



Perfil del Personal de Seguridad en Cómputo

Juan Carlos Guel Lopez(cguel@seguridad.unam.mx)

Septiembre 2002



Perfil de Seguridad en Cómputo

Temario :

1. Introducción
2. El Problema
3. Situación Actual
4. Características del Personal
5. Comentarios y Sugerencias
6. Conclusiones



Perfil de Seguridad en Cómputo

Definiciones de Diccionario

Seguridad - (sustantivo femenino). Certeza, firmeza, confianza. (locución adverbial). Sin riesgo.

Seguridad - (sust.) Dícese de las cosas ciertas, firmes y/o libres de peligro o riesgo. Estado de las cosas bajo protección.



Perfil de Seguridad en Cómputo

"En cualquier sociedad, un pequeño porcentaje de la gente es maliciosa. Se estima que Internet ahora tiene de 30 a 40 millones de usuarios. Aún si el porcentaje de usuarios maliciosos es menor del 1% de esa sociedad, el número potencial de usuarios maliciosos es tan grande que debiera preocuparle".

❖ *Building Internet Firewalls; B. Chapman, E. Zwicky; O' Reilly & Associates; 1995)*



Perfil de Seguridad en Cómputo

¿Qué busca la seguridad?

- Proteger derechos
 - ✓ El derecho a la privacidad
 - ✓ El derecho a estar informados
- Proteger activos
 - ✓ Información (Bases de datos)
 - ✓ Equipos (Sistemas de Control, Redes, ...)
- Reforzar las reglas
 - ✓ Leyes, políticas y procedimientos



Perfil de Seguridad en Cómputo

Definiciones de Seguridad

"Un sistema es seguro si se comporta como los usuarios esperan que lo haga".

- Dr. Eugene Spafford
 - Director del CERIAS (Center for Education and Research on Information Assurance and Security)
 - Libro: Practical UNIX Security



Perfil de Seguridad en Cómputo

¿Realmente necesitamos estar en Internet ?

- ✓ Si no estas en Internet no existes.
- ✓ Debes tener tu portal de Internet
- ✓ Debemos evolucionar a Internet2
- ✓ Debes tener tu sistema de registro de control escolar en Línea...Bajo que riesgos ???
- ✓ Y la Administración y la Seguridad de los equipos de Cómputo???



Perfil de Seguridad en Cómputo

¿Quién es el Enemigo?

- ✓ Clasificaciones
 - Conocimientos
 - Recursos
 - Tiempo
 - Motivación

- ✓ Nombres
 - Script Kiddies
 - Saboteadores
 - Crackers profesionales



Perfil de Seguridad en Cómputo



El Problema



Perfil de Seguridad en Cómputo

El Problema

Existen una gran variedad de herramientas que los intrusos utilizan hoy día para tratar de introducirse a nuestros sistemas.

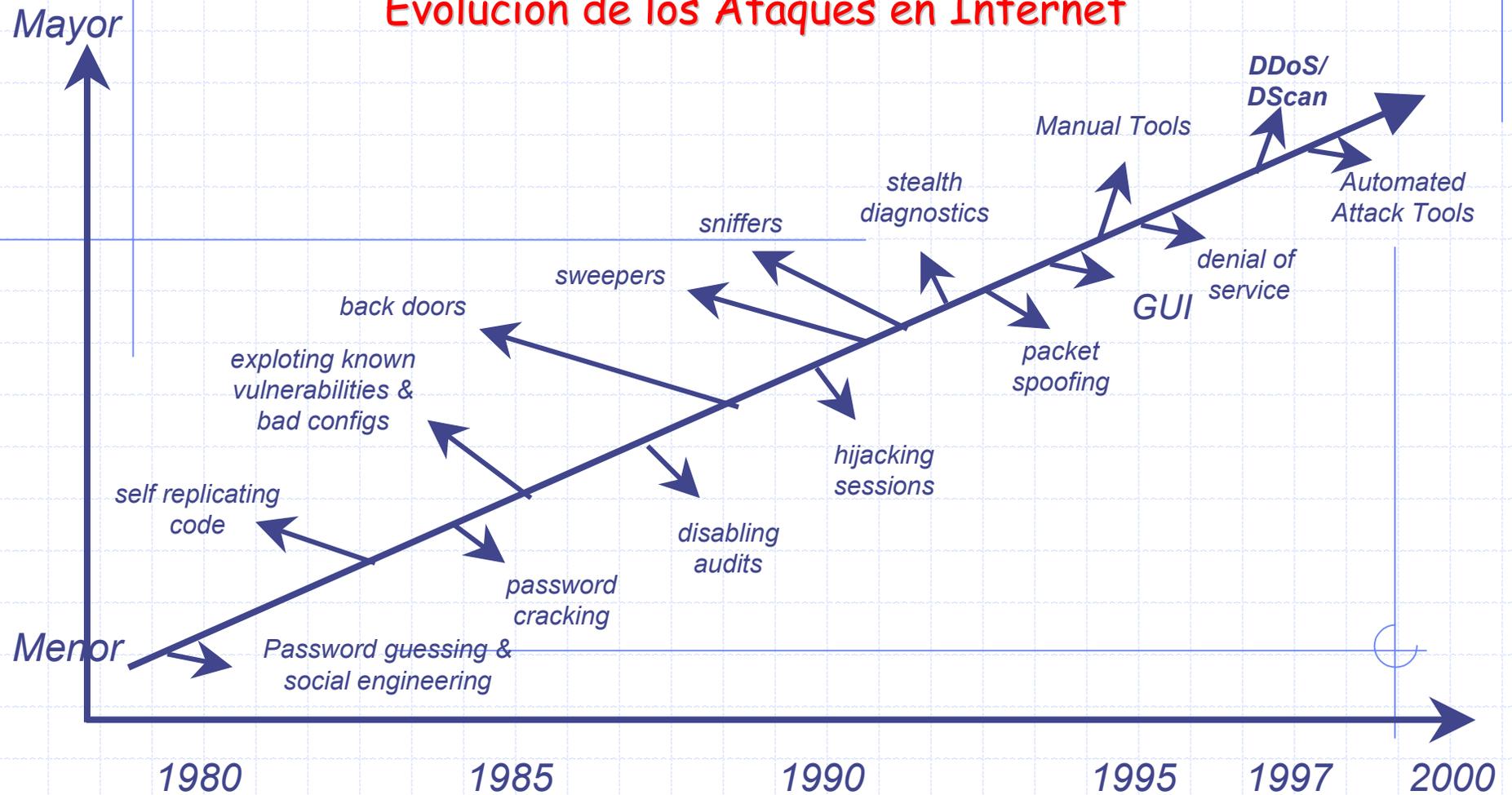
El problema crece cuando distintos intrusos de diversos países intentan penetrar nuestra organización usando herramientas simples y fáciles de obtener.

Agreguemos los nuevos y sofisticados ataques y formas de explotación de los sistemas.



Perfil de Seguridad en Cómputo

Evolucion de los Ataques en Internet





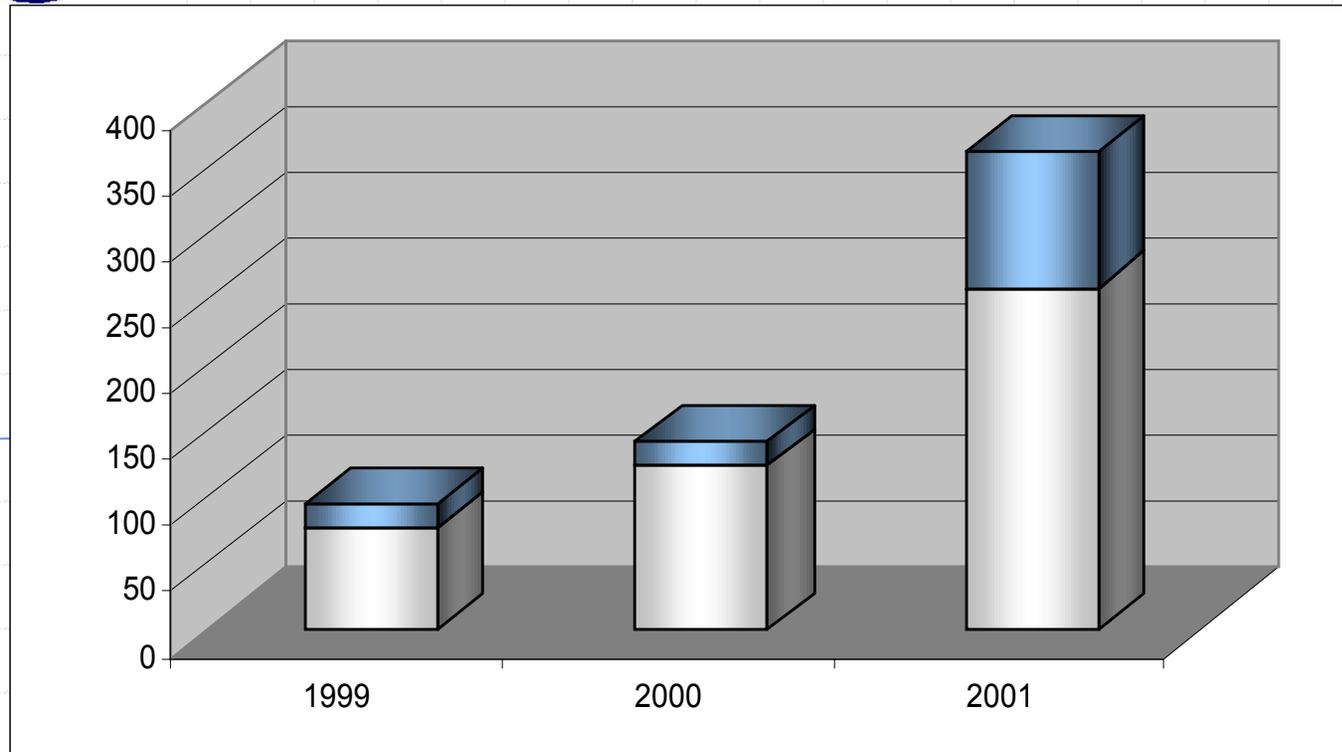
Perfil de Seguridad en Cómputo

El mercado de la seguridad

- ✓ Pérdidas financieras por más de 377 millones de dólares en 2001
 - 186 organizaciones reportantes
- ✓ 91% de abuso interno
 - http://www.gocsi.com/prelea_000321.htm
- ✓ En México, más de 450 defacements a páginas web de 1999 a Agosto de 2002
 - <http://www.attrition.org/mirror/attrition/mx.html>
 - Falta agregar los casos no reportados



Páginas Web alteradas por intrusos en el periodo de 1999 al 2001



■ Sitios Web de IES
■ Sitios Web de otras organizaciones

En el periodo de 1999 al 2001 fueron reportadas en México un total de 463 páginas web alteradas por intrusos.

Año	Otros sitios web	Sitios web de IES	% de IES afectadas en relación al total
1999	77	19	24%
2000	126	17	13%
2001	260	103	39%
TOTAL	463	139	30%

Del total de páginas reportadas durante ese periodo, 139 correspondían a páginas web de instituciones de educación superior, lo cual implica un 30% respecto al total.

Fuentes: Attrition.org (www.attrition.org)
Alldas (defaced.alldas.de)

Nota: Estas cifras son sólo aproximaciones, pues algunas instituciones nunca reportan sus incidentes de seguridad en cómputo.



Perfil de Seguridad en Cómputo

Situación Actual

Ese total ha ido creciendo en los últimos 12 meses de forma alarmante, afectando principalmente a las universidades tanto públicas como privadas del país, generando inseguridad en muchos de los servicios que se prestan en los ambientes académicos, tales como:

- Bases de Datos
- Registro Escolar
- Información de las Universidades
- Proyectos de Investigación



Perfil de Seguridad en Cómputo

Situación Actual

- No Existe la palabra seguridad en las aulas, maestrías, doctorados en México.
- No se trabaja de forma conjunta entre universidades.
- No existe un organismo oficial que los pueda coordinar en materia de Administración y de Seguridad.
- Se trabaja de forma aislada.
- Y los problemas de Virus, gusanos??
- Que hay de las Vulnerabilidades en los sistemas, como se enteran??, como lo coordinan en sus campus universitarios??



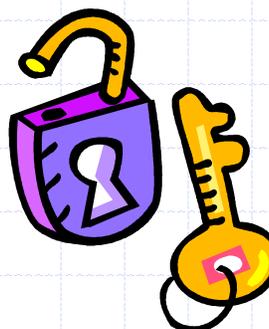
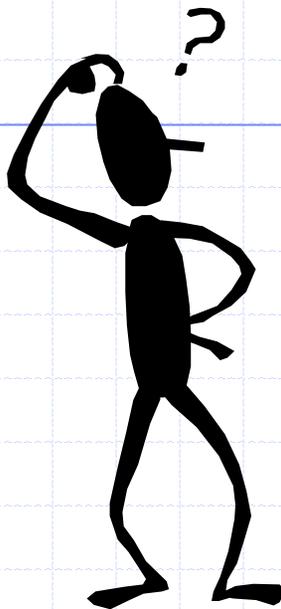
Perfil de Seguridad en Cómputo

Situación Actual

- Que hay de la implantación de esquemas seguros en las universidades?
- Como se protegen las Bases de Datos, registros de alumnos, inscripciones, etc, etc.
- Se realizan análisis académicos para determinar que es lo mas importante para la organización??...o solo por justificar dinero y presupuestos comprando el software mas bonito??
- Que solución y respuesta se proporciona a la comunidad estudiantil en este rubro??



Características del Personal





Perfil de Seguridad en Cómputo

Características

Al analizar los distintos problemas y la situación actual se requiere que se analicen los siguientes puntos a fondo antes de elegir y tomar una decisión ante la persona que sea designada para trabajar en cuestiones de seguridad en cómputo en cada IES:

- Sea de total confianza y designada por los rectores
- Muestre características de liderazgo
- Muestre ser honesto.



Perfil de Seguridad en Cómputo

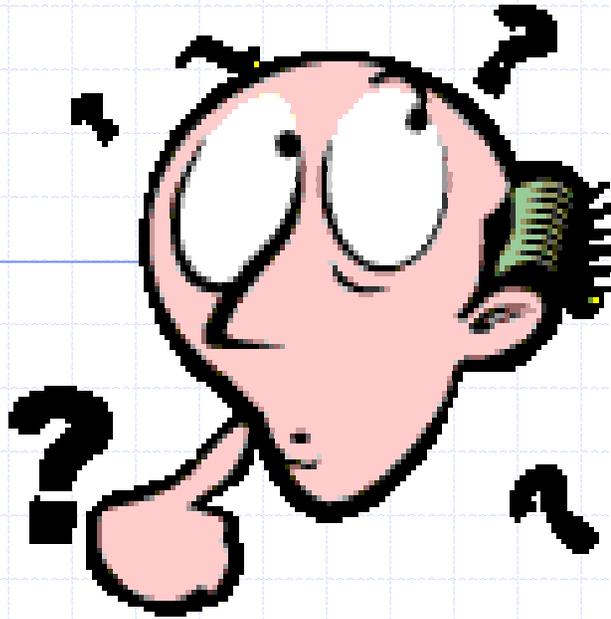
- Muestre principios de ética y profesionalismo bien establecidos.
- Características de trabajo en grupo y coordinar esfuerzos
- Sea un punto de enlace y haga llegar la información, boletines, emergencias a través de dichos puntos de contacto, que se generan a través de UNAM-CERT.
- Sepa manejar los niveles de difusión de Información.
- Pueda fomentar entre las comunidades estudiantiles la palabra "Seguridad en Cómputo", como un hecho y realidad que convivimos día con día, fomentar su cultura y uso.



Perfil de Seguridad en Cómputo

Características

- Sea capaz de asimilar los problemas, ataques y situaciones a las que se enfrenta el personal de seguridad día con día a través de un plan de capacitación.
- Antes de cualquier decisión, tener bien en claro que deseamos proteger; cuanto tiempo, cuanto dinero y cuanto esfuerzo estoy dispuesto a invertirle en mi IES.
- Tener en mente que la seguridad es un proceso y no querer correr sin saber antes caminar en este rubro.
- Nunca dejar de tener en mente que la seguridad es un rubro que requiere inversión constante.



Preguntas....



Departamento Seguridad en Cómputo UNAM-CERT

DGSCA - UNAM

<http://www.seguridad.unam.mx>

<http://www.unam-cert.unam.mx>

<ftp://ftp.seguridad.unam.mx>

seguridad@seguridad.unam.mx