Seguridad TIC

Desafíos y oportunidades para emprendimientos de base tecnológica en Argentina

Iván Arce – Programa de Seguridad en TIC Fundación Dr. Manuel Sadosky

Córdoba Tech Day – 2 de septiembre de 2014

Ministerio de Ciencia, Tecnología e Innovación Productiva
Presidencia de la Nación

fundación SADOSKY
Investigación y Desarrollo en TIC

cessi ArgenTIna

CICOMRA

Presentación

…… - 2012 PROGRAMA STIC – Fundación Dr. Manuel Sadosky

Organización sin fines de lucro público-privada dedicada a promover, robustecer y articular las actividades de investigación, desarrollo e innovación en TIC entre el sector privado, sistema científico-tecnológico y estado argentino.

http://www.fundacionsadosky.org.ar

2011-1996 CORE SECURITY TECHNOLOGIES – Fundador & CTO

Empresa de software y servicios de seguridad informática fundada en 1996 en Argentina.

Primera en desarrollar software comercial para penetration testing (2002, CORE IMPACT)

Hoy: 1600+ clientes en todo el mundo (NASA, Cisco, Apple, Chevron, Lockheed Martin, Raytheon, Boeing, Abbot, Pfizer, GE, Honeywell, AT&T, BT, Qualcomm, US FAA, US NRC…)

150-200 empleados, centro de I+D en Buenos Aires, oficinas comerciales en Boston, EEUU.

9 patentes internacionales otorgadas, 100+ publicaciones técnicas, 100+ vulnerabilidades

http://www.coresecurity.com

2014-2003 IEEE Security & Privacy Magazine – Editor Asociado / Miembro del Consejo Editorial

Revista especializada en seguridad y privacidad de la Sociedad de Computación del IEEE

http://www.computer.org/portal/web/computingnow/securityandprivacy

2014 – Miembro fundador del Center for Secure Design de IEEE-CS

http://cybersecurity.ieee.org/center-for-secure-design.html

Qué es la Fundación Sadosky ?

- La Fundación Dr. Manuel Sadosky es una institución público-privada cuyo objetivo es promover la articulación entre el sistema científico - tecnológico y la estructura productiva en todo lo referido a las Tecnologías de la Información y la Comunicación (TIC)

- Formalmente creada por Decreto del Poder Ejecutivo Nacional en Junio de 2009, comenzó a funcionar a fines de 2011

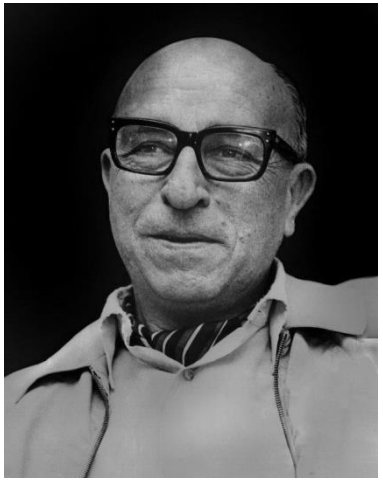
- Lleva el nombre de quien fuera un pionero y visionario de la informática tanto en el país como en la región

- MinCyT, CESSI y CICOMRA

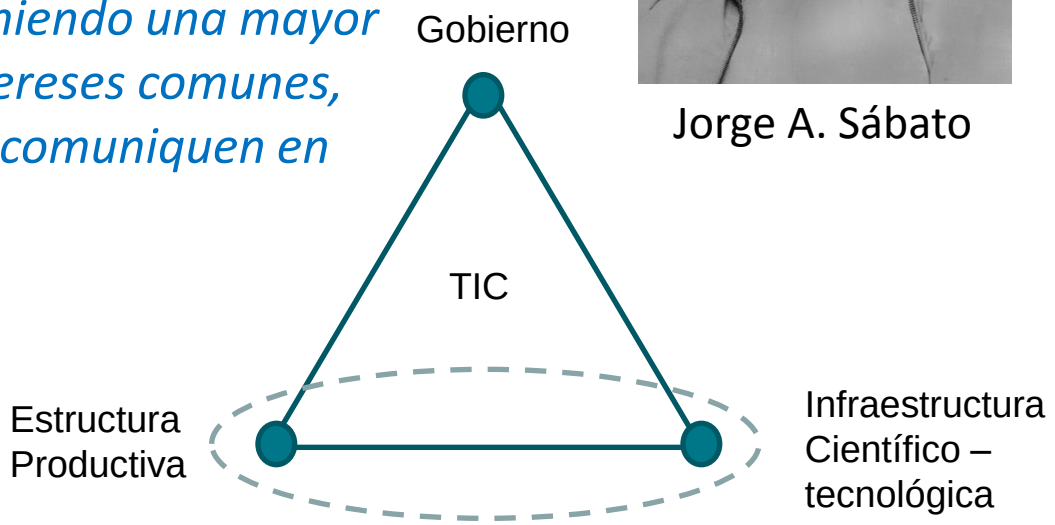
Dr. Manuel Sadosky
(1914-2005)

Tenemos objetivos de mediano y largo plazo

*"La **interacción** necesaria entre el **gobierno**, la **estructura productiva** y la **infraestructura científico-tecnológica** no se alcanza con la sola expresión de deseo, mediante un decreto, sino que es consecuencia de un proceso socio-político que se acelera en la medida en que sus protagonistas vayan teniendo una mayor conciencia de su rol, posean intereses comunes, definan objetivos comunes y se comuniquen en un lenguaje común"*



Jorge A. Sábato



Cuál es el propósito del Programa STIC?

Visión

“Las TIC como factor transformador para una sociedad con un cultura emprendedora que promueve e impulsa la creación de conocimiento, la innovación productiva y sustentable, la competitividad de la economía y la mejora de la calidad de vida de la población **sin que ello redunde en un aumento de la dependencia tecnológica o de la vulnerabilidad de la infraestructura crítica**“

Funciones del Programa STIC

1. **Desarrollar y robustecer capacidades de I+D+i**

2. **Articulación Academia-Industria-Estado**

3. **Divulgación, asesoría y capacitación**

4. **Vinculación regional y extra-regional con centros de I+D de Seguridad TIC**

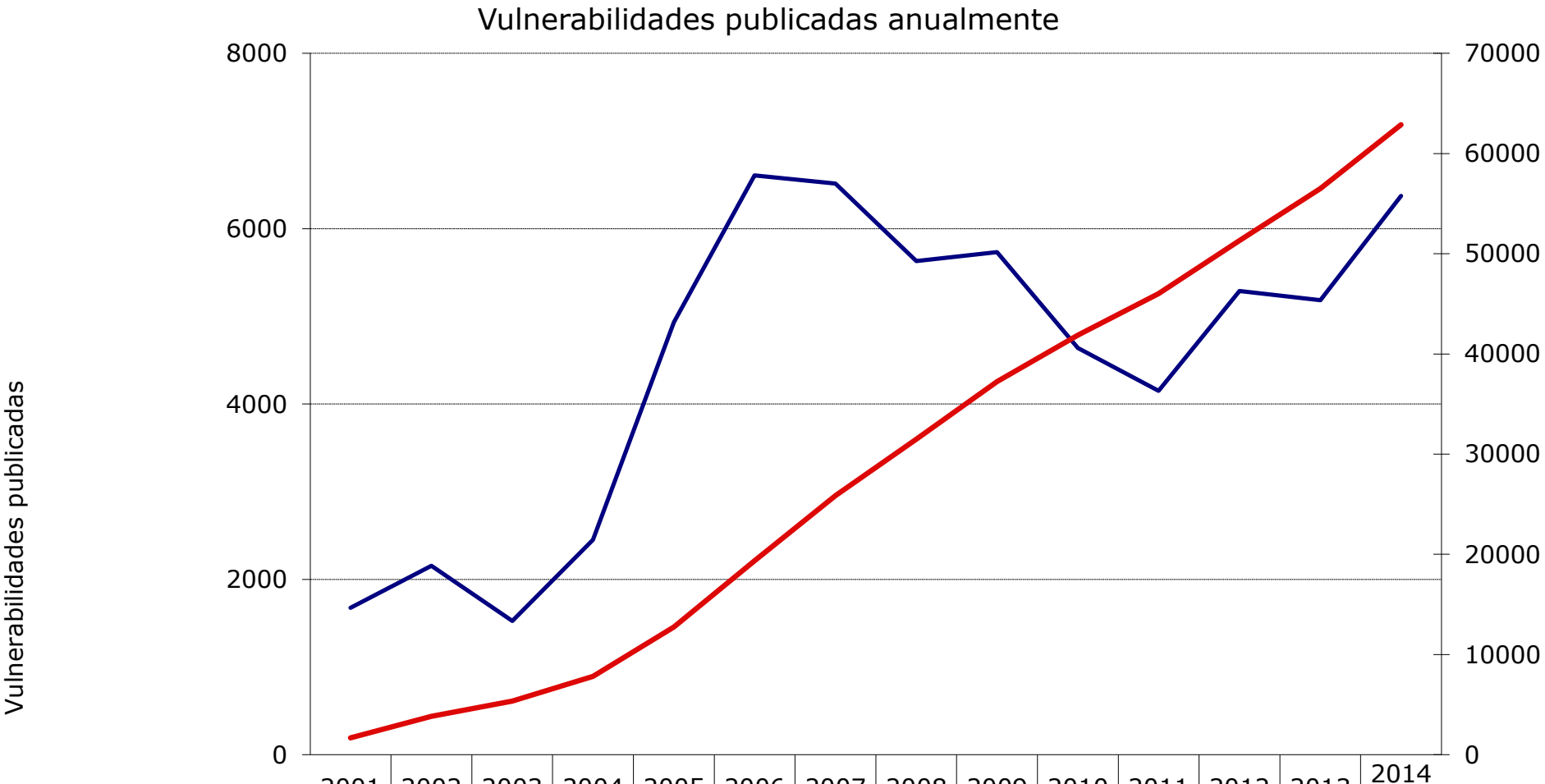
5. **Proyectos Faro de I+D+i**

Seguridad TIC
Por qué hablar de esto acá?

Porqué hablar de Seguridad de TIC ?

- Tiene relevancia estratégica para nuestro país y nuestra región
- Problemática real con impacto directo sobre todos los habitantes
- Sin seguridad no hay privacidad ni posibilidad de garantizar otros derechos fundamentales.
- Seguridad de TIC es transversal, el software es omnipresente
- **Investigación, Desarrollo e Innovación**
  Clave para la “soberanía tecnológica”
  Ataque y Defensa son complementarios, ambos necesarios.
- Es necesario pero no suficiente:
  Políticas nacionales, regulación e implementación de controles
  Desarrollo del sector productivo
  Crear y robustecer un ecosistema sustentable

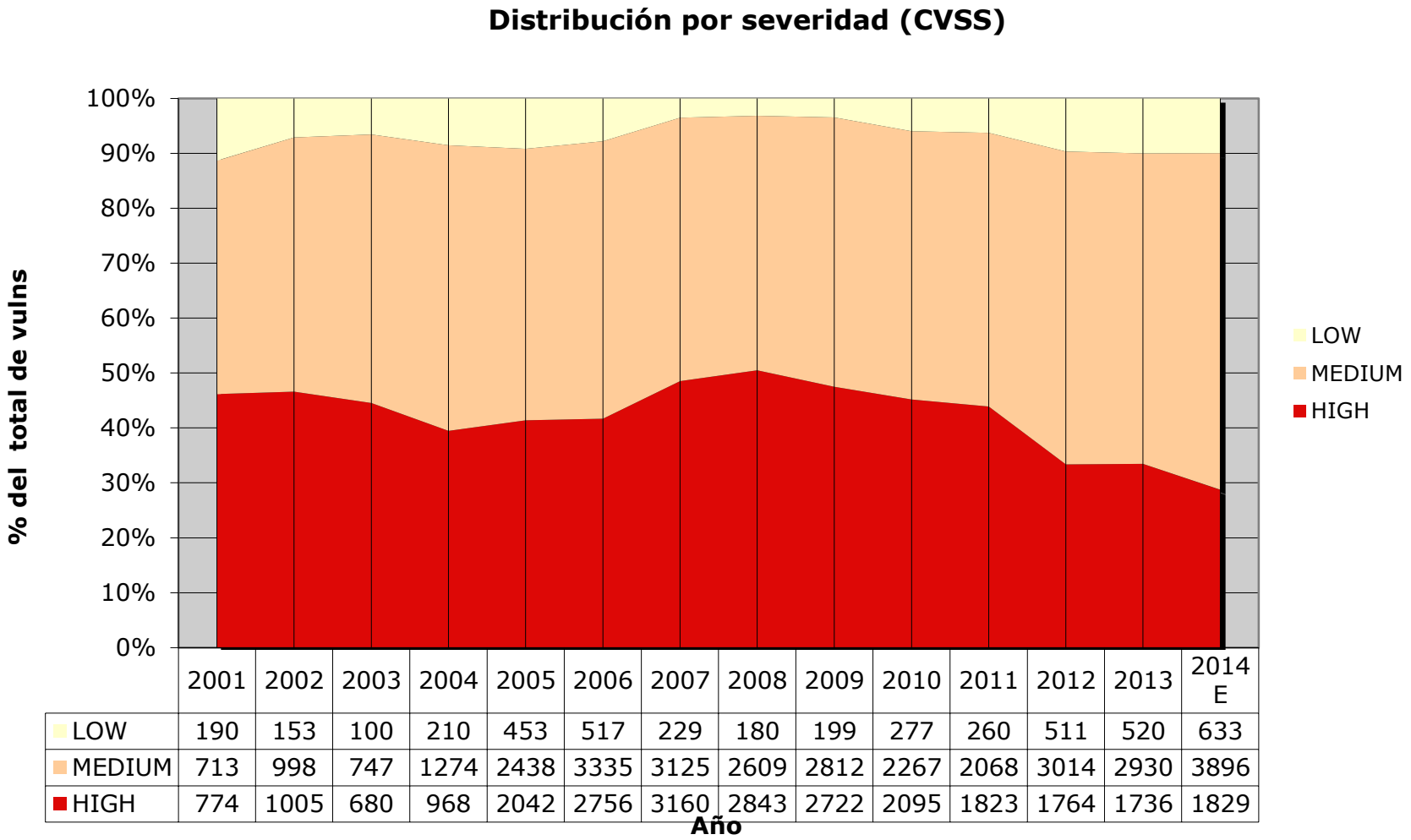
La seguridad TIC y el software



	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014 E
Vuln nuevas (NVD)	1677	2156	1527	2452	4933	6608	6514	5632	5733	4639	4151	5289	5186	6375
Acumulado (NVD)	1677	3833	5360	7812	12745	19353	25867	31499	37232	41871	46022	51311	56497	62872

Fuente: National Vulnerability Database, National Institue of Standards and Technology (NIST), EEUU

Si, hay muchos *bugs*, pero son graves?



	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014 E
LOW	190	153	100	210	453	517	229	180	199	277	260	511	520	633
MEDIUM	713	998	747	1274	2438	3335	3125	2609	2812	2267	2068	3014	2930	3896
HIGH	774	1005	680	968	2042	2756	3160	2843	2722	2095	1823	1764	1736	1829

Fuente: National Vulnerability Database, National Institue of Standards and Technology (NIST), EEUU

Cuál es el alcance del problema?

- Las estadísticas mostradas son de:
  - Problemas de implementación (bugs)
  - Publicados por fabricantes o terceros (investigadores, industria, etc.)
  - Catalogados con un ID único (CVE) por Mitre.org
  - Solo aplicables a software comercial ya desplegado

- Se estima que los *bugs* solo representan el 50% de los problemas de seguridad del software. El otro 50% corresponde a fallas de diseño (*flaws*)

- La cantidad de bugs es al menos 1 o 2 órdenes de magnitud mayor si consideramos software a medida o desarrollado para uso interno.

- El costo de arreglar un bug crece exponencialmente en el tiempo:

{Requerimientos, diseño, implementación, testing, despliegue, mantenimiento}

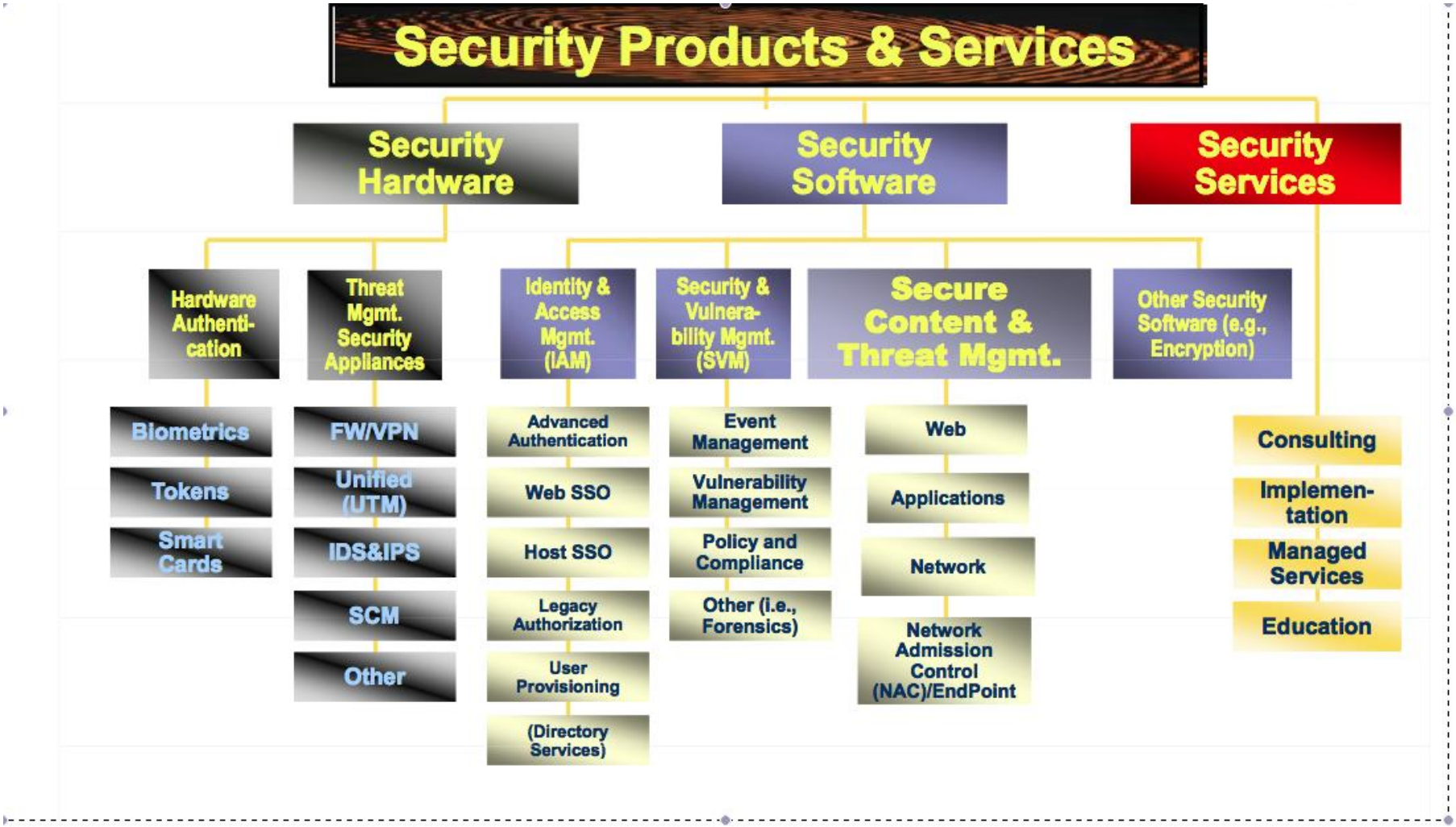
Seguridad TIC
El mercado y la industria

Mercado global de software y servicios de seguridad TIC

- Mercado global: 71.100MM USD* (2014)
  - Seguridad Computadoras de Escritorio y Servers: $7.170 MM USD (2010)
  - Seguridad de Redes: $7.540MM USD (2010)
  - Gestión de Identidades y Accesos: $4.450MM USD (2010E)
  - Gestión de Seguridad y Vulnerabilidades : $3.400MM USD (2010)
  - Seguridad Web: $1.700MM USD (2010)
  - Protección contra Filtración de Datos (DLP): $680MM (2013) Crecimiento estimado > 18% para el 2014
- Crecimiento estimado al 2015: 76.900 MM USD* (8,2%)
- >1.000 Empresas de Seguridad TIC $10MM USD/año
- **Menos del 1% son de capitales o tecnología nacional**

* Forecast Overview: Information Security, Worldwide, 2012-2018, 2Q14 Update, Agosto 2014, Gartner

Mercado global de seguridad de las TIC



“One Ring to rule them all, One Ring to find them,

One Ring to bring them all and in the darkness bind them“

El anillo de Sauron, *El Señor de los Anillos*
Novela de J.R.R. Tolkien, 1954-1955

QUE TIENEN EN COMÚN TODAS LAS SOLUCIONES DE LA INDUSTRIA?

- **Ninguna funciona bien…**
- **Todas introducen nuevos puntos de falla**
- **Arquitectura del siglo pasado (1980-1990)**
- **Interfaz gráfica del siglo pasado (1980-2000)**
- **Generación centralizada de valor (contenido)**
- **Distribución centralizada de valor**
- **Estructuras jerárquicas de gestión, topología estrella**
- **Chapucerismo y charlatanismo tecnológico**

PROBLEMAS AUN NO RESUELTOS

- Cómo desarrollar software sin vulnerabilidades
- Cómo encontrar bugs en forma eficiente
- Cómo explotar bugs en forma eficiente
- Cómo arreglar bugs en forma eficiente (y efectiva)
- Cómo determinar si un programa es bueno o malo
- Cómo determinar si un programa es una variante de otro
- Cómo determinar si alguien nos está atacando
- Cómo determinar la mejor forma de atacar a otro
- Cómo guardar un secreto
- Cómo computar en secreto
- Cómo gestionar la seguridad TIC de una organización

∄ programa que determine ...

```
/* abo1.c                                *
 * specially crafted to feed your brain by gera */

/* Dumb example to let you get introduced...    */

int main(int argv,char **argc) {
        char buf[256];

        strcpy(buf,argc[1]);
}
```

- ✓ Si el programa tiene un defecto de seguridad
- ❑ El alcance del problema de seguridad.
- ❑ Si el programa es “bueno” o “malo”
- ❑ Que input hay que darle para que imprima:
  “Aguante Belgrano de Córdoba!”

Seguridad de TIC
Internet

El gobierno formal y el gobierno real

- Componentes fundamentales
  - Internet Protocol (IP)
  - Domain Name System (DNS)
  - Border Gateway Protocol (BGP)
  - Secure Socket Layer (SSL)
  - Network Time Protocol (NTP)

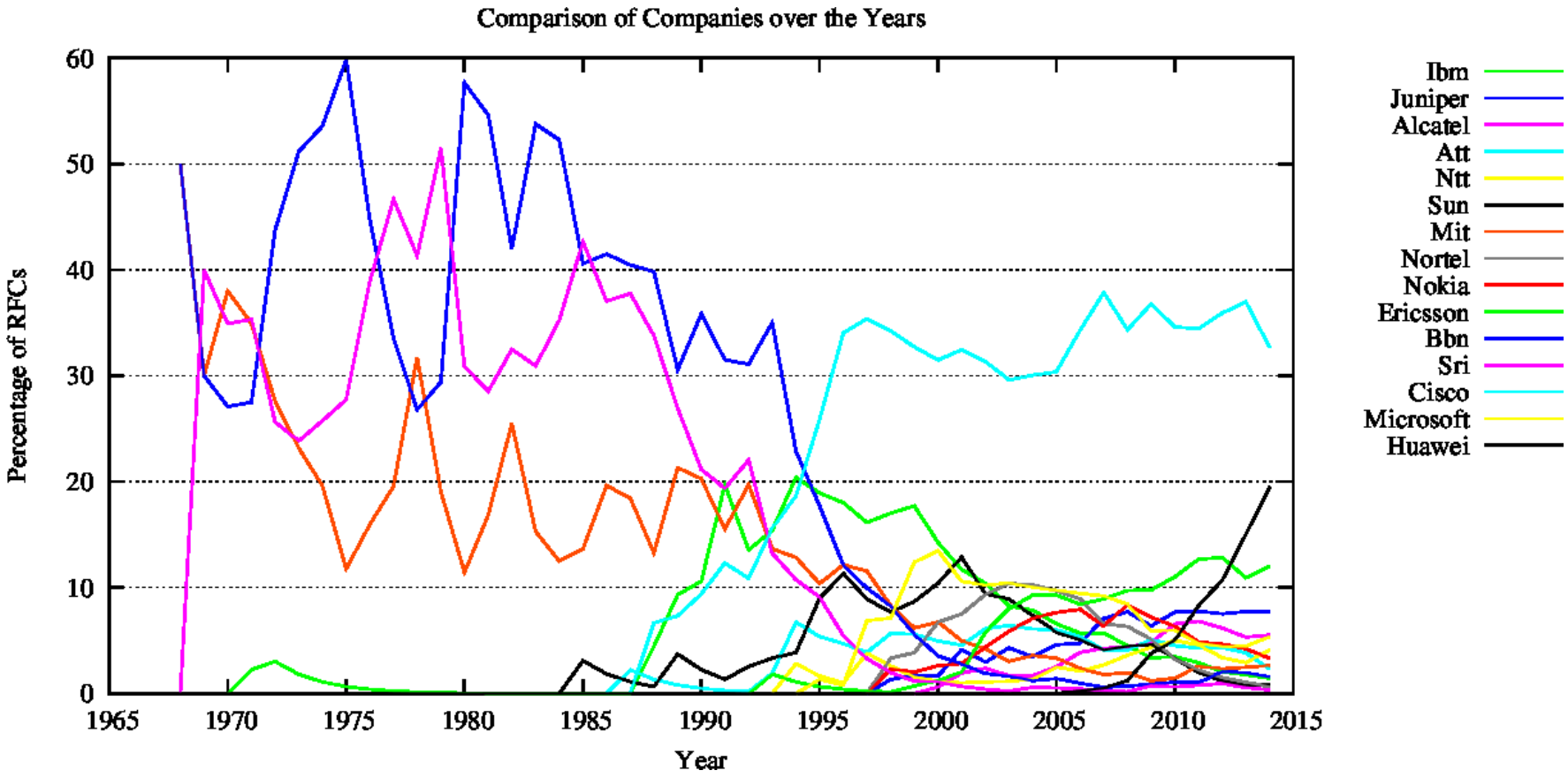
  En los últimos 15 años todos ellos "evolucionaron" hacia la centralización del comando y control de su funcionamiento

- 10 de 13 DNS root servers operan bajo jurisdicción de EEUU
  http://www.iana.org/domains/root/servers

- 3 autoridades certificantes (bajo jurisdicción de EEUU) firman mas del 75% de los certificados SSL
  http://www.netcraft.com/internet-data-mining/ssl-survey

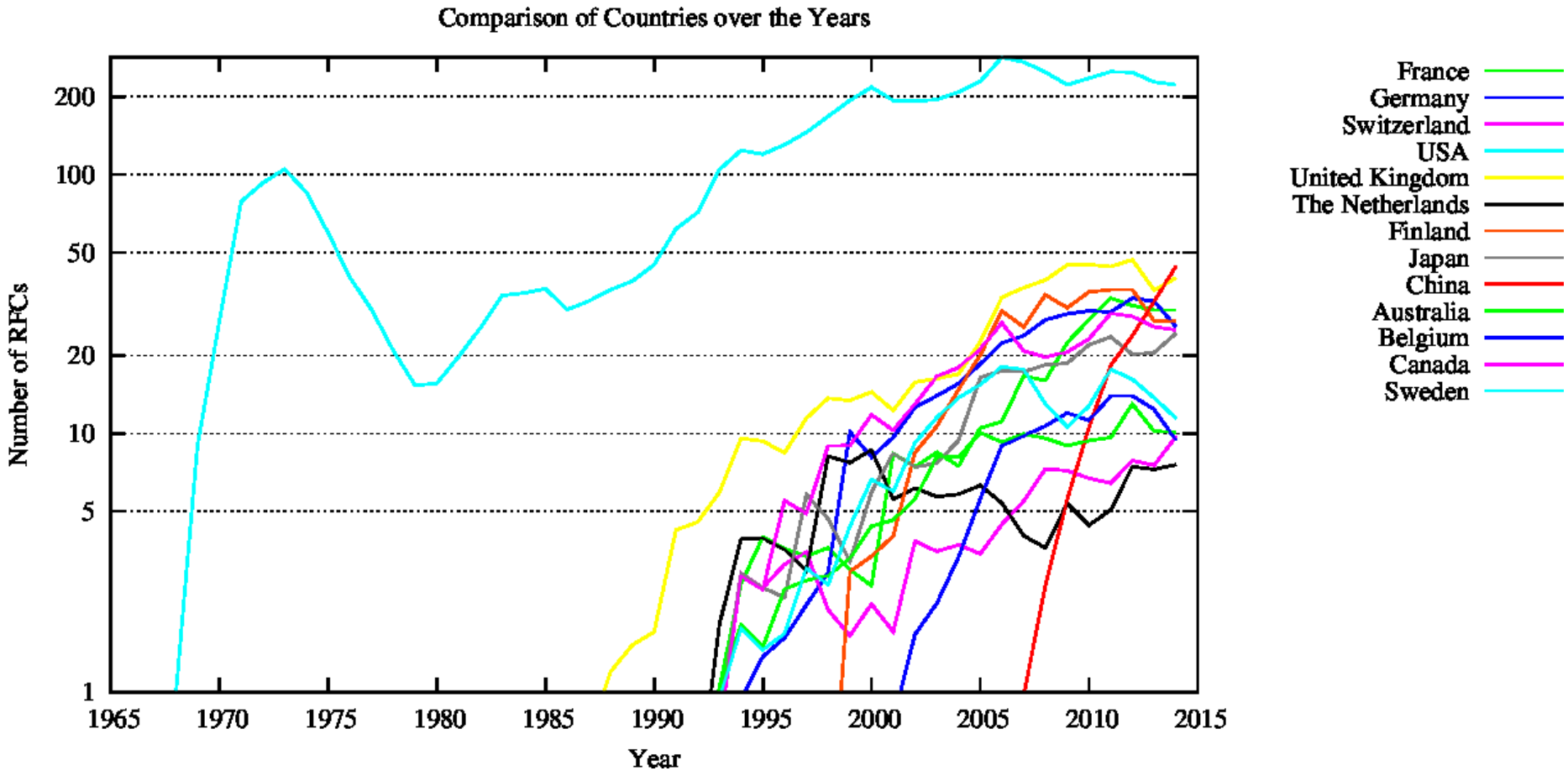
- Los 10 principales proveedores de inter-conectividad en Internet (Tier 1) son extra-regionales
  http://as-rank.caida.org/?mode0=org-ranking

Quienes definen los estándares técnicos ?



Fuente: http://www.arkko.com/tools/rfcstats/companydistrhist_norm.html

De dónde son los autores de los estándares técnicos?



Argentina:30 (0,34%) Brasil:7 (0,08%) México: 3 (0,03%) Colombia: (0,03%)

Fuente: http://www.arkko.com/tools/allstats/d-countrydistr.html

Seguridad TIC
Contexto legal y regulatorio

Contexto Legal

- Espionaje informático (*ciberespionaje*)

  Ley 25.520 "Inteligencia Nacional"

- Delito informático (*ciberdelito)*

  Ley 26.388 "Delito Informático"

  Ley 35.326 "Protección de los datos personales"

  Convenio sobre ciberdelincuencia (Budapest)

  - Panamá y Rep Dominicana, unicos paises signatarios de la región
  - Potencial efecto negativo sobre actividades de I+D (Articulo 6)

http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

- Guerra cibernética (*ciberguerra*)

  - Wassenaar Arrangement (Dic. 2013)

  El "software de intrusión" agregado a la lista de tecnologías de uso dual con controles de exportación (Categoría 4)

  http://www.wassenaar.org/controllists/index.html

Legislación y regulación extranjera

- Sarbanes-Oxley Act (*SOX*) – EEUU
  Establece obligaciones pare empresas que cotizan en bolsa

- Payment Card Industry Data Security Standard (*PCI-DSS)*
  Requerimientos y estándares para organizaciones que operan con datos de tarjetas de crédito.

- Gramm-Leach-Bliley Act (*GLB*) – EEUU
  Establece requerimientos a la industria financiera (bancos, aseguradoras, financieras, etc.) para la protección de la información financiera de sus clientes

- Data Protection Directive (Directive 95/46/EC) – UE
  Regula procesamiento de datos personales por paises miembros de la UE. Parte componente de las leyes de privacidad y derechos humanos.

Conclusiones

I+D+i para Seguridad de las TIC en Argentina

- **Existe una oportunidad de negocios en el mercado global de STIC**
- **Tiene relevancia estratégica para nuestro país**
- **Problemática real con impacto directo sobre todos los habitantes**
  - **Hay software por todos lados y cada vez más**
  - **Sin seguridad no hay privacidad**
- **Es necesario pero no suficiente**
  Regulación e implementación de controles operativos
  Desarrollo del sector productivo
  Crear y robustecer un ecosistema sustentable

- **El estudio de la Seguridad TIC requiere enfoque multi e interdisciplinario**.

Email: stic@fundacionsadosky.org.ar

GRACIAS!

Seguridad TIC
Ataque y defensa