

Infraestructuras críticas y Seguridad de la Información

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

Seminario Regional de Ciberdefensa. – CDS-UNASUR – Mayo 2014



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

fundación
SADOSKY
Investigación y Desarrollo en TIC

cessi
Argen**Tina**



Quién es este tipo?

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 de 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>

2012-2003 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>

Que es la Fundación Sadosky

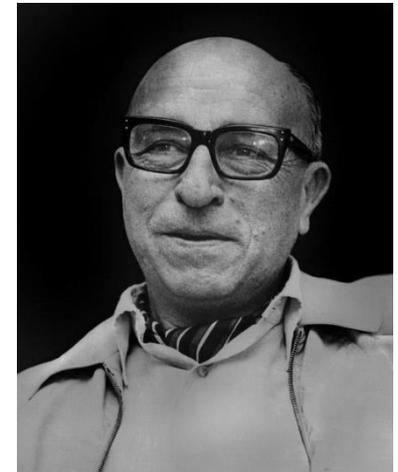
- La Fundación Dr. Manuel Sadosky es una institución público-privada cuyo objetivo es promover la articulación entre el sistema científico - tecnológico y la estructura productiva en todo lo referido a las Tecnologías de la Información y la Comunicación (TIC)
- Formalmente creada por Decreto del Poder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

Dr. Manuel Sadosky
(1914-2005)

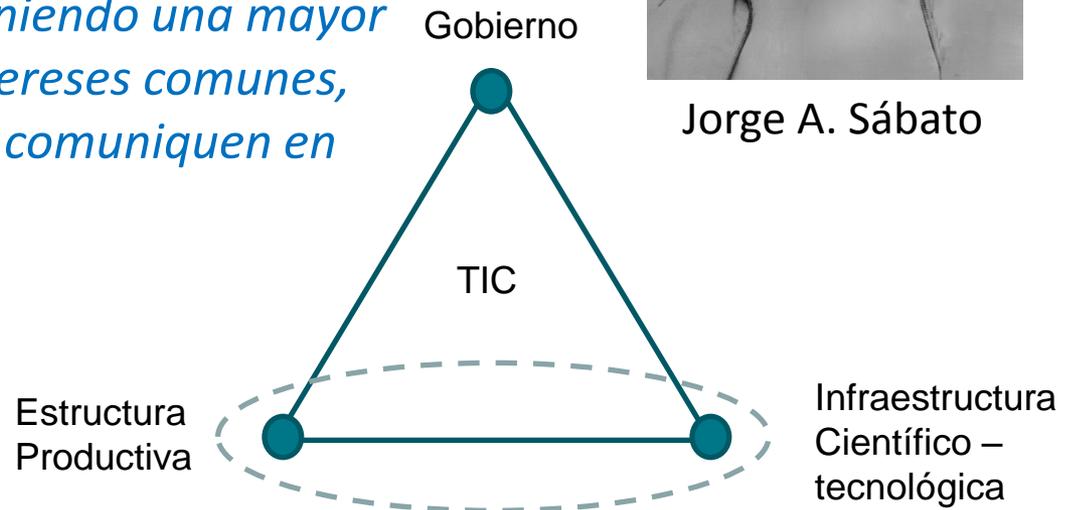


Tenemos objetivos de mediano y largo plazo

*“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. Sabato



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**“

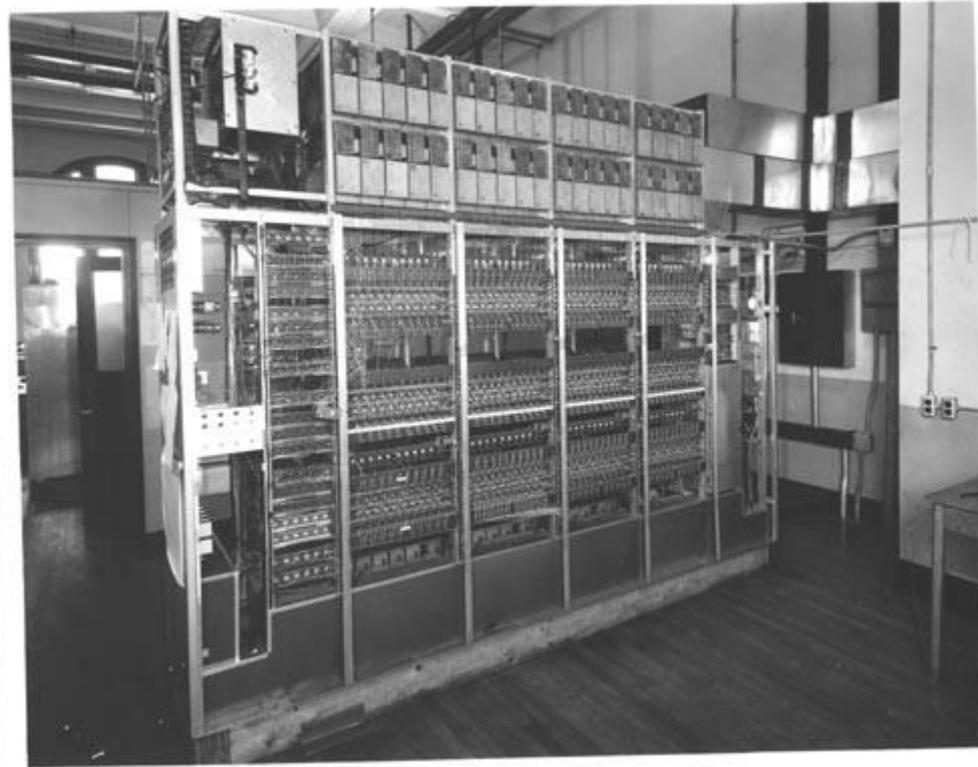
Funciones del Programa STIC

- 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 de la Información

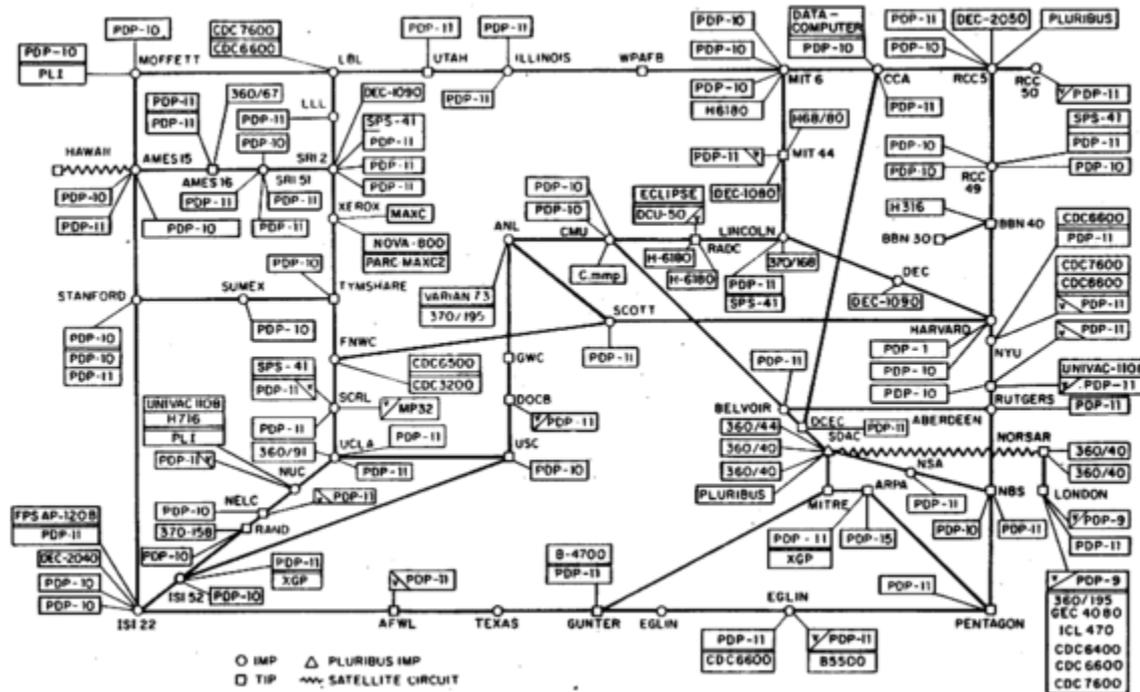
Ataque y defensa

1950-1970



1970-1980

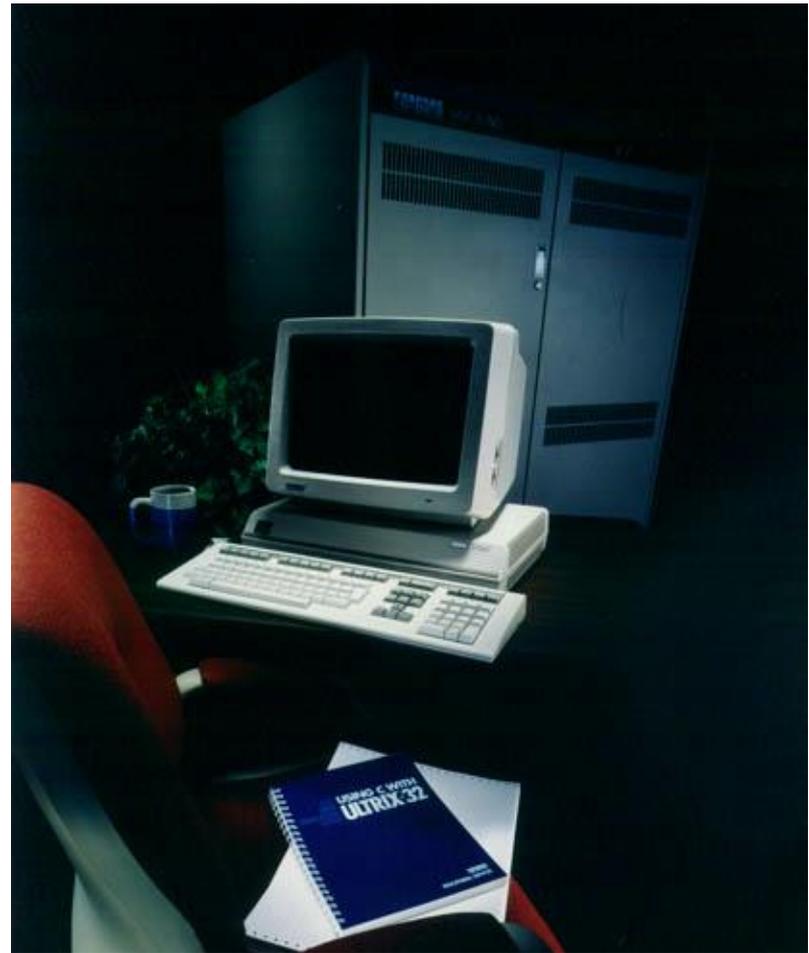
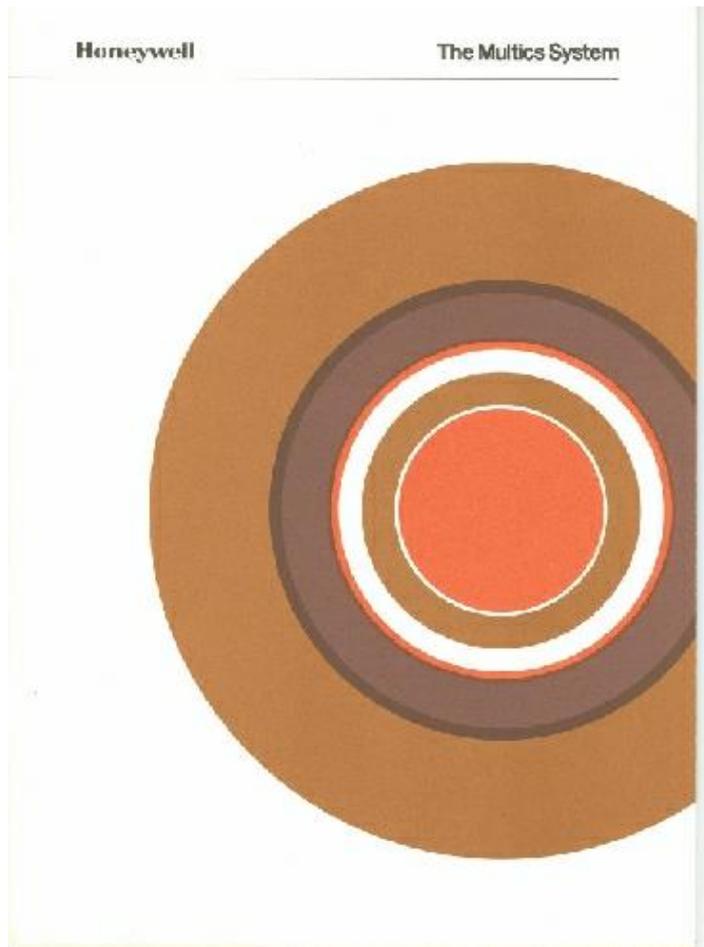
ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE MOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY.)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

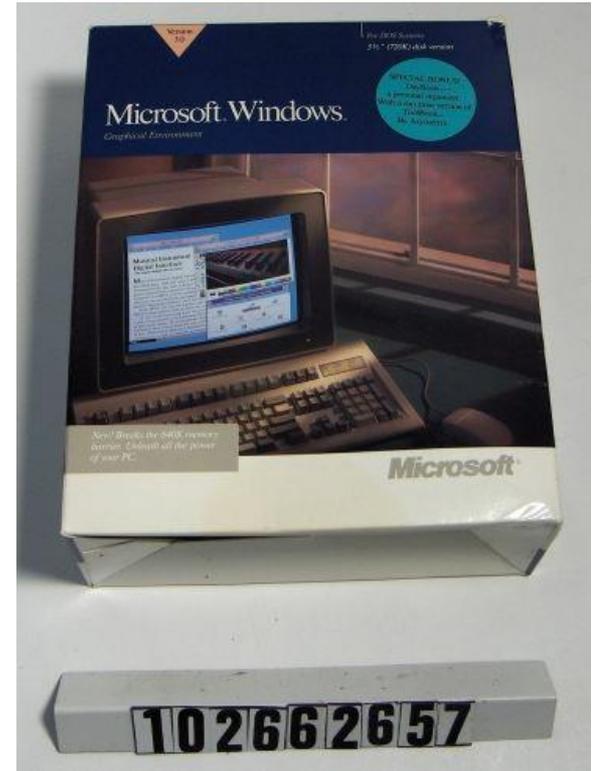
1970-1980



1970-1980



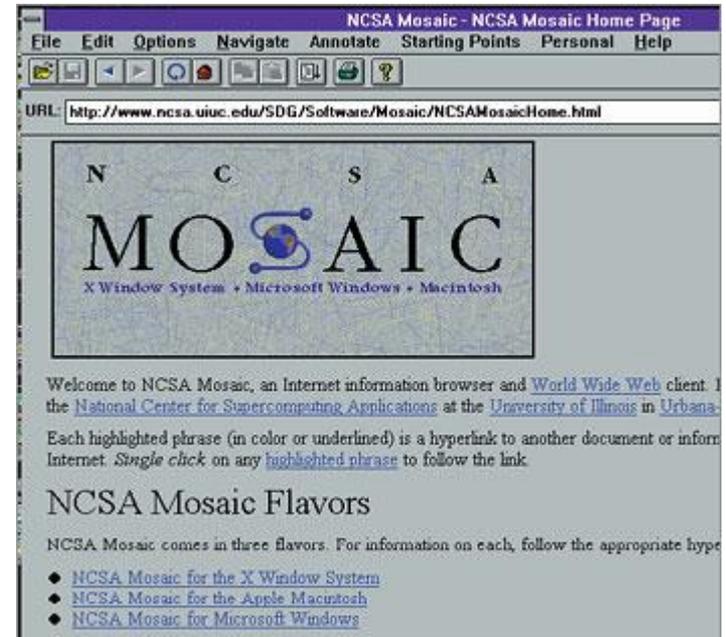
1980-1990



1990-2001



We make the net work.



2001-2010

amazon.com[®]



ebay[®]

2010+

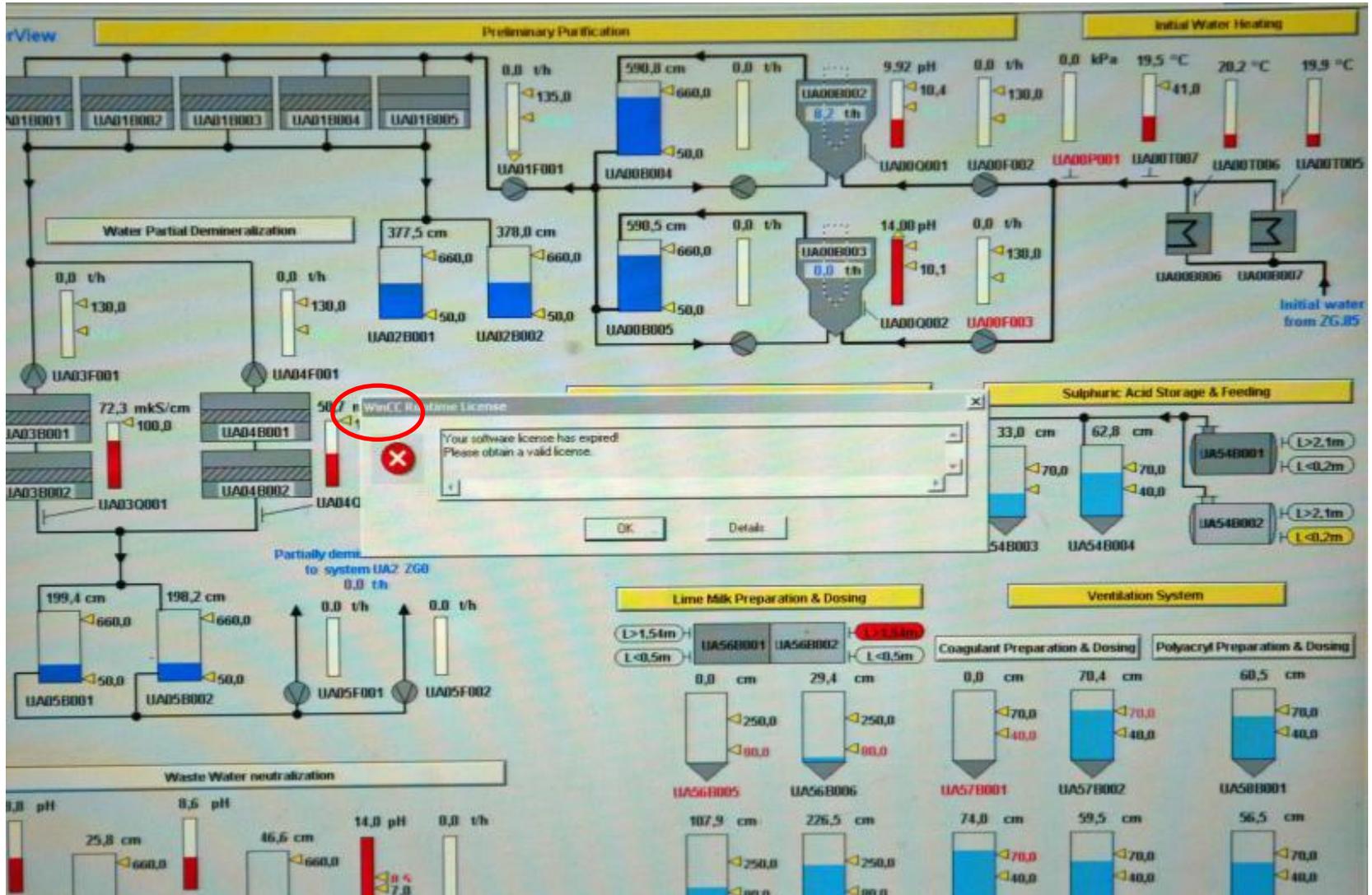


FLAME: THE SPY MALWARE INFILTRATING COMPUTERS IN THE MIDDLE EAST

Number and location of Flame infections detected by Kaspersky Lab on customer machines



Que tan difícil puede ser?



SIEMENS

What's the smartest
route to more productivity
in all processes?

[→ Learn more](#)

Higher visibility in production
SIMATIC WinCC SCADA system

With the SCADA system SIMATIC WinCC, Siemens offers an innovative, scalable process visualization system with numerous high-performance functions for monitoring and controlling processes. Whether in a single-user system or a distributed multi-user system with redundant servers, the system offers complete functionality for all industries and features optimum performance.

[Automation Technology](#) ▶ [Deutsch](#)[Contact](#) ▶ [Index](#)[Site Explorer](#)[Automation Technology](#) > [Operator control and monitoring systems](#) > [HMI Software](#) > [SCADA System SIMATIC WinCC](#)

SCADA System SIMATIC WinCC

- > [SIMATIC WinCC](#)
- > [WinCC Options](#)
- > [WinCC Add-ons](#)

Process visualization with Plant Intelligence

Our SCADA system offers maximum functionality and a user-friendly user interface. With this configurable and scalable system, you have the advantage of absolute openness to both the office environment and to production. An integrated process database and Plant Intelligence, for example, ensure transparency in



SPS IPC Drives 2012

27. - 29. November [Get More Info](#)



Siemens Industry Reference Center

Automation Technology Language Contact

Product: SCADA System SIMATIC WinCC
Enter search term [] Find [] Remove all filters []
Industry: Please select Region: Americas Service: Please select

6 article(s) found Show 10 | 20 | 50 articles per page

- > **Jacksonville water supply project, Florida, USA**
Siemens helps utility JEA keep the waters flowing in Northeast Florida by introducing SINAUT telecontrol
- > **Cutting-edge treatment**
Cobb County Georgia taps Siemens automation to improve wastewater treatment operations
- > **Iaco Agricola – Brazil**
- > **New Cycle for Washing Drums**
The Condor industrial laundry in North Buenos Aires increased the efficiency of its machines by using Simatic S7-200 and Micromaster 440 drives. It not only increased the washing quality but also reduced the energy consumption.



Text size []

Most viewed

- > Building Automation using PROFINET at AZ Sint-Jan - Realized by Actemium Belgium
- > Full process automation and control of Vesta Tank Terminal using WinCC and integrated Safety
- > More efficiency and flexibility with WinCC at Vopak Leftbank Terminal Antwerp - Realized by Actemium Belgium
- > At Kemira, WinCC brings the productivity and quality of feed to a higher level
- > Strong stuff
- > Wireless waste processing at Vanheede Environmental Group - Realized by CDC Automatisatie
- > Water treatment plant Xiangcheng, Suzhou, China
- > North China Pharmaceutical Group Corp., China
- > Automation of the Oguz-Gabala-Baku water pipeline, Azerbaijan
- > Jacksonville water supply project, Florida, USA

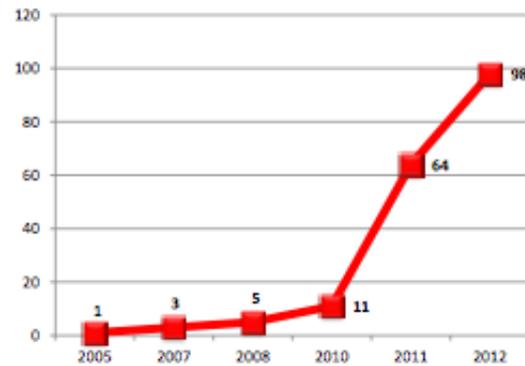


Figure 1. Dynamics of the Number of Vulnerabilities

3.3. The Number of Vulnerabilities in the ICS systems of Various Vendors

The highest number of vulnerabilities for the reporting period (42) was discovered in the components of the ICS developed by Siemens. The second place goes to Broadwin/Advantech (22 vulnerabilities); the third, to Schneider Electric (18 vulnerabilities).

Tab. 2. The Number of Vulnerabilities in the ICS Systems of Various Vendors

Vendor	Vulnerability Total	Vendor	Vulnerability Total
Automated Solutions	2	WellinTech	9
Schweitzer Engineering Laboratories	2	7-Technologies	12
RuggedCom	2	General Electric	15
Lantronix	3	Invensys Wonderware	15
Progea	3	Schneider Electric	18
ABB	3	Advantech/Broadwin	22
Sielco Sistemi	3	Siemens	42
Iconics	5	Emerson	6
Measuresoft	6	Rockwell Automation	9
Ecava	5		
Emerson	6		

2013+

“viento plateado del oeste”

- Captura de comunicaciones en tránsito en EEUU
- Acceso a la red vía socio (proveedor de comunicaciones)
- Específico para Sur y Centro América
- Captura: Metadata, Voz y Fax (DNR)
- Captura: Metadata Y contenido (DNI)

“habilitando inteligencia de señales”

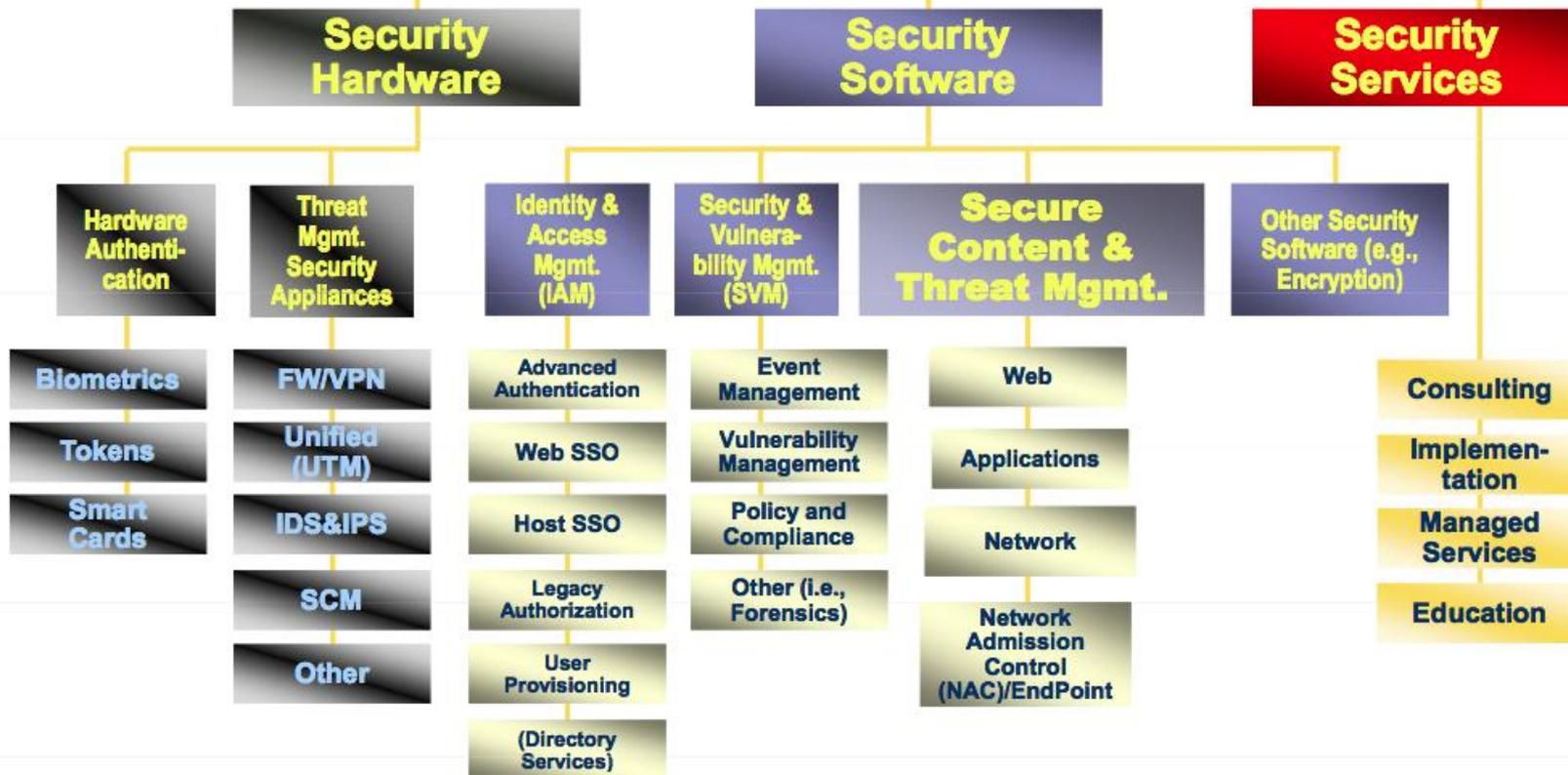
- Busca influir subrepticamente o modificar activamente el diseño de productos de la industria TIC de EEUU y extranjera para hacerlos susceptibles a actividades de obtención de inteligencia
- Presupuesto 2013: \$255mm USD, 141 empleados (personal contratado)
- Insertar vulnerabilidades en sistemas comerciales de cifrado, dispositivos de red, sistemas IT, dispositivos de usuario.
- Influir sobre políticas y estándares técnicos de criptografía
- Subvertir chips de dispositivo comerciales para cifrado de VPN y Web (SSL)
- Captura de comunicaciones VoIP P2P
- Captura y decifrado de comunicaciones 4G/LTE

Seguridad de la Información

El mercado y la industria

Mercado global de seguridad de las TIC

Security Products & Services



Mercado global de software y servicios de seguridad TIC

- Mercado global > 60.000MM USD* (anual)
 - 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)
- Crecimiento estimado al 2016: 86.000 MM USD* (CAGR 9,4%)
- >1.000 Empresas de Seguridad TIC \$10MM/año (< 1% .AR)

Seguridad de la Información

Herramientas técnico-legales

Algunas consideraciones necesarias

- Espionaje informático (*ciberespionaje*)

- 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 países signatarios de la región

 - Potencial efecto negativo sobre actividades de I+D (Artículo 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>

Guerra cibernética: Cuestiones no resueltas

- Qué es? Hace falta una definición precisa?
La teoría del efecto cinético
La teoría de la velocidad de la luz
El 5to dominio
Cuestiones Operativas, Tácticas y Estratégicas
- Disuación
- No proliferación
- Atribución
- Reglas del juego
Jus ad Belum
Jus in Bello

Seguridad de la Información 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)

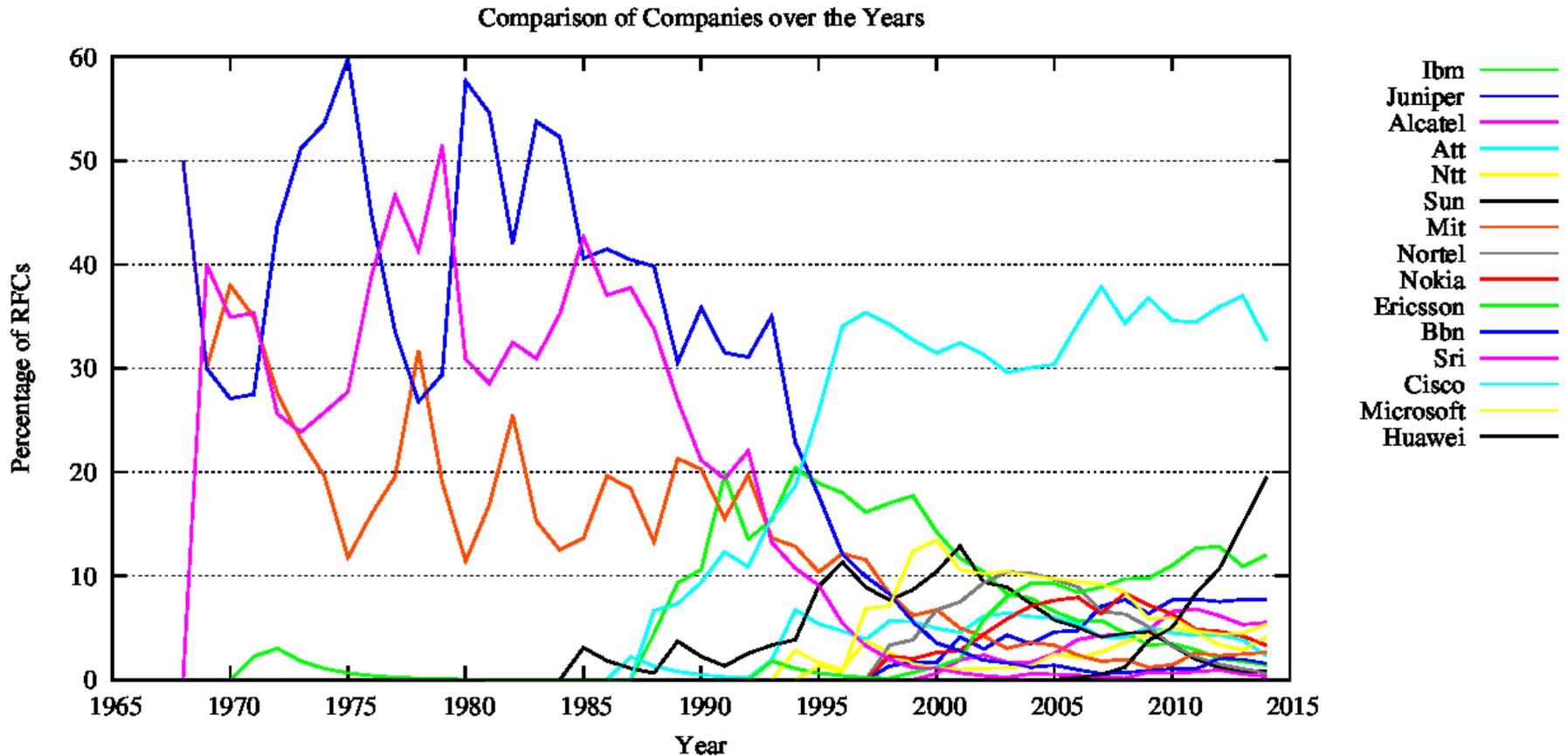
En los últimos 15 años todos ellos “evolucionaron” hacia la centralización del comando y control de su funcionamiento

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

- 3 autoridades certificadoras (bajo jurisdicción de EEUU) firman más 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>

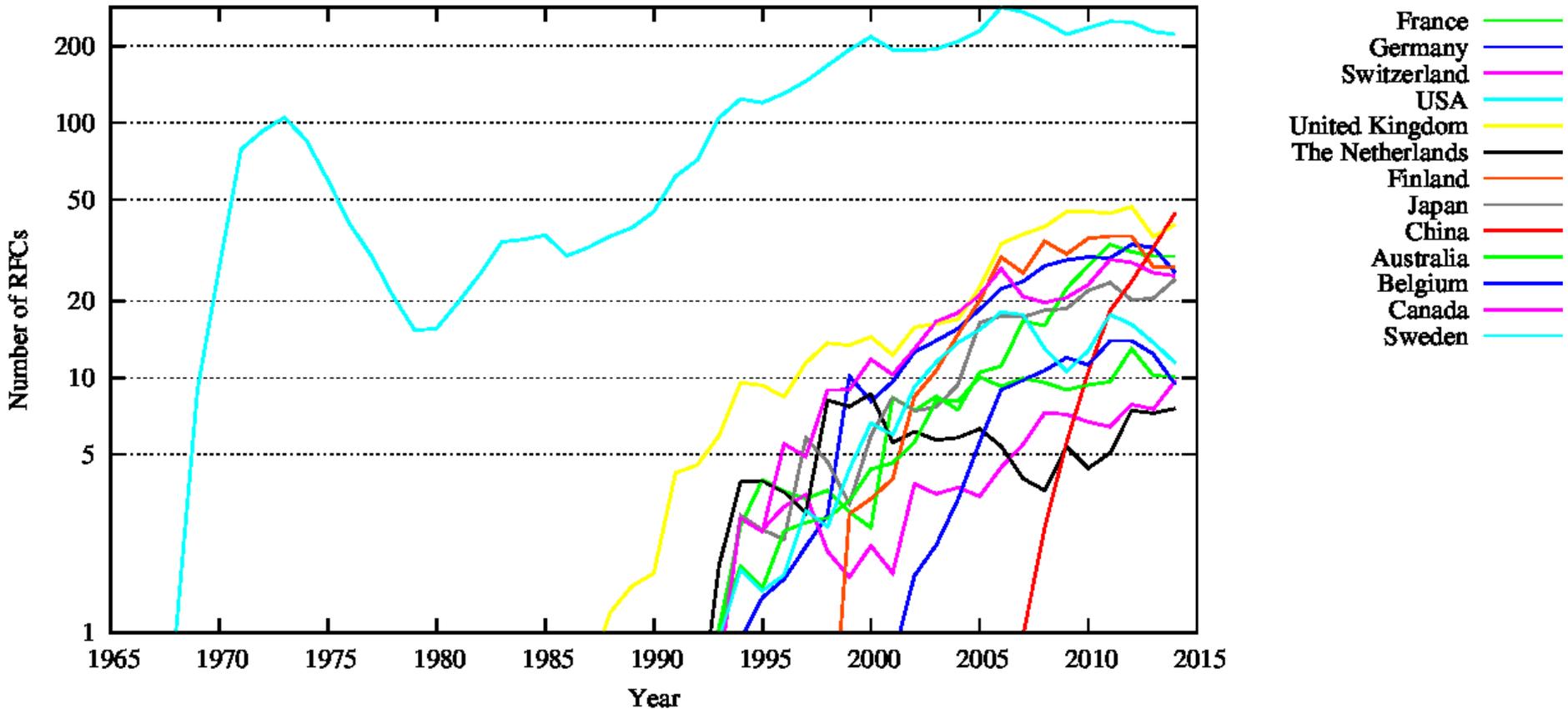
Quienes definen los estándares técnicos ?



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

De dónde son los autores de los estándares técnicos?

Comparison of Countries over the Years



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>

Conclusiones

Claves para una estrategia regional

- 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 las TIC es transversal, el software es omnipresente
- Investigación, Desarrollo e Innovación
Claves 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

Email: stic@fundacionsadosky.org.ar

GRACIAS!