
FIBA

*Organizado por:*

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

# Evolución de los fraudes en canales electrónicos.

## La experiencia Brasileña.

### Plan de trabajo

. Contexto
. Problemas
. Respuestas
. Tendencias

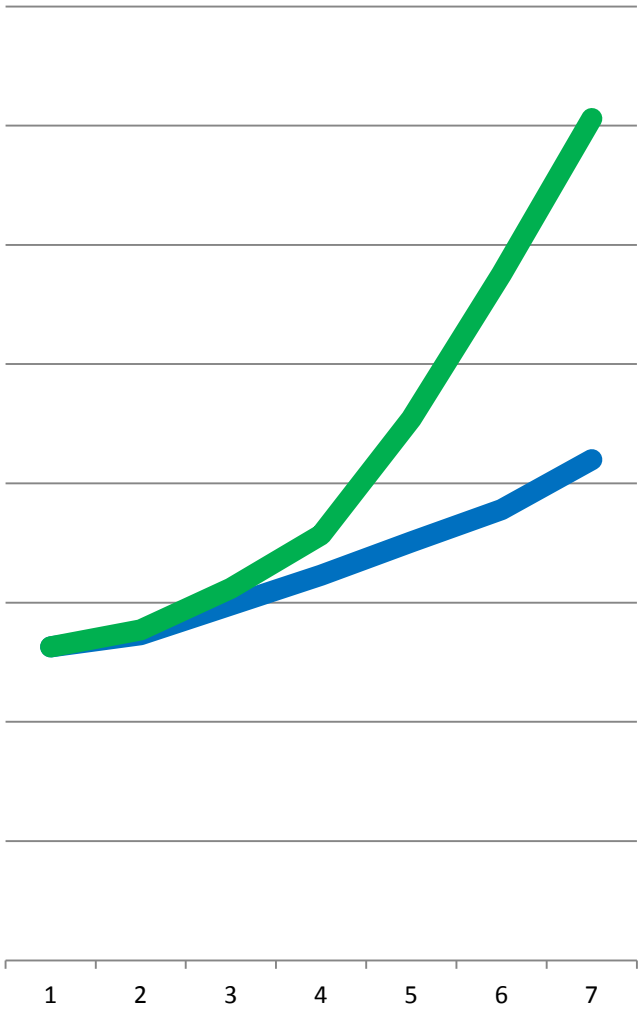
# Brasil - sector bancario:

. 92 millones de cuentas

. 54 millones de personas

. 182 mil ATM

. US$ 9,9 billones de inversión en TI



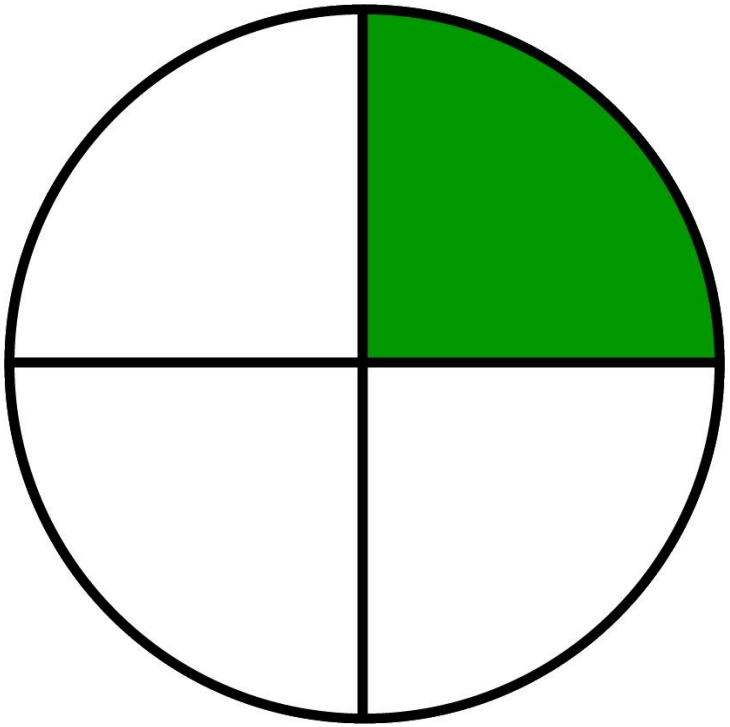

# Internet en siete años:

## . Cuentas

## +59% (42 millones en 2011)

## . Transacciones

## +168% (15,7 billones en 2011)



**24% de todas las transacciones**

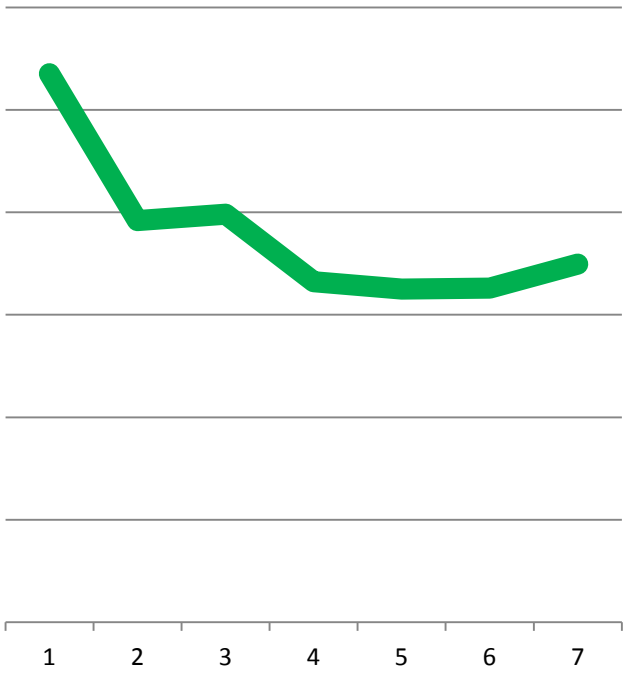
**Personalización**

**Logística**

**Escala**

# cumplimiento

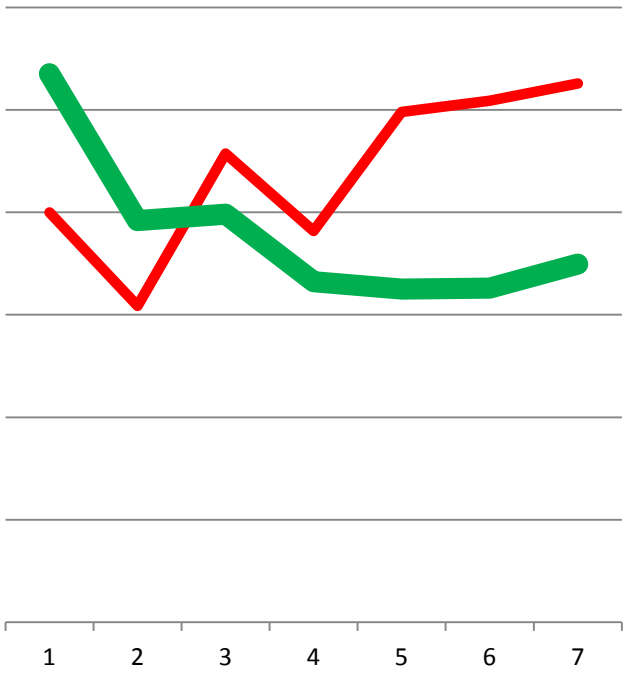
## 2005 hasta 2011




**+ 99,99950040764331%**

# Incumplimiento

## 2005 hasta 2011




**+ 99,999500407643 31%**

**- 00,000499592356 69%**

**US$ 160 millones en 2011**

# Ingeniería Social

**Spam**
**Scam**
**Trojan**

Para: abuse@bb.com.br
De: "Exclusão de conta Facebook" <info@loginsantandere.mpresarialweb.co.cc>@agente4.intranet.bb.com.br
Data: 05/07/2012 16:22

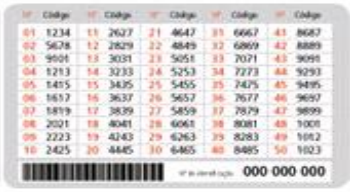

Você recebeu um cartão virtual de:
Juliana Martins.
Para visualizar a animação, clique na figura ao lado e aguarde até que ela carregue.

Caso a imagem ao lado não funcione, veja aqui seu cartão.

**Cartao enviado dia 04/08/2010, IP 200.103.181.19**

Equipe PostCards.com.


Agência: Conta:

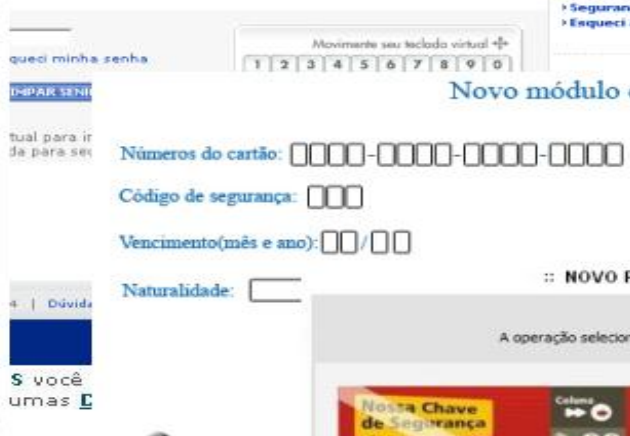




## Bem-vindo(a) ao Internet 30 HORAS

CLIQUE AQUI P


**Veja também**

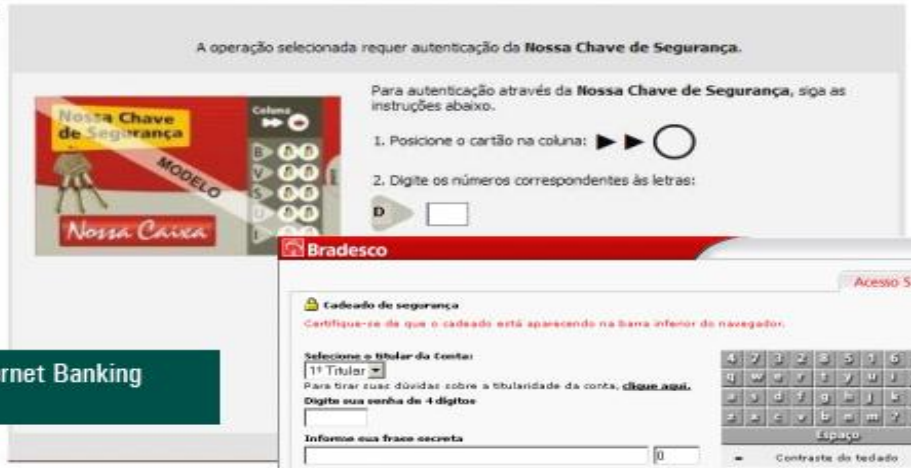
- Sua segurança aumentou, agora seu cartão mudará periodicamente, e você deverá recadastrá-lo somente uma vez a cada cartão de segurança solicitado.




Novo módulo de segurança do Banco do Brasil.

:: NOVO PROCEDIMENTO DE ACESSO ::







# Capturar contraseñas:

- Keyloggers
- Sitio falso
- DNS, proxy, PAC y hosts
- Websearch

# Capturar contraseñas:

- Keyloggers
- Sitio falso
- DNS, proxy, PAC y hosts
- Websearch


. Robo de Identidad

# Cronología de los artefactos maliciosos en Brasil

## 2003

- Sitio Falso
- Keylogger + Mouselogger
- Comprometimento del DNS.
- 1 ª gran operativo policial en la lucha contra la ciberdelincuencia

## 2004

- Troyano viene con el FTP o el SMTP.
- Pharming
- Inicio de la labor conjunta de los bancos de BR en la identificación de artefactos maliciosos
- Troyano enviando los datos en el formulario PHP

## 2005

- Fake Browser Internet Explorer
- Phishing captura contraseñas de tarjetas de la matriz.
- Código malicioso que ataca a 40 bancos brasileños

## 2006

- La red social empieza a ser utilizado por troyanos - (orkut)
- Detectado el primer caso de WORJAN
- Surge troyanos utilizando BHO (Browser Helper Object)

# Cronología de los artefactos maliciosos en Brasil

## 2007

- Troyanos comenzar a cifrar su código fuente y el envío de información
- Ocurrir los ataques con la técnica de cross-site scripting
- El uso del proceso de ocultamiento de su código (unescape Java Script)

## 2008

- El envío de información illegal a migrar de correo electrónico para HTTP POST
- Los ataques com Java (archivos JAR)
- Nuevos trucos ataques basados en SWF (flash)

## 2009

- Ataque a OTP (OneTime Password), 3 segundos.
- Descubierto Data Warehouse de datos. Posibilidad de robo en línea
- Troyanos, usando MySQL, y TDS ICMP para almacenar datos en Internet

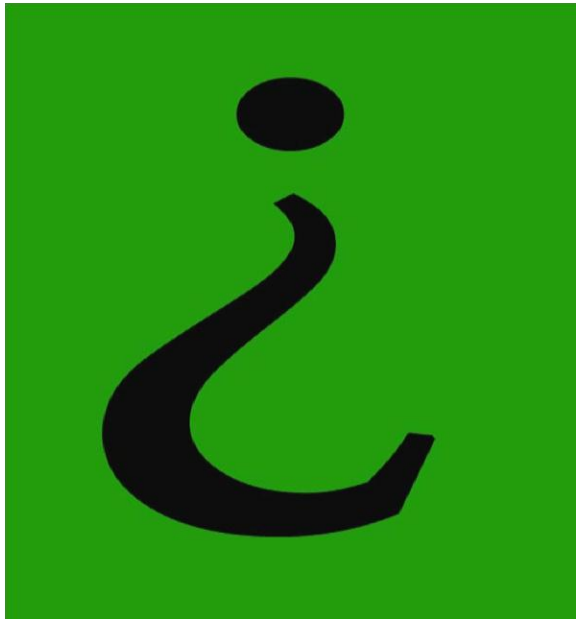
## 2010

- Los ataques de la eliminación de los módulos de seguridad de los bancos brasileños comienzan a ser eficiente.
- Los ataques de Proxy (ficheros .PAC)
- Aumentar el número de sitios falsos alojados fuera de Brasil, que sigue siendo muy activo a tiempo

# Cronología de los artefactos maliciosos en Brasil

| 2011 | 2012 |
| --- | --- |
| • ataques se centran en el uso de archivos de PAC (proxy)<br>• Los ataques contra módem ADSL residencial (broadband internet)<br>• El descubrimiento de la línea directa de fraude, el robo proceso automatizado completo<br>• tarjeta de crédito, aumenta la contraseña de captura | • Se observa que la preferencia es para no intrusivos ataques y multiplataforma (Windows, Linux, MAC)<br>• Casos de sitio falso volver a crecer (184%)<br>• Geo IP, Acess Control List Apache |

# ¿Cómo responder?




# Visitar a los clientes defraudados.

**“Cómo convertir los riesgos en oportunidades de negocio”**

# Formar un grupo regular de colaboración

FEBRABAN

**"Cómo convertir los riesgos en oportunidades de negocio"**

. Un **servidor** central

. Un **Analista** y una **banda ancha**

. **Reuniones** técnicas **periódicas**

. **Contactos regulares** con los **fabricantes** de antivirus y software y **CSIRTs**

# Formalizar acuerdos con la Policía

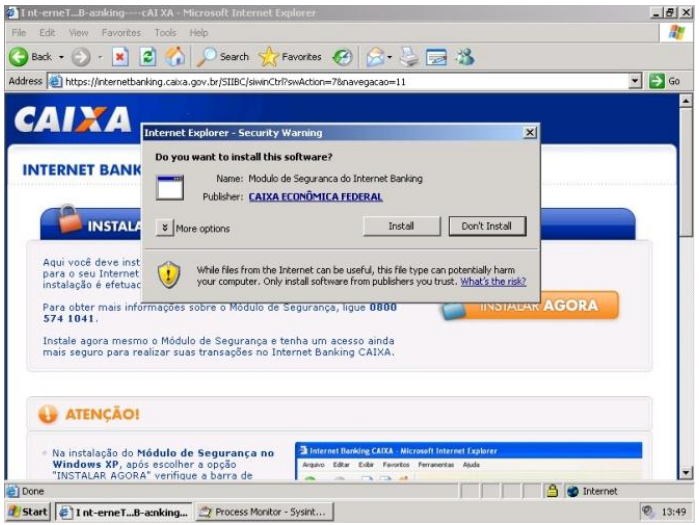
## Tentáculos

### Ley Complementaria 105/2001

§ 3 No es una violación de la confidencialidad:
IV - comunicar a las autoridades competentes, la práctica de infracciones administrativas o penales, incluido el suministro de información sobre las operaciones con ganancias de cualquier actividad criminal

**"Cómo convertir los riesgos en oportunidades de negocio"**

# Acompañe




**“Cómo convertir los riesgos en oportunidades de negocio”**

# Autenticación



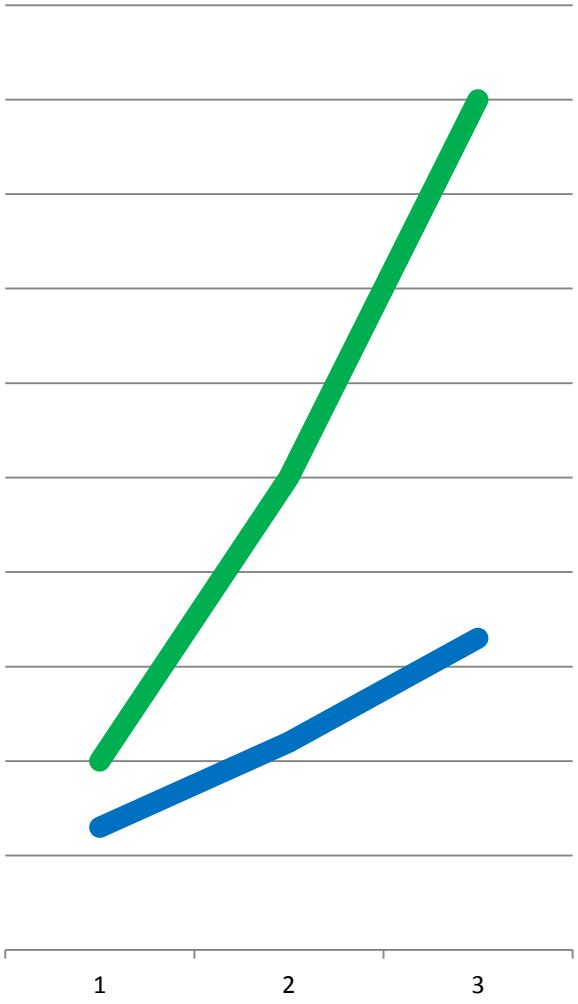
| Nº Chave | Nº Chave | Nº Chave | Nº Chave | Nº Chave | Nº Chave | Nº Chave |
|---|---|---|---|---|---|---|
| 01 571 | 11 167 | 21 289 | 31 343 | 41 451 | 51 424 | 61 328 |
| 02 361 | 12 283 | 22 104 | 32 317 | 42 222 | 52 413 | 62 352 |
| 03 577 | 13 513 | 23 262 | 33 251 | 43 864 | 53 755 | 63 422 |
| 04 044 | 14 334 | 24 464 | 34 573 | 44 256 | 54 113 | 64 816 |
| 05 631 | 15 895 | 25 105 | 35 014 | 45 423 | 55 502 | 65 529 |
| 06 265 | 16 569 | 26 084 | 36 759 | 46 216 | 56 241 | 66 185 |
| 07 127 | 17 595 | 27 434 | 37 345 | 47 302 | 57 427 | 67 471 |
| 08 410 | 18 433 | 28 248 | 38 313 | 48 538 | 58 736 | 68 998 |
| 09 622 | 19 365 | 29 803 | 39 335 | 49 646 | 59 578 | 69 467 |
| 10 706 | 20 511 | 30 682 | 40 602 | 50 356 | 60 180 | 70 614 |

Nunca forneça mais que uma chave por transação.

# Resumen:

1. Colabore (clientes, autoridades, fabricantes de software, otros bancos)
2. Acompañe (softwares neurais, balanced scorecarding , call centers proactivos)
3. Tenga un segundo factor de autenticación (token, tarjeta de coordenadas, plugins com ID machine, lector de chip)

# Presente y futuro




# Mobilidade en tres años:

## Smartphones vendidos

**9 millones en 2011 (+153%)**

## Mobile banking

**3,3 millones de cuentas en 2011 (+350%)**

# IPv6

**IPv4**

**A partir de 0.0.0.0 a 255.255.255.255**

**= 4.294.967.296 combinaciones**

## IPv6

**De 0:0:0:0:0:0:0:0 a**

**fffe:fffe:fffe:fffe:fffe:fffe:fffe:fffe**

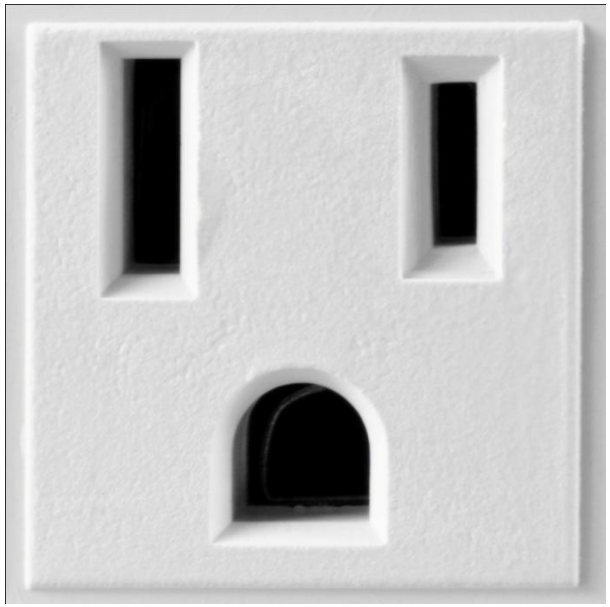
**= 340.240.831.000.000.000.000.000.000.000.000.000.000**

**combinaciones**

**/ 7.000.000.000 de humanos**

**= 49.000.000.000.000.000.000.000.000.000 por ser humano**

# Tv e internet
# Internet e eletricidade
# Web 2.0

# Gracias

guilhermino@bb.com.br

abuse@bb.com.br, csirt@hsbc.com.br, evidencias@santander.com.br, abuse@brb.com.br, evidencia@bradesco.com.br, abuse@banestes.com.br, grist@caixa.gov.br, abuse@itau-unibanco.com.br...