

Universidad Nacional Autónoma de Bucaramanga

Panorama general de los principales ataques y defensas de un sistema informático

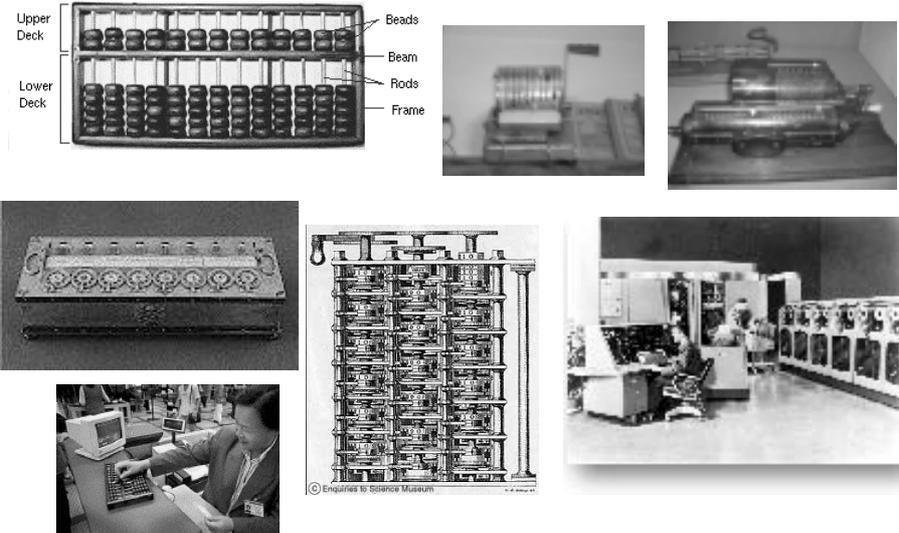
Roberto Gómez
rogomez@itesm.mx
<http://webdia.cem.itesm.mx/ac/rogomez>

Lámina 1 Dr. Roberto Gómez C.

 **Primeras computadoras** 

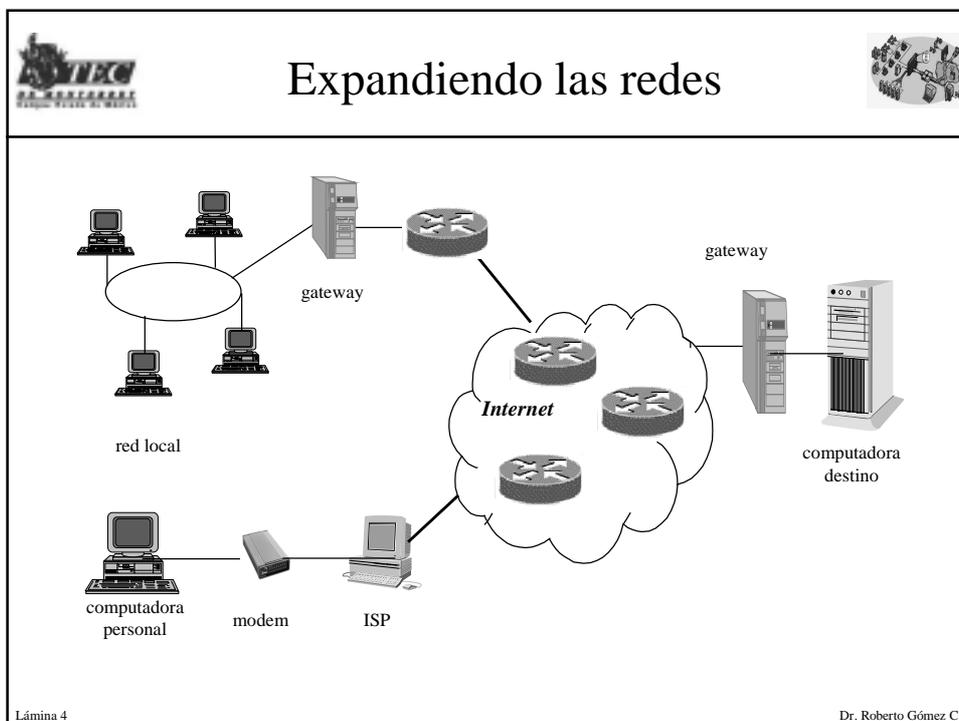
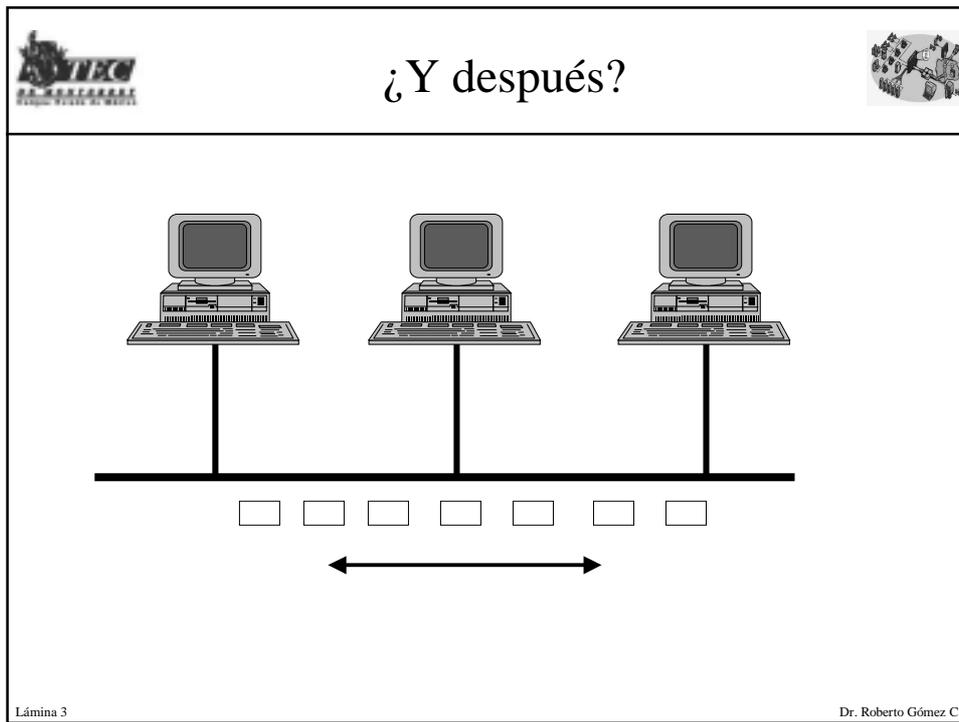
Upper Deck
Lower Deck

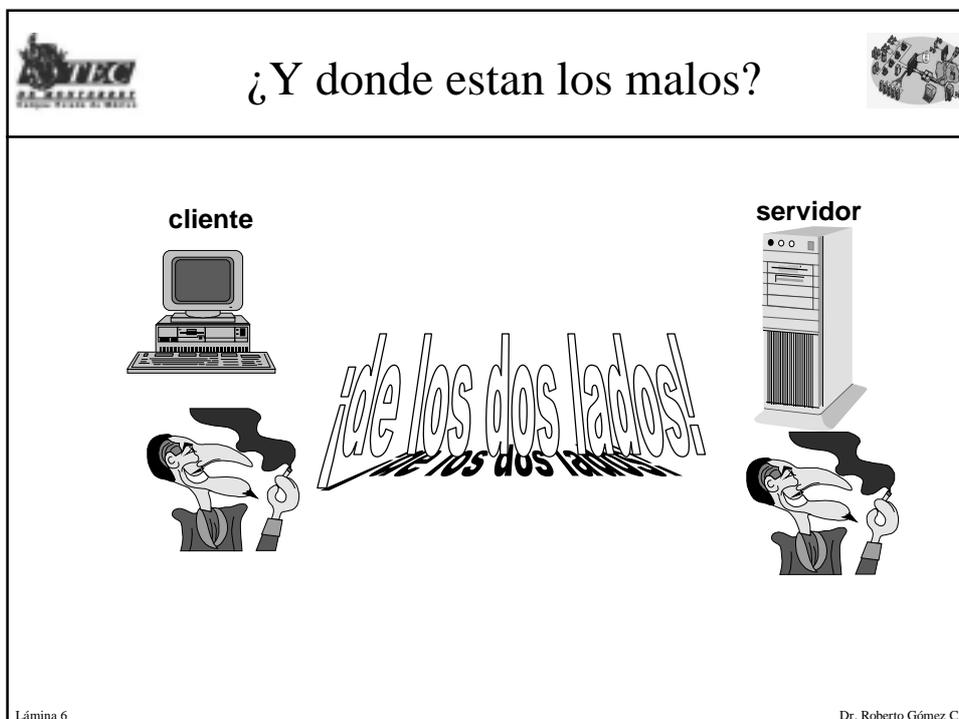
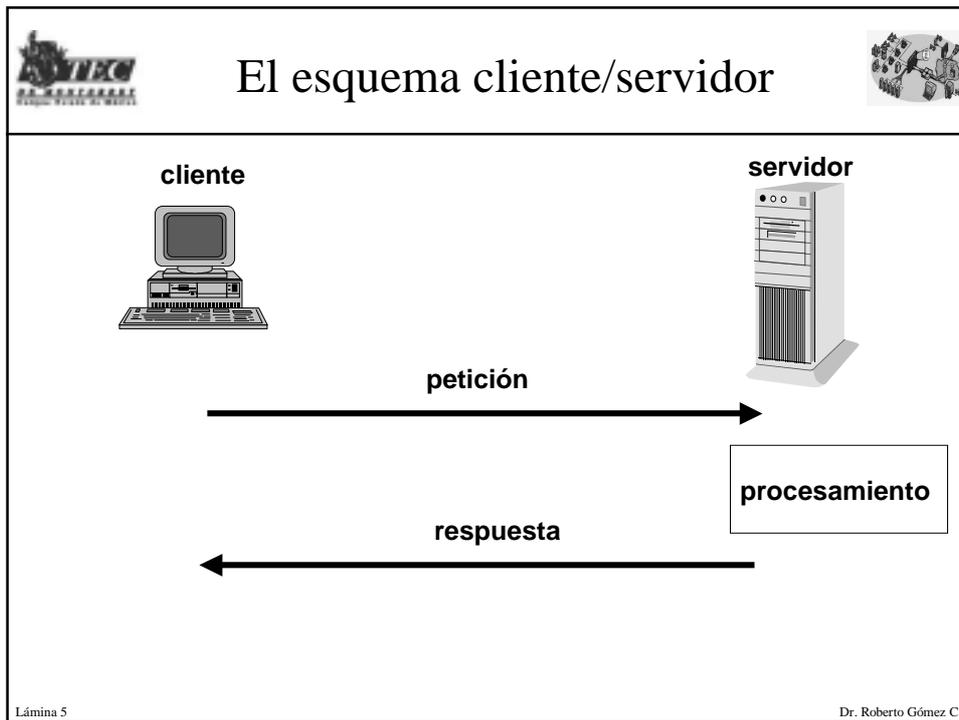
Beads
Beam
Rods
Frame



© Engraved to Science Museum

Lámina 2 Dr. Roberto Gómez C.







¿Y quienes son los malos?



- Los hackers
- Los crackers
- Los script kiddies

```

Last login: Mar 12 07:03:29 on console
Welcome to os4!
> telnet -a -b ABSOLUT 192.168.100.1:8080
> enter login: #####
> enter passw: #####
> invalid passw ERROR (retype)
> retype passw #####
> OK you are SUCCESFULLY logged in
> cd /usr/.ABSOLUT/SECRETS
> ls -l -a BACKDOORVIRUSES
-rwxr-xr-- TROJANHORSE#BF1 - 306 Mar 7 20:55
-r-xr-xr-- TROJANHORSE#CA0 - 1026 Mar 11 00:13
-r-xr-xr-- TROJANHORSE#CB9 - 716 Mar 5 14:15
-rwxrw-r-- TROJANHORSE#CF9 - 4865 Feb 9 22:06
-r-xr--r-- TROJANHORSE#D2C - 48 Jan 28 17:24
-r-xr--r-- TROJANHORSE#D8A - 512 Mar 2 02:22
-r-xr-xr-x TROJANHORSE#DA6 - 512 Mar 7 04:46
-r-xr--r-- TROJANHORSE#DD7 - 642 Feb 13 01:58
-r-xr--r-- TROJANHORSE#DF2 - 1784 Dec 31 11:33
-rwxr-xr-- TROJANHORSE#EA3 - 1256 Mar 4 14:56
-rwxrw-r-- TROJANHORSE#EB4 - 2873 Mar 5 08:17
-r-xr--r-- TROJANHORSE#ED8 - 255 Feb 17 10:45
-r-xr--r-- TROJANHORSE#FA3 - 207 Feb 17 10:57
> sudo -sp TROJANHORSE#D2C
System is about to reboot
Killing all processes .....
                
```

ABSOLUT HACKER.

ABSOLUT COUNTRY OF SWEDEN VODKA & LOGO, ABSOLUT, ABSOLUT BOTTLE DESIGN AND ABSOLUT CALLIGRAPHY ARE TRADEMARKS OWNED BY V&S P&F AB. THOSE WHO APPRECIATE QUALITY ENJOY IT RESPONSIBLY. THIS AD WAS MADE BY P&F 2000.






Lámina 7

Dr. Roberto Gómez C.



El Hacker: La Vieja Guardia

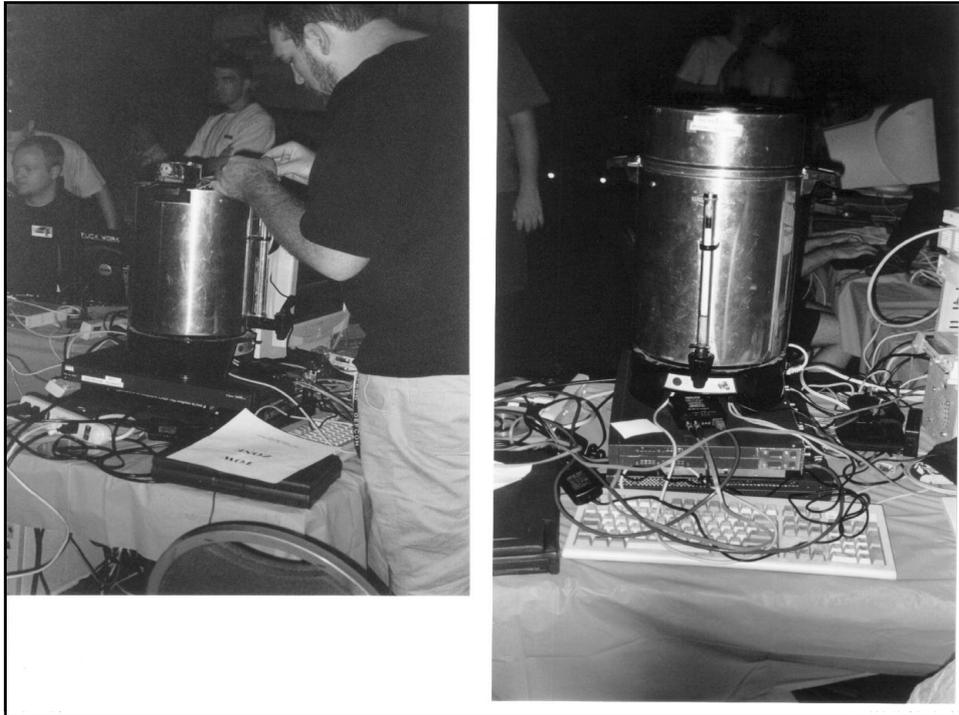




- Origen del término a finales de los 60.
- Programador con alto dominio de su profesión, capaz de solucionar problemas a través de hacks (segmentos de código muy ingenioso).
- Verdaderos conocedores de la tecnología de cómputo y telecomunicaciones (85-93).
- La búsqueda del conocimiento siempre fue su fuerza impulsora.

Lámina 8

Dr. Roberto Gómez C.



El cracker

- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas computacionales.
- Una vez logrado el acceso produce daños a los recursos del sistema atacado.
- No necesariamente tiene el mismo nivel de conocimientos que el hacker.

Lámina 10

Dr. Roberto Gómez C.



El Hacker: la nueva generación o los "Script-kidies"



- Gente con la capacidad de buscar un programa en la red y ejecutarlo.
- No hay una meta fija.
- Necesidad de pertenencia, aunque sea al *inframundo*.
- No hay preocupación por las consecuencias reales de sus actos.
- Se sienten muy "cool".



Lámina 11 Dr. Roberto Gómez C.



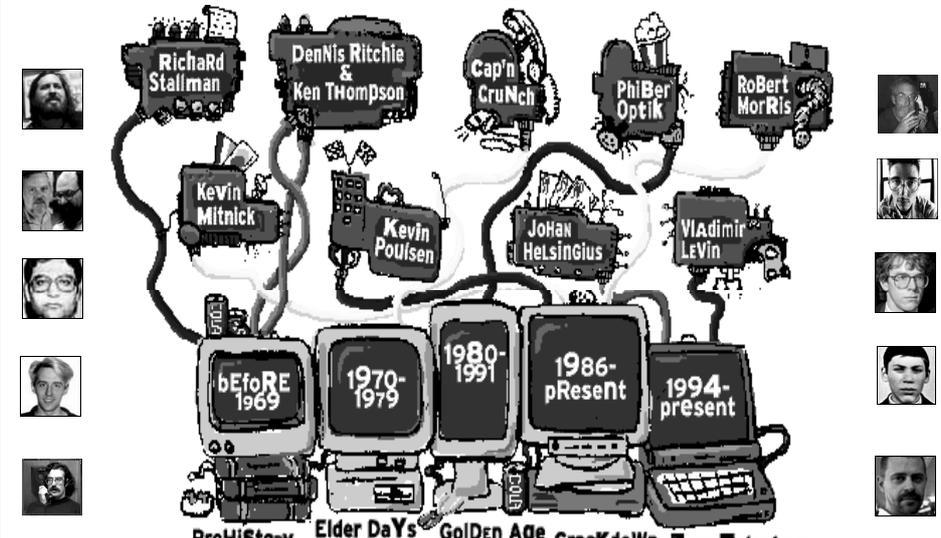
El Hacker: La Visión del Resto de los Usuarios



- ¿Qué es eso?
- Eso pasa solo en las películas.
- Así como los de "The Net"
- Yo soy hacker.
- Yo apenas sé como se usa una computadora.
- Bill Gates se va a encargar de ellos.

Lámina 12 Dr. Roberto Gómez C.

 El hall de la fama de los hackers 



Richard Stallman, Dennis Ritchie & Ken Thompson, Cap'n Crunch, PhiBer Optik, Robert Morris, Kevin Mitnick, Kevin Poulsen, Johan Helsingius, Vladimir Levin

before 1969, 1970-1979, 1980-1991, 1986-present, 1994-present

PreHistory, Elder DaYs, Golden Age, CrackDown, Zero Tolerance

Lámina 13 www.discovery.com/area/technology/hackers/hackers.html Dr. Roberto Gómez C.

 El hacker Kevin Mitnick 



Lámina 14 Dr. Roberto Gómez C.



Algunos términos y personajes relacionados



- Geeks EsTo TiPo De TiPoGrAfla Ya No EsTa De MoDa Y yA nO sE uSa
- Lammer 3ST0 S3RI4 UN 3J3MPLO D3 DICH0 L3NGU4J3
- Wracker
 - programas shareware o freeware
- Newbie
- Rider
- Sneaker
 - espía informático por excelencia
- Carding 



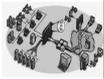
**Una madrecita
Aprendiendo a
“Hackear”.**

Lámina 15

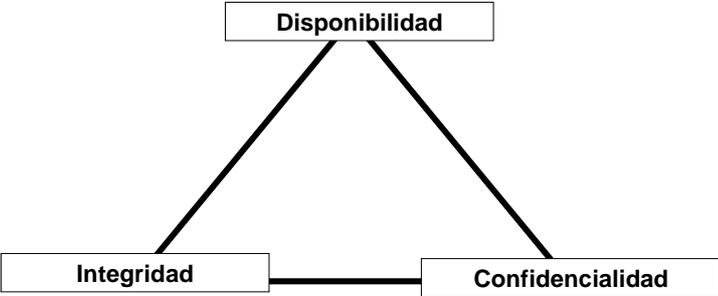
Dr. Roberto Gómez C.



Seguridad Computacional



El conjunto de políticas y mecanismos que nos permiten garantizar la *confidencialidad*, la *integridad* y la *disponibilidad* de los recursos de un sistema.



```

graph TD
    A[Disponibilidad] --- B[Integridad]
    A --- C[Confidencialidad]
    B --- C
            
```

Lámina 16

Dr. Roberto Gómez C.

 **El principio básico** 

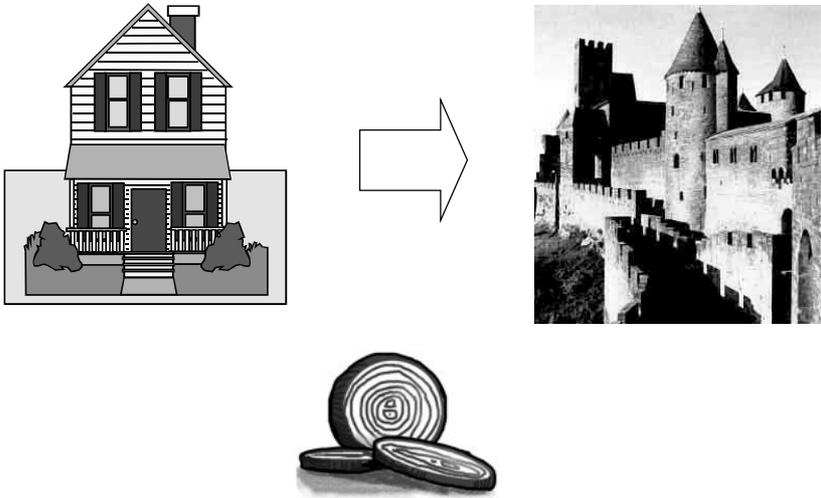


Lámina 17 Dr. Roberto Gómez C.

 **La estrategia es un ciclo** 

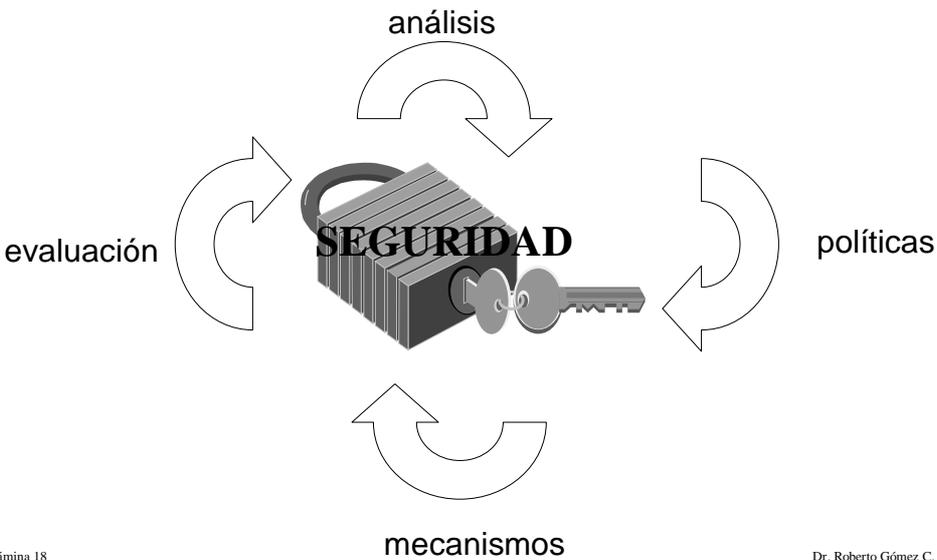


Lámina 18 Dr. Roberto Gómez C.



Asegurando el sistema



- **Objetivo**
 - minimizar los riesgos potenciales de seguridad
- **Análisis de riesgos**
 - análisis amenazas potenciales que se pueden sufrir,
 - las pérdidas que se pueden generar
 - y la probabilidad de su ocurrencia
- **Diseño política de seguridad**
 - definir responsabilidades y reglas a seguir para evitar tales amenazas o
 - minimizar sus efectos en caso de que se produzcan
- **Implementación**
 - usar mecanismos de seguridad para implementar lo anterior

Lámina 19 Dr. Roberto Gómez C.



Pasos en un análisis de riesgos



1. Identificación costo posibles pérdidas (L)

Identificar amenazas

Se cierra el ciclo

3. Identificar posibles acciones (gasto) y sus implicaciones. (B)

Seleccionar acciones a implementar.

¿ $B \leq P * L$?

2. Determinar susceptibilidad.

La probabilidad de pérdida (P)

Lámina 20 Dr. Roberto Gómez C.



Política de Seguridad



- Especifica las características de seguridad que un sistema debe observar y proveer
 - conjunto de reglas que deben respetarse para mantener la seguridad de la información.
- Especifica las amenazas contra las que la organización debe protegerse y cómo debe protegerse
- Depende de los objetivos y metas de la organización.
- Generalmente es expresada en un lenguaje o idioma.



Lámina 21 Dr. Roberto Gómez C.



Paradigmas



- *Paranoico*: Nada está permitido.
- *Prudente*: Lo que no está expresamente permitido, está prohibido.
- *Permisivo*: Lo que no está expresamente prohibido, está permitido.
- *Promiscuo*: Todo está permitido.

Lámina 22 Dr. Roberto Gómez C.



Ejemplo de Política (en lenguaje natural)

- Sólo se permitirá el intercambio de correo electrónico con redes de confianza.
- Toda adquisición de software a través de la red debe ser autorizada por el administrador de seguridad.
- Debe impedirse la inicialización de los equipos mediante disco.

Lámina 23 Dr. Roberto Gómez C.



¿Que es un ataque?

- Acción o acciones que tienen por objetivo el que cualquier parte de un sistema de información automatizado, deje de funcionar de acuerdo con su propósito definido.
- Esto incluye cualquier acción que causa la destrucción, modificación o retraso del servicio no autorizado.

Lámina 24 Dr. Roberto Gómez C.

Aclaración ataque

- No es un ataque físico (aunque puede ser).
- Un ataque no se realiza en un solo paso.
- Depende de los objetivos del atacante.
- Puede consistir de varios pasos antes de llegar a su objetivo.

Lámina 25

Dr. Roberto Gómez C.

Tipos de Ataques

Ataques Pasivos.

Ataques Activos.

Lámina 26

Dr. Roberto Gómez C.



Principales Ataques



- Virus
- Caballo de Troya
- Gusanos (Worms)
- Bugs
- Trapdoors
- Stack overflow
- Pepena
- Bombas lógicas
- Secuestro sesiones
- Dedos inexpertos
- Falsificación
- Usurpación
- Sniffers
- Spoofing
- Spam
- Grafiti
- Ingeniería Social
- Negación de servicio

Lámina 27 Dr. Roberto Gómez C.



Virus



- Un virus se define como una porción de código de programación cuyo objetivo es implementarse a si mismo en un archivo ejecutable y multiplicarse sistemáticamente de un archivo a otro.
- Además de esta función primaria de "invasión" o "reproducción", los virus están diseñados para realizar una acción concreta en los sistemas informáticos..



Lámina 28 Dr. Roberto Gómez C.



Ejemplos de virus

- El caballo de Troya
- El pakistaní
- El cascada
- El Alabama
- El Jerusalén
- El Miguel Angel
- El ping pong
- El Viena
- El natas
- El dos piernas
- El stoned noit
- El DARK AVEGER
- El ping pong
- El I love you
- El trojan
- El killer

Lámina 29 Dr. Roberto Gómez C.



Variantes relacionadas con virus

- En ocasiones se habla de estas variantes como si se tratara de virus , cuando en realidad son conceptualmente diferentes.
- Algunos antivirus pueden detectarlos.
- Estas variantes son:
 - Troyanos
 - Gusanos
 - Bomba lógica

Lámina 30 Dr. Roberto Gómez C.



Los gusanos



Es un programa que produce copias de sí mismo de un sistema a otro a través de la red; en las máquinas que se instala, produce enormes sobre-cargas de procesamiento que reducen la disponibilidad de los sistemas afectados.



Lámina 31



El gusano navidad.exe (1)



[Fwd: Matematicas, sueno o pesadilla: resena del Cafe] - Inbox - Netscape Folder

File Edit View Go Message Communicator Help

Name	Subject	Sender	Date	Priority	Stat...
	R: Medidas de seguridad	Ma. de los Angeles Junco	Sat 11:11 AM		read
	proj_soll	Angel Gabriel Zanatta Juárez	Sat 2:33 PM		read
	game genius juego de ing...	aribal diaz	Sat 4:07 PM		read
	R: CompMovVirtual.ppt	Dr. Javier Gómez Tagle Rangel	Sat 5:25 PM		read
	duda proyecto 3p	Omar Arias	Sun 5:41 PM		read
	[Fwd: Dot Conference]	Roberto Gomez Cardenas Depart...	Tue 9:40 PM		read
	RV: Programa	Shafia Suvar	11/16/2000 9:51 ...		read

Subject: Matematicas, sueno o pesadilla: resena del Cafe
Date: Thu, 16 Nov 2000 09:50:55 -0600
From: Shafia Suvar <shafia@quirote.ugto.mx>
To: francia-mexico@casadefrancia.org.mx

para seguimiento e informacion, encontraran en attachment el boletin de prensa del ultimo CAFE DE CIENCIA sobre MATEMATICAS, SUEÑO O PESADILLA.
 saludos
 Annie
 Attachment Converted: "C:\Eudora\Attach\Bol. Matemáticas.doc"

 Navidad18.exe	Name: Navidad18.exe Type: unspecified type (application/octet-stream) Encoding: base64
---	---

Total messages: 75 Unread messages: 0

Lámina 32

El gusano navidad.exe (2)

Subject: Cuidado!!!!
Date: Wed, 15 Nov 2000 22:26:36 -0600
From: "Salvador G. Medina" <adan@servidor.unam.mx>
To: Shafia Sucar <shafia@quijote.ugto.mx>, francia-mexico@casadefrancia.org.mx

Hola,
 Desgraciadamente el virus del que nos hablo Ofelia ya circulo en esta lista, en mensajes aparentemente enviados por Shafia (con fecha de mañana 16), no abran los attachment (Navidad18 y Navidad22) y limpien su maquina con Norton 2000, antes de enviar mensajes. Usuarios de Mac solo borren los attachment.
 Saludos, Salvador.

At 09:51 -0600 16/11/00, Shafia Sucar wrote:
 >>Annie,
 >>

Lámina 33

El gusano navidad.exe (3)

Subject: Re: Cuidado!!!!
Date: Fri, 17 Nov 2000 00:44:06 -0600
From: Shafia Sucar <shafia@quijote.ugto.mx>
To: "Salvador G. Medina" <adan@servidor.unam.mx>
CC: francia-mexico@casadefrancia.org.mx
References: 1

Estimados Lectores,

Lamento mucho haber sido la culpable de que mensajes que yo No envie, pero que si salieron de mi correo, llegaran hasta ustedes. Evidentemente este virus toma direcciones de correo electronico y se auto-envia. Esto me sucedio ayer miercoles, y desafortunadamente no sabia aun de este virus.
 Por favor no abran dicho ejecutable y eliminen todo aquello que diga Navidad!

Nuevamente les pido disculpas!

Saludos,
 Shafia.

Lámina 34



Lo bueno y lo malo de navidad

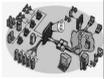


- Lo malo del Navidad es que contiene rutinas destructivas que se activan, al menos en teoría, el 25 de diciembre.
- Lo bueno es que debido a errores en el procedimiento de instalación, quizá nunca llegue a activarse la rutina destructora.
- Lo malo es que después de instalarse, no funcionará prácticamente ningún programa del usuario

Lámina 35
Dr. Roberto Gómez C.



Otro ejemplo virus/gusano



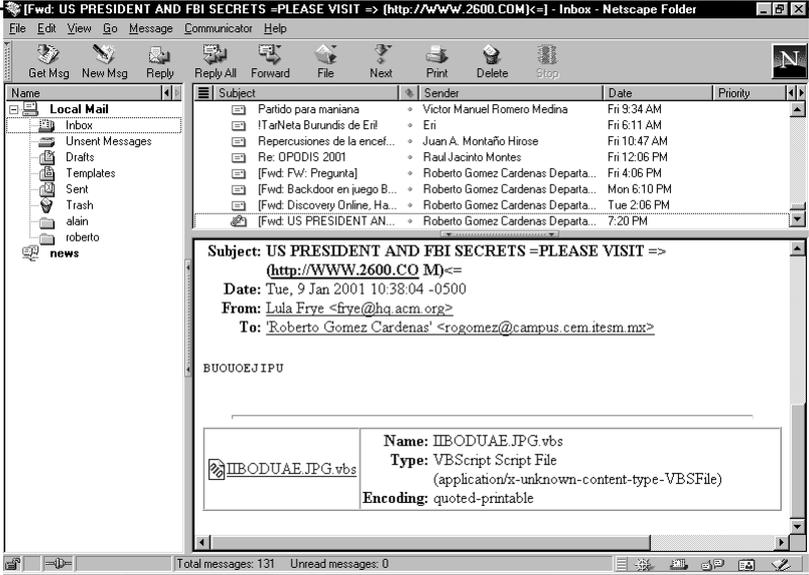
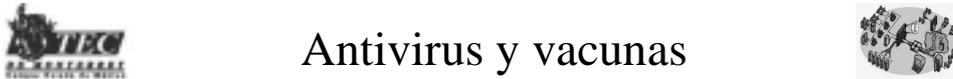


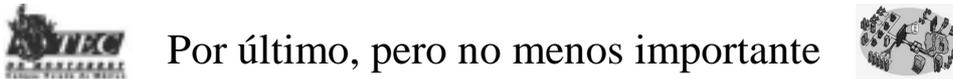
Lámina 36
7:17 PM > Gómez C.



Antivirus y vacunas

- Programa encargado de la detección de virus.
- Algunos intentan parar el virus en el momento en que se produce el ataque (sistemas de prevención)
 - la mayoría vigilan la entrada desde disco pero no desde internet
- Otros comprueban el código del programa antes de que se ejecute.
 - usuario puede ser avisado de los posibles peligros del programa que va a ejecutarse
 - el proceso se conoce vulgarmente como “escaneado”
- Una vacuna esta diseñada para limpiar un virus en concreto, solamente un virus

Lámina 39 Dr. Roberto Gómez C.



Por último, pero no menos importante

- Mantener al día el antivirus
 - algunos lo hacen de forma automática
- Nunca instalar y ejecutar más de un antivirus
- Usar sentido común
 - ¿vale la pena examinar lo que me llego por correo electrónico?
 - verificar el origen del correo
 - ¿conozco a la persona que lo envío?
 - ¿en realidad necesito el archivo que viene con el correo?
 - ¿acaso yo pedi dicho archivo?

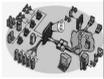
Lámina 40 Dr. Roberto Gómez C.



Los plugins

- Distribución de SW por Internet
- Plug-ins desarrollados por terceros diferentes a los creadores de los browsers, que toman el control de la máquina
- Ofrecen soporte de nuevos formatos de archivos y aplicaciones
 - acroread, real player, etc
 - fondos de pantalla
 - protectores de pantalla

Lámina 41 Dr. Roberto Gómez C.



Riesgos plugins

- Afectan configuraciones de otros productos ya instalados.
- Posibilidad de que el software realice más actividades que las originales.
 - caballos de troya
 - puertas traseras (backdoors, trapdoors)

Lámina 42 Dr. Roberto Gómez C.

El Caballo de Troya

- Objetivo principal: recuperación información confidencial de un organismo o un usuario.
- Se basa en substituir un programa de servicio común por uno alterado por el intruso para recuperar información.

Lámina 43

Un ejemplo de caballo de Troya

- El Caballo de Troya por login es uno de los más comunes.
- En este ataque, el usuario encuentra su estación de trabajo con una pantalla solicitándole su login.
- El usuario inadvertido teclea su login y su password como de costumbre; esta vez recibiendo un mensaje de error.

```
login: mbui
Password:
Login incorrect
```

Lámina 44

Dr. Roberto Gómez C.



Continuación del ejemplo



- En el segundo intento, el usuario logrará acceder al sistema.
- El no sabe que su password fue almacenado en algún archivo donde, más tarde, el creador del Caballo de Troya lo recuperará.
- El falso programa de login, después de almacenar el password robado, invoca el verdadero programa de login, dejando al usuario actuar con una nueva sesión de login.

Lámina 45Dr. Roberto Gómez C.



Trapdoors, backdoors o puertas traseras



- Es frecuentemente creado por el diseñador del sistema; sin embargo, en ocasiones existe por accidente.
- Algunas veces es creado durante las pruebas de implementación de un sistema y después es olvidado.
- Otras veces, es usado por el proveedor para “atar” al cliente que compro dicho sistema.



Lámina 46Dr. Roberto Gómez C.



Ejemplo puerta trasera



- Programa buscaminas de Windows 2000
- Correr Minesweeper, teclear “xyzyzy” y presionar Shift + Enter.
- Buscar un pixel blanco en la parte superior izquierda de la pantalla
 - si no se ve configurar pantalla
 - conforme se mueve el raton por las celdas del buscaminas el pixel desaparece y aparece: desaparece cuando hay una mina en la celda y viceversa

Lámina 47 Dr. Roberto Gómez C.



Precauciones a tomar en cuenta



- Estar seguros de que en realidad se necesita el software
- No pueden proporcionarmelo en el área de sistemas.
- Preguntar si alguien más lo ha usado y si ha tenido problemas.
- De preferencia que se software recomendado por la misma marca del browser.

Lámina 48 Dr. Roberto Gómez C.



Hoax (engaño, burla, petardo)



- Típicamente son alertas de peligro, o peticiones de ayuda, empezadas por gente maliciosa - y divulgadas por usuarios inocentes que piensan que están ayudando a la comunidad al espacir la advertencia.
- El incremento de virus y programas troyanos muchos usuarios han usado Internet como un medio para alertar a amigos y colegas de trabajo acerca de estos menesteres.

Lámina 49
Dr. Roberto Gómez C.



Algunos ejemplos de hoax



<ul style="list-style-type: none"> • A Virtual Card For You • A.I.D.S. Virus Hoax • ANTHRAX Virus Hoax • Anticristo Virus Hoax • AOL4FREE • ASPARTAME HOAX • Big Brother Hoax • BLOAT VIRUS HOAX • BUDSAVER.EXE • SULFNBK Hoax • Win A Holiday 	<ul style="list-style-type: none"> • Celulares Hoax • D@fit Hoax • Dangerous HIV Hoax • Death Ray • Deeyenda Virus Hoax • NEW YORK BIG DIRT HOAX • Perrin Hoax • PIKACHUS BALL HOAX • PKZ300 Warning
---	---

Lámina 50
Dr. Roberto Gómez C.



1er. ejemplo Hoax

Mr. Xxxxx wrote:
Unanse a esta buena causa:
SE TRATA DE LA PEQUEDA LLAMADA JESSICA MYDEK TIENE SIETE ANOS DE EDAD Y SUFRE DE UN AGUDO Y MUY RARO CASO DE CARCINOMA CEREBRAL ESTA ENFEREMEDAD TERMINAL PROVOCA LA APARICION DE DIVERSOS TUMORES MALIGNOS EN EL CEREBRO.
LOS DOCTORES LE HAN PRONOSTICADO A JESSICA SEIS MESES DE VIDA, Y COMO PARTE DE SUS ULTIMOS DESEOS ELLA QUIZO INICIAR UNA CADENA DE E-MAILS INFORMANDO DE SU CONDICION Y ENVIAR EL MENSAJE A LA GENTE PARA QUE VIVA AL MAXIMO Y DISFRUTEN DE CADA MOMENTO DE SU VIDA, UNA OPORTUNIDAD QUE ELLA NUNCA TENDRA.
ADICIONALMENTE, LA SOCIEDAD AMERICANA DE LUCHA CONTRA EL CANCER, JUNTO CON OTRAS EMPRESAS PATROCINADORAS, ACORDARON DONAR TRES CENTAVOS QUE SERAN DESTINADOS A LA INVESTIGACION DEL CANCER POR CADA PERSONA QUE ENVIE ESTE MENSAJE. POR FAVOR, DENLE A JESSICA Y A TODAS LAS VICTIMAS DEL CANCER UNA OPORTUNIDAD.

Lámina 51 Dr. Roberto Gómez C.



1er. ejemplo Hoax (cont)

Lo unico que tienen que hacer para incrementar el numero de personas en esta cadena es:

Primero: dirija este e-mail a ACS@aol.com
Segundo: en la parte donde dice CC agregue los e-mails de todos los amigos y colegas que conozca

Saludos cordiales,
Alfonso

Lámina 52 Dr. Roberto Gómez C.



¿Y para que quiere alguien direcciones electrónicas?



Software para Marketing - Seguridad - Netscape Folder

File Edit View Go Message Communicator Help

Get Msg New Msg Reply Reply All Forward File Next Print Delete Stop

Name Subject Sender Date Priority

Software para Marketing DIRECTORIOS DE MEXICO más 10:54

NOS PERMITIMOS INFORMARLE LO SIGUIENTE:

TENEMOS UN DIRECTORIO DE 300,000 CORREOS ELECTRONICOS

Y EL PROGRAMA -SOFTWARE-

PARA ENVIOS MASIVOS, EN C.D

EDICION 2002

¡ LO MAS ECONOMICO Y EFECTIVO PARA ANUNCIARSE !

LA RESPUESTA ES INMEDIATA Y LOS RESULTADOS POSITIVOS, SORPRENDENTES.

AL ANUNCIARSE O PROMOCIONARSE POR e-mail, USTED RECIBE MAS PEDIDOS A UN

COSTO MUCHO MENOR, QUE POR CUALQUIER OTRO MEDIO PUBLICITARIO.

OBJETIVOS

Total messages: 24 Unread messages: 0

19:18 Roberto Gómez C.

Lámina 53



¿Y es negocio?



Software para Marketing - Seguridad - Netscape Folder

File Edit View Go Message Communicator Help

Get Msg New Msg Reply Reply All Forward File Next Print Delete Stop

Name Subject Sender Date Priority

Software para Marketing DIRECTORIOS DE MEXICO más 10:54

PUBLICITAR NUEVOS PRODUCTOS

COBERTURA

D.F. y Zona Conurbada: 230,000 Direcciones Electrónicas

Provincia: 70,000 Direcciones Electrónicas

Empresas 84% Universidades 11% Particulares 5%

PRECIO: \$ 19,950.00 más I.V.A.

SOLAMENTE SE LE VENDERÁ A 10 COMPRADORES PARA QUE REALMENTE LES SEA MUY PRODUCTIVO.

INFORMACION COMPLEMENTARIA DEL DIRECTORIO DE 300,000 CORREOS ELECTRONICOS

ZONIFICACION	Cantidad
ZONA NORTE (D.F. y AREA METROPOLITANA)	118,000
ZONA SUR (D.F. y AREA METROPOLITANA)	112,000

Total messages: 24 Unread messages: 0

19:19 Roberto Gómez C.

Lámina 54



2do. ejemplo hoax



Este reenvío lo recibí de un amigo hoy y es verdad lo busqué con estas instrucciones y lo encontré, lo tenía sin saberlo. No lo detecta el Norton 2001 ni McAfee, los tengo instalado y pasó igual. Un virus está llegando a través de los mails de modo oculto. Gracias a un aviso pude detectarlo (lo tenía sin saberlo) y eliminarlo. Buscarlo del siguiente modo:

1. Ir a Inicio
2. Luego: Buscar
3. Archivo o carpeta
4. Tippear el archivo: sulfnbk.exe
5. Eliminar (NO ABRIRLO)
6. Eliminar de la papelera de reciclaje

Gracias a estas instrucciones lo eliminé..
suerte..

Lámina 55 Dr. Roberto Gómez C.



Spam



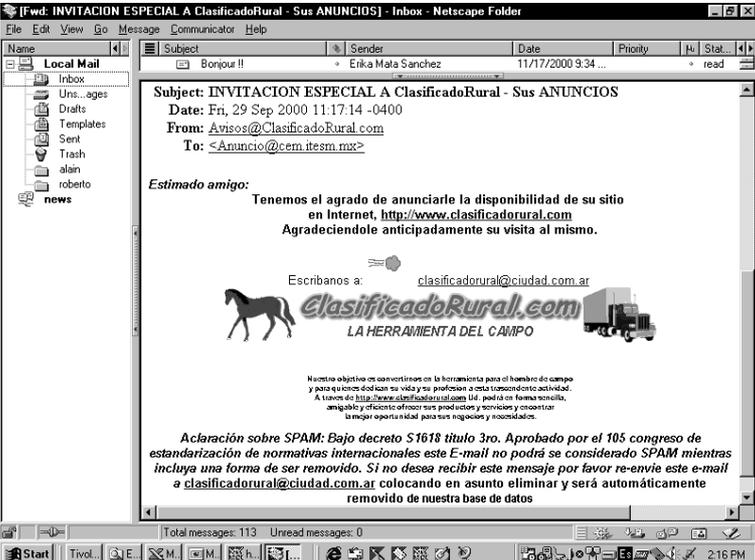
- Intento de entregar un mensaje, a través de Internet, a una persona que hubiera elegido de otra forma no
- Cada vez recibimos más deseados:
 - Ventas.
 - Insultos.
 - Bombardeos.
 - Pornografía
 - Hoax

Lámina 56



Ejemplo SPAM





Subject: INVITACION ESPECIAL A ClasificadoRural - Sus ANUNCIOS
Date: Fri, 29 Sep 2000 11:17:14 -0400
From: Avisos@ClasificadoRural.com
To: <Anuncio@cem.itemex.mx>

Estimado amigo:

Tenemos el agrado de anunciarle la disponibilidad de su sitio en Internet, <http://www.clasificadorural.com>
 Agradeciendole anticipadamente su visita al mismo.

Escribanos a: clasificadorural@ciudad.com.ar

 **ClasificadoRural.com** 
 LA HERRAMIENTA DEL CAMPO

Nuestro objetivo es convertirse en la herramienta para el hombre de campo y para quienes dedican su vida y su profesión a esta trascendente actividad. A través de <http://www.clasificadorural.com> Ud. podrá en forma sencilla, amigable y eficiente ofrecer sus productos y servicios y conocer la mejor oferta actual para sus intereses y necesidades.

Aclaración sobre SPAM: Bajo decreto S1618 título 3ro. Aprobado por el 105 congreso de estandarización de normativas internacionales este E-mail no podrá ser considerado SPAM mientras incluya una forma de ser removido. Si no desea recibir este mensaje por favor re-envíe este e-mail a clasificadorural@ciudad.com.ar colocando en asunto eliminar y será automáticamente removido de nuestra base de datos

Lámina 57 Dr. Roberto Gómez C.



¿Qué hacer con los hoaxes/spams?



- No redireccionar mensajes de este tipo.
 - sistema correo puede colapsar debido al redireccionamiento de este tipo de mensajes
- Los corporativos pueden confrontar este tipo de problemas, con un políticas del estilo:
 - usuarios finales no deben difundir alertas de viurs
 - cualquier informe de virus se debe enviar al departamento de sistemas de información

Lámina 58 Dr. Roberto Gómez C.



Ingeniería Social.





Es una de las formas más comunes para penetrar sistemas de “alta seguridad”.

- Uso de trucos psicologicos, por parte de un atacante externo, sobre usuarios legitimos de un sistema para obtener información (usernames y passwords) necesaria para acceder a un sistema.
- Se basa en ataques como: usurpación de identidad, pepena, inocencia de la gente, relaciones humanas, etc.



Lámina 59 Dr. Roberto G



Ejemplos Ingeniería Social





Cuidate de los hackers con piel de oveia

Empleados de importantes empresas mexicanas revelan sin objeción sus passwords, arriesgando la integridad de los sistemas de las compañías

Cambio de password
"¿Hola? ¿Sistemas? Soy Juan Pérez, de contabilidad. Ope, perdi mi password, ¿no podrías cambiarlo? Gracias. Sí, que el password nuevo sea..."

Por teléfono
¿Juan Pérez? Hola, soy Pedro López, de sistemas; tuvimos un problema con tu cuenta, parece que se corrompió el archivo de passwords. ¿Te pudiste conectar bien hoy? Ajá, perfecto. A ver, tu nombre de usuario es ¿perez, verdad? ¿Y tu password es perez01? ¿No? Ah, ese es el problema, ¿me puedes decir tu password?

Correo electrónico
De: soporte@correo.com
Para: jperez@correo.com
Estimado señor Pérez:
Lamentamos informarle que su cuenta de correo presenta un problema. Para realizar una revisión, requerimos que nos responda a este mensaje, enviando su nombre de usuario y su password. La revisión es gratuita, y en menos de 24 horas podremos arreglar el problema. Agradecemos la atención prestada a la presente".

IRC y mensajería instantánea
ATENCIÓN: Has sido infectado con un virus que permite que los hackers se metan en tu máquina y lean tus archivos, etc. Te sugiero que bajes este archivo y limpies tu máquina. El archivo está en...

Aclaración: Los nombres de usuario y passwords obtenidos vía telefónica no se escribieron en ninguna parte, por lo que Grupo Reforma no guarda registro de ellos.



Medidas a tomar

- Verificar la identidad de la persona con la que estamos conversando.
- Verificar la información transmitida con las fuentes
- Reportar cualquier anomalía

Lámina 61 Dr. Roberto Gómez C.



Graffiti

- Consiste en susbtituir páginas de un organismo por otras.
- El objetivo es dañar la reputación de la empresa
- Este tipo de ataques no tiene un periodo de duración grande

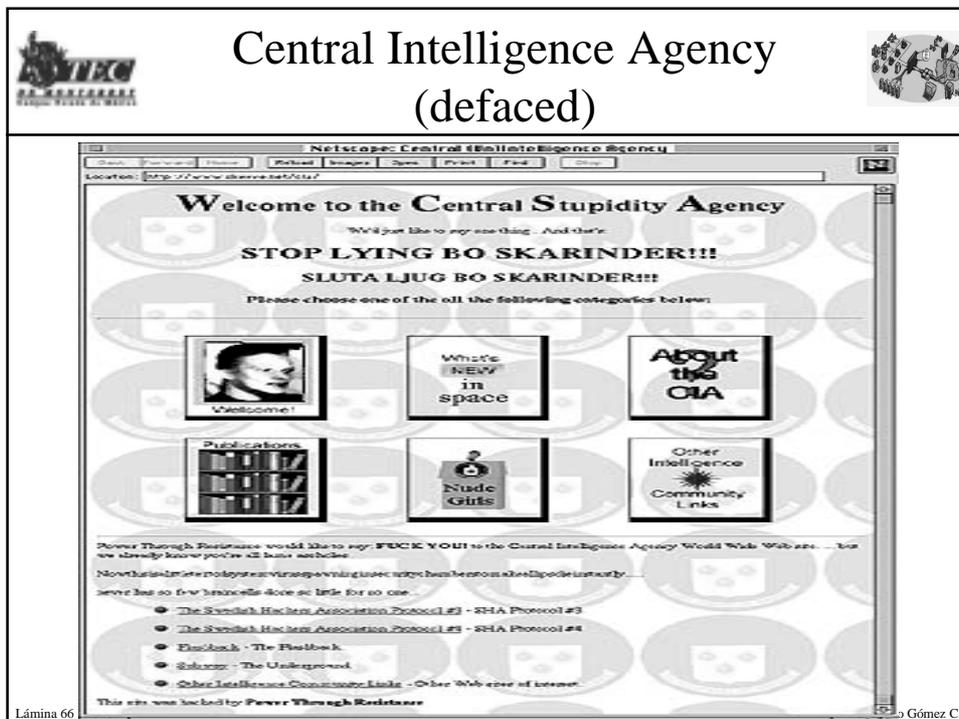
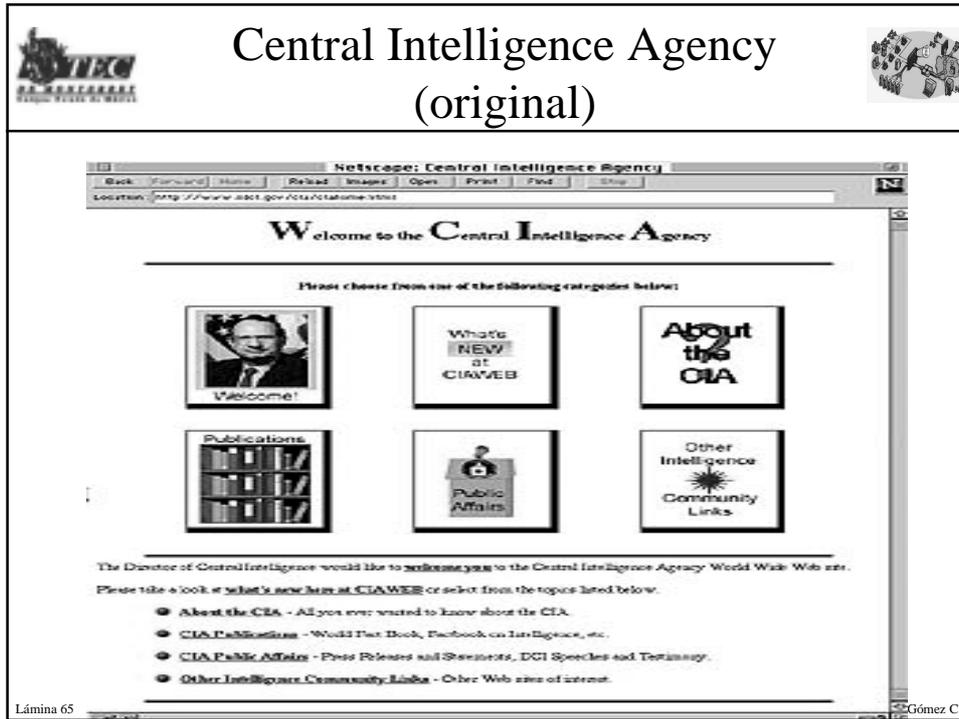
Lámina 62 Dr. Roberto Gómez C.

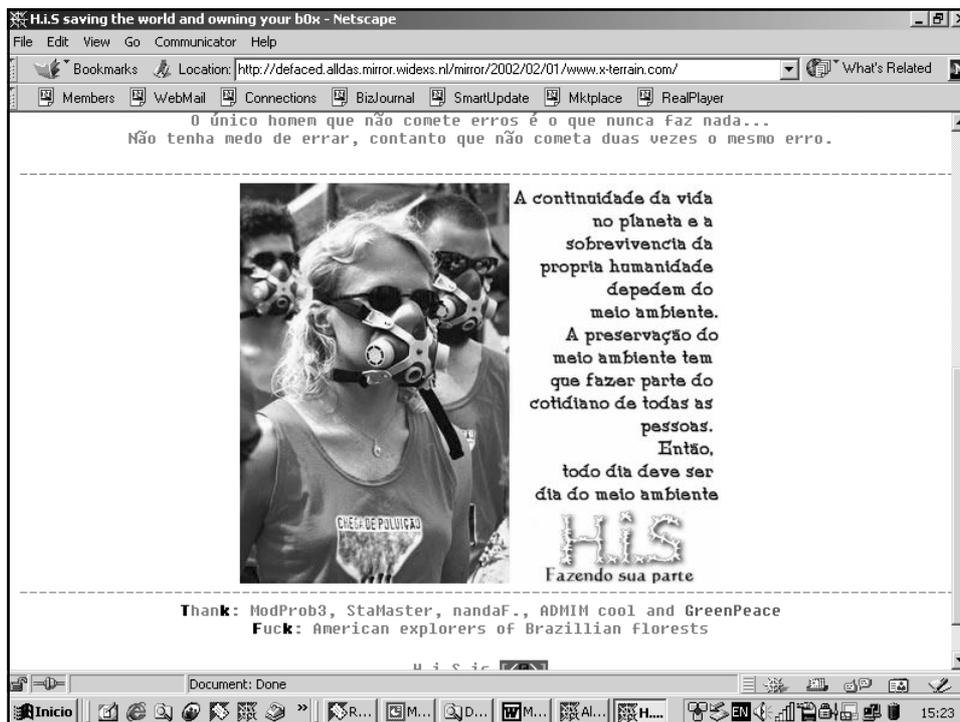
Partido laboral (original)

Lámina 63 Dr. Roberto Gómez C.

Partido Laboral (defaced)

Lámina 64 Dr. Roberto Gómez C.







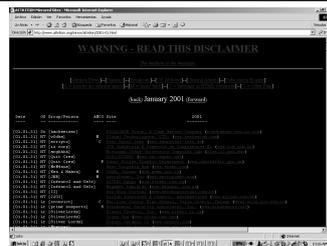
Defaced pages



- Primero fue attrition
 – <http://www.attrition.org>

- Después fue alldas
 – <http://defaced.alldas.de/>

- Ahora es:
 – <http://www.zone-h.org/defacements/onhold>



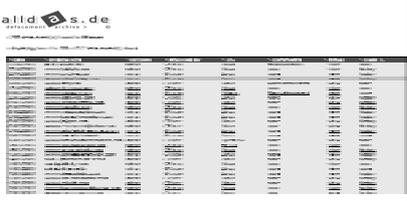
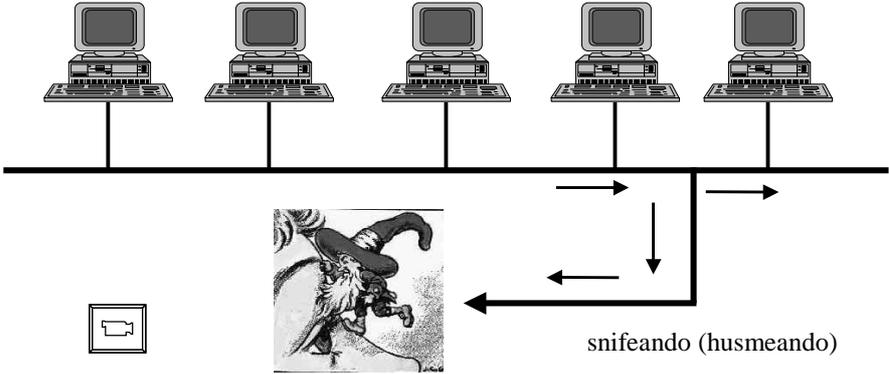


Lámina 68
Dr. Roberto Gómez C.

 **Sniffers** 

¿Cómo se comunican dos computadoras en una red local?



computadora en modo promiscuo

snifeando (husmeando)

Lámina 69 Dr. Roberto Gómez C.

 **¿Y como me protejo de los sniffers?** 

- Programas de detección sniffers
 - detección muy pobre
- Redes switcheadas
 - sniffers activos
- Encriptación
 - IPSec
 - SSL
 - SSH

Lámina 70 Dr. Roberto Gómez C.



Métodos Criptográficos



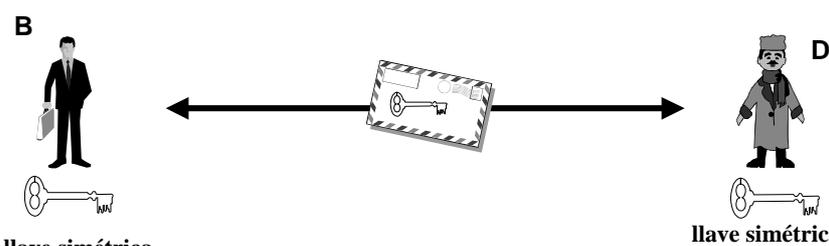
- Métodos simétricos
 - llave encriptado coincide con la de descifrado
 - la llave tiene que permanecer secreta
 - emisor y receptor se han puesto de acuerdo previamente o existe un centro de distribución de llaves
 - son propios de la criptografía clásica o criptografía de llave secreta
- Métodos asimétrico
 - llave encriptado es diferente a la de decriptado
 - corresponden a la criptografía de la llave pública, introducida por Diffie y Hellman en 1976

Lámina 71
Dr. Roberto Gómez C.



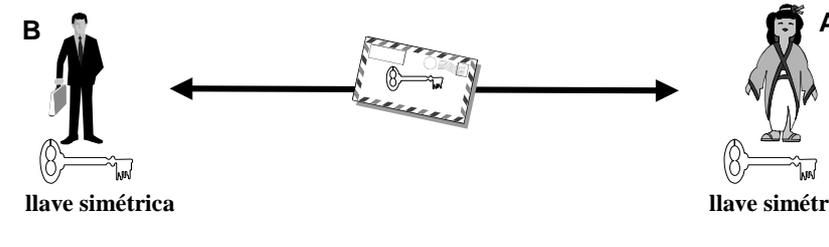
Esquema general encriptación llave secreta





B   **llave simétrica**

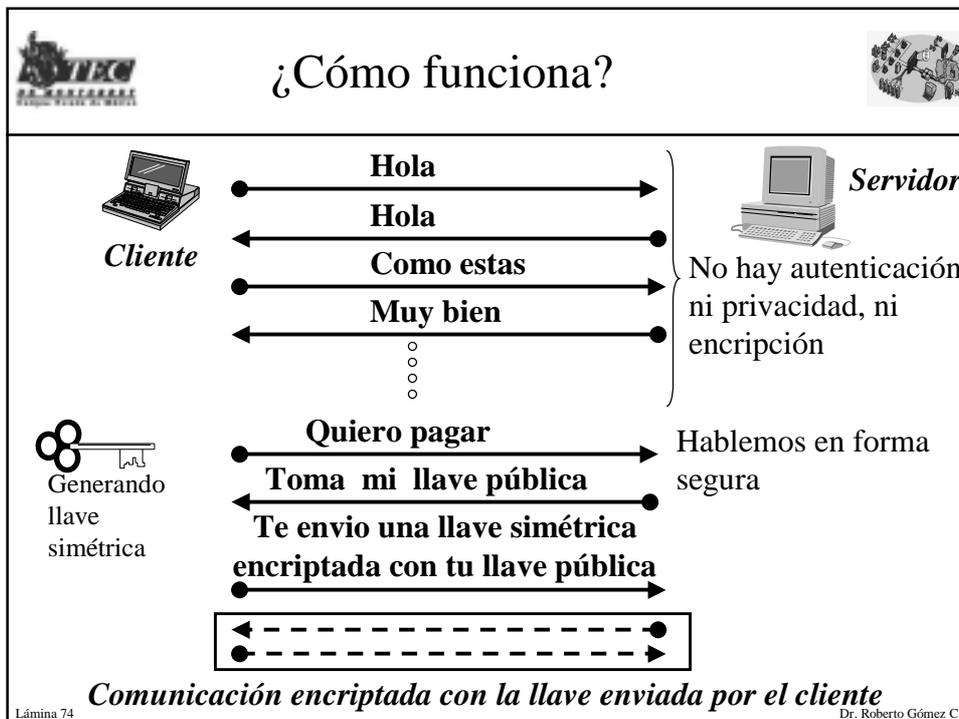
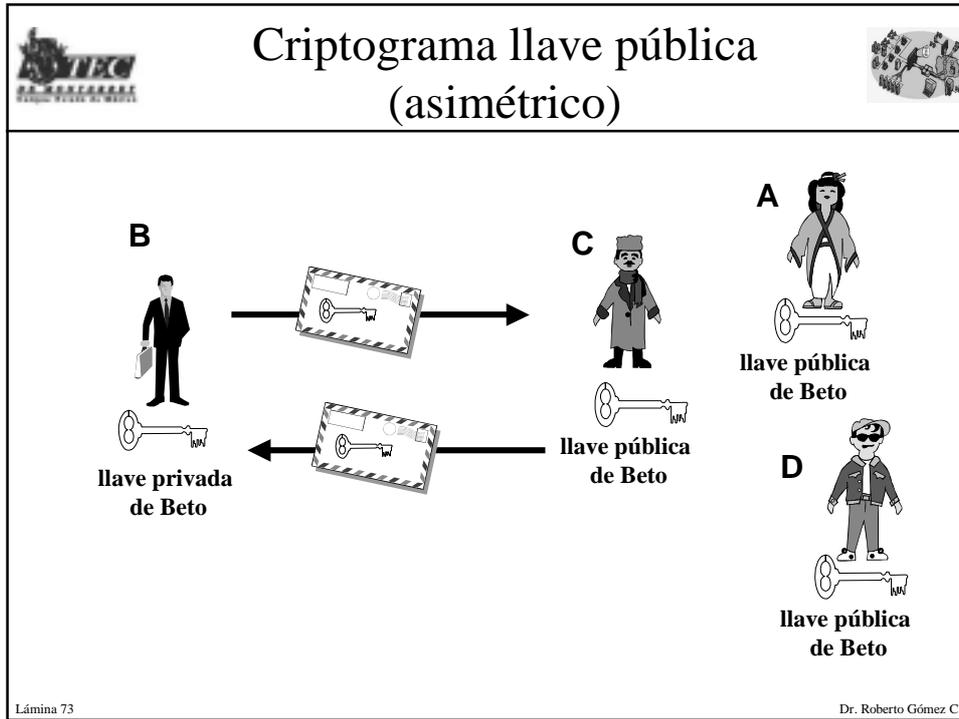
D   **llave simétrica**



B   **llave simétrica**

A   **llave simétrica**

Lámina 72
Dr. Roberto Gómez C.





Protocolos transmisión encriptados



Amazon.com: buying info: Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edit - Netscape

Location: amazon.com/exec/obidos/ASIN/0471117099/qid=97114521/sr=2/102-5972864-6451304

amazon.com

SEARCH **Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition** by Bruce Schneier

Book Information: Explore this book, buying info, table of contents, Amazon.com, articles, editorial reviews, customer reviews

Price: List Price: \$64.95, Our Price: \$43.96, You Save: \$10.99 (20%)

Availability: Usually ships within 24 hours.

READY TO BUY? Add to Shopping Cart, Shopping with us is 100% safe. Guaranteed.

Lámina 75Dr. Roberto Gómez C.



Protocolos transmisión encriptados



Amazon.com Checkout: Sign In - Netscape

Location: https://www.amazon.com/exec/obidos/checkout-sign-in/103-4763853-4624626

amazon.com

WELCOME ADDRESS ITEMS WRAP SHIP PAY CONFIRM

*** Please fix the areas indicated below. ***

*** You didn't provide an e-mail address. We'll need it to communicate with you about the status of your orders. And, when you visit us again, you'll use it to access your account. ***

Ordering online is easy. We'll walk you through the process, step by step.

Enter your e-mail address:

I am a new customer. (You'll create a password later.)

I am a returning customer, and my password is:

Forgot your password?

Sign in using our secure server

Amazon.com Safe Shopping Guarantee: We guarantee that every transaction you make at Amazon.com will be 100% safe. This means you pay nothing if unauthorized charges are made to your credit card as a result of shopping at Amazon.com.

Lámina 76Dr. Roberto Gómez C.



Esteganografía??



- Area similar a la de criptología.
- Viene del griego stegos (ocultar).
- Conjunto de técnicas que nos permiten ocultar o camuflar cualquier tipo de datos.
- La información puede esconderse de cualquier forma
 - esconder documentos electrónicos dentro de imagenes.
 - aprovechar campos no usados de los paquetes de protocolos de redes.

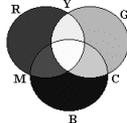
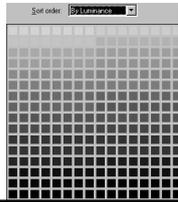



Lámina 77



Spoofing



cliente



servidor

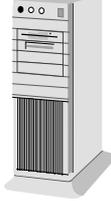





Lámina 78 Dr. Roberto Gómez C.



Los certificados



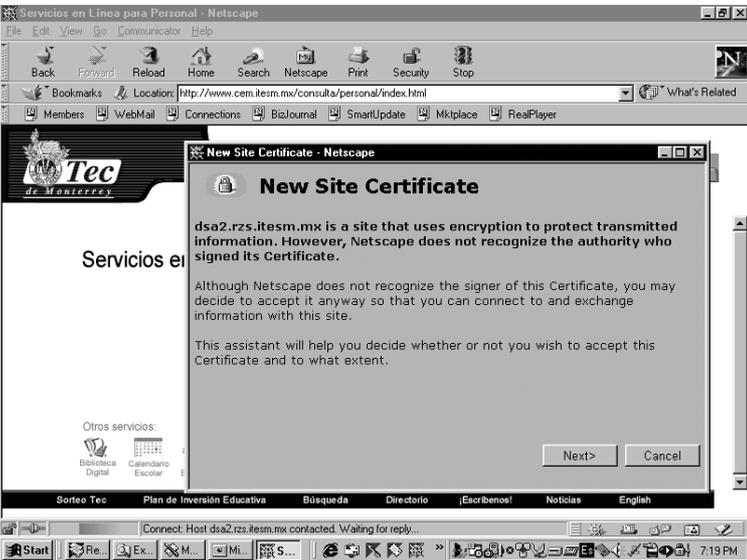


Lámina 79
Dr. Roberto Gómez C.

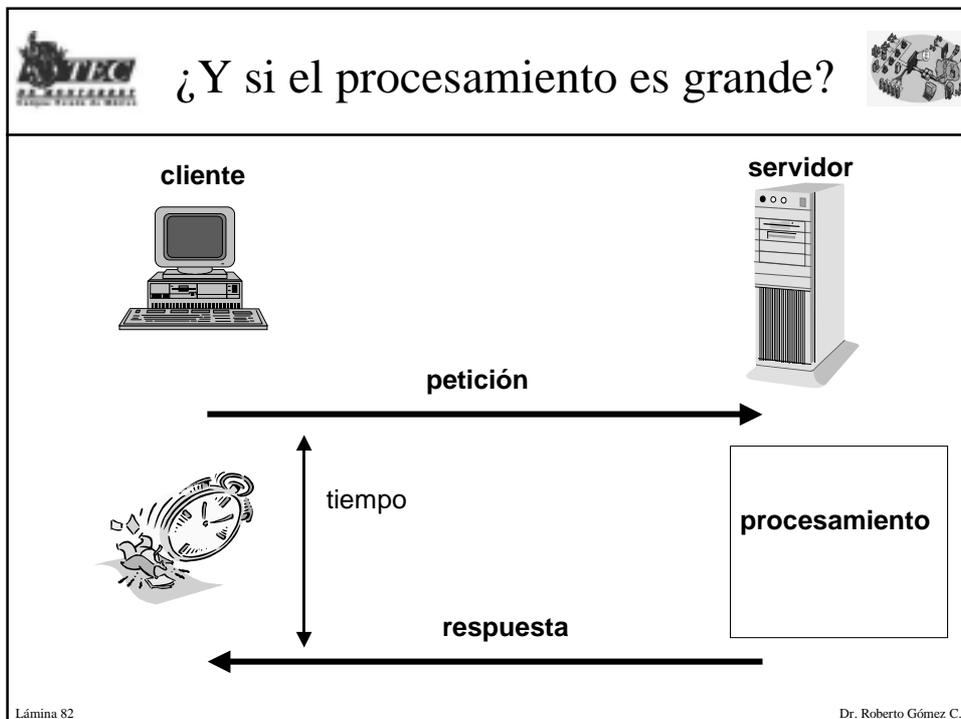
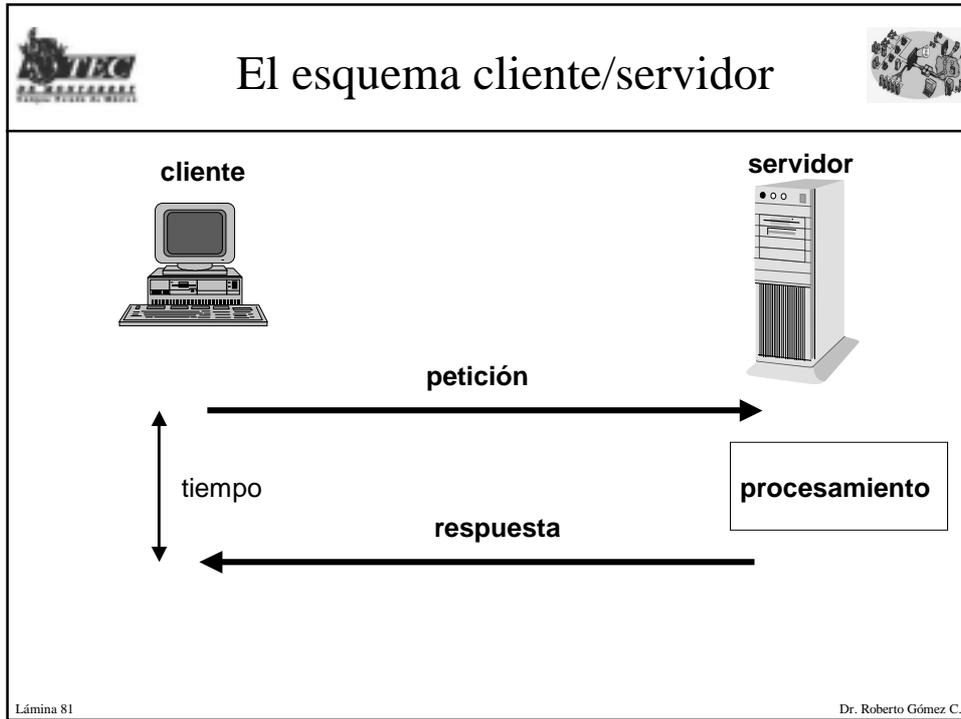


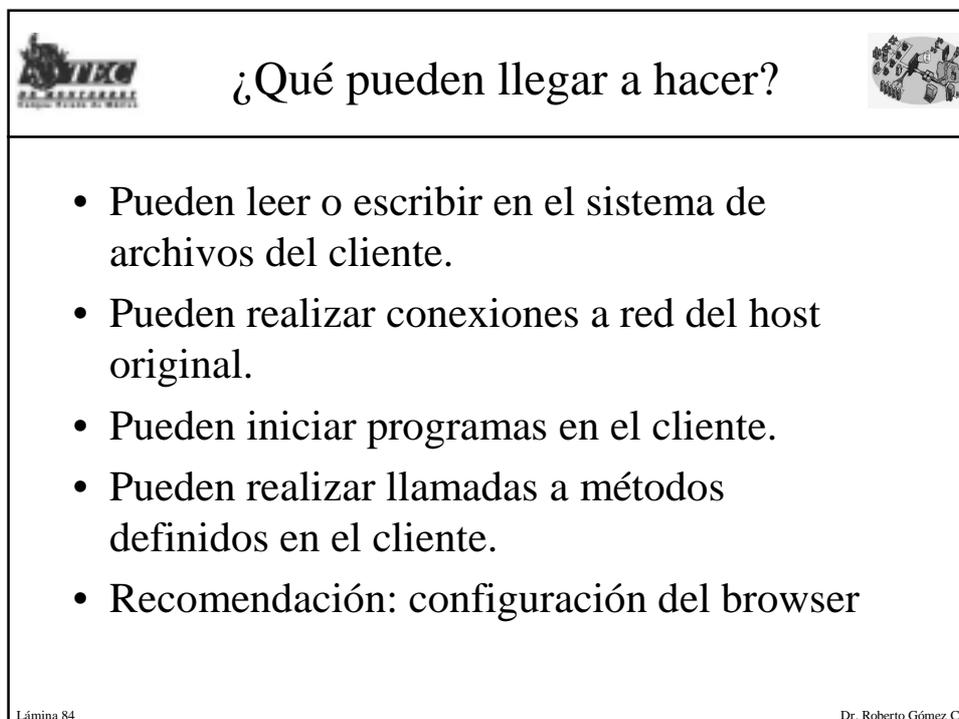
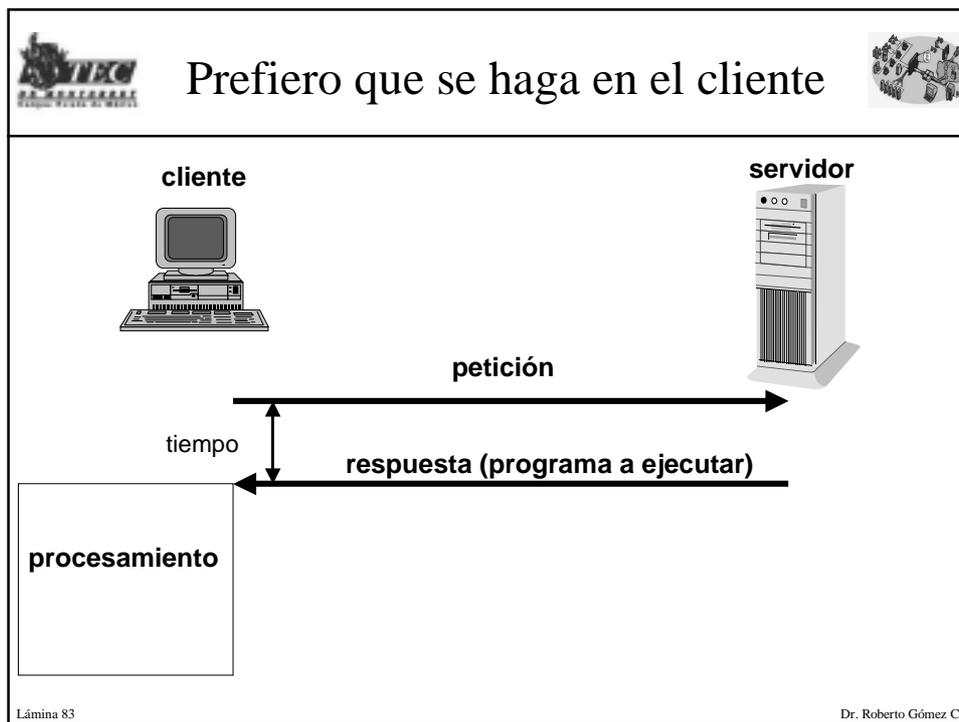
El código móvil



- Los *browsers* son la herramienta que usan los usuarios para navegar por internet.
- Dos elementos fundamentales en internet:
 - cliente: el que realiza la búsqueda de información
 - servidor: el que coloca la información en algún servidor
- Cuando la aplicación en el servidor es muy pesada
 - preferible realizar el trabajo en el cliente
 - desempeño (tiempo respuesta) mejora bastante
- Dos tecnologías:
 - active x
 - los applets de java

Lámina 80
Dr. Roberto Gómez C.







Las cookies



- Es información que un sitio Web escribe en el disco duro, de tal forma que pueda recordar algo acerca del usuario tiempo después.
- Tecnicamente:
 - información para uso futuro almacenada por el servidor en el cliente
- Su ubicación depende del browser.
- Permite al servidor almacenar información acerca del usuario en su propia máquina.
- Principal problema: privacidad

Lámina 85Dr. Roberto Gómez C.



Configuración Microsoft Internet Explorer



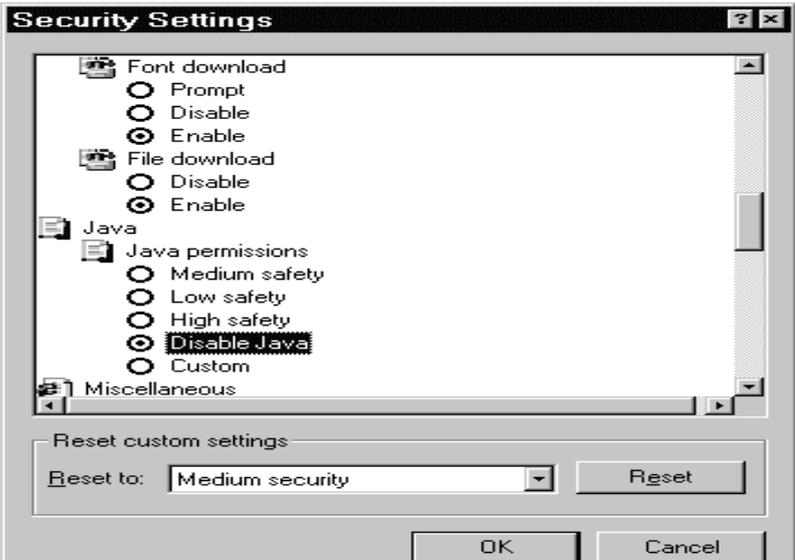


Lámina 86Dr. Roberto Gómez C.



Protegiendo el perímetro



- ¿Quién quiere entrar?
 - autenticación
- ¿A donde puede ir?
 - control de acceso
- Rechazar lo no deseado
 - filtros y firewalls
- ¿Qué quiere hacer adentro?
 - proxies
- Cerrando las puertas traseras
 - cerrando los servicios
- Contratando vigilantes
 - los IDS

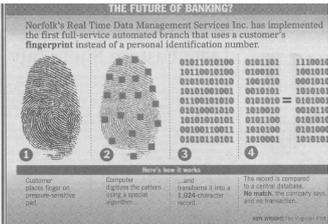
Lámina 87
Dr. Roberto Gómez C.



Autenticación



- La autenticación se refiere a demostrar la identidad de las entidades involucradas en una comunicación.
- Evita que alguien tome la identidad de otro. Generalmente toma dos formas.



THE FUTURE OF BANKING?
Norfolk's Real Time Data Management Services Inc. has implemented the first full-service automated branch that uses a customer's fingerprint instead of a personal identification number.



ERIKA IVETTE LOPEZ PADILLA
451385
DOCTORADO

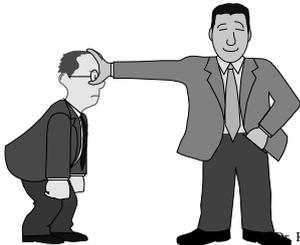
Lámina 88
Dr. Roberto Gómez C.



Control de acceso



- Permite definir quién puede tener acceso a ciertos recursos, dependiendo de los privilegios o atributos que posea.
- Permite proteger los recursos del sistema contra el uso no autorizado.
- Se aplica a los usuarios y procesos que ya han sido autenticados.



Roberto Gómez C.

Lámina 89



Filtrando la información



- Examinar los paquetes que van hacia afuera o vienen entrando a la red.
- Se definen reglas que permiten dejar pasar el paquete o descartarlo.
- Las reglas se fijan en función de las direcciones, protocolos y puertos, básicamente.
- Programación del ruteador para filtrar paquetes.

Lámina 90

Dr. Roberto Gómez C.

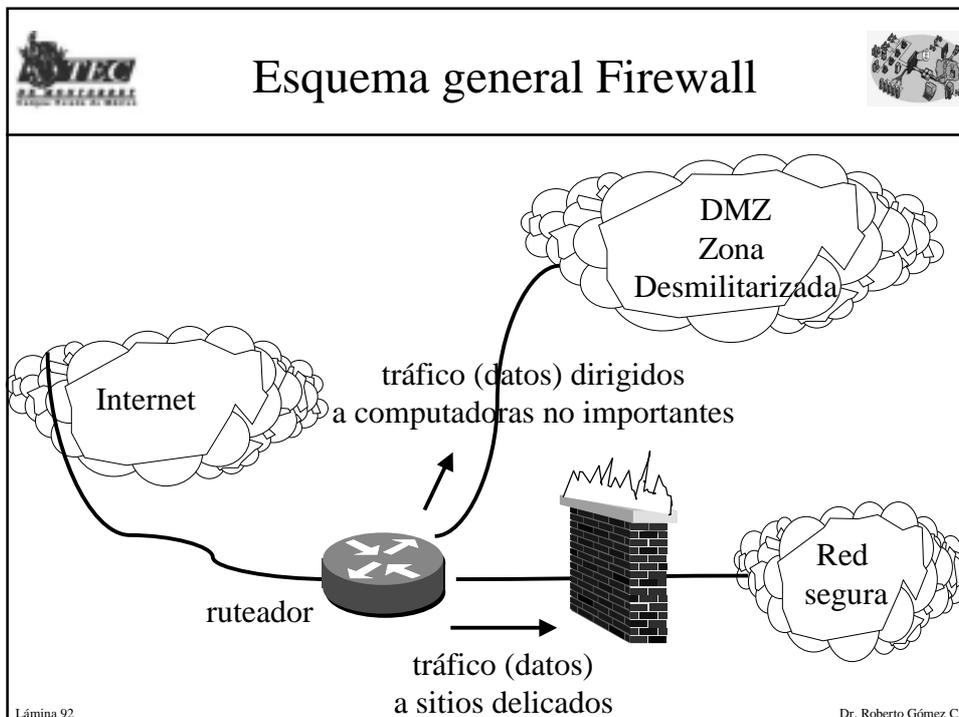
 

¿Qué es un firewall?

Podemos definirlo como una colección de componentes colocados entre dos redes, que en conjunto poseen las siguientes propiedades:

- Todo el tráfico de afuera hacia adentro, y viceversa, debe pasar por el firewall.
- Sólo tráfico autorizado, como establecido previamente en las políticas de la organización, puede pasar a través del firewall.

Lámina 91 Dr. Roberto Gómez C.





Ejemplo reglas de acceso



Demonstration - FireWall-1 Security Policy

File Edit View Manage Policy Window Help

Security Policy | Address Translation | Generate an alert for suspicious activity

No.	Source	Destination	Service	Action	Track	Install C
1	Any	Web_Server	http	accept	Short	Gatew
2	Local_Net	Any	Any	accept	Short	Gatew
3	Any	Any	Any	drop	Alert	Gatew

With three simple rules, you have implemented access control for your network.

MAIN MENU EXIT

Lámina 93 Gómez C.

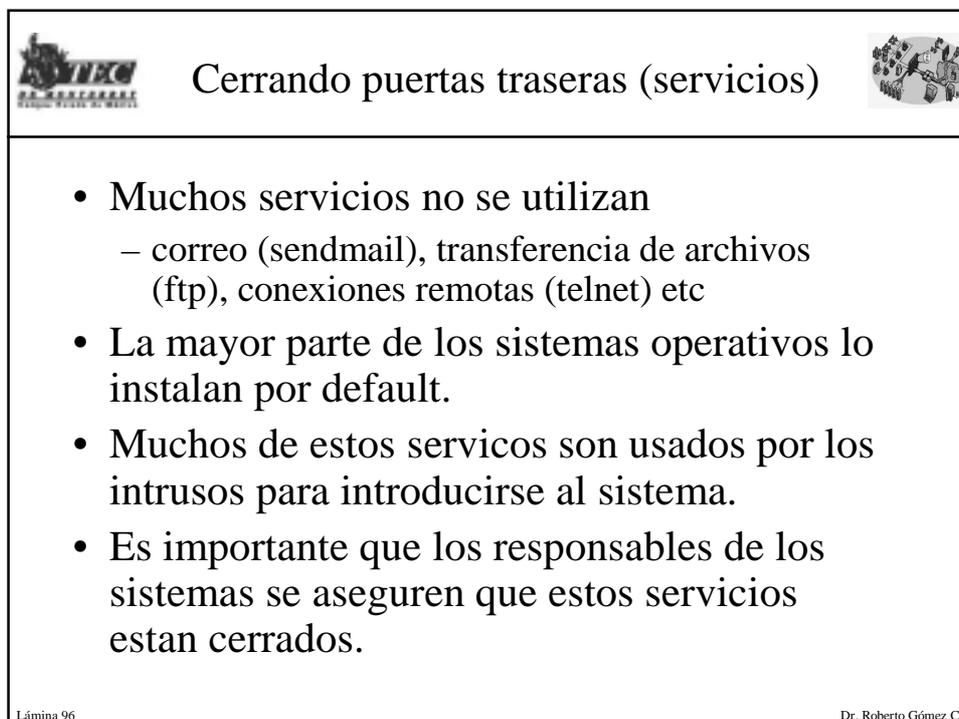
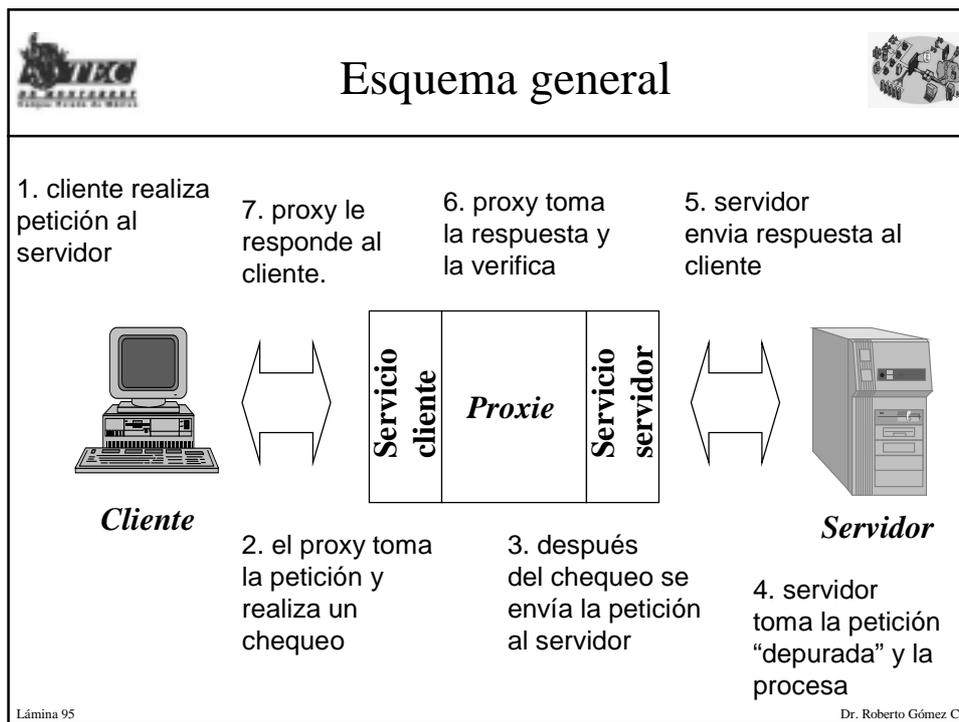


¿Qué quiere hacer adentro: proxies?



- Es un intermediarios entre cliente y servidor.
- Un servidor proxy realiza una conexión con un servidor de alguna aplicación, de la parte de un cliente.
- Desde el punto de vista del cliente, hace la conexión con el proxy, pensando que ésta es con el servidor.

Lámina 94 Dr. Roberto Gómez C.



Cerrando puertas traseras (conexiones)

- Hoy en día la mayor parte de las computadoras cuentan con una tarjeta fax/modem.
- Algunos usuarios se pueden conectar a internet sin pasar por los perímetros definidos.
- Es importante que el usuario este consiente de que esto puede poner en peligro la seguridad.
 - políticas de seguridad
- Los encargados de seguridad deben supervisar que lo anterior no sea posible.

Lámina 97

Dr. Roberto Gómez C.

¿Y si contratamos vigilantes?

IDS

Lámina 98

Dr. Roberto Gómez C.



IDS



- Intrusion Detection Systems.
- Software específicamente diseñado para reconocer los patrones de un comportamiento no deseado.
- Pueden proporcionar un medio para registrar intentos, detener intentos en progreso y cerrar hoyos que coincidan con algunos patrones de ataques, bloqueando la secuencia para que ya no ocurra.
- Busca automatizar la detección y eliminación de intrusos.

Lámina 99
Dr. Roberto Gómez C.



Integrando todo



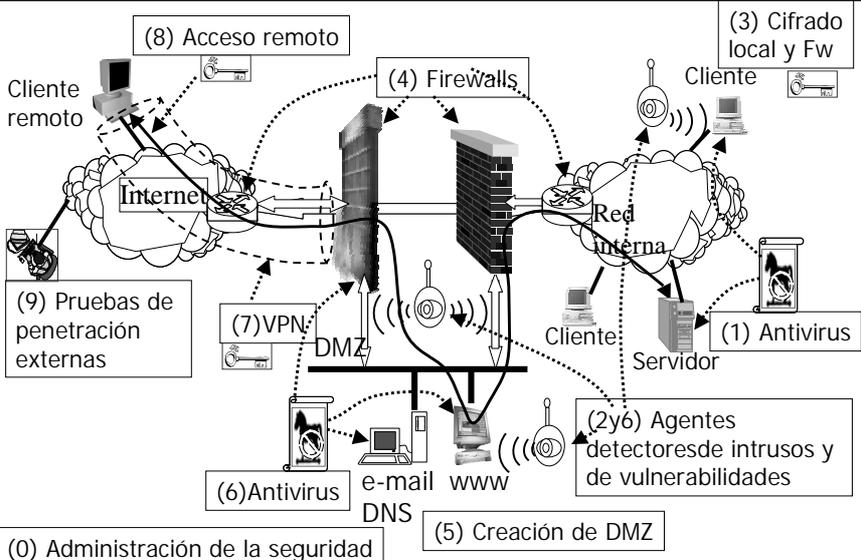


Lámina 100
Dr. Roberto Gómez C.



¿Y las redes inalámbricas?



- El medio de transmisión más utilizado es el cable, pero para el caso de una red inalámbrica ese medio físico es el aire.
- WLAN: Siglas en inglés de Wireless Local Area Network.

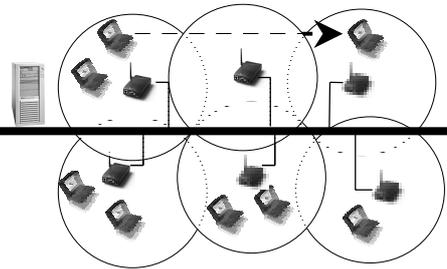





Lámina 101
Dr. Roberto Gómez C.



Riesgos de una WLAN



- Monitoreo de tráfico inalámbrico
 - datos de usuarios
 - localización de usuarios
 - identidad de usuarios
 - análisis de tráfico
- Acceso no autorizado a una red a través de un enlace inalámbrico
 - persona pasaendose en una bicicleta
- Corrupción de servicios inalámbricos
- Descubrimiento
 - wardriving




Lámina 102
Dr. Roberto Gómez C.



Consejos



- Habilitar WAP
 - si no es posible habilitar WEP con llave de 104 bits (128 bits)
- Conectar los Access Points en una zona de seguridad “pública” (ó de bajo riesgo) posiblemente en una DMZ, jamás conectar la red inalámbrica a la red alámbrica de manera transparente.
- Implementar un segundo nivel de seguridad:
 - VPN
 - IPSEC
 - SSL
 - SSH

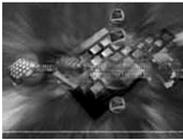


Lámina 103 Dr. Roberto Gómez C.



Conclusiones y Recomendaciones



- 100% de seguridad **no existe!!!!**
- Seguridad a través de educación.
- Programas de seguridad integral.
- Contar con una caja de herramientas
- Creación de departamentos o divisiones especializados en seguridad computacional.
- Leer, leer, leer...
- Estar al segundo en cuestiones de seguridad.
- Los ataques tienen estructura, por lo tanto se pueden detectar en su mayoría.

Lámina 104 Dr. Roberto Gómez C.



Páginas para mayor información

- Security Focus: www.securityfocus.com
- CERT : www.cert.org
- SANS: www.sans.org
- Securiteam: www.securiteam.com
- Snort: www.snort.com
- ISS: www.iss.net
- Página seguridad RSA: www.rsasecurity.com
- Cypherpunks: www.vnunet.com
- Bruce Schneider: www.counterpane.com
- Security Space: www.securityspace.com
- Ernst&Young: www.esecurityonline.com

Lámina 105 Dr. Roberto Gómez C.



Gracias por su atención

Panorama general de los principales ataques y defensas de un sistema informático

Roberto Gómez
rogomez@itesm.mx
<http://webdia.cem.itesm.mx/ac/rogomez>

Lámina 106 Dr. Roberto Gómez C.