

The logo for BAICOM networks is centered on a dark blue rectangular background. The word "BAICOM" is written in a bold, white, sans-serif font. Below it, the word "networks" is written in a lighter blue, lowercase, sans-serif font.

**BAICOM**  
networks

10 de Junio de 2005 - Universidad de San Andrés

# Presentación Institucional

BAICOM networks S.A. es una empresa fundada por un grupo de ingenieros que integraron y trabajaron con importantes empresas de renombre en Argentina adquiriendo gran experiencia en el campo de las Telecomunicaciones y la Informática.

Tenemos una fuerte especialización en Seguridad Informática y servicios profesionales basados en soluciones de código abierto.

Algunos de nuestros clientes son empresas como:



# Disertantes

Ing. Pablo Masoero  
Presidente  
pam@baicom.com

Ingeniero en Informática, con una fuerte especialización en Networking y Seguridad Informática aplicada a los negocios.

Posee una vasta experiencia en el área de Seguridad Informática y Networking, habiéndose desempeñado en dichas áreas en empresas como Techint, AT&T Latin América, Alcatel y PriceWaterhouse & Coopers.

Desde Junio de 2003 se desempeña como Presidente y Director Comercial de la empresa, siendo a su vez uno de sus fundadores.

Alejandro Gramajo  
Director de Ingeniería  
ang@baicom.com

Posee elevada especialización en el área de Seguridad Informática.

Ha realizado diversas publicaciones de artículos en el ámbito académico y en Internet sobre distintas tecnologías. Se ha encargado en UOL-Sinectis de las operaciones de red, investigación y desarrollo de distintas plataformas utilizadas actualmente por el proveedor.

Desde Agosto de 2004 se desempeña como Director de Ingeniería de la empresa, teniendo a su cargo, entre otras, el área de investigación y desarrollo de Seguridad Informática.

# Agenda

- 1. Seguridad Informática en el mundo**
  - Historia
  - Puntos relevantes
  - Situación actual
- 2. Estadísticas**
  - Evolución de incidentes publicados
  - Evolución de vulnerabilidades
- 3. Administración de la Seguridad Informática**
  - Organización y reportes
- 4. Fraude Digital - Casos de Estudio**
  - Acceso no permitido a base de datos
  - Captura de tráfico sensible en la red interna

# Historia

- Durante los años noventa, la tecnología tuvo el salto mas grande, y fue el período en el cual las empresas mas invirtieron en tecnología
- El concepto de seguridad informática no estaba instalado
- Las empresas fueron volcando sus procesos de core sobre distintas tecnologías
- Pasando la segunda mitad de los años noventa se comenzaron a descubrir vulnerabilidades sobre los sistemas instalados ...

Fuente: Ernst & Young – 2004 Global Security Survey

# Puntos relevantes

- El 90% de las organizaciones afirman que la seguridad sobre sus sistemas de información es de vital importancia para alcanzar sus objetivos generales.
- El 78% las organizaciones afirman que la reducción de riesgos es el principal objetivo de los gastos en Seguridad Informática.

## Sin embargo ...

- Una de cada tres organizaciones consideran que no es adecuada su capacidad para:
  - Determinar si sus sistemas son vulnerables
  - Responder a incidentes de seguridad
- Sólo una de cada tres organizaciones aseguran que cumplen con regulaciones de seguridad.
- Más de la mitad de las organizaciones coinciden en que las restricciones presupuestarias son el principal obstáculo para implementar un programa efectivo de seguridad informática.

Fuente: Ernst & Young – 2004 Global Security Survey

## Puntos relevantes (cont.)

**Las mayores implicancias de la Seguridad Informática se pueden resumir en los siguientes puntos:**

- A pesar de la generalizada visión sobre la criticidad de una evaluación de riesgos, sólo el 27% de las empresas considera que “los resultados de una evaluación de seguridad de la información” se encuentra entre los tres factores más influyentes.
- La tecnología es el imán más poderoso para conseguir fondos dentro de las organizaciones. De estas inversiones, lo invertido en Seguridad Informática aparenta ser extremadamente bajo comparado con tecnología.
- Los virus y los “troyanos” son las principales preocupaciones de seguridad y continúan captando la mayor atención de los medios y el público.

Fuente: Ernst & Young – 2004 Global Security Survey

# Situación Actual

**El 52 % de las empresas reconocen haber sufrido interrupciones inesperadas o no programadas de sus sistemas críticos de negocio.**

- Se producen aproximadamente 200 incidentes diarios de gravedad en el mundo
- El 90% de las empresas del mundo son víctimas de ataques informáticos contra sus redes
- El 70% de los ataques provienen desde Internet
- Se detectaron 1220 nuevas vulnerabilidades en lo que va del año
- Aparece el concepto de “Managed Security”
- Aparecen los SSP (Security Service Provider)

**“En 2004 los ataques provocaron pérdidas de entre 40.000 y 50.000 M de dólares”**

# Evolución de incidentes publicados

## 1988-1989

Year	1988	1989
Incidents	6	132

## 1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

## 2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

Total incidents reported (1988-2003): **319,992**

Fuente: CERT

# Evolución de vulnerabilidades

## Vulnerabilities reported 1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

## 2000-2005

Year	2000	2001	2002	2003	2004	1Q,2005
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	1,220

Total vulnerabilities reported (1995-1Q,2005): **17,946**

Fuente: CERT

# Organización y Reportes

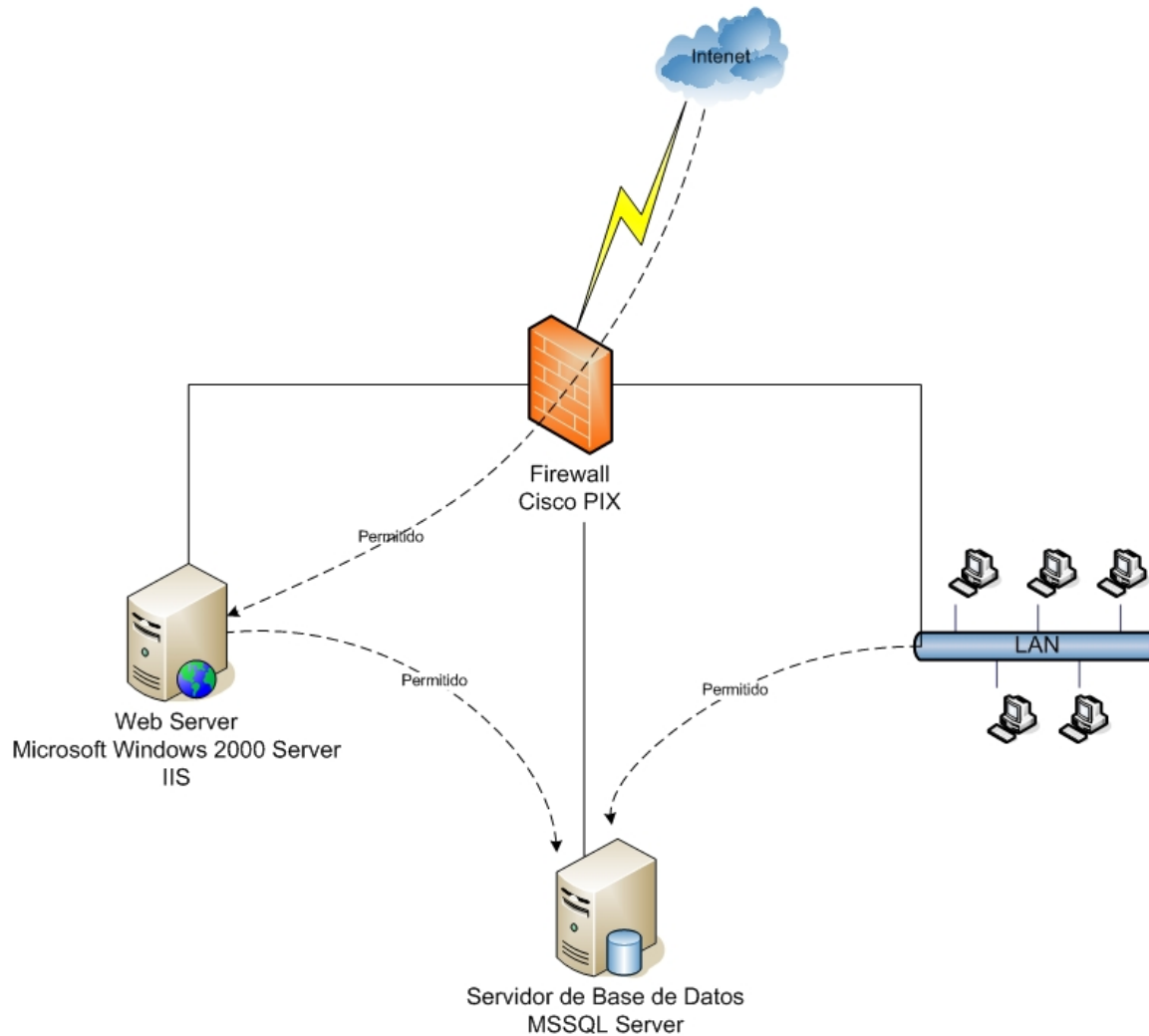
**Se analiza con que frecuencia las organizaciones proporcionan al Directorio o entidad equivalente un informe sobre el estado de la seguridad de la información o incidentes de seguridad.**

- El 36% de los consultados reportan incidentes de seguridad al directorio al menos trimestralmente, mientras que,
- El 12% realizan los reportes en forma semestral
- El 38% lo hacen anualmente o aún menos
- El 14% nunca reportó al directorio

Fuente: Ernst & Young – 2004 Global Security Survey

# Fraude Digital - Casos de Estudio

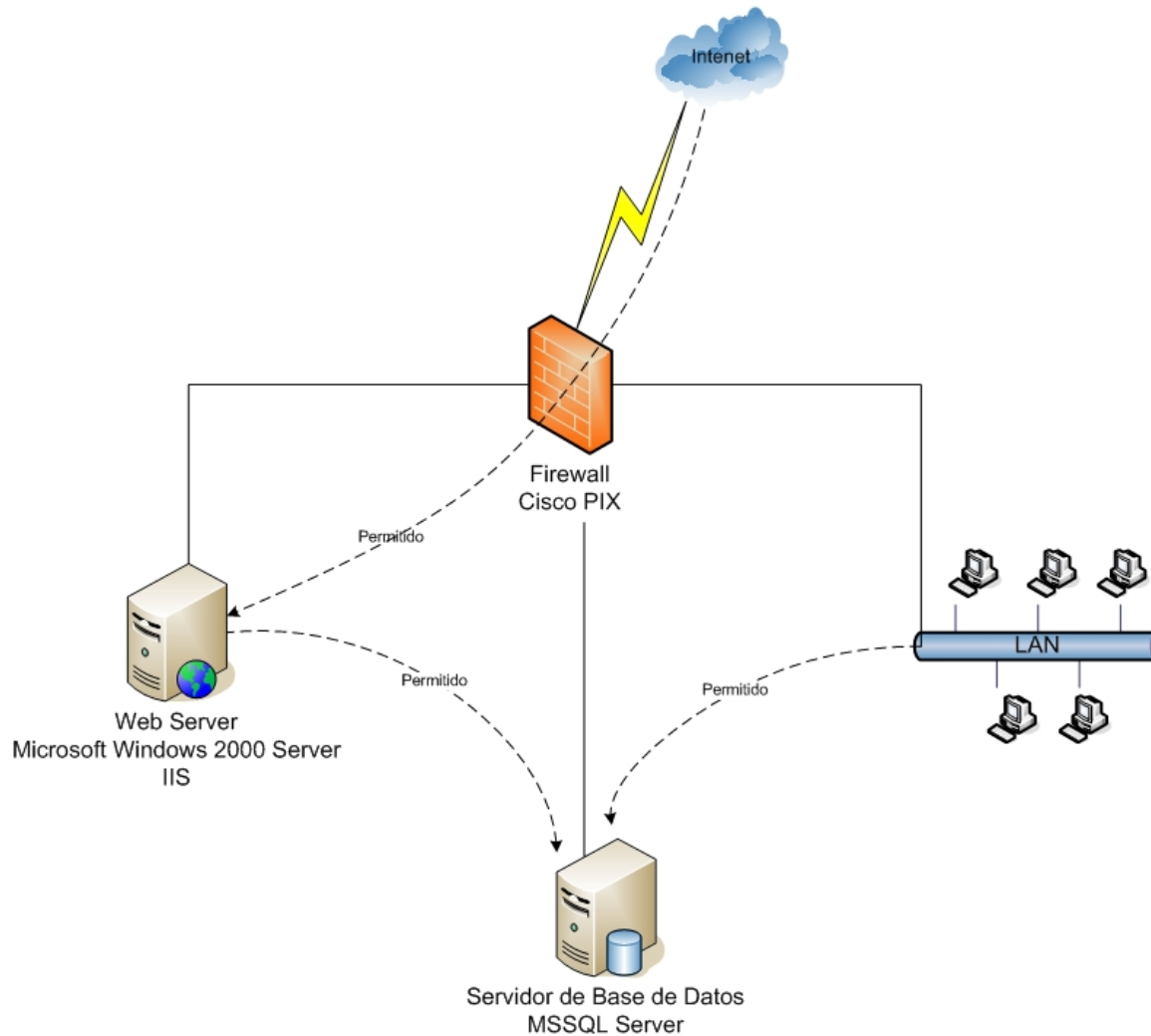
# Acceso no permitido a Base de Datos



## La red:

- El firewall permite acceso al Web Server desde Internet (portal con vistas de algunas tablas para mostrar datos)
- IIS no se actualiza (posee varios bugs: WebDav)
- IIS puede consultar a la base de datos, el firewall lo permite.

# Acceso no permitido a Base de Datos (cont.)



## Políticas:

- Tiene todas las pólizas de seguros en "la base de datos"
- El cobro de una póliza depende del estado aprobado o desaprobado (un campo)
- Sólo un grupo específico dentro de la empresa tiene acceso para modificarlo

# Acceso no permitido a Base de Datos (cont.)

Nos encontramos con un sujeto que busca la manera de cometer un fraude a una empresa de seguros...

Un atacante externo puede:

- Entrar al IIS explotando el bug del WebDav
- De ahí verificar el código que se conecta a la base de datos
- Conectarse a la base de datos
- Modificar el o los registros, cambiar la aceptación de la póliza.
- Ir a cobrar la póliza :-)

# Acceso no permitido a Base de Datos (cont.)

Problemas que se encuentra el atacante:

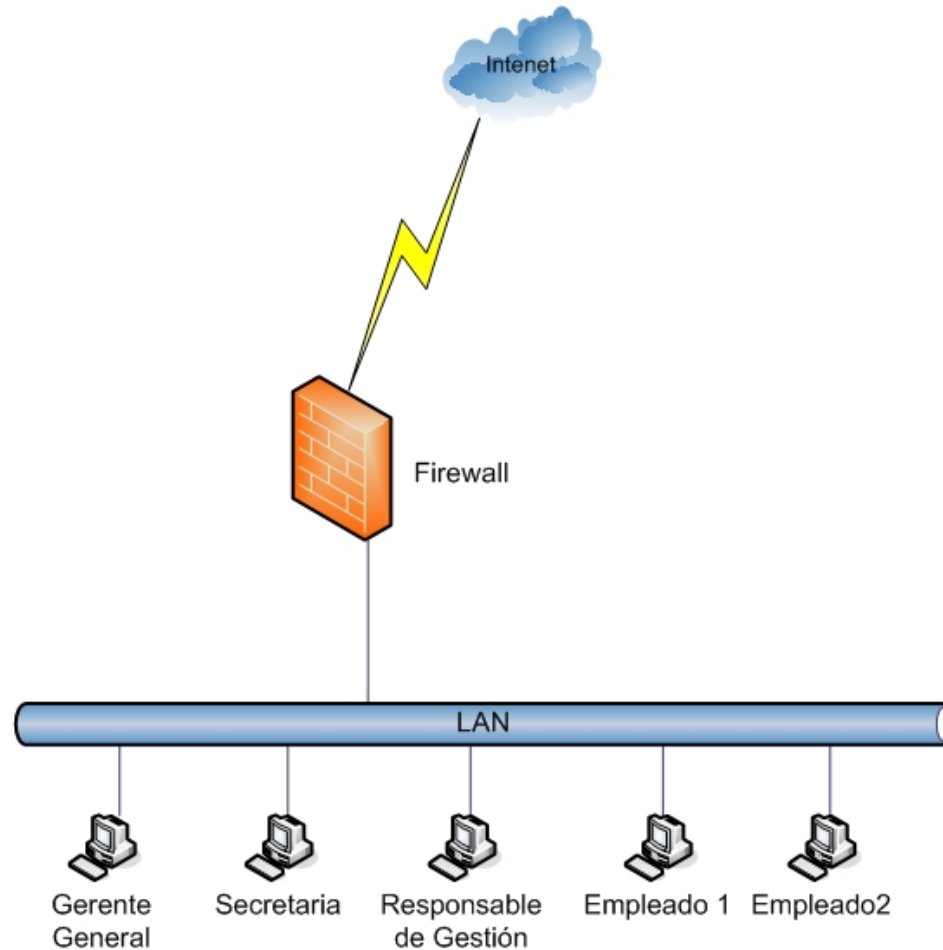
- No conoce la base
- Solo necesita tiempo
- O un informante INTERNO
- Fallas en los exploits, modificar y volver a probar

# Acceso no permitido a Base de Datos (cont.)

Como evitar este ataque:

- Actualización periódica de la seguridad en los servers WWW y DB
- Auditorias periódicas de seguridad (WWW y DB)
- Revisión de logs. (Intentos de conexiones fallidas)
- Administradores actualizados en materia seguridad

# Captura de tráfico sensible en la red interna



## La red:

- El tráfico viaja a todos los puestos de trabajo (culpa del Hub) (igualmente si no es un Hub, se puede mandar exceso de tráfico del Switch llenando su memoria, de esa manera se transforma en un Hub)
- Empleados pueden, sin autorización escuchar tráfico de la red

# Captura de tráfico sensible en la red interna (cont.)

Un atacante (o empleado descontento) puede:

- Capturar todos los mails
- Capturar los mensajes de MSN
- Capturar sesiones de home banking (usando proxy ssl / tunel ssl)

# Captura de tráfico sensible en la red interna (cont.)

Luego...

- Borrar los rastros en los logs (si es un experto es fácil)
- Vender la información a la competencia
- Comprar una Ferrari

# Captura de tráfico sensible en la red interna (cont.)

Como evitar este ataque:

- Tener empleados motivados y felices.
- Usar mails encriptados para la información sensible (gpg / smime)
- No usar MSN (o encriptarlo usando Simp)
- Usar home banking con transacciones SSL seguras, verificar la información del certificado.

## De donde seguir leyendo

- <http://www.frsirt.com/> (ex k-otik)
- <http://www.packetstormsecurity.org/>
- <http://cve.mitre.org/cve/>
- <http://www.securiteam.com/>
- <http://icat.nist.gov/>
- <http://www.osvdb/>
- Listas de correo (Full-Disclosure, Vulnwatch, SANS, Vuln-Dev)  
repositorio de listas: <http://archives.neohapsis.com/>

# Consultas y Preguntas

# Muchas Gracias