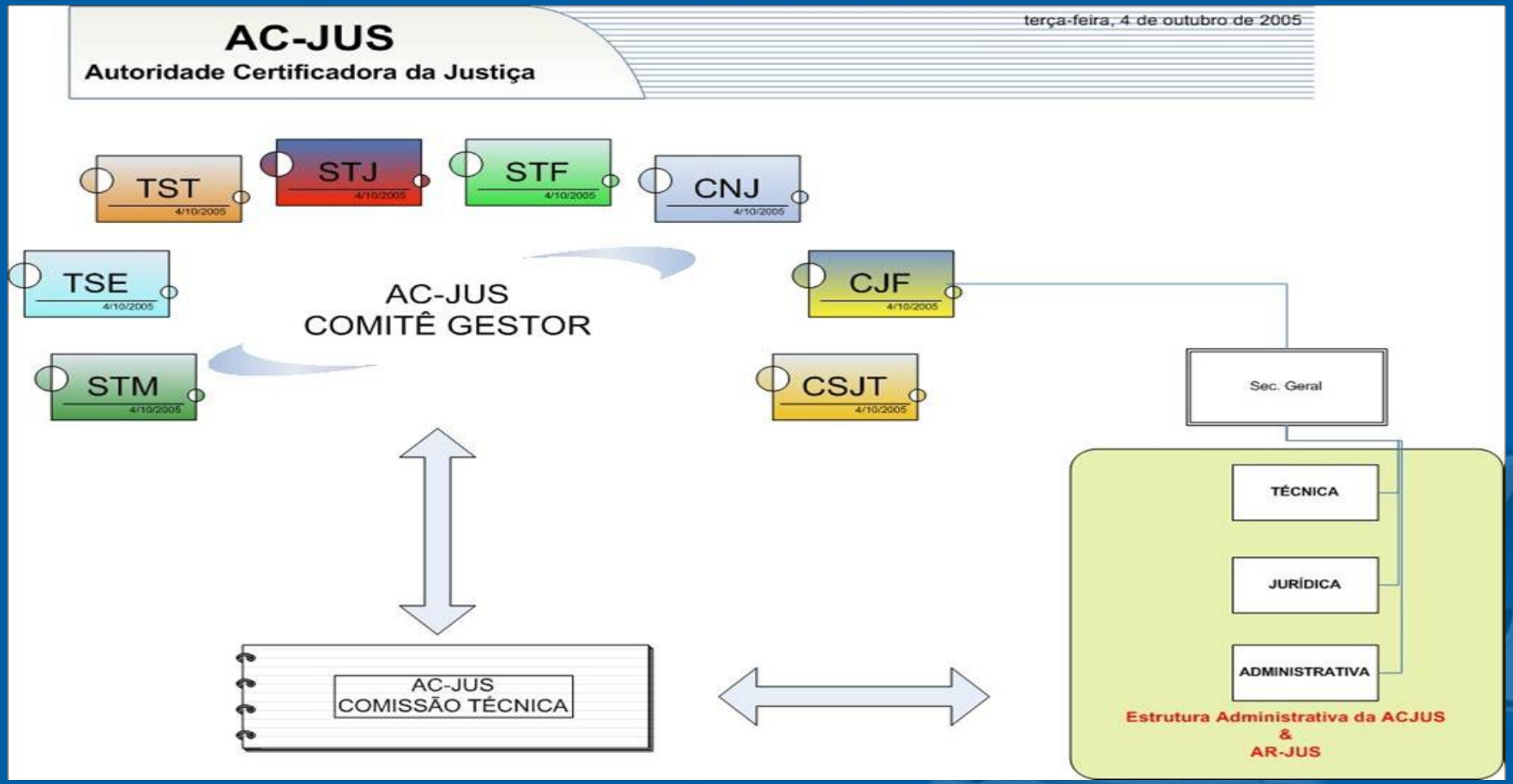
- Política de Segurança de Informações, consoante com a PS da instituição
- Ambiente físico seguro
- Redundância
- Equipamentos de armazenamento e cópias dos dados
- Certificação digital (AC-JUS)
- Sistemas seguros (e-DJ e e-RE)



Certificação Digital
AC-JUS

- Interoperabilidade de toda a cadeia de confiança garantida pela ICP-Brasil
- Segurança nas transações
- Agilidade nos processos/procedimentos
- Smart card com dupla ou mais funções, agregando identidade civil, funcional, crachá, além da identidade digital

Segurança de Redes



Segurança de Redes

Obrigado!

Perguntas?

Paulo Roberto Pinto
Supremo Tribunal Federal
Secretaria de Tecnologia da Informação