Voto Electrónico y Seguridad en TIC

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

Presentación para DialogandoBA, 11 de julio de 2016, Ciudad Autónoma de Buenos Aires

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

fundación SADOSKY
Investigación y Desarrollo en TIC

cessi ArgenTIna

CICOMRA

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).

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.

10s patentes internacionales otorgadas, 100s publicaciones técnicas, 100s vulnerabilidades.

http://www.coresecurity.com

2015-2003 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

2015 – Center for Secure Design – IEEE Computer Society- Miembro fundador

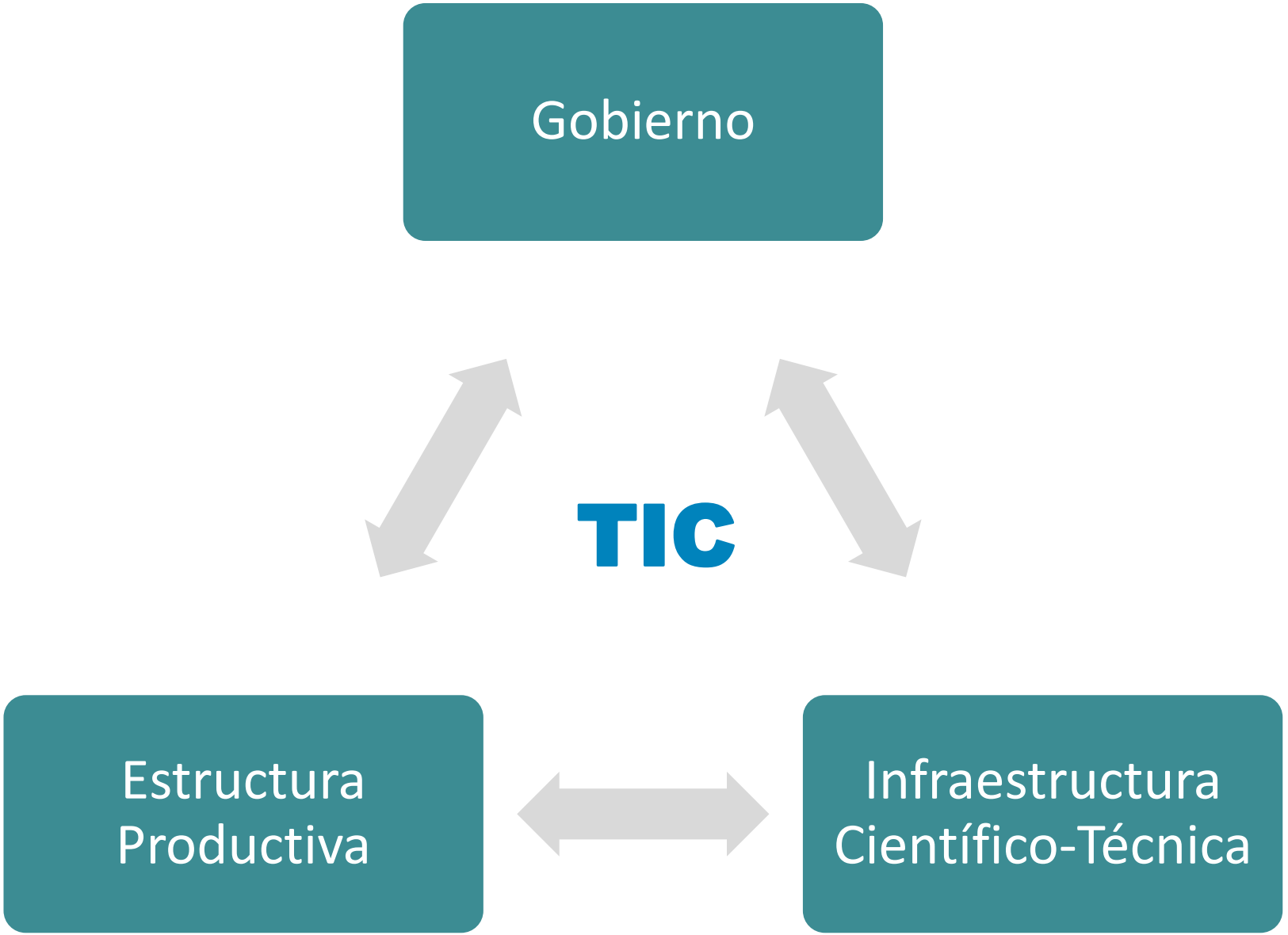
Centro dedicado al estudio del diseño de software seguro.

http://cybersecurity.ieee.org/centr-for-secure-design

Qué es la Fundación Dr. Manuel Sadosky?

- **La Fundación Dr. Manuel Sadosky es una institución público-privada cuyo objetivo es favorecer y promover la articulación entre el sistema científico - tecnológico y la estructura productiva en todo lo referido a las Tecnologías de la Información y Comunicación (TIC)**
- **Fue formalmente creada por Decreto del Poder Ejecutivo Nacional en Junio de 2009, y comenzó a funcionar en 2011**
- **Lleva el nombre quien fuera un pionero y visionario de la Informática en el País y la región**

Manuel Sadosky
(1914-2005)


Gobierno
TIC
Estructura Productiva
Infraestructura Científico-Técnica

El Programa de Seguridad en TIC

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 las TIC aplicada al Voto Electrónico

Sobre el uso de TIC en el voto electrónico

- Los requerimientos de seguridad son **únicos**

  Se debe:

  1- **Capturar la intención** de voto de manera fidedigna

  2-.**Registrar** el voto de acuerdo a la intención capturada

  3- **Contar** el voto de acuerdo a lo registrado

  Con un sistema que**:**

  - **Garantice** la integridad de los datos en todo el proceso
  - **Garantice** la confidencialidad de los datos en todo el proceso
  - Sea **verificable** por el votante
  - No sea **verificable** por terceros (secreto)
  - Sea **auditable** por cualquiera
  - Este disponible siempre que se lo necesite.
  - Sea **confiable**
  - **Opere en presencia de adversarios** sofisticados
  - Sea **escalable** y **usable** por millones de “usuarios”

NO ES POSIBLE CONSTRUIR UN SISTEMA QUE GARANTICE EL CUMPLIMIENTO DE LA PROPIEDADES DESEADAS

Reiteramos…

NO ES POSIBLE CONSTRUIR UN SISTEMA QUE GARANTICE EL CUMPLIMIENTO DE LA PROPIEDADES DESEADAS

En el mundo de las Ciencias de la Computación, “garantice” implica la **demostración matemática (verificación formal)** de uno o más teoremas acerca de las propiedades del sistema.

.

y entonces…qué podemos hacer?

Arreglarse con implementaciones imperfectas que no pueden garantizar las propiedades requeridas.

La seguridad de las TIC se ocupa precisamente de eso.

Gestionar riesgos usando las herramientas de análisis y las técnicas del método científíco

La seguridad de un sistema es una **propiedad emergente**. (no un *feature*)

La Seguridad TIC no es como la meteorología

"Operar en presencia de un adversario (sofisticado)"

Adversario : Actor inteligente pero no necesariamente racional.
…además de los fenómenos naturales.

Es además un actor económico (relación costo/beneficio)

Es necesario caracterizar al adversario

1. OPORTUNISTA
2. GRUPO ACTIVISTA
3. JAQUER (HACKER)
4. COLABORADOR CONTRARIADO
5. PROFESIONAL SEGURIDAD TIC
6. ORGANIZACION DELICTIVA
7. AGENCIA PRIVADA DE INTELIGENCIA
8. CORPORACION PRIVADA
9. ORGANIZACION DELICTIVA TRASNACIONAL
10. AGENCIA NACIONAL DE INTELIGENCIA

Capacidades técnicas, recursos económicos, motivación, incentivos

Implicancias prácticas

Cualquier modelo de amenazas DEBE incluir al proveedor del sistema

Un sistema de voto electrónico es una combinación de hardware, software, prácticas y procedimientos de desarrollo tecnológico.

La seguridad debe ser contemplada y atendida durante todo el ciclo de desarrollo. No es simplemente una característica del producto final.

Una auditoría no es una certificación

Una certificación no es una garantía

Existe un conjunto de “buenas prácticas” para el desarrollo de soluciones tecnológicas con niveles de seguridad “aceptables”

Ello implica:

- Definir un criterio de aceptación
- Foco en los resultados Y en los procesos con los que se obtienen

Algunas buenas prácticas

- Capacitación
- Modelado de amenazas
  El proveedor del sistema y su cadena de abastecimiento
- Revisión de seguridad del diseño
- Análisis de seguridad de la arquitectura
- Elaboración de casos de abuso
- Auditorías de código
- Testing de seguridad
- Penetration testing
- Gestión de configuración y vulnerabilidades
- Gestión de incidentes de seguridad.

p.e. el modelo BSIMM identifica 113 actividades usadas en el mundo real por organizaciones con iniciativas de seguridad

Principios básicos a tener en cuenta

- Principio de Kerckhoffs (1883)
- Saltzer & Schroeder (1974)
  - **KISS - Economía del mecanismo**
  - Principio de menor sorpresa
  - Fallar de manera segura
  - Intermediación total
  - Menor privilegio
  - **Mecanismo mínimo de uso en común** (aislamiento)

- Anderson (1972), Karger & Schell (1974)
  - Ataque y Defensa se complementan, ambos necesarios
- Thompson (1984)
  - Seguridad en toda la cadena de abastecimiento

Una última reflexión sobre la potencialidad de fraude

No es posible demostrar inexistencia de "**canales laterales**" (side channels)
Es posible implementar "**canales encubiertos**" (covert channels)
Como consecuencia de ello es posible:

- Coerción
- Compra de votos

Determinar el número necesario de actores en colusión.

La auditoría de resultados post-elección es necesaria pero no suficiente.

- Diseñada en función de los resultados
- Diseñada para detectar "micro-fraude"
- No detecta todos los problemas posibles (ver arriba)

Gracias!