CERT´s Académicos y su Aportación a la Sociedad

Juan Carlos Guel Lopez
UNAM-CERT

Temas

* Introducción

* Que es un CERT?

* Los IRT y su aporte

* IRT´s en México

* Conclusiones

I n t r o d u c t i o n

* En la actualidad, cualquier computadora conectada a Internet es potencialmente blanco de un ataque.

* Existen varios factores que pueden afectar los ambientes de cómputo de las organizaciones y usuarios.

* Uno de estos factores: **La gestión del riesgo,** que se ha convertido en un problema para las organizaciones

* Especialmente complicado gestionar el riesgo en aquellas empresas cuyos procesos críticos reposan en tecnologías de la información, un ejemplo claro lo es la Banca en Línea.

UNAM CERT

Introducción

* Es necesario llegar a un equilibrio en la organización entre inversión y riesgo asumido voluntariamente, y éste es el objetivo principal de la gestión de los riesgos.

* En una organización dependiendo de su rango de constitución es imperante conocer cuales son los riesgos asociados a sus tecnologías de información, datos, etc.

* En la presente plática analizaremos como un CERT Académico puede aportar a la sociedad y ayudar a solucionar problemas de seguridad informática.

UNAM CERT

Que es un CERT?

Por definición :

“CERT (Computer Emergency Response Team), es una organización dedicada a asegurarse de la aplicación de buenas prácticas a nivel gerencial de la tecnología y que los sistemas empleados en la organización sean utilizados de manera apropiada para mitigar y reducir riesgos de ataques contra sistemas de red y así asegurar la continuidad de los servicios críticos”.

Que es un CERT?

* Servicios Reactivos

* Servicios Proactivos

* Servicios de Calidad en el manejo de Seguridad en TI

Funciones de un CERT

Funciones Reactivas

* Alertas y Boletines de Seguridad
* Manejo de Incidentes
* Análisis de Vulnerabilidades
* Análisis e Investigación de Artifactos

Funciones de un CERT (2)

Funciones Proactivas

* Anuncios
* Análisis de TI
* Auditorías y análisis de Seguridad
* Configuración y manejo de Herramientas de seguridad, aplicaciones e infraestructura.
* Desarrollo de Herramientas de Seguridad
* Servicios de Detección de Intrusos
* Análisis de información y casos relacionados a la Seguridad en cómputo.

UNAM CERT

Funciones de un CERT (3)

Funciones de Manejo de Calidad de la Seguridad en TI

* Análisis de Riesgos
* Plan de Continuidad y de Recuperación ante desastres
* Consultoría de Seguridad
* Impulso por una Cultura de Prevención
* Educación, entrenamiento
* Evaluación de Productos o certificación.

Que no es un CERT?

* Policía

* Procurador de Justicia

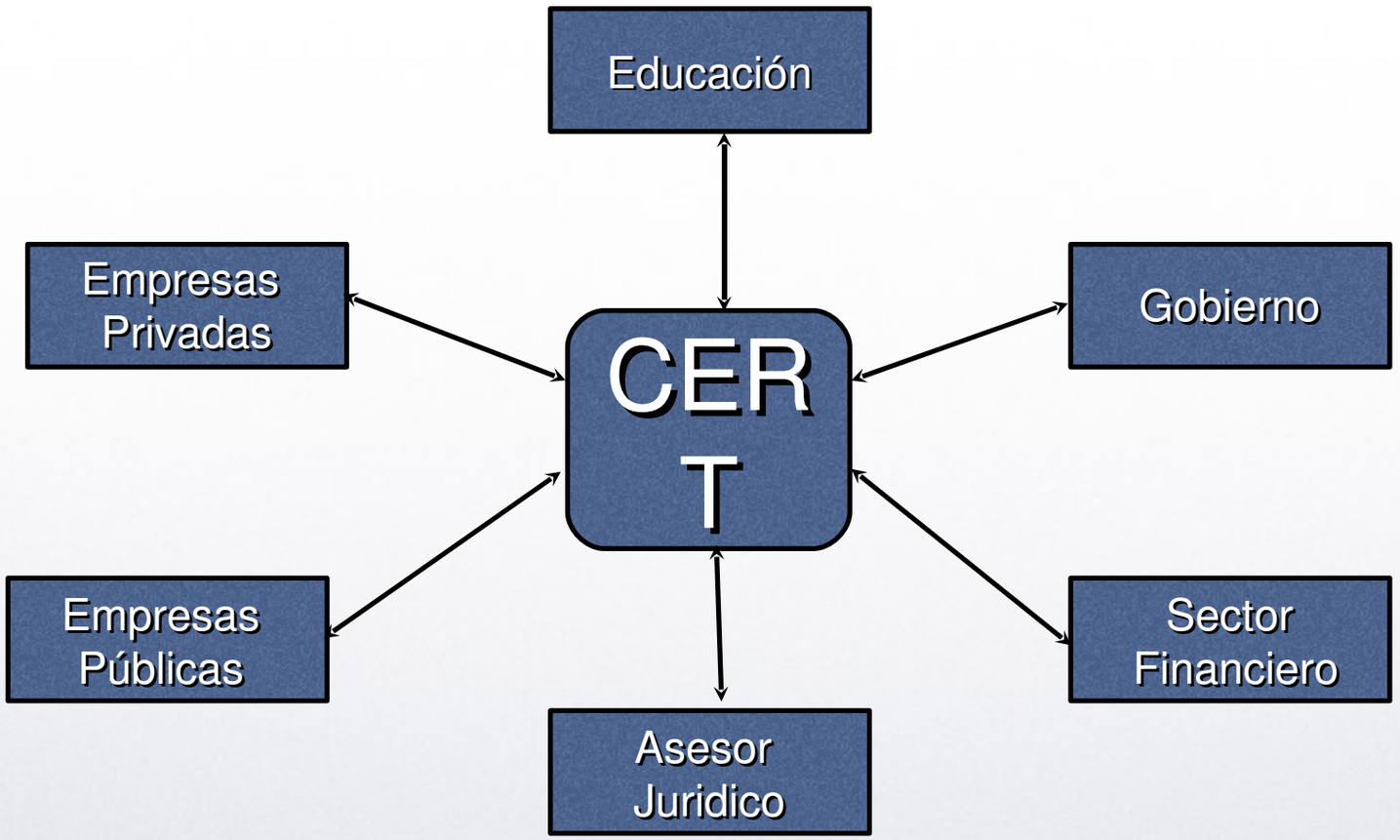
* Abogados

* Solucionador de Conflictos Internos en una empresa o corporación.

* Tareas en línea

Que Puede Hacer un CERT?

Un CERT puede relacionarse con múltiples instancias de un país:



U N A M - C E R T

* En Mexico, UNAM-CERT es un CERT académico, el cual colabora con diversas iniciativas entre las que sobresalen:

1. Gobierno (Policía Cibernética, PFP)
2. Sector Privado (Empresas, Asociaciones)
3. Sector Publico (Srías de Gobierno, Presidencia de la Republica)
4. Sector Financiero (Bancos, AMB)
5. Sector Educativo (ANUIES, CUDI, RedCLARA)
6. Asesor Jurídico (Esfuerzos Legislativos)

CERTS Académicos

1. Sector Gobierno:

    * Análisis forense en casos Mayores
    * Capacitación a Ministerios Públicos
    * Capacitación a Policía Cibernética
    * Asesoría y estudio de Principales problemas (P. ej. Ataques a Presidencia de la República)
    * Reuniones Mensuales (ISP´s, empresas gobierno, empresas privadas, sector legislativo, Academia, bancos, etc.)
    * Establecimiento de puntos de contacto

UNAM CERT

CERTS Académicos

2. Sector Privado:

* Trabajo con asociaciones principales (AMIPCI, AMITI, etc)
* Impulso de Iniciativas (Navega seguro por Internet, Policia cibernética, Portal de usuario Casero, etc.)
* Apoyo en incidentes mayores
* Solución de problemas específicos de tecnología
* Respuesta a incidentes.
* Establecimiento de puntos de contacto

CERTS Académicos

3. Sector Público:

* Análisis forense en casos Mayores
* Capacitación a diversas Secretarias de gobierno
* Capacitación a órganos de inteligencia
* Asesoría y estudio de Principales problemas (P. ej. Ataques ala infraestructura, paginas WEB, fraudes, etc.)
* Solución de problemas de tecnología
* Respuesta a incidentes de seguridad
* Establecimiento de puntos de contacto

CERTS Académicos

4. Sector Financiero:

* Trabajo con Asociación Mexicana de Bancos
* Apoyo en incidentes mayores (Phishing Scam, DDoS)
* Solución de problemas específicos de tecnología (Teclados Virtuales, Doble Autenticación, etc).
* Respuesta a incidentes.
* Establecimiento de puntos de contacto

CERTS Acad micos

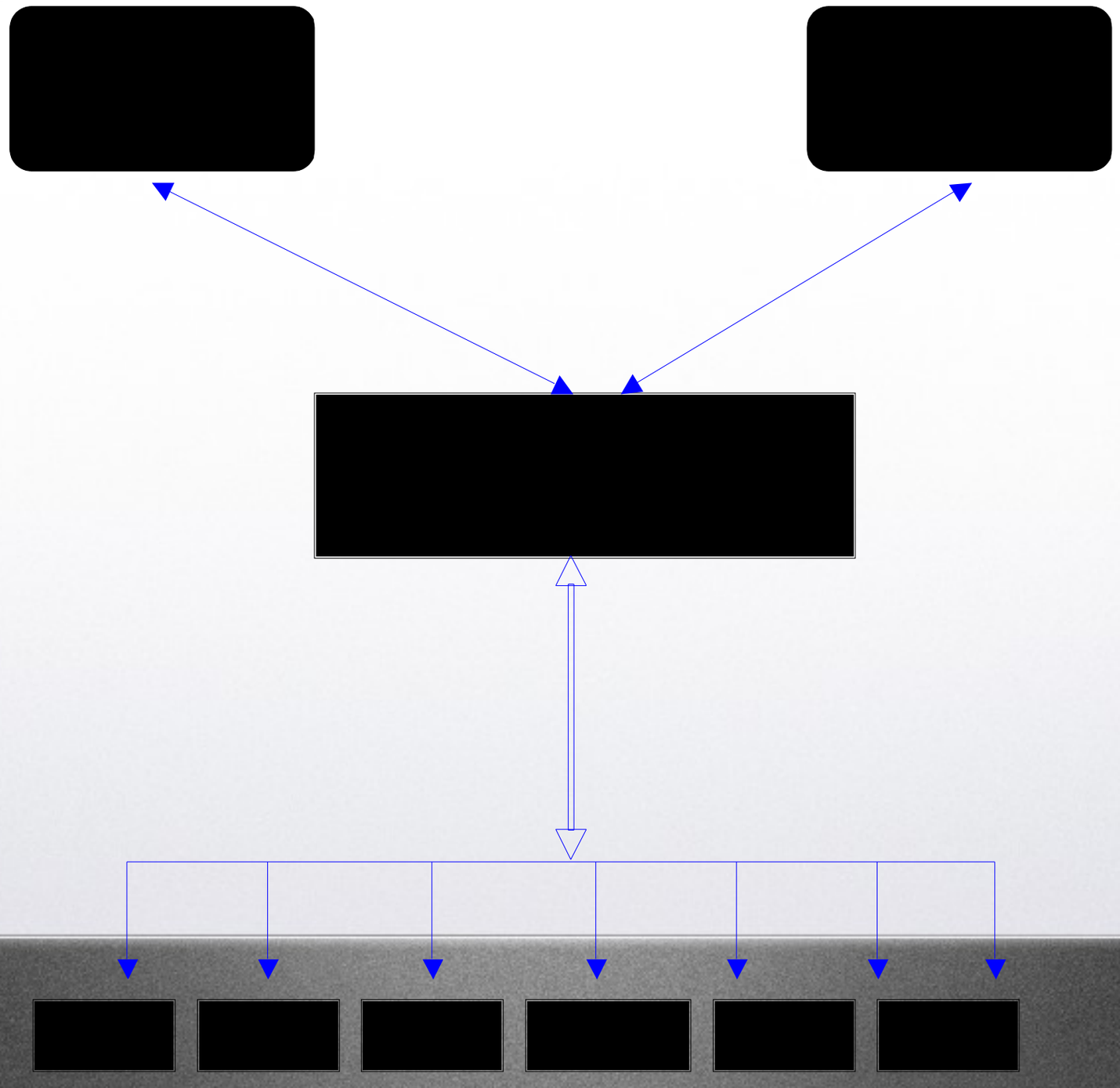
4. Sector Financiero:

```
00167440                               C:\Documents and
00167480   Settings\UNAM-CERT\Favoritos\Vi
001674C0  nculos  +    EWF_SYS_0=61118042-ff0a-11d0-98df-006097
00167500  b70359&EWF_SYS_1=8H8Z@6QQLM4NTEZQPKV5UEWXMCPE7NSX82ZNN5SQ&EWF_FC
00167540  RM_NAME=MAIN+NEW+LOGON&USERID=Un4mC3r7&PASSWORD=P455C3r7&tinicia
00167580  l=ZBIE&DATA7=ZMUS&DATA1=Un4mC3r7%7CP455C3r7%7C%7C&EWF_BUTTON_Sub
001675C0  mit=Submit&EXTRA1=SPANISH%7C0735%7C10%7C%2Fmenu_group.htm%7Cwww1
00167600  -11&EXTRA2=&EXTRA3=&EXTRA4=NO_ERRORög-▮^  +     ´:w      ðþ
00167640          C:\WINDOWS\Driver Cache
00167680  Vínculos  0▮  &       (à  ï [redacted]
001676C0          www[redacted].com.[redacted].net              80  pP  ¨Õ
00167700            ab     Security=Impersonati
00167740  on Static True `        \\?\GLOBALRO
00167780  OT\Device\HarddiskVolume10  ¶
001677C0   {  ÿÿÿÿ            öE river Ca         C
```

UNAM CERT

CERTS Académicos

4. Sector Financiero:



CERTS Académicos

5. Sector Educativo:

* Coordinación con Asociación Nacional de Universidades de Educación superior del país (140 IES, 100 Tecnológicos, 50 Univ. Politécnicas)
* Establecimiento de fideicomiso para Capacitación a 40 miembros de la red de Universidades.
* 2 programas de capacitación intensiva por 1 año.
* Impartición de cursos TRANSITS México
* Coordinación en Redes Académicas Latinoamericanas para Internet RedCLARA (GT-Seg)
* Impartición de Lineas de Especialización (Congreso de Seguridad)

CERTS Académicos

6. Sector Legislativo:

* Asesoría en el desarrollo de “Ley de Protección de Datos personales”

* Capacitación a órganos colegiados en TI del Sector Legislativo

* “Norma de uso de firma Digital en sector Económico”

* Asesoría en “Ley AntiSpam en México”

* Reuniones Periódicas con los legisladores del país para sensibilizar y dar a conocer la problemática real del estado del arte de la seguridad informática.

UNAM CERT

CERTS Académicos

Otras iniciativas - DISC 2005 (Computer Security Day) Nov. 25.

* Convocada por la ACM

* El Día Internacional de la Seguridad en Cómputo inició en 1988

* Su objetivo primordial es incrementar e impulsar la cultura de seguridad informática en las organizaciones.

* En DISC cada organización y cada individuo es responsable en proteger sus datos y recursos informáticos.

UNAM CERT

CERTS Académicos

DISC 2005 (Computer Security Day) Nov. 25.

* Cada persona dentro de la organización juega un papel importante en la seguridad en cómputo.

* Se invita a participar a toda América Latina y España a participar en este día.

Más información:

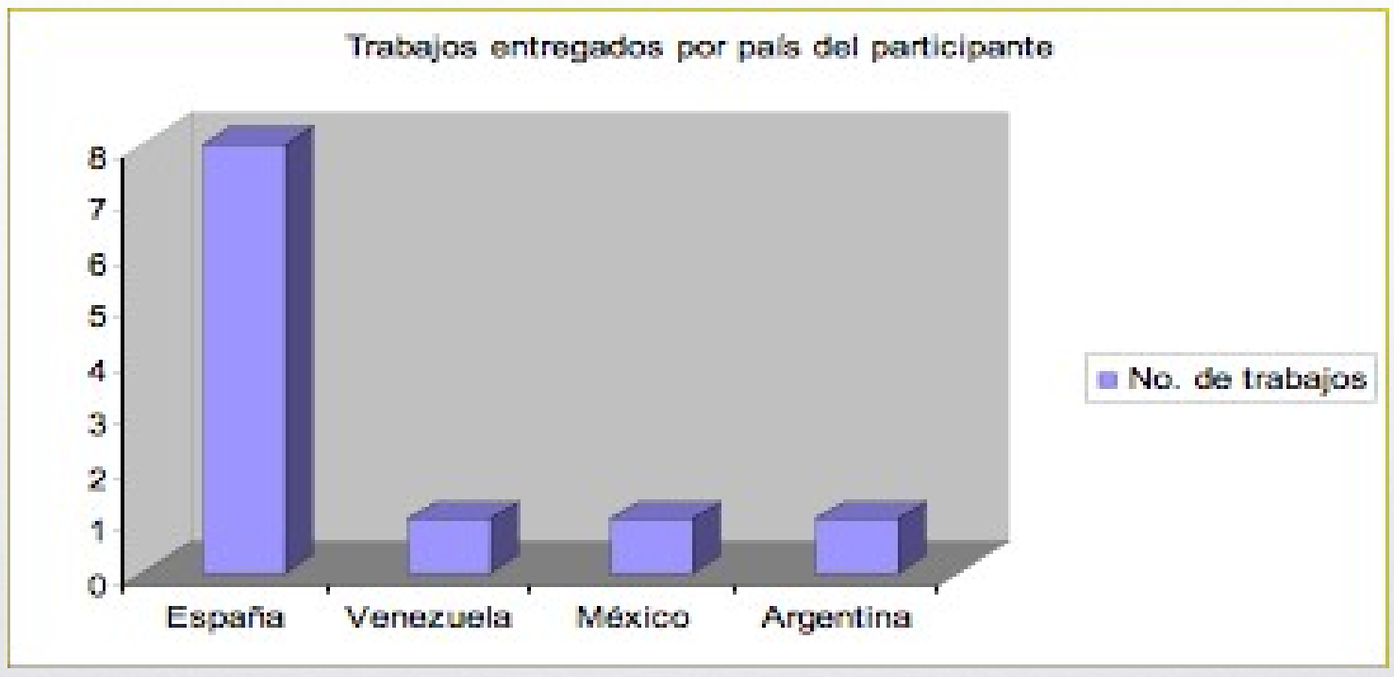
http://www.disc.unam.mx

UNAM CERT

CERTS Académicos

Reto Forense V2.0

* Convocado por UNAM-CERT y RedIRIS (Nov. 2004)
* El objetivo primordial consiste en promoveer una de las ramas de mayor especialización en Seguridad Informática "Análisis Forense"
* 1000 Inscritos, 11 Trabajos entregados



UNAM CERT

Reto Forense V2.0

* Es importante señalar que el 3er lugar (Juan Antonio Fernández Gómez) utilizo únicamente herramientas UNIX.

* A resaltar la diferencia que existe en la comunidad de análisis forense de España con el resto de habla castellano, sin embargo se noto un gran interés de la comunidad de AL, inclusive usuarios nos reportan herramientas en desarrollo.

* Creación de 2 comunidades de Análisis Forense, Listas de discusión, etc.

CERTS Academicos

Reto Forense V3.0 ????

Noviembre 25, 2005

UNAM CERT

CERTS Académicos

Conclusiones

* La academia siempre será base del cambio, generador de ideas y su aportación a los diversos sectores de la sociedad denotara grandes avances para el manejo apropiado de la información.

* En la evolución de una Sociedad del Conocimiento un CERT es vital para la optima evolución y protección de los datos e información.

* Dia a día los gobiernos de cada país consideran ampliamente la creación de un CERT Nacional, debido a al imperante necesidad de informar, catalogar y procesar los problemas mayores de Seguridad en Cómputo.

UNAM CERT

CERTS Académicos

Conclusiones

* Un CERT Académico nos ha demostrado ser una fuente primaria de investigación a los principales ataques informáticos (Gusanos informáticos,Ataques DDoS,Honeypots,Phishing Scams,etc).

* Ello ha permitido revolucionar las técnicas de Análisis Forense, predecir ataques y manejo apropiado de incidentes.

* Con la evolución y valía de lo que nos han demostrado los CERT Académicos a través de los años, han provocado una evolución en las organizaciones, llevando la infraestructura de un CSIRT en areas de procesos críticos de la información.

UNAM CERT

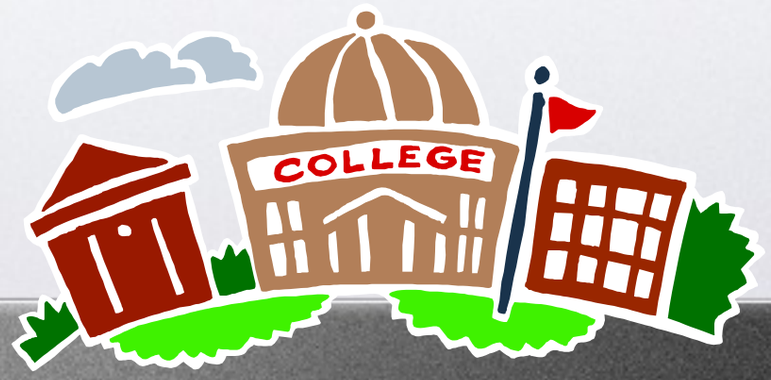
CERTS Académicos

Conclusiones

* No hay una solución única, para solucionar los problemas de seguridad informática.

* Se necesita una estrategia en diversos niveles para combatir el delito informático

CSIRT



UNAM CERT

Preguntas??

Juan Carlos Guel López
cguel@seguridad.unam.mx