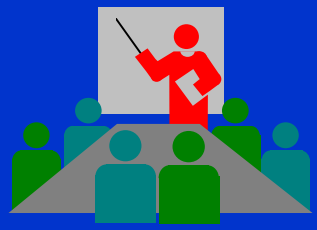
# Capítulo 4
# Calidad de Información y Programas Malignos

## Seguridad Informática y Criptografía

Material Docente de
Libre Distribución

Ultima actualización del archivo: 01/03/06
Este archivo tiene: 27 diapositivas

Dr. Jorge Ramió Aguirre
Universidad Politécnica de Madrid

# ¿Qué es la información?

- Bajo el punto de vista de la ingeniería:
  - Estudio de las características y estadísticas del lenguaje que nos permitirá su análisis desde un enfoque matemático, científico y técnico.
- Bajo el punto de vista de la empresa:
  - Conjunto de datos propios que se gestionan y mensajes que se intercambian personas y/o máquinas dentro de una organización.

# Teoría de la información de Shannon

- El estudio hecho por Claude Shannon en años posteriores a la 2ª Guerra Mundial ha permitido, entre otras cosas:
  - Cuantificar la cantidad de información.
  - Medir la entropía de la información.
  - Definir un sistema con secreto perfecto.
  - Calcular la redundancia y la ratio del lenguaje.
  - Encontrar la distancia de unicidad.

  Todo el estudio de Shannon está orientado a criptosistemas clásicos que cifran letras, que tienen escaso interés en este libro. No obstante, en un capítulo posterior se verán estos sistemas con un mínimo detalle pues permiten analizar con cierta facilidad sistemas con secreto perfecto.

http://es.wikipedia.org/wiki/Claude_Shannon

# La información en la empresa

- Se entenderá como:
  - Todo el conjunto de datos y ficheros de la empresa.
  - Todos los mensajes intercambiados.
  - Todo el historial de clientes y proveedores.
  - Todo el historial de productos.
  - En definitiva, el *know-how* de la organización.
- Si esta información se pierde o deteriora, le será muy difícil a la empresa recuperarse y seguir siendo competitiva. Por este motivo, es vital que se implanten unas políticas de seguridad y que, además, se haga un seguimiento de ellas.

# Importancia de la información

- El éxito de una empresa dependerá de la calidad de la información que genera y gestiona. Así, una empresa tendrá una información de calidad si ésta posee, entre otras características, las de confidencialidad, de integridad y de disponibilidad.
- La implantación de una política y medidas de seguridad informática en la empresa comienza a tenerse en cuenta sólo a finales de la década pasada. En este nuevo siglo, es un factor estratégico en el desarrollo y éxito de la misma. Después de atentados terroristas, incendios, huracanes y diversas amenazas, muchas empresas han desaparecido por no haber sido capaces de recuperarse tras haber perdido toda su información.

# Vulnerabilidad de la información

- La información (datos) se verá afectada por muchos factores, incidiendo básicamente en los aspectos de confidencialidad, integridad y disponibilidad de la misma.

Un empleado descontento...

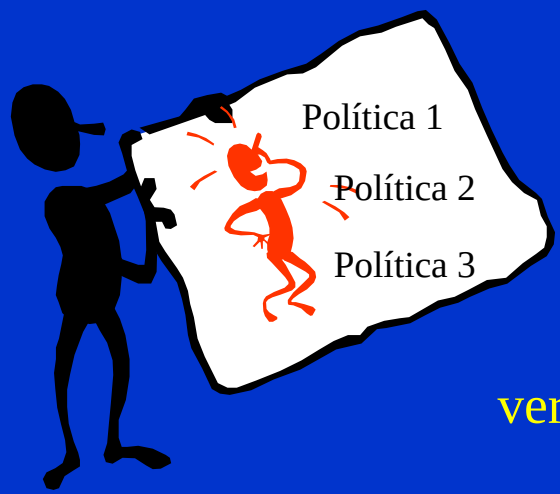
- Desde el punto de vista de la empresa, uno de los problemas más importantes puede ser el que está relacionado con el delito o crimen informático, bien por factores externos o internos. Habrá que estar muy atentos al factor humano interno.

# Hay que implantar políticas de seguridad

El tratamiento y vulnerabilidad de la información se verá influida por otros temas, como por ejemplo los aspectos legales vigentes. Además, las empresas cada día dependen más de sus comunicaciones y de su trabajo en red, lo que aumenta su inseguridad.

Solución ?

La solución parece muy sencilla: crear y aplicar políticas de seguridad...




... Y solamente ahora comienza a tomarse verdaderamente en serio.

http://www.rediris.es/cert/doc/docu_rediris/poliseg.es.html

# Acciones contra los datos

- Una persona no autorizada podría:
  - Clasificar y desclasificar los datos.
  - Filtrar información.
  - Alterar la información.
  - Borrar la información.
  - Usurpar datos.
  - Hojear información clasificada.
  - Deducir datos confidenciales.

Por lo tanto, la protección de datos resulta obvia

# Copias de seguridad: backup

- La medida más elemental para la protección de los datos es determinar una buena política de copias de seguridad o backups:
  - Copia de seguridad completa
    - Todos los datos (la primera vez).
  - Copias de seguridad incrementales
    - Sólo se copian los ficheros creados o modificados desde el último backup.
  - Elaboración de un plan de backup en función del volumen de información generada
    - Tipo de copias, ciclo de esta operación, etiquetado correcto.
    - Diarias, semanales, mensuales: creación de tablas.
  - Establecer quién, cómo y dónde se guardan esos datos.

http://www.criptored.upm.es/guiateoria/gt_m001l.htm

# Hackers, crakers, script kiddies...

- Hacker:
  - Definición inicial de los ingenieros del MIT que hacían alardes de sus conocimientos en informática.
  - Entre muchas clasificaciones están las de White Hat (generalmente no delictivos), Blak Hat (generalmente es delictivo) y Grey Hat (reconvertidos por la empresa).
- Cracker:
  - Persona que intenta de forma ilegal romper la seguridad de un sistema por diversión o interés.
- Script kiddie:
  - Un inexperto, normalmente un adolescente, que usará programas que se descarga de Internet para atacar sistemas.

Más información en:

http://www.umanizales.edu.co/encuentrohackers/tiposh.htm

# Puntos vulnerables en la red

Las empresas relacionadas con las Nuevas Tecnologías de la Información NTIs hacen uso de varias técnicas y herramientas de redes para el intercambio de datos:

- Transferencia de ficheros (ftp)
- Transferencia de datos e información a través de Internet (http)
- Conexiones remotas a máquinas y servidores (telnet)

Todo esto presentará importantes riesgos de ataques por parte de delincuentes informáticos, pero ...

# ¿Dónde está el verdadero enemigo?

Por muy organizados que puedan estar estos grupos de delincuentes, primero que nada hay que ponerse en el lugar que nos corresponde y no caer en la paranoia.

Además, debemos pensar que el peor enemigo puede estar dentro de casa. Según estadísticas fiables, cerca del 80% de las amenazas de seguridad provienen de la propia organización.

La solución sigue siendo la misma: la puesta en marcha de una adecuada política de seguridad en la empresa.

# Algunos ataques y delitos informáticos

Son acciones que vulneran la confidencialidad, integridad y disponibilidad de la información.

– Ataques a un sistema informático:

- Fraude
- Malversación
- Robo
- Sabotaje
- Espionaje
- Chantaje
- Revelación
- Mascarada
- Virus
- Gusanos
- C. de Troya
- Spam

http://www.delitosinformaticos.com/delitos/

# Fraude y sabotaje

## Fraude

Acto deliberado de manipulación de datos perjudicando a una persona física o jurídica que sufre de esta forma una pérdida económica. El autor del delito logra de esta forma un beneficio normalmente económico.

## Sabotaje

Acción con la que se desea perjudicar a una empresa entorpeciendo deliberadamente su marcha, averiando sus equipos, herramientas, programas, etc. El autor no logra normalmente con ello beneficios económicos pero pone en jaque mate a la organización.

# Chantaje y mascarada

## Chantaje

Acción que consiste en exigir una cantidad de dinero a cambio de no dar a conocer información privilegiada o confidencial y que puede afectar gravemente a la empresa, por lo general a su imagen corporativa.

## Mascarada

Utilización de una clave por una persona no autorizada y que accede al sistema suplantando una identidad. De esta forma el intruso se hace dueño de la información, documentación y datos de otros usuarios con los que puede, por ejemplo, chantajear a la organización.

# Virus y gusanos

## Virus

Código diseñado para introducirse en un programa, modificar o destruir datos. Se copia automáticamente a otros programas para seguir su ciclo de vida. Es común que se expanda a través de plantillas, las macros de aplicaciones y archivos ejecutables.

## Gusanos

Virus que se activa y transmite a través de la red. Tiene como finalidad su multiplicación hasta agotar el espacio en disco o RAM. Suele ser uno de los ataques más dañinos porque normalmente produce un colapso en la red como ya estamos acostumbrados.

# Caballos de Troya y spam

## Caballos de Troya

Virus que entra al ordenador y posteriormente actúa de forma similar a este hecho de la mitología griega. Así, parece ser una cosa o programa inofensivo cuando en realidad está haciendo otra y expandiéndose. Puede ser muy peligroso cuando es un programador de la propia empresa quien lo instala en un programa.

## Spam

El spam o correo no deseado, si bien no lo podemos considerar como un ataque propiamente dicho, lo cierto es que provoca hoy en día pérdidas muy importantes en empresas y muchos dolores de cabeza.

# Ataques y delitos recientes

Tres amenazas que se han incrementado en el año 2005:

Cartas nigerianas: correo electrónico que comenta la necesidad de sacar una gran cantidad de dinero de un país africano a través de un "cómplice" de otro país, justificando una persecución política.

Ingeniería social: correo electrónico en el que "se fuerza" al usuario a que abra un archivo adjunto que supuestamente le interesa o bien está muy relacionado con su trabajo, utilizando así el eslabón más débil de una cadena de seguridad como es el ser humano.

Phising: simulación, algunas veces perfecta, de una página Web de un banco solicitando el ingreso de claves secretas, con la excusa de la aplicación de nuevas políticas de seguridad de la entidad. Dentro del enlace a la noticia de Hispasec, se recomienda la visualización de los vídeos explicativos en flash con los altavoces del PC encendidos.

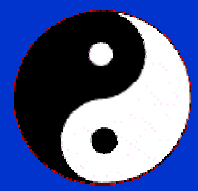
http://en.wikipedia.org/wiki/Phising

http://www.hispasec.com/unaaldia/2406

# Aparecerán nuevos ataques

En un futuro inmediato y en los próximos años aparecerán nuevos delitos y ataques a los sistemas informáticos y redes que, a fecha de hoy, no sabemos cómo serán ni a qué vulnerabilidad atacarán.

Este constante enfrentamiento entre el lado oscuro o el mal (conocido como el Yin) y el lado claro o el bien (el Yang), como muestra este símbolo propio de filosofías ancestrales, será inevitable en sistemas intercomunicados y abiertos como los actuales.



Las comunicaciones crecerán cada vez más hacia ese entorno abierto, como las actuales redes inalámbricas, con lo que irán apareciendo nuevas amenazas...

# Breve introducción a virus informáticos

- Las próximas diapositivas son sólo una breve y elemental introducción al tema de los virus informáticos, orientado además sólo al mundo de los PCs y del llamado entorno Windows. No pretende ser ni mucho menos un documento que trate los virus informáticos y programas malignos con la profundidad que debería hacerse y que este tema en realidad se merece.
- Se incluye este apartado precisamente en este capítulo como un factor más a tener en cuenta en cuanto a la calidad de la información que manejamos.
- Mucha gente cataloga a éste como un tema menor; sin embargo, dentro de las empresas es uno de los mayores problemas a los que se enfrentan los responsables de seguridad informática.

# Historia y tipos de virus

- Primer ejemplo: John von Neuman en 1949.
- Primer virus: M. Gouglas de Bell Laboratories crea el Core War en 1960.
- Primeros ataques a PCs entre 1985 y 1987:
  - Virus Jerusalem y Brain.
- Inofensivos (pelotas, letras que se mueven, etc.)
  - Sólo molestan y entorpecen el trabajo pero no destruyen información. Podrían residir en el PC.
- Malignos (Viernes 13, Blaster, Nimbda, Netsky, Klez, etc.)
  - Destruyen los datos y afectan a la integridad y la disponibilidad del sistema. Hay que eliminarnos.

Más información en:

http://alerta-antivirus.red.es/virus/ver_pag.html?tema=V

# Transmisión de virus y malware

- Se transmiten sólo mediante la ejecución de un programa. Esto es muy importante recordarlo.
- El correo electrónico por definición no puede contener virus al ser sólo texto. No obstante, muchas veces contienen archivos añadidos o bien los visualizadores ejecutan código en el cliente de correo del usuario y éstos pueden tener incluido un virus.
- No obstante hay que estar muy atentos pues ya a comienzos de 2006 hacen su aparición virus que se ejecutan desde la simple visualización de un gráfico jpg, gif, etc., usando para ello una vulnerabilidad conocida de procesamiento de WMF (Windows Meta File) que permite la ejecución de código arbitrario.

http://www.hispasec.com/unaaldia/2639

# Peligros del entorno Web

- El entorno web es mucho más peligroso. Un enlace puede lanzar un programa que se ejecute en el cliente y nos infecte o comprometa la máquina, dejándola abierta para otros ataques o bien dejarla como un zombie que colabore en otros ataques.
- Si se atreve y su sistema tiene AntiSpyware haga una prueba: busque en Google una página web porno supuestamente seria, navegue unos 10 minutos y luego al salir observe que dicho programa seguramente le avisará de varios programas spyware, más de algún dialer que se quiere instalar, etc. ☹
- Punto más crítico de la seguridad respecto a virus y accesos a Internet: usuario que confiado en la dirección del remitente o de un servidor, por curiosidad, engañado con la denominada ingeniería social, etc., ... abre archivos o entra a ese servidor.

# Tipos de ataque de un virus

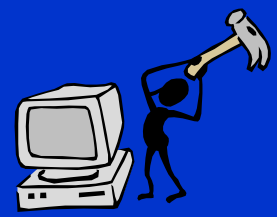
- Están aquellos que infectan a programas con extensión exe, com y sys, por ejemplo.
  - Residen en memoria al ejecutarse el huésped y de ahí se propagan a otros archivos.
- Y también aquellos que infectan el sistema y el sector de arranque y tablas de entrada (áreas determinadas del disco).
  - Se instalan directamente allí y por lo tanto residen en memoria.

# Algunas medidas básicas de prevención

- Proteger los discos extraíbles -hoy principalmente usando la tecnología flash con USB- con la pestaña de seguridad. Es una protección de escritura fácil y muy elemental.
- Instalar un antivirus y actualizarlo de forma periódica. Es muy recomendable que se haga al menos una vez por semana.
- Ejecutar el antivirus a todo el disco duro una vez al mes.
- Ejecutar siempre el antivirus a todo disco o CD que se introduce al sistema y a los archivos que descargamos desde Internet o vienen adjuntos en un e-mail.
- Si se tiene dudas, recurra a herramientas libres en Internet (*).
- Controlar el acceso de extraños al computador.
- Aunque esto puede ser más complicado ... use software legal.

(*) http://www.virustotal.com/

# ¿Qué hacer en caso de estar infectado?



- Detener las conexiones remotas.
- No mover el ratón ni activar el teclado.
- Apagar el sistema y desconectarlo.
- Arrancar con un disquete de arranque o emergencia protegido.
- Ejecutar luego un programa antivirus.
- Si es posible, hacer copia de seguridad de sus archivos para poder compararlas con copias anteriores.
- Formatear el disco duro a bajo nivel (si puede hacerlo claro) y si no le queda otra solución ☹.
- Instalar nuevamente el sistema operativo y restaurar las copias de seguridad... ¿ahora se acuerda que debe hacerlas a menudo?

De todas maneras, recuerde que la seguridad informática total no existe... ¿ha pensado que su disco duro puede quemarse ahora mismo por una repentina subida de voltaje? Y estas cosas son más habituales de lo que piensa.

Fin del capítulo

# Cuestiones y ejercicios (1 de 1)

1. ¿Qué diferencia hay entre el concepto de información y su calidad según lo entienda una empresa o los estudios de ingeniería?
2. ¿Por qué se dice que la información de una empresa es su activo más valioso? Compare este activo con el personal de la misma y póngase en situaciones en las que ambos se pierden, ¿qué situación podría ser es más perjudicial para la continuidad de dicha empresa?
3. Como responsables de seguridad hemos detectado que alguien está realizando acciones no lícitas, por ejemplo copias no autorizadas de información. ¿Qué actitud debemos tomar?
4. ¿Qué medidas podrían ser las más adecuadas de cara a minimizar los ataques por virus en nuestra empresa?
5. Si deseamos que nuestra empresa esté debidamente protegida tanto física como lógicamente, ¿qué deberíamos hacer?