GATI: Tratamento de Incidentes de Segurança no MJ e DPF

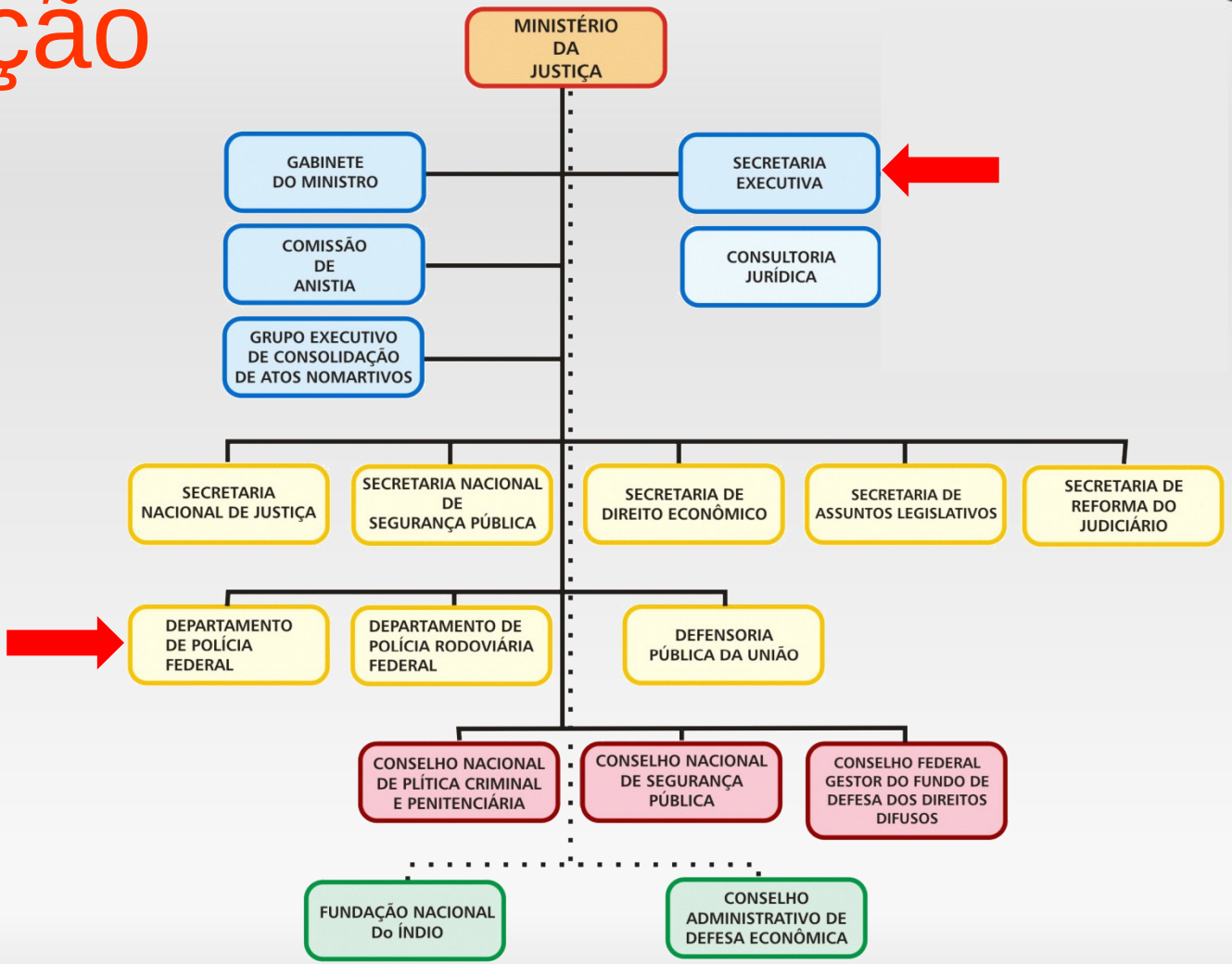
Ivo de Carvalho Peixinho
Perito Criminal Federal

Jorilson da Silva Rodrigues
Perito Criminal Federal

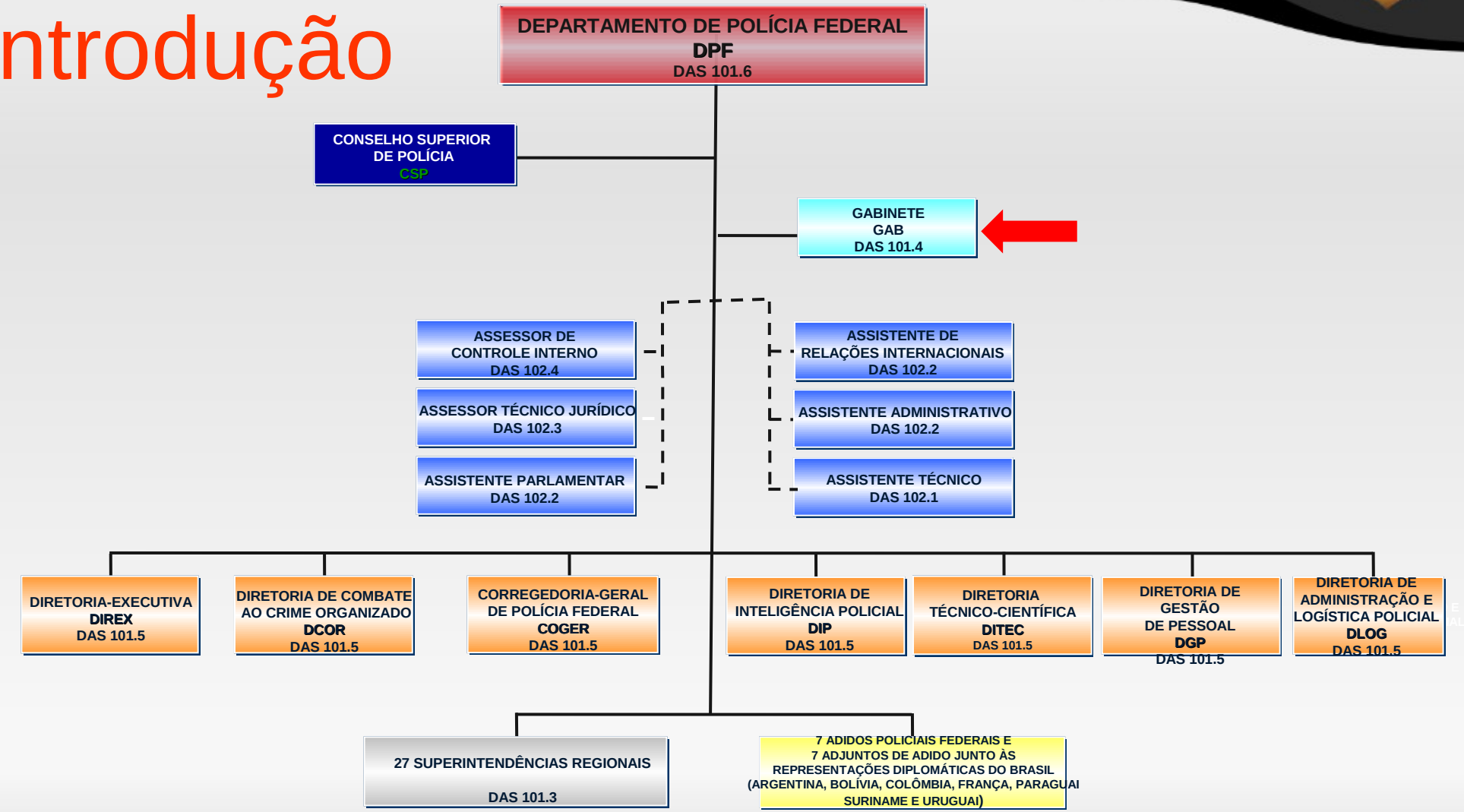
Agenda

1. Introdução
2. Motivação
3. Histórico
4. GATI
5. GATI-DPF
6. Tratamento de Incidentes
7. Próximos passos

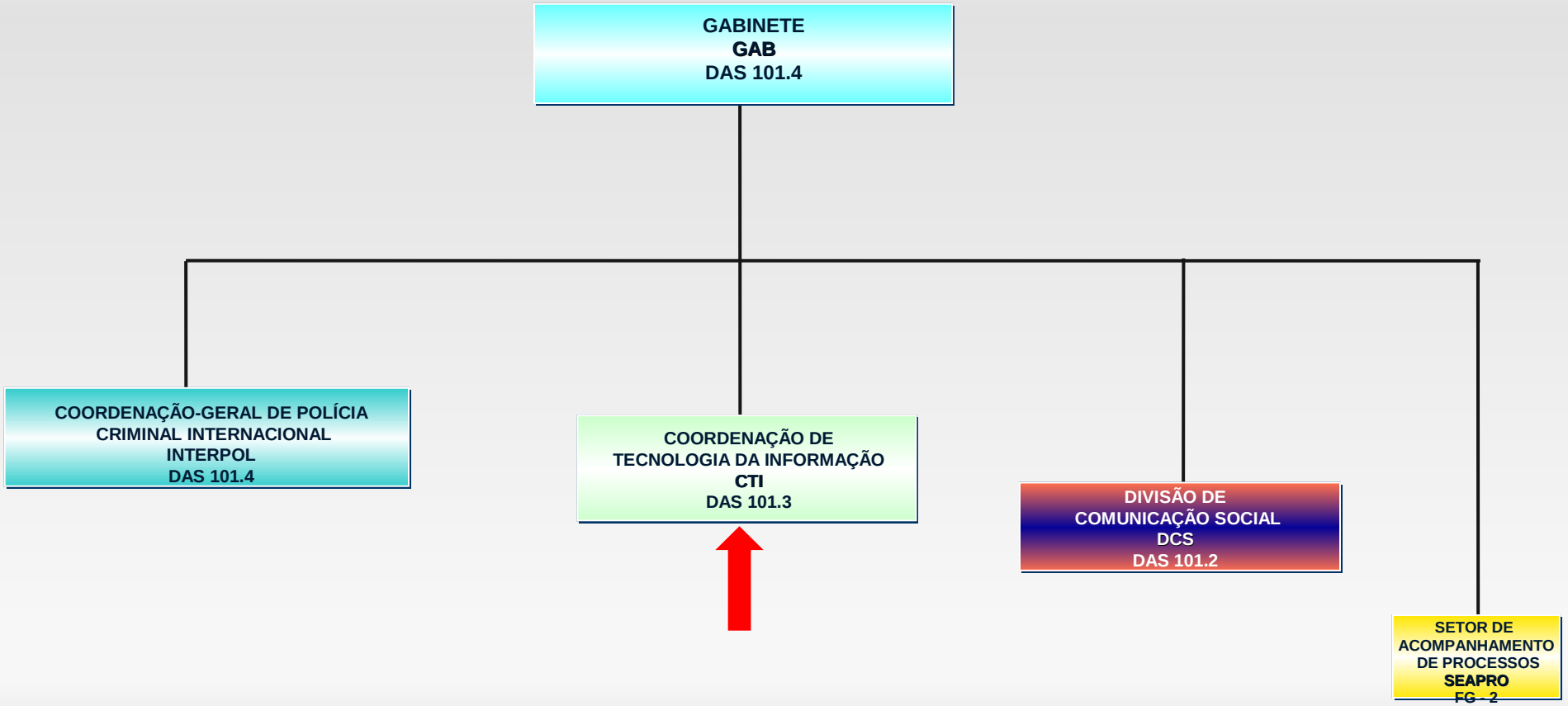
Introdução


MINISTÉRIO DA JUSTIÇA
GABINETE DO MINISTRO
SECRETARIA EXECUTIVA
COMISSÃO DE ANISTIA
CONSULTORIA JURÍDICA
GRUPO EXECUTIVO DE CONSOLIDAÇÃO DE ATOS NOMARTIVOS
SECRETARIA NACIONAL DE JUSTIÇA
SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA
SECRETARIA DE DIREITO ECONÔMICO
SECRETARIA DE ASSUNTOS LEGISLATIVOS
SECRETARIA DE REFORMA DO JUDICIÁRIO
DEPARTAMENTO DE POLÍCIA FEDERAL
DEPARTAMENTO DE POLÍCIA RODOVIÁRIA FEDERAL
DEFENSORIA PÚBLICA DA UNIÃO
CONSELHO NACIONAL DE PLÍTICA CRIMINAL E PENITENCIÁRIA
CONSELHO NACIONAL DE SEGURANÇA PÚBLICA
CONSELHO FEDERAL GESTOR DO FUNDO DE DEFESA DOS DIREITOS DIFUSOS
FUNDAÇÃO NACIONAL Do ÍNDIO
CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA

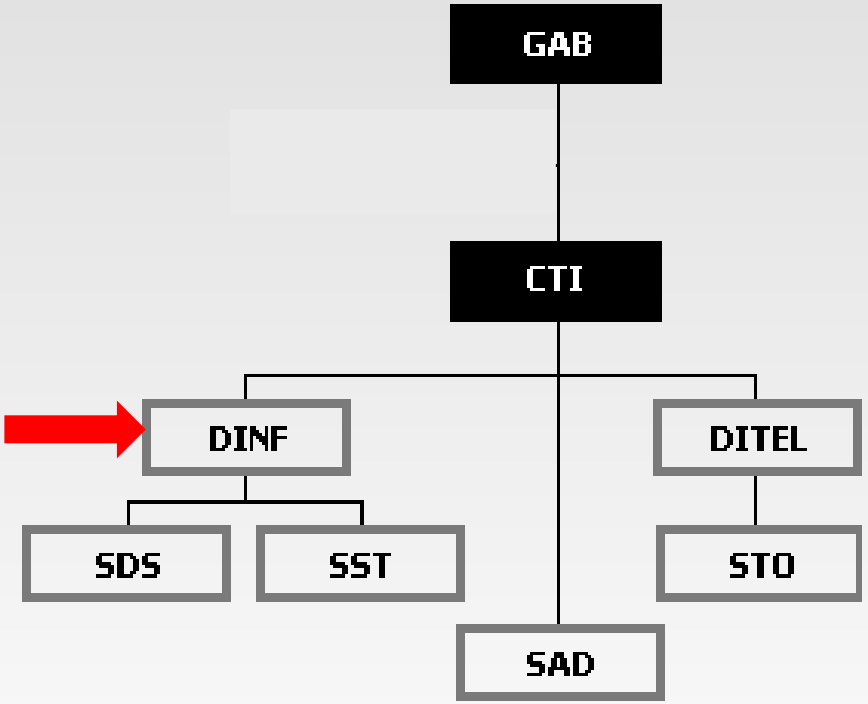
Introdução


DEPARTAMENTO DE POLÍCIA FEDERAL
DPF
DAS 101.6
CONSELHO SUPERIOR DE POLÍCIA
CSP
GABINETE
GAB
DAS 101.4
ASSESSOR DE CONTROLE INTERNO
DAS 102.4
ASSESSOR TÉCNICO JURÍDICO
DAS 102.3
ASSISTENTE PARLAMENTAR
DAS 102.2
ASSISTENTE DE RELAÇÕES INTERNACIONAIS
DAS 102.2
ASSISTENTE ADMINISTRATIVO
DAS 102.2
ASSISTENTE TÉCNICO
DAS 102.1
DIRETORIA-EXECUTIVA
DIREX
DAS 101.5
DIRETORIA DE COMBATE AO CRIME ORGANIZADO
DCOR
DAS 101.5
CORREGEDORIA-GERAL DE POLÍCIA FEDERAL
COGER
DAS 101.5
DIRETORIA DE INTELIGÊNCIA POLICIAL
DIP
DAS 101.5
DIRETORIA TÉCNICO-CIENTÍFICA
DITEC
DAS 101.5
DIRETORIA DE GESTÃO DE PESSOAL
DGP
DAS 101.5
DIRETORIA DE ADMINISTRAÇÃO E LOGÍSTICA POLICIAL
DLOG
DAS 101.5
27 SUPERINTENDÊNCIAS REGIONAIS
DAS 101.3
7 ADIDOS POLICIAIS FEDERAIS E
7 ADJUNTOS DE ADIDO JUNTO ÀS
REPRESENTAÇÕES DIPLOMÁTICAS DO BRASIL
(ARGENTINA, BOLÍVIA, COLÔMBIA, FRANÇA, PARAGUAI
SURINAME E URUGUAI)

Introdução


GABINETE
GAB
DAS 101.4
COORDENAÇÃO-GERAL DE POLÍCIA CRIMINAL INTERNACIONAL
INTERPOL
DAS 101.4
COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO
CTI
DAS 101.3
DIVISÃO DE COMUNICAÇÃO SOCIAL
DCS
DAS 101.2
SETOR DE ACOMPANHAMENTO DE PROCESSOS
SEAPRO
FG - 2

Introdução



Motivação

- IN 01/2008-GSI/PR
  - Disciplina a gestão de SI na administração pública federal
  - Art 5º Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:
    - V – **instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais**

Histórico

- Ministério da Justiça
  - Portaria 2086-05-MJ
    - Art. 1º: Cria o Comitê Gestor de Segurança da Informação – CGSI.
    - Art. 4º: Cria o Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação – GATI, com o objetivo de implantar e operacionalizar o tratamento da Segurança da Informação, no âmbito do MJ.

Histórico

- Departamento de Polícia Federal
  - CTR - Centro de Tratamento e Resposta a Incidentes de Segurança Informação
    - Autorizado pela DG em 2001
    - Em operação até 2004
  - CRIAÇÃO DE UM CENTRO DE TRATAMENTO DE INCIDENTES EM REDES DE COMPUTADORES NO ÂMBITO DO DPF
    - Monografia apresentada no XV Curso Especial de Polícia em 2007

Histórico

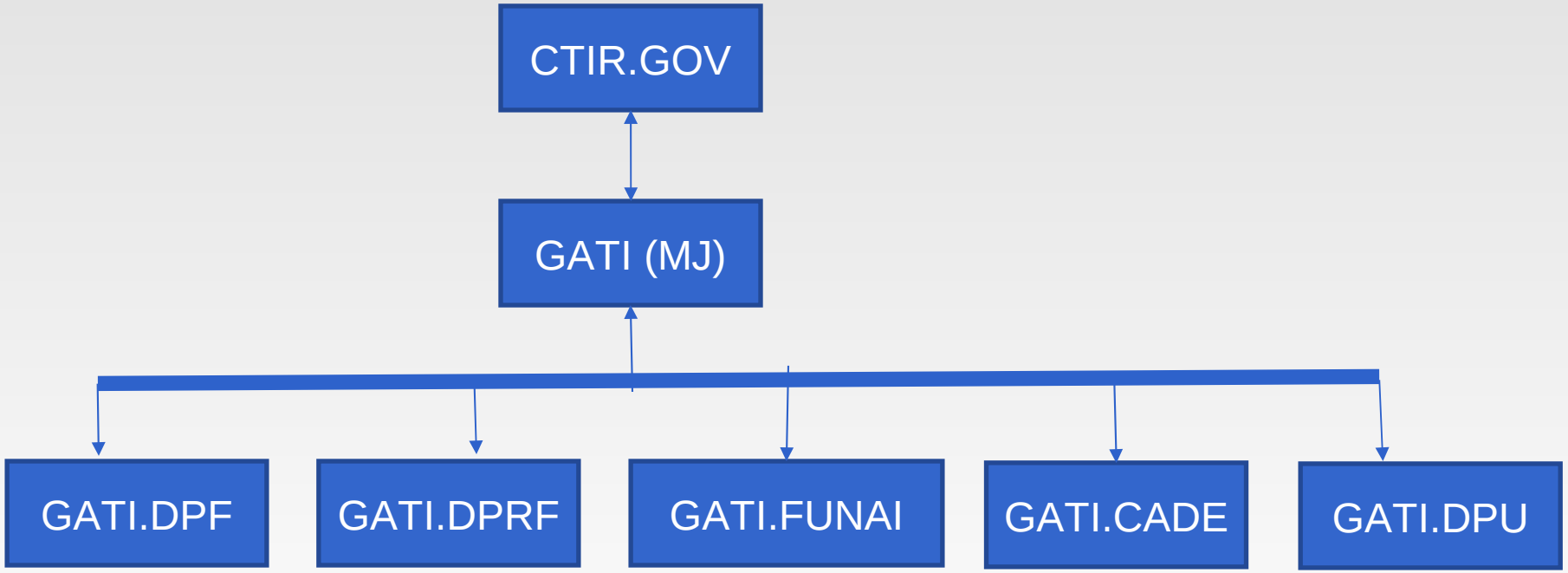
- Departamento de Polícia Federal
  - PORTARIA No. 156/2009-DG/DPF, DE 20 DE MARÇO 2009
    - Alterou a constituição e atribuições da Comissão de Segurança Institucional
    - Art. 3º. Compete a CSI:
      - IX – propor a constituição e as atribuições de Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação – GATI com dedicação exclusiva às atividades relacionadas a segurança da informação e comunicações;

Histórico

- Departamento de Polícia Federal
  - 31/03/2009 – Reunião ordinária GATI
    - Alinhamento GATI/DPF com GATI/MJ
      - Padronização da forma de comunicação
    - Apresentação projeto DNSSEC - DPF
    - Apresentação projeto SAMURAI – MJ

GATI

- Estrutura



GATI

- Estrutura
  - GATI seccionais
    - Representações do GATI nos diversos órgãos do MJ
    - Articulam incidentes internos com setores dos órgãos
    - Articulam incidentes externos com o GATI (MJ)
  - GATI (MJ)
    - Representação central
    - Articula incidentes externos com o CTIR.GOV

GATI

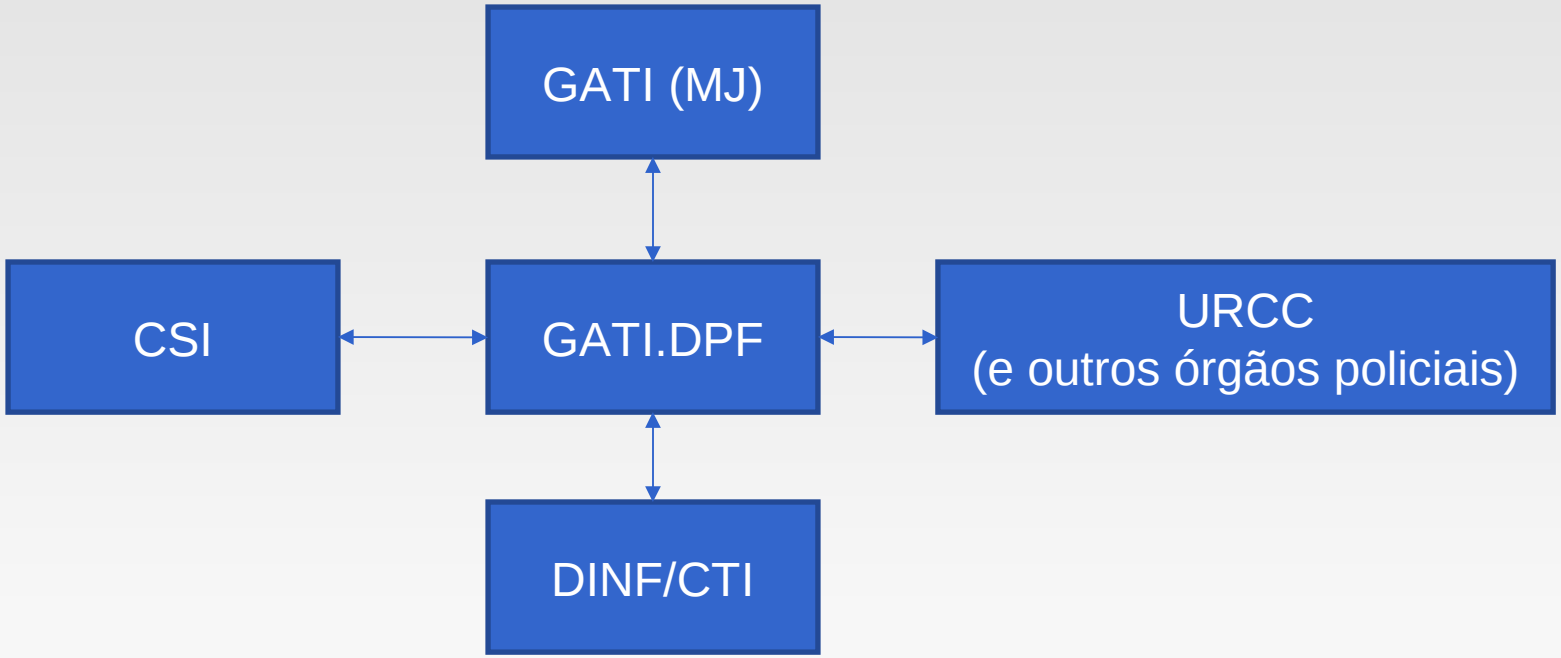
- Membros
  - Secretaria Executiva
  - Gabinete do Ministro da Justiça
  - **Departamento de Polícia Federal**
  - Departamento de Polícia Rodoviária Federal
  - Defensoria Pública da União
  - Fundação Nacional do Índio
  - Conselho Administrativo de Defesa Econômica

GATI.DPF

- Localização
  - DINF/CTI/DPF
  - Setor Policial Sul – Brasília/DF
- Estrutura
  - 1 PCF
  - 1 APF
  - Equipe de segurança (apoio)
    - 1 AADM + 2 Terceirizados

GATI.DPF

- Articulação



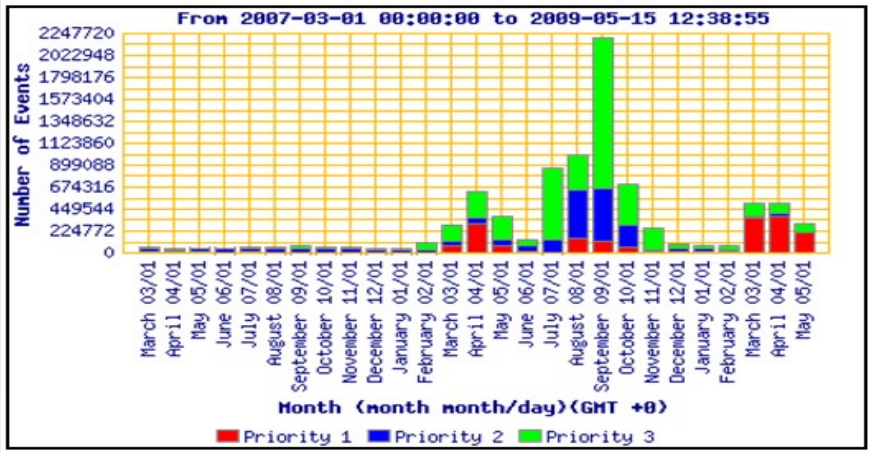
Tratamento de Incidentes

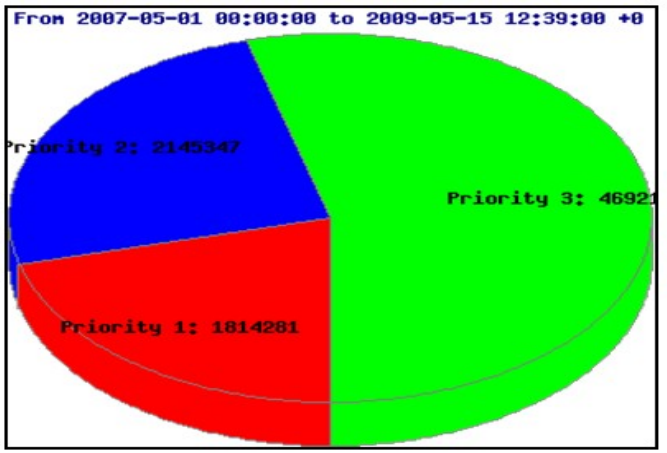
- SAMURAI
  - Ferramenta de *detecção* e resposta a incidentes
  - Desenvolvida pelo GATI (MJ) utilizando *software livre*
  - Capaz de
    - Detectar incidentes na rede
    - Realizar bloqueios temporários automaticamente
    - Encaminhar automaticamente incidentes

Tratamento de Incidentes

- SAMURAI
  - Arquitetura
    - Sensores (*snort)*
    - Repositório (*postgresql)*
    - Gerência de assinaturas (*ids policy manager*)
    - Console de monitoramento (*apache* + *perl*)
    - Sistema de bloqueio temporário (*guardian*)

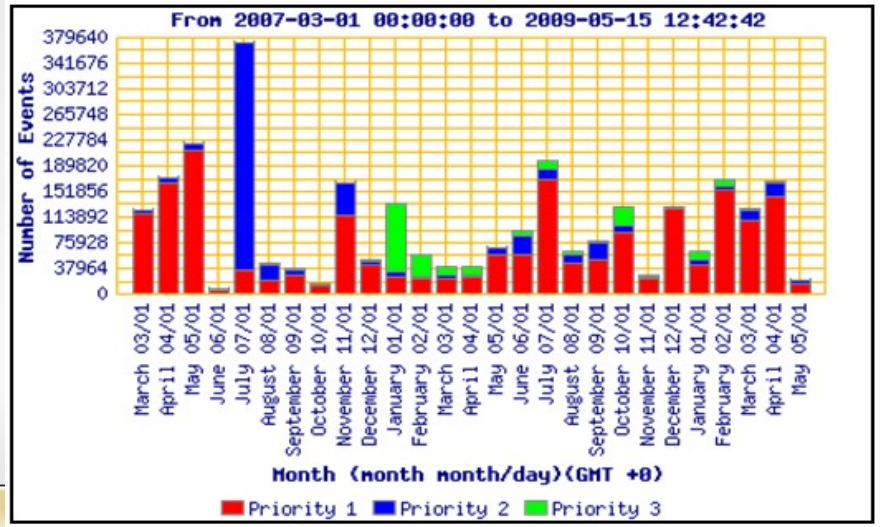
Tratamento de Incidentes

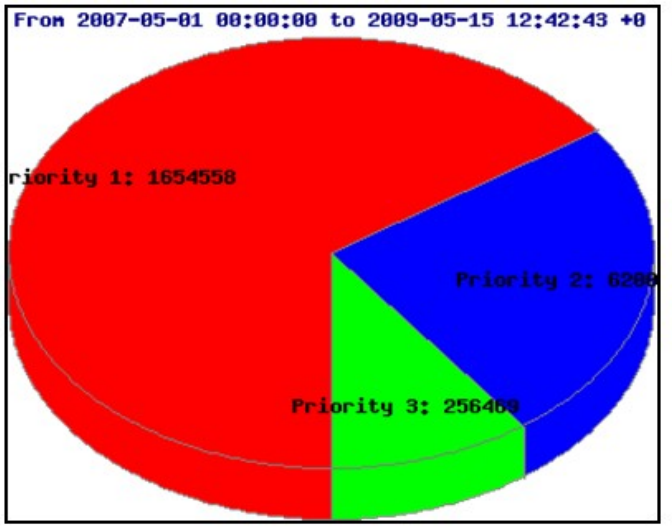




GRAPH REPORTS

1 HOUR
24 HOURS
7 DAYS
30 DAYS
45 DAYS
1 YEAR





GRAPH REPORTS

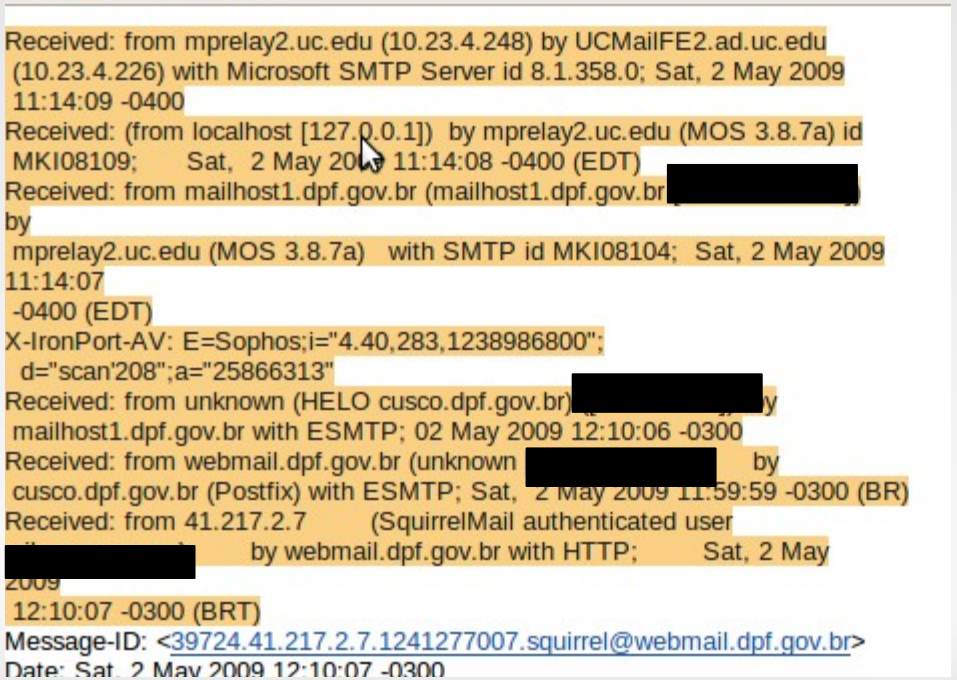
1 HOUR
24 HOURS
7 DAYS
30 DAYS
45 DAYS
1 YEAR

Tratamento de Incidentes

- SAMURAI
  - Números (MJ)
    - Eventos regstrados
      - Internet: 7.696.335
      - Local: 5.407.875
    - Notificações: 621.099
    - Assinaturas: 21.538

Tratamento de Incidentes

- Casos Interessantes
  - Caso 1: Email de reclamação de SPAM



```
Received: from mprelay2.uc.edu (10.23.4.248) by UCMailFE2.ad.uc.edu
 (10.23.4.226) with Microsoft SMTP Server id 8.1.358.0; Sat, 2 May 2009
 11:14:09 -0400
Received: (from localhost [127.0.0.1])  by mprelay2.uc.edu (MOS 3.8.7a) id
 MKI08109;      Sat,  2 May 2009 11:14:08 -0400 (EDT)
Received: from mailhost1.dpf.gov.br (mailhost1.dpf.gov.br [redacted])
by
 mprelay2.uc.edu (MOS 3.8.7a)   with SMTP id MKI08104;  Sat, 2 May 2009
11:14:07
 -0400 (EDT)
X-IronPort-AV: E=Sophos;i="4.40,283,1238986800";
  d="scan'208";a="25866313"
Received: from unknown (HELO cusco.dpf.gov.br) ([redacted])
 mailhost1.dpf.gov.br with ESMTP; 02 May 2009 12:10:06 -0300
Received: from webmail.dpf.gov.br (unknown [redacted] by
 cusco.dpf.gov.br (Postfix) with ESMTP; Sat,  2 May 2009 11:59:59 -0300 (BR)
Received: from 41.217.2.7       (SquirrelMail authenticated user
[redacted]       by webmail.dpf.gov.br with HTTP;       Sat, 2 May
2009
 12:10:07 -0300 (BRT)
Message-ID: <39724.41.217.2.7.1241277007.squirrel@webmail.dpf.gov.br>
Date: Sat, 2 May 2009 12:10:07 -0300
```

Tratamento de Incidentes

- Caso 1: reclamação de SPAM
  - Usuário autenticado no webmail (*squirrelmail*)
    - Usuário legítimo enviando SPAM?
    - Exploração automatizada do squirrelmail?
    - Botnet?
  - De onde vieram os acessos?
    - Logs do servidor web...

Tratamento de Incidentes

- 41.220.75.x - - [03/May/2009:13:11:54 -0300] "GET /src/webmail.php HTTP/1.1" 200 1099 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6; InfoPath.2; Crazy Browser 3.0.0 RC1)"
- 41.220.75.x - - [03/May/2009:13:11:55 -0300] "GET /images/novoBrasaoDPF.jpg HTTP/1.1" 304 - "https://webmail.dpf.gov.br/src/webmail.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6; InfoPath.2; Crazy Browser 3.0.0 RC1)"
- 41.220.75.x - - [03/May/2009:13:11:59 -0300] "GET /favicon.ico HTTP/1.1" 404 340 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6; InfoPath.2; Crazy Browser 3.0.0 RC1)"
- 41.220.75.x - - [03/May/2009:13:12:05 -0300] "GET /src/login.php HTTP/1.1" 200 3356 "https://webmail.dpf.gov.br/src/webmail.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6; InfoPath.2; Crazy Browser 3.0.0 RC1)"

Tratamento de Incidentes

- Whois
  - inetnum: 41.220.75.0 - 41.220.75.255
  - netname: MTNNG-0001-MDSN01-OJT
  - descr: IP Block Assigned for Mobile Data Services Network at Ojota
  - country: NG
- Nigéria??
- Crazy Browser??

Tratamento de Incidentes

- Caso 1: providências
  - Auditoria das contas de webmail
  - *Captcha*
  - Bloqueio de Alteração do From:
  - *Log* do *squirrel* habilitado

Tratamento de Incidentes

- Novos logs
  - 41.220.75.x - - [06/May/2009:05:44:16 -0300] "GET /src/login.php HTTP/1.1" 200 3859 "https://webmail.dpf.gov.br/src/redirect.php" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Crazy Browser 2.0.1)"
  - 41.220.75.x - - [06/May/2009:05:44:18 -0300] "GET /plugins/captcha/backends/csi/CaptchaSecurityImages.php?width=120&height=40&characters=5&font=monofont.ttf&sq=1241599456 HTTP/1.1" 200 946 "https://webmail.dpf.gov.br/src/login.php" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Crazy Browser 2.0.1)"
  - ...
  - 41.220.75.x - - [06/May/2009:05:44:47 -0300] "GET /src/compose.php?mailbox=INBOX&startMessage=1 HTTP/1.1" 200 7478 "https://webmail.dpf.gov.br/src/right_main.php" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Crazy Browser 2.0.1)"

Tratamento de Incidentes

- Conclusão?
  - Bot que envia SPAM por squirrelmail com captcha?
  - Bug no squirrelmail?
- ou?
  - Nigerianos enviando SPAM usando contas com senha fácil manualmente?

Tratamento de Incidentes

- Caso 2: e-mail suspeito

PARA QUEM VIAJA MUITO PARA O EXTERIOR. VEJAM ONDE CHEGOU O PODER DO ESTADO.

IMPORTANTE, MUITO INTERESSANTE E INACREDITÁVEL!!!Esta informação, apesar de confidencial, é demasiado importante para ser guardada.
Sabiam que estamos todos "fichados" nos principais Serviços de Informações do Mundo?
Consultem, o "site" abaixo indicado e verifiquem que todos os dados dos nossos passaportes estão acessíveis, por qualquer pessoa, nos cadastros da NATO.

http://www.scrolllock.nl/passport/

É inimaginável!!! Basta colocar o 1º e o último nome, o País e depois, da lista das pessoas que vão aparecer, escolher a cidade e a rua da morada do proprietário do passaporte... O resto tá tudo lá !!! Até o IRPF e a fotografia.

O absurdo a que chegamos, não temos mais nenhum controle de nossa privacidade!!!!

Por favor divulguem

Tratamento de Incidentes

International Passport's Record Bureau.

privacy policy

Use the form below to search our database.

Search any Passport Information here:

First Name

Last Name

Citizen of ---Select a country---

Search Database

The information you provide is only used to search the database and is not used in any other manner.

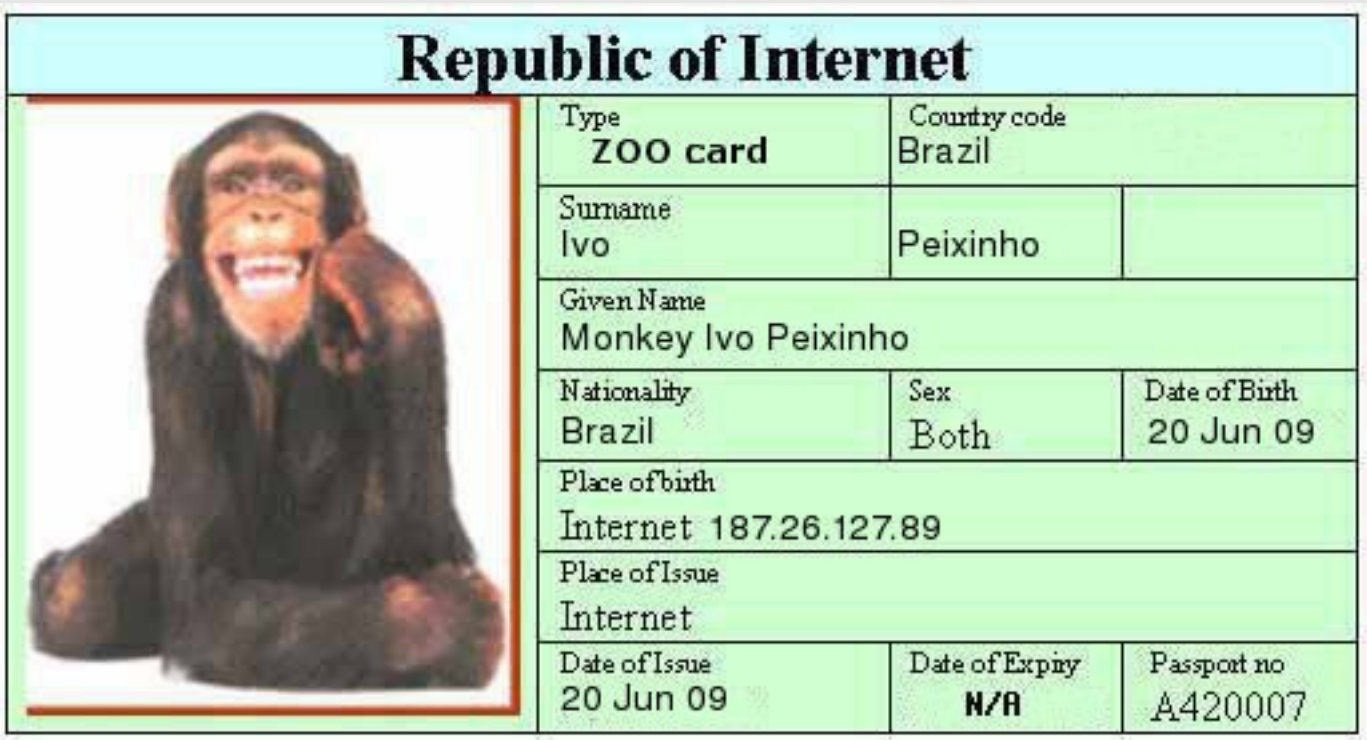
Welcome to the **World Passport Record Bureau** web site - where you can search our online database. We have over 6 Billion Passports currently on file, absolutely FREE!

Under the recent International Passport Act (INPA - enacted on Nov 2, 2003), every country in the world is required to make available to the public a digitized copy of each and every valid passport issued, in their respective country.

We managed to sign a mutual agreement with INPA, to create the world's only centralized database of Passports, on the more than 6 Billion Passports, in the World. We are still updating our database, and if you donot find your passport information here, comeback after a couple of days.

Tratamento de Incidentes

- Caso 2: e-mail suspeito



Republic of Internet

Type: ZOO card	Country code: Brazil	
Surname: Ivo	Peixinho	
Given Name: Monkey Ivo Peixinho		
Nationality: Brazil	Sex: Both	Date of Birth: 20 Jun 09
Place of birth: Internet 187.26.127.89		
Place of Issue: Internet		
Date of Issue: 20 Jun 09	Date of Expiry: N/A	Passport no: A420007

Próximos Passos

- Definição de ferramenta de tickets
  - RTIR
  - Desenvolvimento próprio
- Desenvolvimento do SAMURAI
  - Integração com outras fontes de incidentes
- Publicação de portaria com atribuições do GATI.DPF

Contatos

GATI (MJ): gati@mj.gov.br

GATI.DPF:gati.dpf@dpf.gov.br

Ivo de Carvalho Peixinho

peixinho.icp@dpf.gov..br