11a. Convención nacional de aseguradores

AMIS

2001

"El Seguro Mexicano ante Nuevos Horizontes"

Control y Administración de Riesgos Electrónicos

MANCERA ERNST & YOUNG

Agenda

CARe
Control y Administración de Riesgos Electrónicos

- Algunas estadísticas globales
- Algunas estadísticas de sus compañías
- ¿Que venden?
- Riesgos de su sector de negocios
- Metodologías de evaluación de riesgos
- Preguntas

Algunas estadísticas globales

CARe
Control y Administración de Riesgos Electrónicos

- 58% de los entrevistados sufrieron violaciones de acceso en los últimos 12 meses
- 24% reportaron intentos de acceso vía Internet
- 66% perdieron más de 50,000 USD
- 18% perdieron más de 1,000,000 USD
- 34% de los ataques son internos

Algunas estadísticas de sus compañías

CARe
Control y Administración de Riesgos Electrónicos

- 12 Instituciones no tienen página
- 19 páginas no abrieron
- De las que abrieron:
  - 35 no tienen venta electrónica
  - 4 presentan políticas de seguridad
  - 7 tienen conexión segura

¿Que venden?

CARe
Control y Administración de Riesgos Electrónicos

- Lo que venden las Instituciones de Seguros son valores como:
  - Protección
  - Seguridad
  - Confianza
  - Tranquilidad
  - Etc.
- ¿Hasta donde llegan o deben llegar estos valores dentro de la organización?

Valores y Tecnología

CARe
Control y Administración de Riesgos Electrónicos

- Si llevamos estos valores a la tecnología de información, podemos hacernos preguntas tales como:
  - ¿Los datos de mis clientes están seguros?
  - ¿Tengo controles adecuados sobre los riesgos derivados del uso de tecnología, para minimisar gastos y poder transmitir ahorros a mis clientes?
  - ¿Existe un conciencia de control difundida en la Institución que apoye los valores que estoy vendiendo?
- Estas preguntas son totalmente dirigidas hacia mis clientes ..... ¿pero cuando hablamos de la confianza interna que pasa?

Valores y Tecnología

- ¿Cuanto vale en el mercado su cartera de clientes?
- ¿Alguna vez
  - se les ha pérdido algún registro?
  - han visto un balanza de comprobación que no cuadre?
  - han prestado o les han prestado una clave de acceso?
  - se les ha caído el sistema por falta de energía eléctrica?
  - los usuarios han participado activamente en la prueba de modificaciones o desarrollos de programas?

Obsesiones

- Las publicaciones no técnicas están obsesionadas con Internet
- Las publicaciones técnicas están obsesionadas con seguridad

> "Es un avance lógico : Ya que la primer emoción de contar con una supercarretera en tu vecindad se reduce, es inevitable notar que no solo te permite viajar, sino también permite que un gran número de personas extrañas aparezcan en donde tú estás, y no todos son personas que hubieras invitado."
>
> Brent Chapman
> "Building Internet Firewalls"
> O'Reilly and Associates, Inc.

Encabezados

CARe
Control y Administración de Riesgos Electrónicos

- Hackers atacan el Ministerio de Defensa de Brasil – Enero 12, 2001
- Se encontró un hueco de seguridad en la base de datos
- de Borland – Enero 12, 2001
- El FBI descubre a 7 Hackers planeando un ataque de virus en víspera de año nuevo – Enero 11, 2001
- El site de Pepsi (Reino Unido) es hackeado – Enero 4, 2001
- El site de Egghead.com es hackeado – Diciembre 22, 2000

El Riesgo

CARe
Control y Administración de Riesgos Electrónicos

- Encuesta de Crimen Computacional 2000 de CSI
  - 90% de los participantes reportaron violaciones en seguridad computacional
  - 74% reconocieron sufrir pérdidas financieras
  - Total de pérdidas = $265 millones USD

Las Amenazas Más Grandes

CARe
Control y Administración de Riesgos Electrónicos

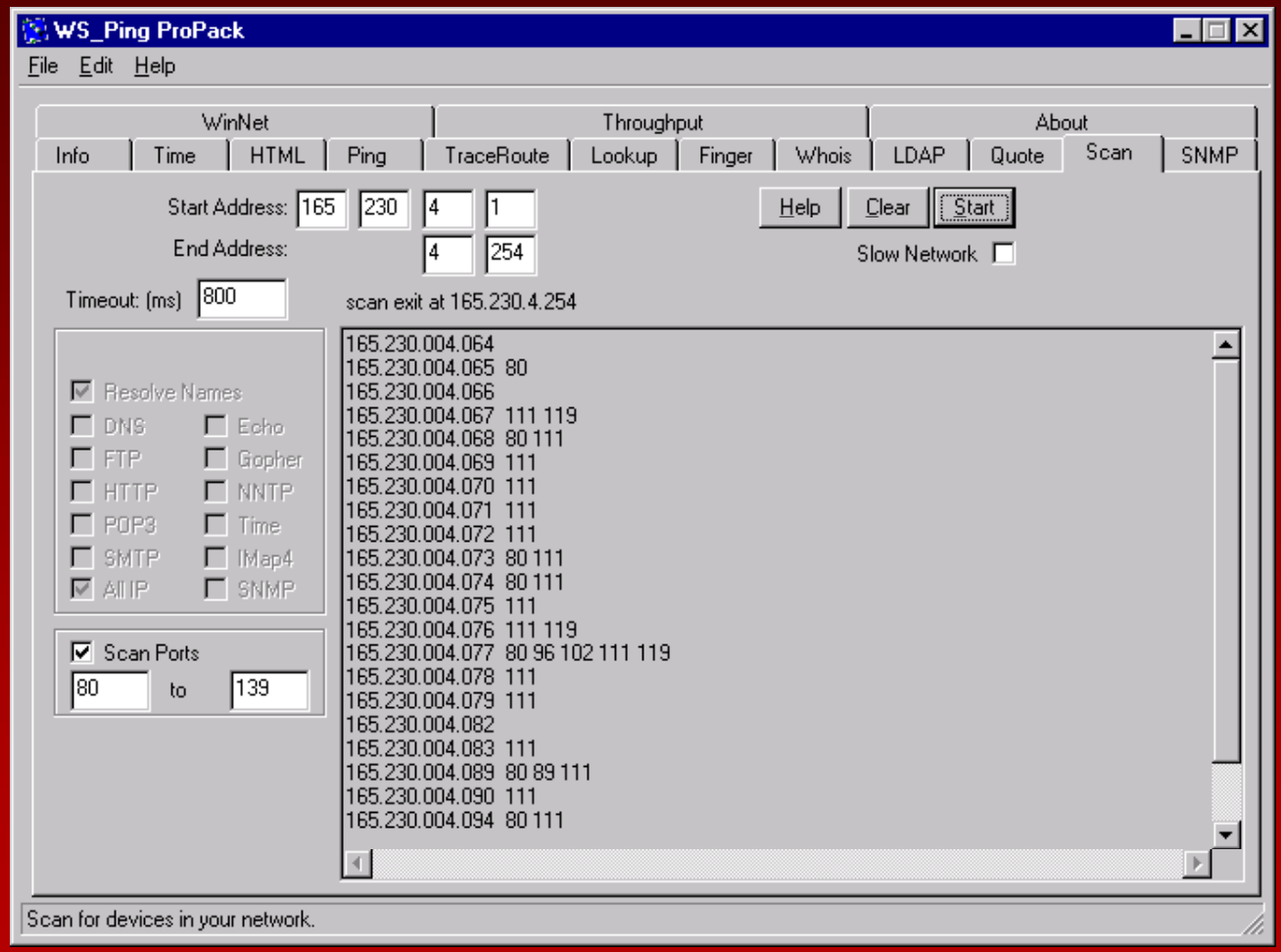
- El Problema Básico:
  - Vulnerabilidades de los proveedores
  - Sistemas no bien configurados
  - Claves de acceso (passwords) por omisión o fácilmente adivinadas
- ¿Cuál de los puntos arriba mencionados es el problema más grande?

¿¿Qué Están Haciendo los Hackers??..

CARe
Control y Administración de Riesgos Electrónicos

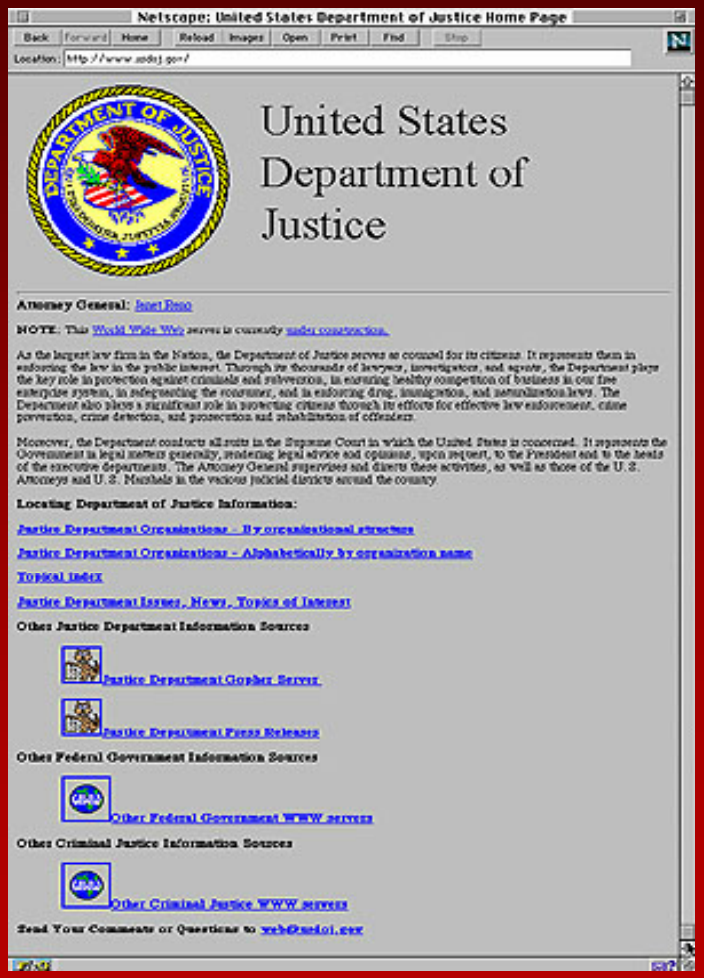
- Los hackers están:
  - Utilizando herramientas automáticas de escaneo
  - Utilizando escaneos “Stealth”
  - Realizando “TCP Finger Printing”
  - Instalando Sniffers
  - Propagando virus, etc. via e-mail
  - Falsificando e-mail
  - Inundando conexiones con el propósito de negación de servicios

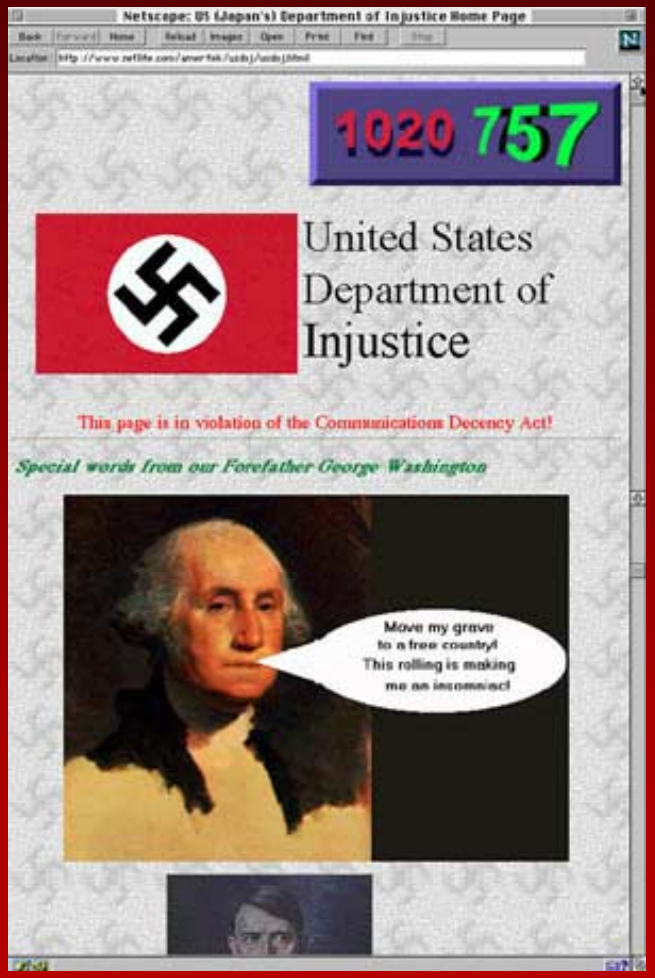
WS PingProPack



Una Mañana de Sábado.....

CARe
Control y Administración de Riesgos Electrónicos

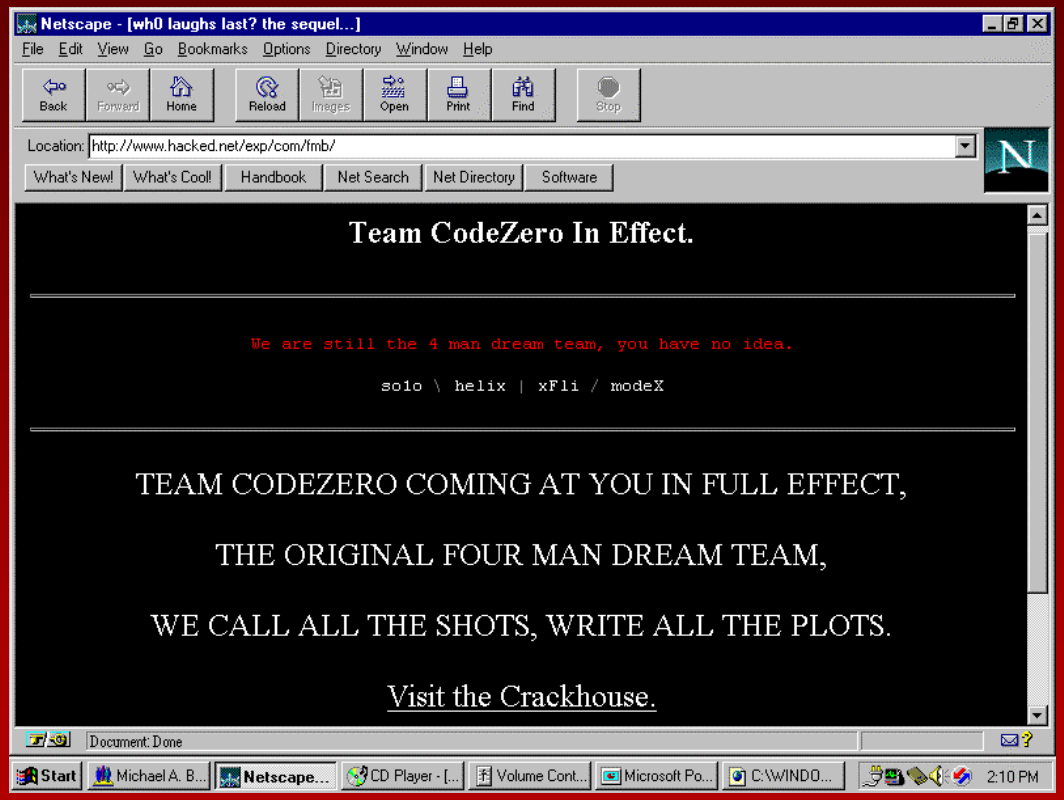




MANCERA ERNST & YOUNG

Más Ejemplos.....

CARe
Control y Administración de Riesgos Electrónicos



MANCERA
ERNST & YOUNG

Probando la Seguridad

CARe
Control y Administración de Riesgos Electrónicos

- ¿¿Qué es lo que se busca??
  - Realizar un Inventario a Nivel Red
    - Determinar todos los dominios asociados con el site
    - Determinar las direcciones IP de los sistemas conectados al Internet y con el Intranet corporativo
    - Determinar los tipos de servicios de red que cada sistema se encuentra ejecutando (Ej. HTTP, HTTPS, SMTP, etc.)
    - Identificar “fugas de información”
    - Determinar la arquitectura específica de cada sistema (Ej. SPARC vs X86).
  - Realizar un mapeo del “estado” de los dispositivos inventariados con vulnerabilidades conocidas
  - Determinar el Riesgo basado en el Proceso del Negocio y/o datos

Herramientas, Herramientas, Herramientas……..

CARe
Control y Administración de Riesgos Electrónicos

- Sitios Web:
  - www.securityfocus.com
  - www.sans.org
  - http://packetstorm.securify.com
- Herramientas:
  - nmap: herramienta freeware para escaneo de redes
  - crack and lopht crack: herramientas freeware para romper passwords

Cuando Has Sido Hackeado…….

CARe
Control y Administración de Riesgos Electrónicos

- Manejo de “Incidentes”:
  - Examinar archivos log (sistema, firewall, etc.)
  - Revisar binarios del sistema
  - Revisar existencia de sniffers de paquetes
  - Revisar configuración del sistema y de la red
  - Buscar archivos inusuales u ocultos
  - Examinar todos los equipos en la red local

Cuando Has Sido Hackeado…….

- Segregar los sistemas afectados del resto de la red
- Notificar al personal apropiado
- Documentar, documentar, documentar
- Establecer custodia
- Controlar flujo de información
- Recuperación de sistemas o preservarlos para tomar acciones legales

Consideraciones

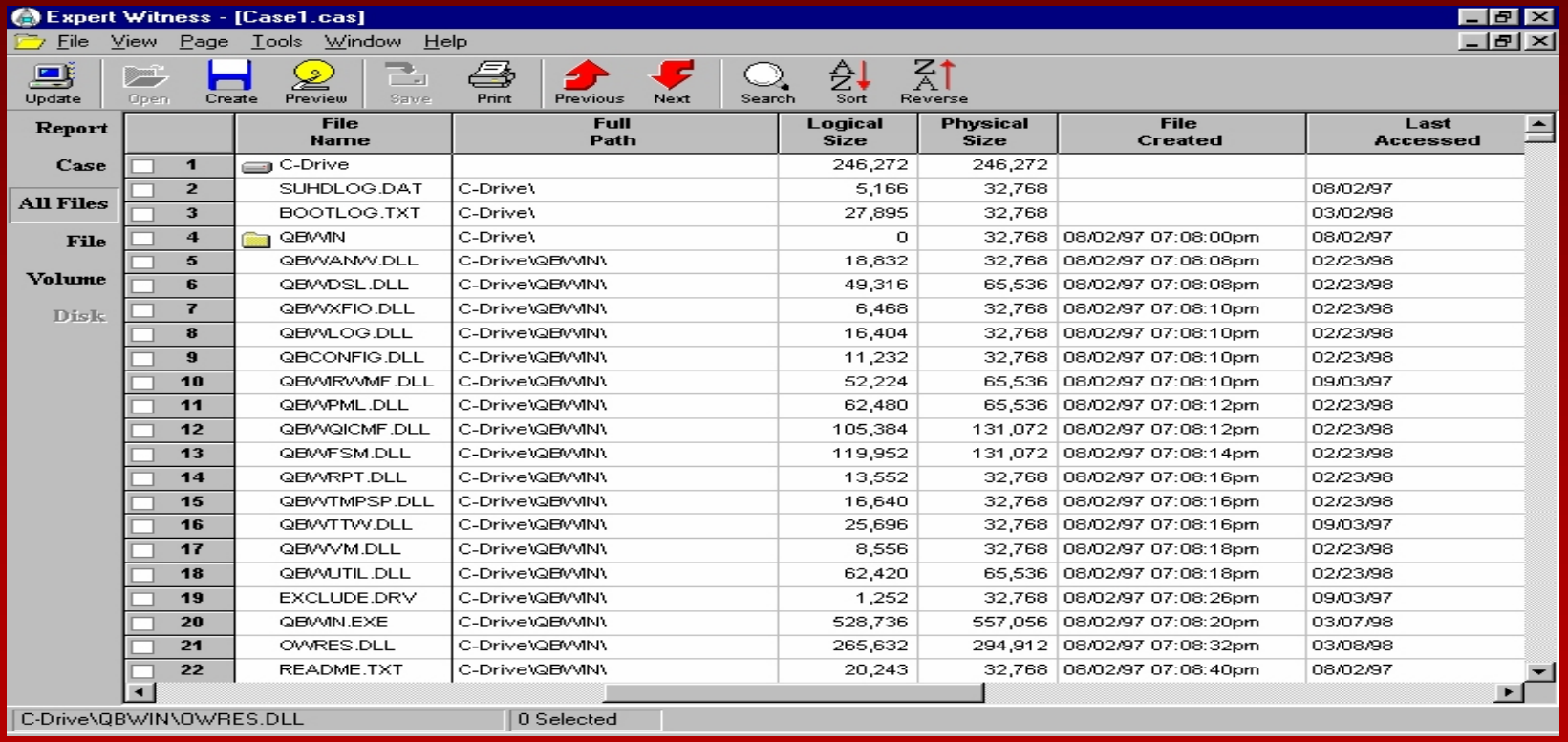
CARe
Control y Administración de Riesgos Electrónicos

- Aplicación de Búsqueda Forense:
  - Estructura de directorio
  - Archivos de aplicación
  - Archivos de Internet
  - Archivos ocultos
  - Archivos borrados
  - Búsqueda de palabras clave

Herramientas, Herramientas, Herramientas

CARe
Control y Administración de Riesgos Electrónicos

Expert Witness – Herramienta de Registro de Evidencia y Análisis



	File Name	Full Path	Logical Size	Physical Size	File Created	Last Accessed
1	C-Drive		246,272	246,272		
2	SUHDLOG.DAT	C-Drive\	5,166	32,768		08/02/97
3	BOOTLOG.TXT	C-Drive\	27,895	32,768		03/02/98
4	QBWIN	C-Drive\	0	32,768	08/02/97 07:08:00pm	08/02/97
5	QBWANVV.DLL	C-Drive\QBWIN\	18,832	32,768	08/02/97 07:08:08pm	02/23/98
6	QBWDSL.DLL	C-Drive\QBWIN\	49,316	65,536	08/02/97 07:08:08pm	02/23/98
7	QBWXFIO.DLL	C-Drive\QBWIN\	6,468	32,768	08/02/97 07:08:10pm	02/23/98
8	QBWLOG.DLL	C-Drive\QBWIN\	16,404	32,768	08/02/97 07:08:10pm	02/23/98
9	QBCONFIG.DLL	C-Drive\QBWIN\	11,232	32,768	08/02/97 07:08:10pm	02/23/98
10	QBWMRVMF.DLL	C-Drive\QBWIN\	52,224	65,536	08/02/97 07:08:10pm	09/03/97
11	QBWPML.DLL	C-Drive\QBWIN\	62,480	65,536	08/02/97 07:08:12pm	02/23/98
12	QBWQICMF.DLL	C-Drive\QBWIN\	105,384	131,072	08/02/97 07:08:12pm	02/23/98
13	QBWFSM.DLL	C-Drive\QBWIN\	119,952	131,072	08/02/97 07:08:14pm	02/23/98
14	QBWRPT.DLL	C-Drive\QBWIN\	13,552	32,768	08/02/97 07:08:16pm	02/23/98
15	QBWTMPSP.DLL	C-Drive\QBWIN\	16,640	32,768	08/02/97 07:08:16pm	02/23/98
16	QBWTTW.DLL	C-Drive\QBWIN\	25,696	32,768	08/02/97 07:08:16pm	09/03/97
17	QBWVM.DLL	C-Drive\QBWIN\	8,556	32,768	08/02/97 07:08:18pm	02/23/98
18	QBWUTIL.DLL	C-Drive\QBWIN\	62,420	65,536	08/02/97 07:08:18pm	02/23/98
19	EXCLUDE.DRV	C-Drive\QBWIN\	1,252	32,768	08/02/97 07:08:26pm	09/03/97
20	QBWIN.EXE	C-Drive\QBWIN\	528,736	557,056	08/02/97 07:08:20pm	03/07/98
21	OWRES.DLL	C-Drive\QBWIN\	265,632	294,912	08/02/97 07:08:32pm	03/08/98
22	README.TXT	C-Drive\QBWIN\	20,243	32,768	08/02/97 07:08:40pm	08/02/97

MANCERA
ERNST & YOUNG

Soluciones a Nivel Ejecutivo

- Soluciones de Administración
  - Comité de Seguridad a nivel toda la empresa
  - Programa de Difusión de Seguridad a nivel Ejecutivo
- Soluciones Técnicas
  - Arquitectura de Seguridad de Información
  - Sistema de Detección de Intrusión
  - Programa de Respuesta a Incidentes

Soluciones a Nivel Ejecutivo

CARe
Control y Administración de Riesgos Electrónicos

- Todas estas soluciones requieren los recursos adecuados:
  - GENTE
  - PROCESOS
  - TECNOLOGÍA
- Si cualquiera de estos componentes falta, el programa no será tan robusto como lo puede ser.....

Comentario Final

CARe
Control y Administración de Riesgos Electrónicos

"Un negocio tendrá buena seguridad si su cultura empresarial es la correcta. Esto depende de una cosa: la conciencia de la alta dirección. No habrán esfuerzos populares que aplasten la negligencia corporativa."

William Malik
VP Investigaciones
Gartner Group
Nov 27, 2000

Riesgos de su sector de negocios

CARe
Control y Administración de Riesgos Electrónicos

- **Pérdida de:**
  - **Imagen**
  - **Datos importantes (robo o contingencia)**
  - **Control de transacciones**
  - **Disponibilidad de sistemas**

¿Hay alguna diferencia con algún otro sector o industria?

Es tiempo de

- Realmente evaluar los nuevos riesgos y su impacto en los procesos tradicionales de negocio
- Recapacitar en las vulnerabilidades que tenemos
- Reconocer que la solución no solo es “tecnología pura”
- No solo asegurar las puertas de Internet, sino hacerlo en forma integral, a través de toda la compañía y de todas las tecnologías en uso
- Incrementar la conciencia de control (cultura), la tecnología nos lleva mucha ventaja ... !Ya está aquí¡

FINAL

CARe
Control y Administración de Riesgos Electrónicos

EL QUE ESTÉ LIBRE DE CULPA, QUE LANCE LA PRIMERA PIEDRA

¿PREGUNTAS?

MANCERA
ERNST & YOUNG