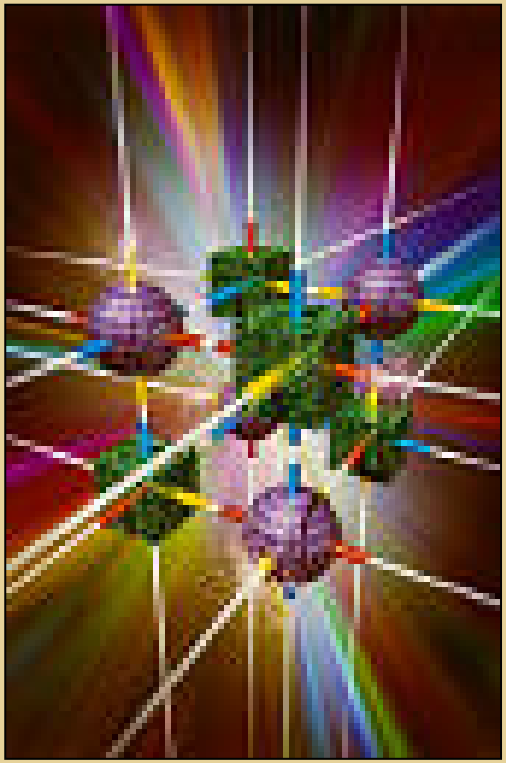
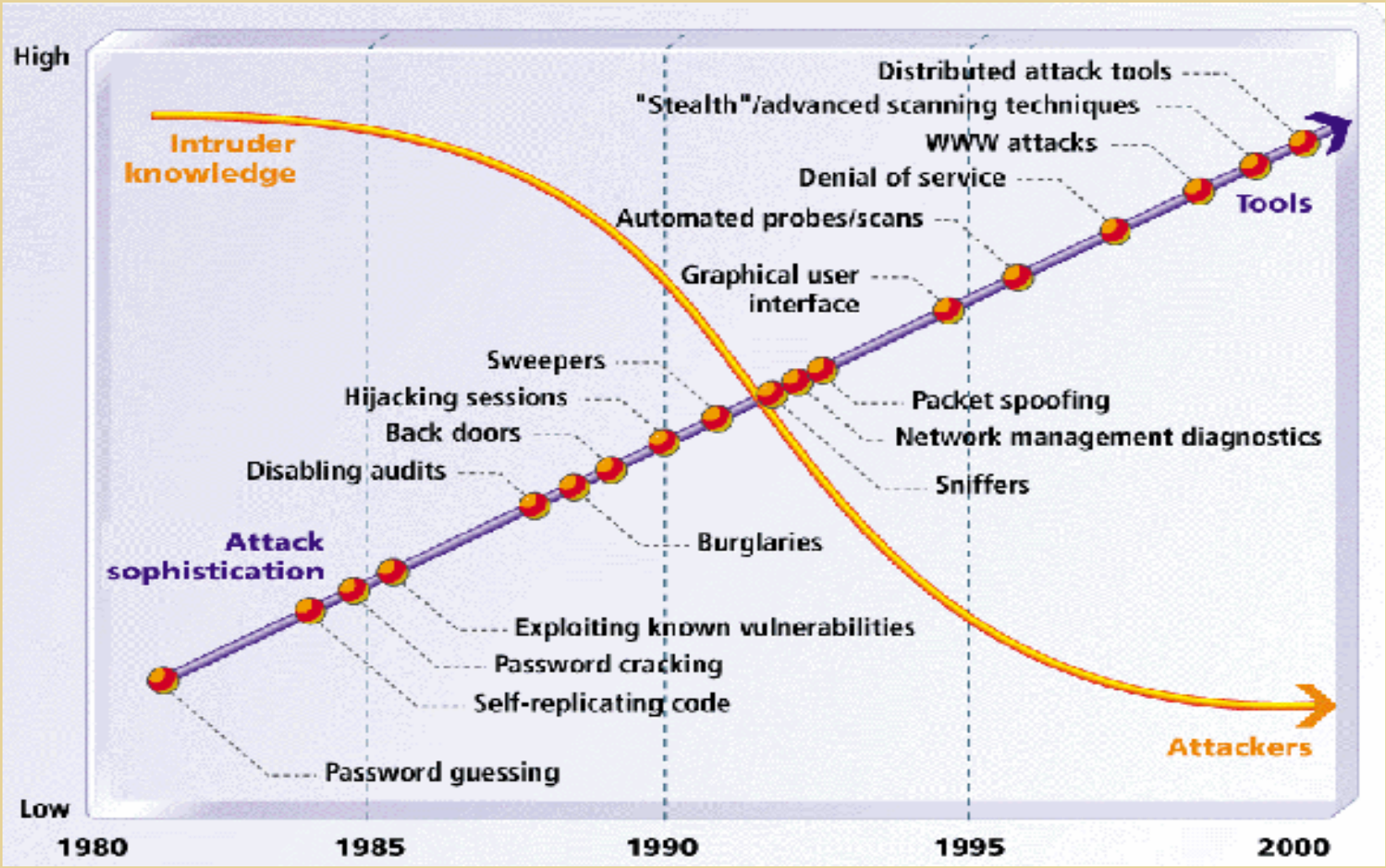
Temario



- Rol que le compete respecto a los incidentes o ilícitos informáticos (Forensic Computing)
- Cómo debe actuar una organización cuando sospecha que ha habido un delito o incidente informático o cuando efectivamente ocurre.
- Evolución del tratamiento dado a los delitos o incidentes informáticos.
- Principales obstáculos para combatirlos.

Brechas de Seguridad



Advisory

Existe la necesidad de Computer Forensic?

Dónde residen los registros :

20%

20% Hard Copy

80%+

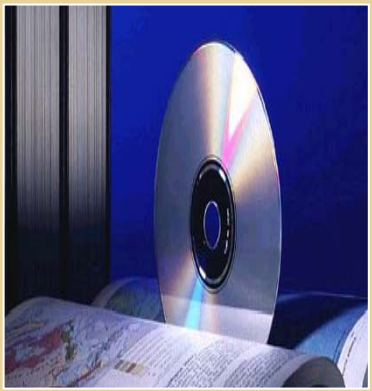
•80%+ medios electrónicos.

Advisory

Investigación de Fraude – Soporte de Forensics

Volúmen de Análisis

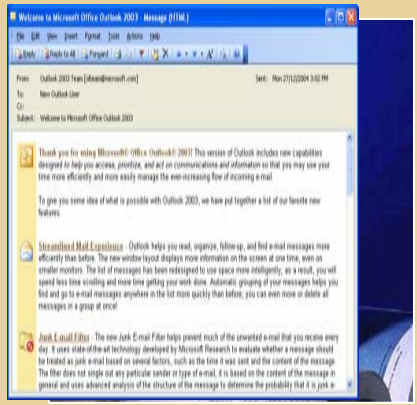
Dispositivos



Datos Numéricos

Amount_Dr	Amount_Cr
50,502.00	50,502.00
859,011.00	859,011.00
10,387,499.92	10,387,499.92
6,790,422.82	6,790,422.82
4,997,926.69	4,997,926.69
1,258,286.00	1,258,286.00
200,000.00	200,000.00

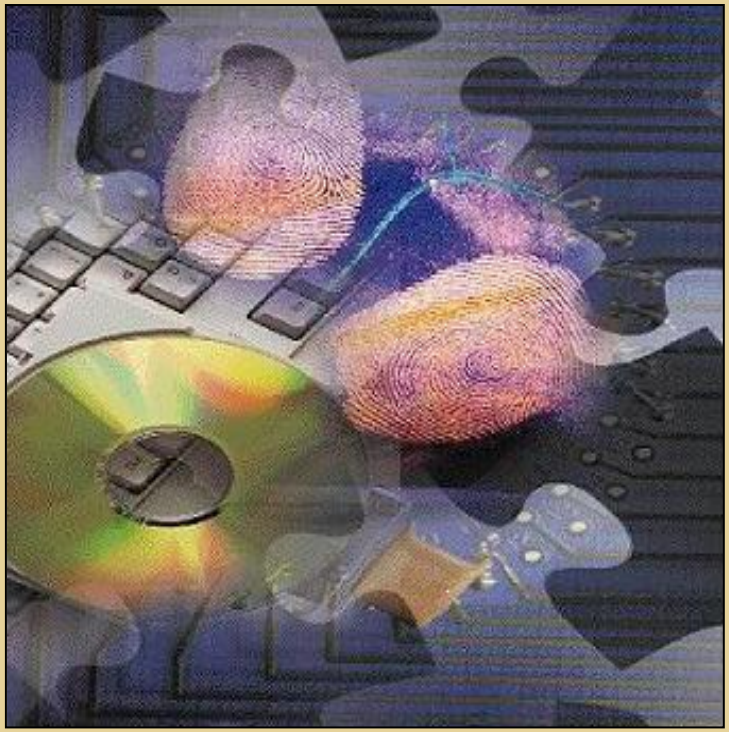
Email



Volúmen

Advisory

Tecnología Forense



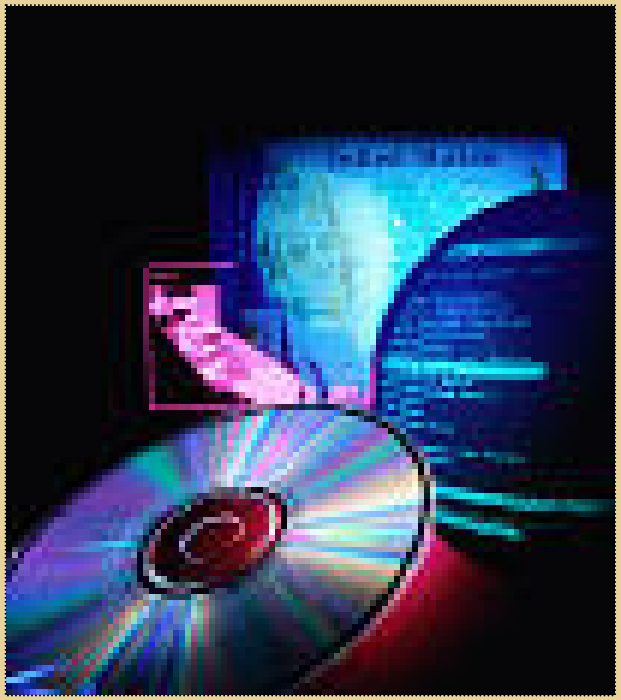
"El uso de IT para detectar o evidenciar actividad criminal "

- **Forensic Computing**
- **Análisis de Información Forense**

Forensic Computing

"La ciencia de **obtener información** para que pueda ser utilizada como evidencia "

Análisis de Información Forense



"La ciencia de **extraer información** significativa manteniendo las huellas evidenciales "

Proceso de la Imagen Forense

- Se emplea un Proceso Controlado de boot;
- Se realiza una imagen forense del disco rígido del objetivo (captura toda la información);
- La imagen se guarda en un medio estable, ej CD ROM;
- En el futuro se puede realizar una copia idéntica.
  - No hay necesidad de obtener el hardware físico

Qué se debe revisar?

- Drives externos
- Floppy disks
- Avisos de Internet
- Laptops & pcs personales
- Almacenamiento USB
- Archivos de Asistentes personales
- Backups de Cintas e información restaurada
- CD's Regrabables
- Sistema de control de acceso al edificio
- Mail
- Firewall logs
- PABX
- Mensajes de buzón de voz
- Web-based email (ej. "HotMail")
- Almacenamiento Free-drive Web-based

"Las Computadoras como fuentes de evidencia"

- **Quién accedió a los archivos?**
- **Cuándo accedió?**
- **Qué archivos modificó?**
- **Qué archivos faltan?**
- **Cuando se grabaron los archivos o carpetas?**
- **De dónde provenían los archivos o carpetas?**
- **A dónde se enviaron los archivos o carpetas?**

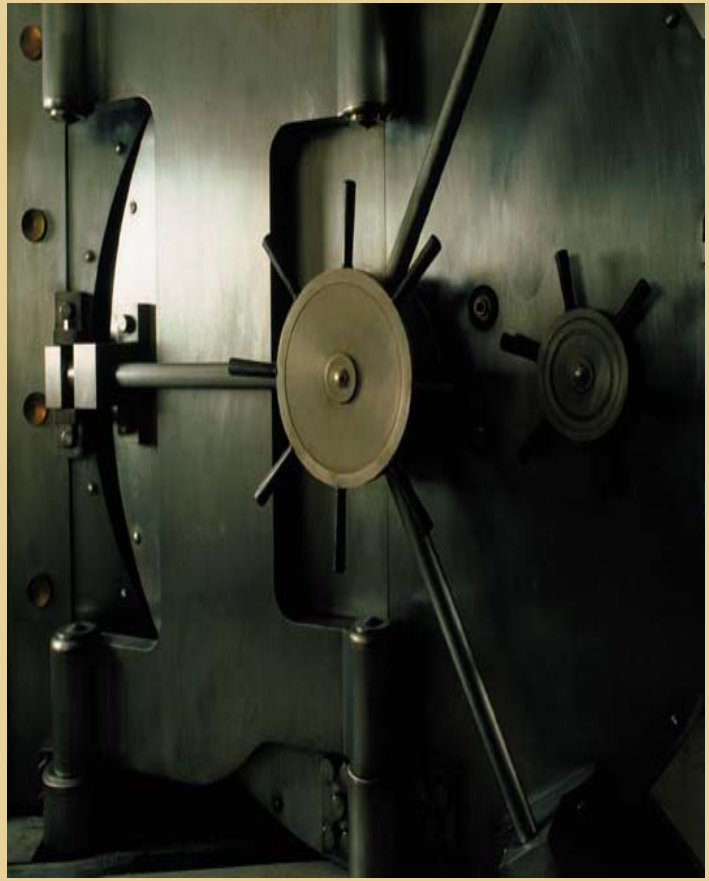
Preservar la Integridad de la Evidencia!

- **Las computadoras pueden presenciar un evento y registrar evidencia importante.**
- **Las actividades de usuarios dejan rastros.**
- **Una acción inmediata asegura la preservación de la memoria más exacta del incidente.**
- **El sólo encender la computadora causa el cambio de la información o la alteración de la fecha y hora del archivo.**
- **<u>Computer forensics preserva la integridad de la evidencia.</u>**

Advisory

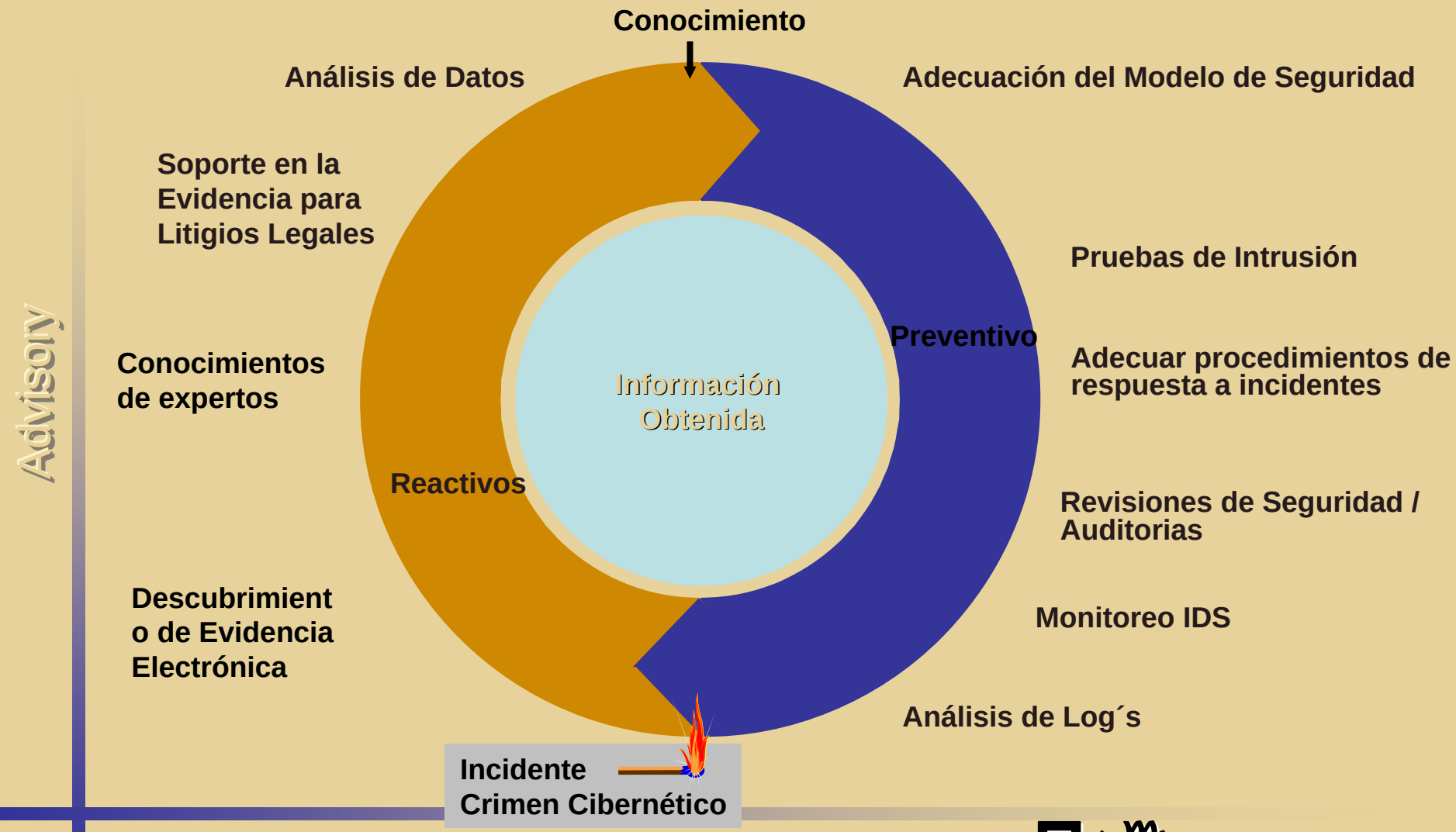
Análisis Forense

- Recuperar Archivos eliminados
- Análisis de las tendencias de eliminación de archivos
- Variedad de Búsquedas – email, palabras clave, tipo de archivo, día & hora
- Detectar el uso de software no autorizado
- Detectar el uso de dispositivos externos
- Analizar los registros de acceso físicos
- Analizar las actividades de red e internet



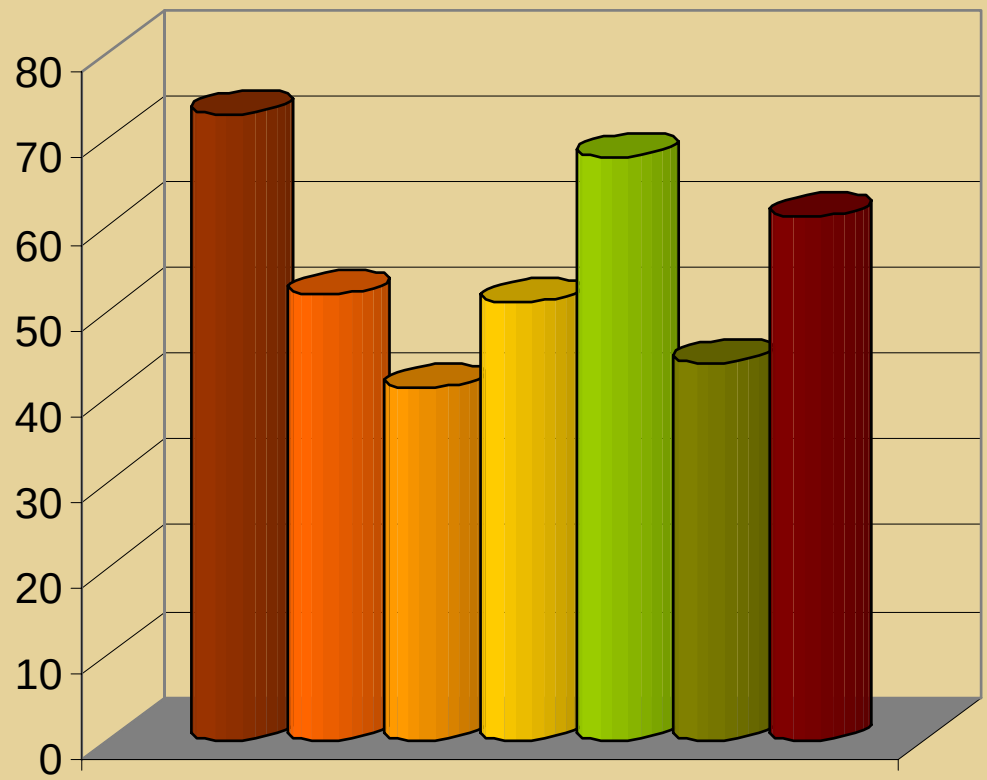
Advisory

Modelo de Administración del Riesgo de Cybercrime



Advisory

Prioridades ante el descubrimiento de un incidente



- Retomar las operaciones normales del negocio
- Prevenir la pérdida de la moral de los empleados
- Reportar el incidente a la policía o regulador
- Recuperar bienes robados
- Prevenir incidentes similares en el futuro
- Disciplinar o demandar a la persona responsable
- Prevenir daños a la imagen de su empresa

Advisory

Source: PwC/dti Information Security Breaches Survey 2002

Barreras en la lucha contra el cybercrime

- **Falta de Experiencia**
- **Falta de Conciencia**
- **Falta de Coordinación**
- **Legislación atrasada con respecto a tecnología**
- **No se requiere reportar un crimen**
- **Criminales más avanzados**
- **Dificultades con evidencias**
- **Temas de jurisprudencia**
- **Falta de recursos**
- **Renuencia a Demandar**

¿ Preguntas ?

Diego Pizzoli – Director

TE: (54) 11 - 4850 - 6815

mail: diego.pizzoli@ar.pwc.com

Advisory