cloud security alliance

# Seminario Regional de Ciberdefensa

## Ecosistemas de Cómputo en la Nube

Lic. Héctor Jara
Ing. Gustavo Presman

Mayo, 2014

# Agenda

- ***Acerca de los expositores***
- ***Acerca CSA***
- ***¿Qué es el cómputo en la nube?***
- ***Nube Gubernamental***
- ***Desafíos***
- ***Recomendaciones***
- ***Cloud Computing Forensics***
- ***Canales de contacto y Preguntas***

cloud CSA security alliance Argentina Chapter

# Acerca de los expositores: Héctor Jara

- ***Lic. En Tecnologías de las Comunicaciones (UADE)***
- ***Especialista en Educación y Nuevas Tecnologías (FLACSO)***
- ***Posgrado en Desarrollo Gerencial (UP)***
- ***ISO 27001 Leader Auditor, CEH y QCS***
- ***Consultor en Seguridad de la Información***
- ***Docente titular en la Universidad Nacional de Quilmes***
  - ✓ *Investigaciones sobre eHealth, Privacidad y Educación y nuevas tecnologías*
- ***Colaborador frecuente en IT Now***
- ***Coautor de los libros Ethical Hacking, Hacking al Descubierto y Ethical Hacking 2.0***

cloud security alliance CSA Argentina Chapter

# Acerca de los expositores: Gustavo Presman

- *Ingeniero Electrónico por la Universidad de Buenos Aires*
- *Master en TIC por el Programa Gadex en España*
- *Certificaciones: ENCE, CCE, FCA, NPFAT*
- *Miembro del board del Capítulo Argentino de CSA (Cloud Security Alliance)*
- *Director de Membresías de ISSA Argentina*
- *Profesor del Master de Seguridad Informática de la Universidad de Buenos Aires*
- *Entrenador autorizado para los cursos oficiales EnCase Forensic*
- *Perito inscripto en Corte Suprema del PJ de la Nación y de la Provincia de BsAs*
- *Consultor de Fuerzas de la Ley y Gobiernos en Latinoamérica*
- *Director del ESTUDIO DE INFORMATICA FORENSE*
- *Frecuente expositor en eventos de Informática Forense*

# Acerca de CSA

*¿Qué es la Cloud Security Alliance (CSA)?*

***"Promover las mejores prácticas a fin de ofrecer confianza dentro del ámbito del Cómputo en la Nube, educando a la comunidad sobre sus usos y colaborando en asegurar todas las otras formas de computo."***

cloud CSA security alliance Argentina Chapter

**Corporate Members**


**Founding Members**

Phil Agcaoili, Dell
Jerry Archer, Intuit
Todd Barbee, New Dominion Bank
Jeff Bardin, Treadstone 71
Girish Bhat, SAVVIS
Alan Boehme, ING
Larry Brock, DuPont
Glenn Brunette, Sun
Jake Brunetto, Intuit
Jon Callas, PGP
Sean Catlett, Barclays
Shawn Chaput, Privity
Jay Chaudhry, Zscaler
Anton Chuvakin, Qualys
Philippe Courtot, Qualys
Dave Cullinane, eBay
Joshua Davis, Qualcomm
Dr Ken Fauth
Robert Fly, Salesforce.com
Jeff Forristal, Zscaler
Pam Fusco, UAT
Francoise Gilbert, IT Law Group
Edward Haletky, AstroArch Consulting
Jim Hietala, The Open Group
Christofer Hoff, Rational Survivability
Dennis Hurst, HP
Michael Johnson, Security GRC2
Shail Khiyara, Cloud Consulting
Subra Kumaraswamy, Sun
Paul Kurtz, Good Harbor Consulting
Mark Leary, Northrop Grumman
Liam Lynch, eBay
Tim Mather, RSA Security
Scott Matsumoto, Cigital
Dave Morrow, Secure Business Operations
Izak Mutlu, Salesforce.com
Brian O'Higgins, Third Brigade
Jean Pawluk, Visa
Josh Pennell, IOActive
Nils Puhlmann, Qualys
Jim Reavis, Cloud Security Alliance
George Reese, enStratus
Jeff Reich, FUDless
Jeffrey Ritter, Waters Edge Consulting
Ben Rothke, BT
Stephen Sengam, Fox/Newscorp
Ward Spangenberg, IOActive
Jeff Spivey, RiskIQ
Michael Sutton, Zscaler
Lynne Terwoerds, Barclays
Dave Tyson, eBay
John Viega, McAfee
Dov Yoran, MetroSITE Group
Josh Zachry, Rackspace

**Founding Charter Companies**


**Founding Affiliate Members**


**Affiliate Members**

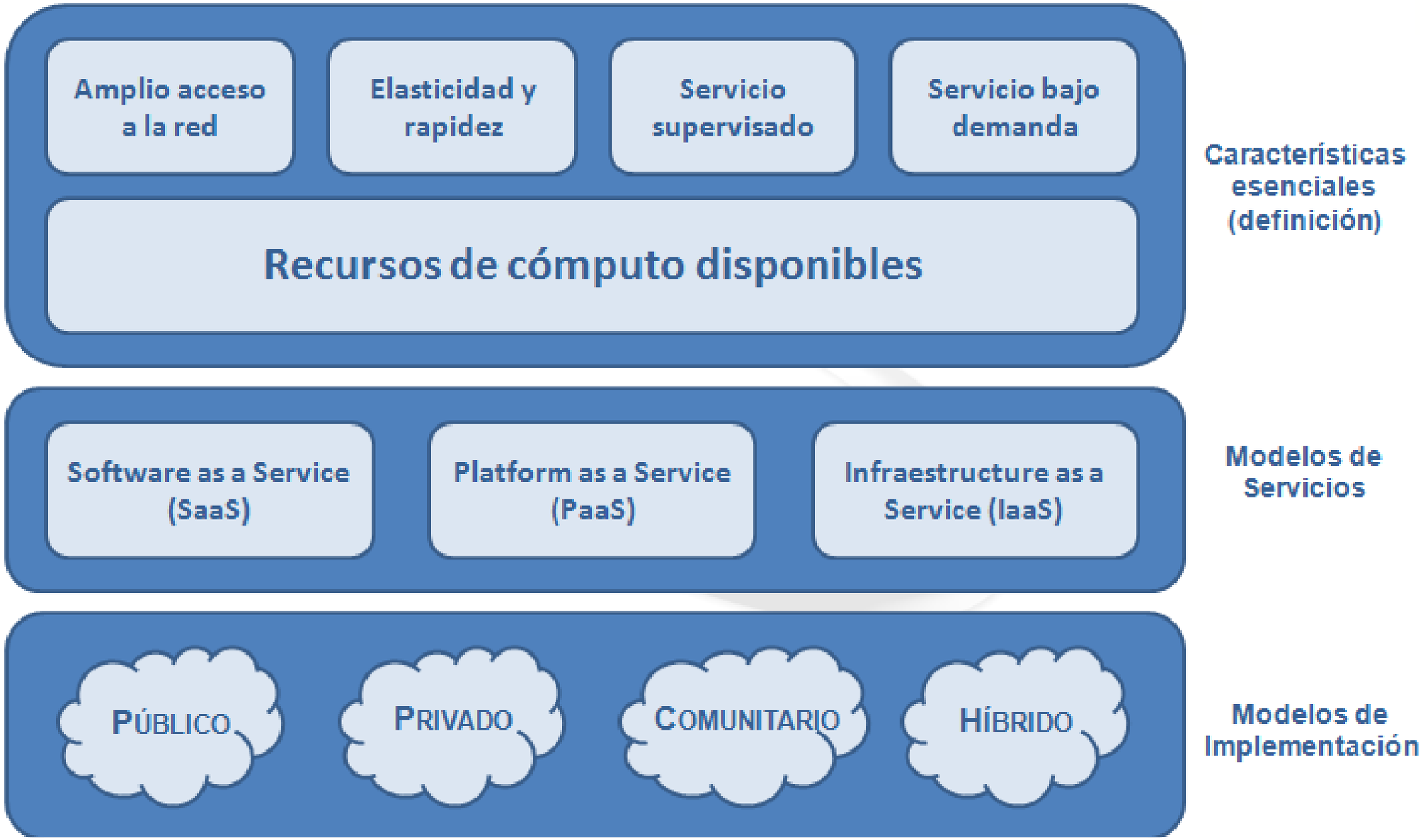

cloud security alliance

CSA

https://cloudsecurityalliance.org/membership/corporate-members/

# ¿Qué es el Cloud Computing?

# ¿Qué es el Cloud Computing? (Cont.)




**Modelo de Cómputo en la Nube (Cloud Computing) definido por el NIST SP800-145 [1]**

http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

cloud security alliance

# NUBE GUBERNAMENTAL

# Nube Gubernamental

- **Nube Privada adaptada a las necesidades del ámbito público (*eGovernment*).**

✓ **Al menos en un principio, no enviar datos sensibles [2]**

✓ **Existen requerimientos específicos para el sector público [3]**

- **Permite simplificar la interacción del ciudadano:**

✓ **Reduciendo el tiempo de procesamiento de la información.**

✓ **Disminuyendo los costos de los servicios gubernamentales.**

✓ **Mejorando la seguridad de sus datos.**

# Nube Gubernamental (Cont.)

TECNOLOGÍA

## Colombia está en el primer puesto de Goverment en Latinoamérica

Según Everis, r
consultora espe
negocio, desarr
mantenimiento
tecnológicas, C
el primer lugar a
Latinoamérica e
implementación
en pro del servi
conocimiento d
ciudadanos.

CARACOL | JUNIO 8 D

Forbes

**New Posts**
+16 posts this hour

**Most Popular**
Amazon's Wholesale Slaughter

LEADERSHIP | 3/20/2012 @ 5:35PM | 991 views

## Australia, Italy and Denmark Lead Government Cloud Adoption

1 comments, 1 called-out + Comment Now + Follow Comments

How are governments around the world planning for and adopting cloud computing, and how much progress have they made?

## Los gobiernos en el mundo se suman al cloud computing

Lun, 07/22/2013 - 15:31

Según el estudio **"Ahorro de dinero a través del cloud computing"** realizado por el centro de investigación **Brookings Institution en Estados Unidos**, gracias a cloud computing **los gobiernos pueden generar ahorros que bordean porcentajes entre el 25 y 50% del gasto en TI.**

# Nube Gubernamental (Cont.)

**CPD Ministerio de Defensa**

**CPD Ministerio de Salud**

**Un CPD por cada organismo**

- Recursos desaprovechados.
- Equipos de IT heterogéneos.
- Medidas de seguridad descentralizadas.
- Mayor costo y complejidad

**CPD Ministerio de Educación**

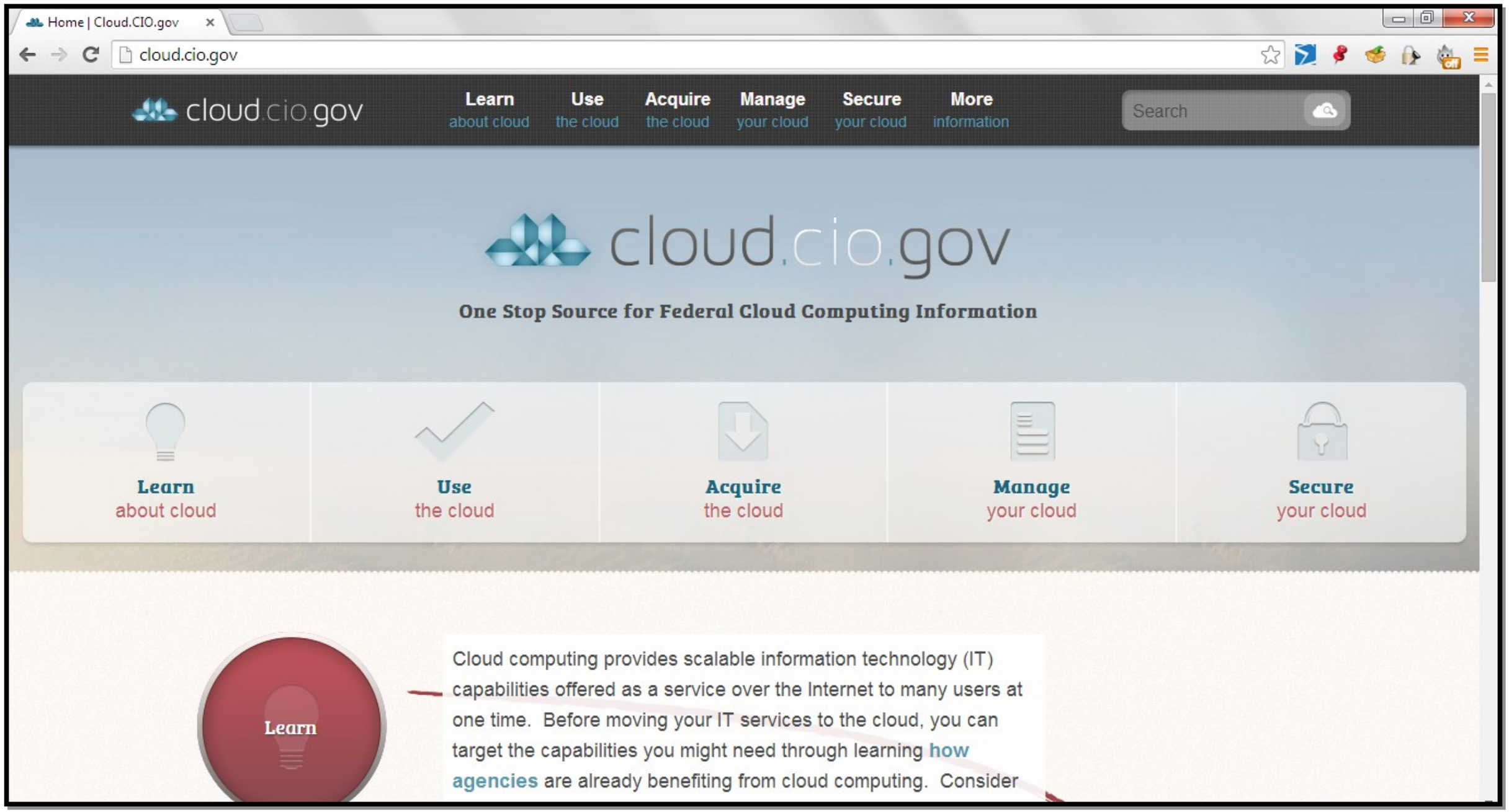
**CPD Ministerio de Economía**

cloud CSA security alliance Argentina Chapter

# Nube Gubernamental (Cont.)

**Nube Gubernamental** [4][5][6]

# Nube Gubernamental (Cont.)



# Nube Gubernamental (Cont.)

cloud.cio.gov

Learn about cloud | Use the cloud | Acquire the cloud | Manage your cloud | Secure your cloud | More information

» Benefits of Cloud Computing » DoD US Army Online Experience Center

## DoD US Army Online Experience Center

**Challenge:** The U.S. Army Experience Center needed a flexible, extendable and customizable recruitment tracking platform to track prospective recruits.

**Solution:** Move to a cloud environment that permits a 360 degree community outreach and relationship management approach.

**Results:**

- Costs down to 8M for full licensing from $83M
- 33% productivity gain
- 30 times higher response rates
- Twitter, Facebook integration
- Geolocation and contact data in the field via iPhone and Blackberry
- Visitor and user surveys for instant information

# Nube Gubernamental (Cont.)


**Ejemplo de Aplicación: eHealth**

cloud security alliance Argentina Chapter

# Desafíos

# Desafíos (Cont.)

- **Los principales desafíos son:**
  - ✓ Aspectos de *Privacidad* [7][8]
  - ✓ Aspectos de seguridad entre usuarios
  - ✓ Aspectos regulatorios y de cumplimiento
  - ✓ *Selección del modelo y los proveedores* [9]

- **Para el caso de Organismos de Defensa**
  - ✓ **Seguridad**

# Desafíos (Cont.)

TECH 3/16/2012 @ 11:33AM | 1.334 views

## The Data Protection And Security Case For Private Clouds


Eric Savitz , Forbes Staff

+ Comment Now + Follow Comments

Don't blame Microsoft. *Any* company that stores data in U.S. jurisdictions – or whose information simply passes through the United States – can be required to hand over that information to U.S. federal authorities, no matter the data's sensitivity. The USA Patriot Act has changed the game when it comes to storing and protecting information in the cloud.

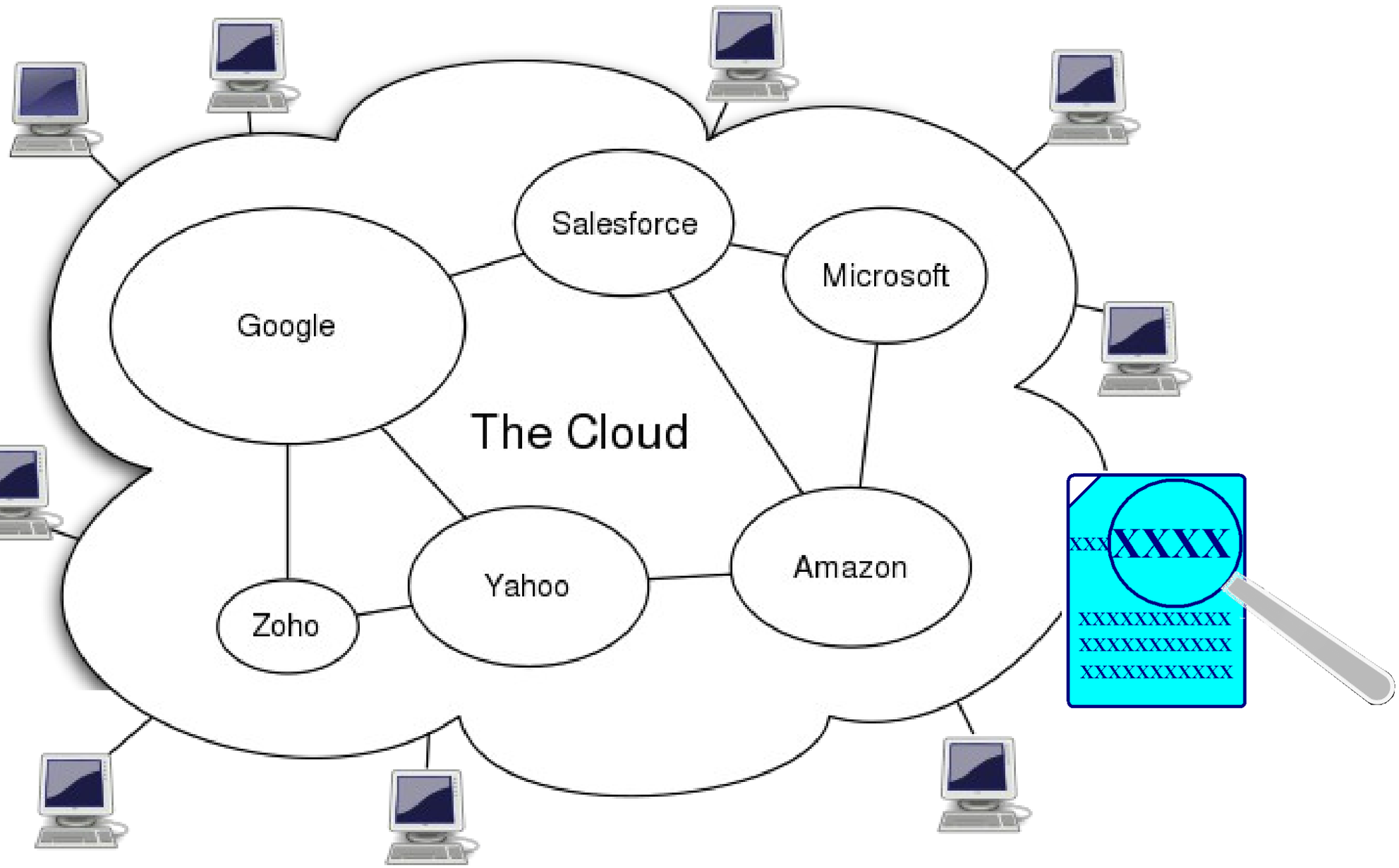
# Recomendaciones

- **Recomendaciones de implementación en el ámbito público [4]**
  - ✓ Desarrollar una estrategia local y regional.
  - ✓ Fomentar la definición de un marco regulatorio común.
  - ✓ Desarrollar un marco común de SLAs.
  - ✓ Apoyar investigaciones y estudios académicos.
  - ✓ Desarrollar disposiciones integrales para proteger la ***Privacidad*** de los ciudadanos (Leyes de Protección de Datos Personales) [7][8]
  - ✓ Utilizar estándares y mejores prácticas (CSA, ENISA, etc) [6][10][11]
  - ✓ **En etapas iniciales no llevar datos sensibles** [2]

cloud security alliance

# CLOUD COMPUTING FORENSICS

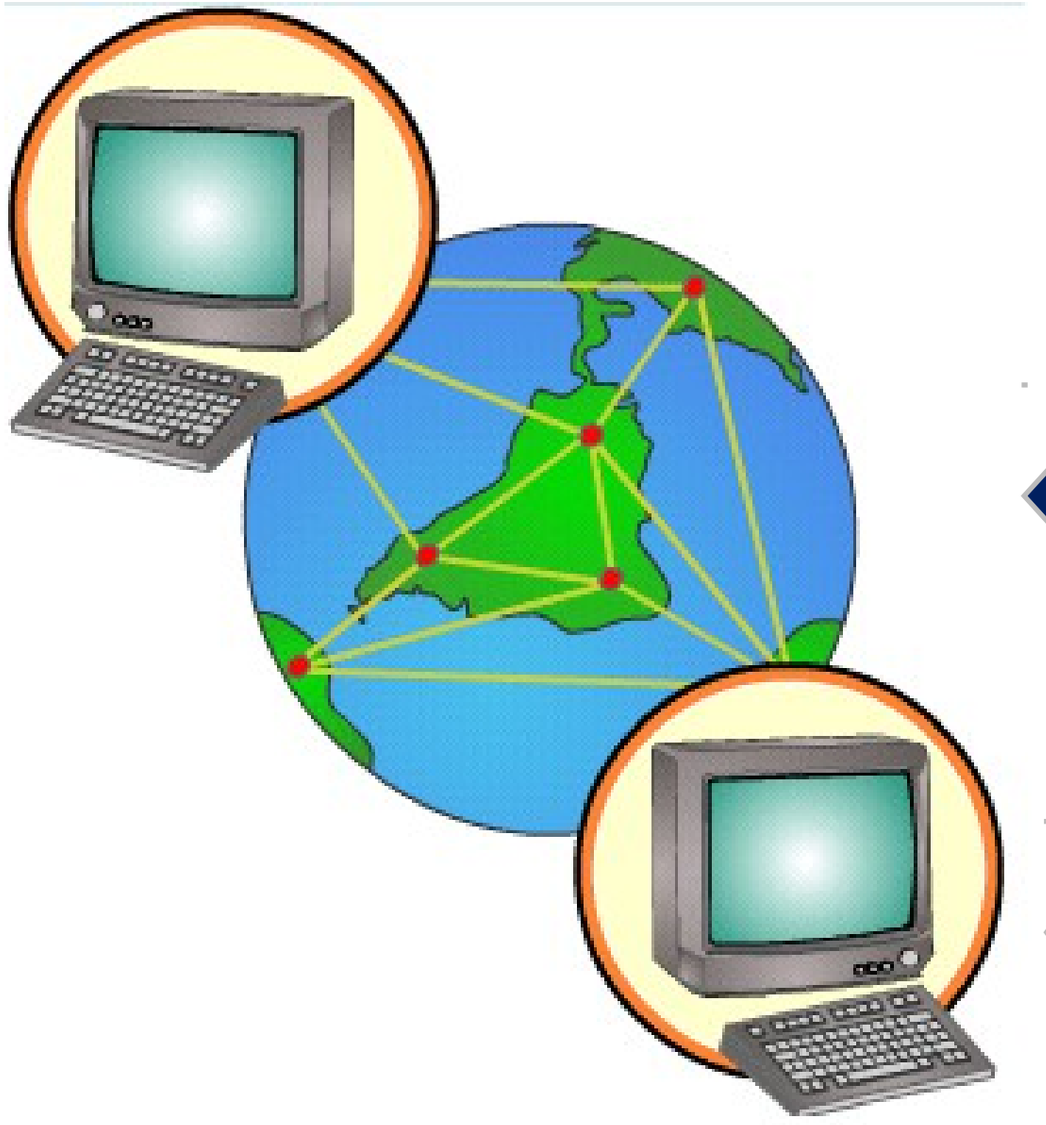
# Nuevos desafíos en la informática forense




cloud security alliance
CSA
Argentina Chapter

# Problemática actual: Ubicuidad de la prueba

**ACCION**



**MEDIO**

**RESULTADO**

**¿Dónde recolecto la prueba?**





cloud security alliance CSA Argentina Chapter

# Incidentes y delitos informáticos en la Nube

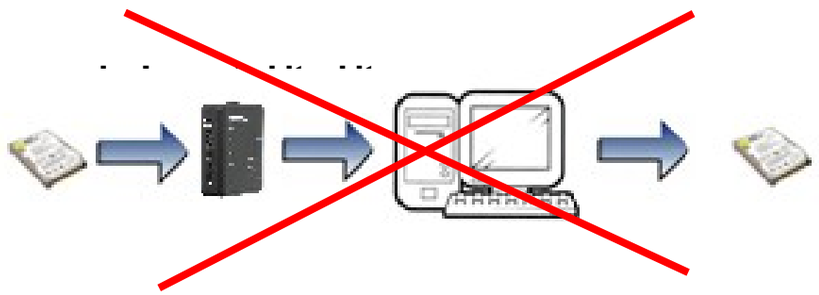
**<u>La nube como</u>:**

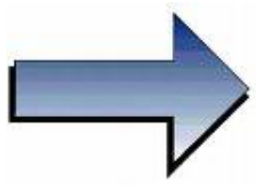
- **Sujeto del delito: Robo de identidad en el acceso a la nube.**
- **Objeto del delito: Acceso no autorizado o daño Informático a la nube, DDOS.**
- **Herramienta delictiva: almacenamiento estático o distribución de material ilegal (PI).**

# Análisis forense informático tradicional

**Adquisición y preservación (estática)**

- **Recolección efectiva**
- **Preservación**





5b748e186f622c1bdd6ea9843d1609c1

## HASHES USUALES

- ✓MD5 (128 bits)
- ✓SHA-1(160 bits)
- ✓SHA-256 (256 bits)

cloud security alliance Argentina Chapter

# Análisis forense informático tradicional

**Adquisición y preservación (dinámica)**

- **Memoria RAM**

- **Celulares**

- **Network Forensics**

**Autenticación por hashes no reproducible (foto)**

# Análisis forense informático en la Nube

**Características**

- ✓ **Tercerización CSPn**
- ✓ **Múltiples Tenedores de servicios dependientes**
- ✓ **Múltiples Jurisdicciones**
- ✓ **Seguridad/Resguardo---SLA**
- ✓ **Recolección de Evidencia en la nu**
  - Formatos de datos diferentes
  - Zonas de Tiempo diferentes


cloud security alliance CSA Argentina Chapter

# Desafíos de prueba en la Nube

- ✓ **No disponemos de los datos**
- ✓ **No tenemos acceso a la infraestructura física**
- ✓ **Son sistemas distribuídos y virtuales**
- ✓ **Tienen espacio de almacenamiento distribuído en ubicaciones cambiantes**
- ✓ **Pueden compartir espacio físico entre usuarios**
- ✓ **Frecuentemente transnacionales**
- ✓ **Con poca o nula colaboración del CSP**

cloud security alliance CSA Argentina Chapter

# Obtención de evidencia digital en la Nube

*La misma puede ser recolectada voluntariamente por la parte* u ordenada por las autoridades legales*

**** Siempre que tenga validez legal y técnica***

## RECOLECCION DE EVIDENCIA EN LA NUBE

- ✓**Por vía indirecta**: A través de artefactos locales en almacenamiento masivo o memoria RAM y en Tráfico de red.

- ✓**Por vía directa**: Con acceso de "*bajo nivel*" a la nube.

# Referencias


**[1] NIST SP800-145: The NIST Definition of Cloud Computing. Disponible en: http://goo.gl/EAO7so**

**[2] Governmental Cloud in the EU - New Agency Report [EN]. Disponible en: http://goo.gl/yc9pK5**

**[3] Government Clouds: Specific public sector requirem. (Danish National IT Agency) [EN]. Disponible en: http://goo.gl/z3ty7r**

**[4] Exploring the Cloud: A global study of Governments Adoption of Cloud [EN]. Disponible en: http://goo.gl/Me0l1l**

**[5] Benefits of Cloud Computing [EN]. Disponible en: http://cloud.cio.gov/topics/benefits-cloud-computing**

**[6] Good Practices Guide for Secure deploying Governmental Clouds [EN]. Disponible en: http://goo.gl/CFqVfZ**

# Referencias (Cont.)


**[7] NIST SP800-144: Guidelines on Security and Privacy in Public Cloud Computing [EN]. Disponible en: http://goo.gl/kxt8VP**

**[8] CSA Modelo Acuerdo de Nivel de Privacidad (PLA) para la contratación de servicios en la Nube [ES]. Disponible en: http://goo.gl/fqOq6z**

**[9] CSA Cloud Control Matrix [ES]. Disponible en: http://goo.gl/IDsXF3**

**[10] NIST SP800-146: Cloud Computing Synopsis and Recommendations [EN]. Disponible en: http://goo.gl/CDJ0hz**

**[11] ENISA Cloud Computing Risk Assessment [ES]. Disponible en: http://goo.gl/ThpmVd**

# Preguntas y Canales de Contacto

- **¡Ayúdenos a trabajar por la Seguridad en la Nube!**

- **CSA Argentina**

  - www: https://chapters.cloudsecurityalliance.org/argentina/
  - mail: contact@ar.chapters.cloudsecurityalliance.org
  - LinkedIn: http://www.linkedin.com/groups?home=&gid=3350613
  - twitter: @cloudsa_arg
  - facebook: CSA.Argentina (página)

cloud security alliance Argentina Chapter

# ¡Muchas Gracias!

cloud security alliance

www.cloudsecurityalliance.org