VII Encuesta Nacional de Seguridad Informática

VII Jornada Nacional de Seguridad Informática

COMPUTACIÓN FORENSE: RASTREANDO LA INSEGURIDAD INFORMÁTICA

JUNIO 20, 21 Y 22 DE 2007

Biblioteca Luís Ángel Arango
Calle 11 No 4-14
Bogotá D.C., Colombia.

Conferencistas:

Jeimy J. Cano, Ph.D

jcano@uniandes.edu.co

Lista de Seguridad Informática
-SEGURINFO-

Andrés R. Almanza, Ms(c)

andres_almanza@hotmail.com

ACIS

Agenda

- Presentación de Resultados
  - Componentes de la Encuesta
  - Datos
- Conclusiones

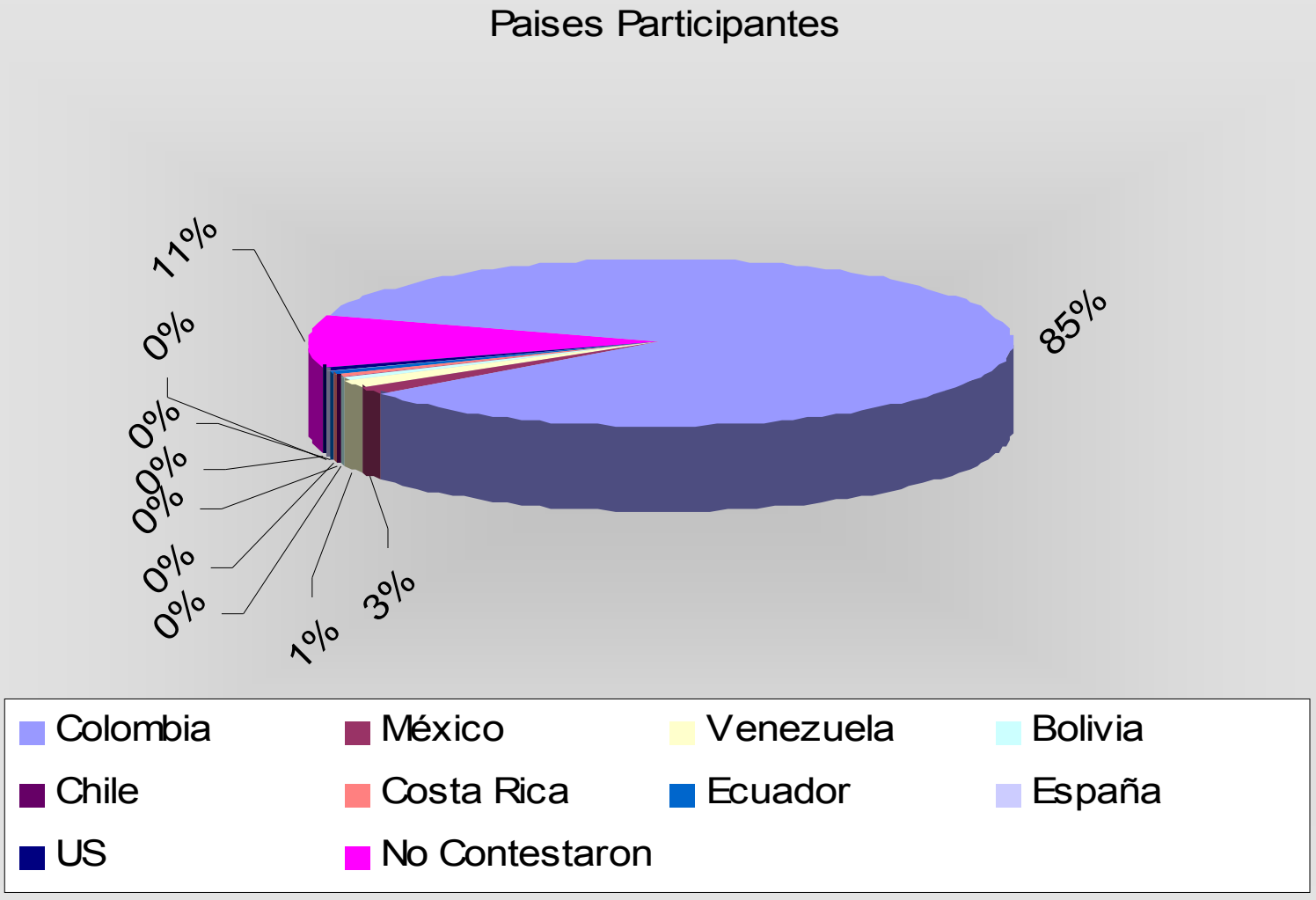
Estructura de la Encuesta

- Cuestionario compuesto por 20 preguntas sobre los siguientes temas:
  - Demografía
  - Presupuestos
  - Fallas de seguridad
  - Herramientas y prácticas de seguridad
  - Políticas de seguridad

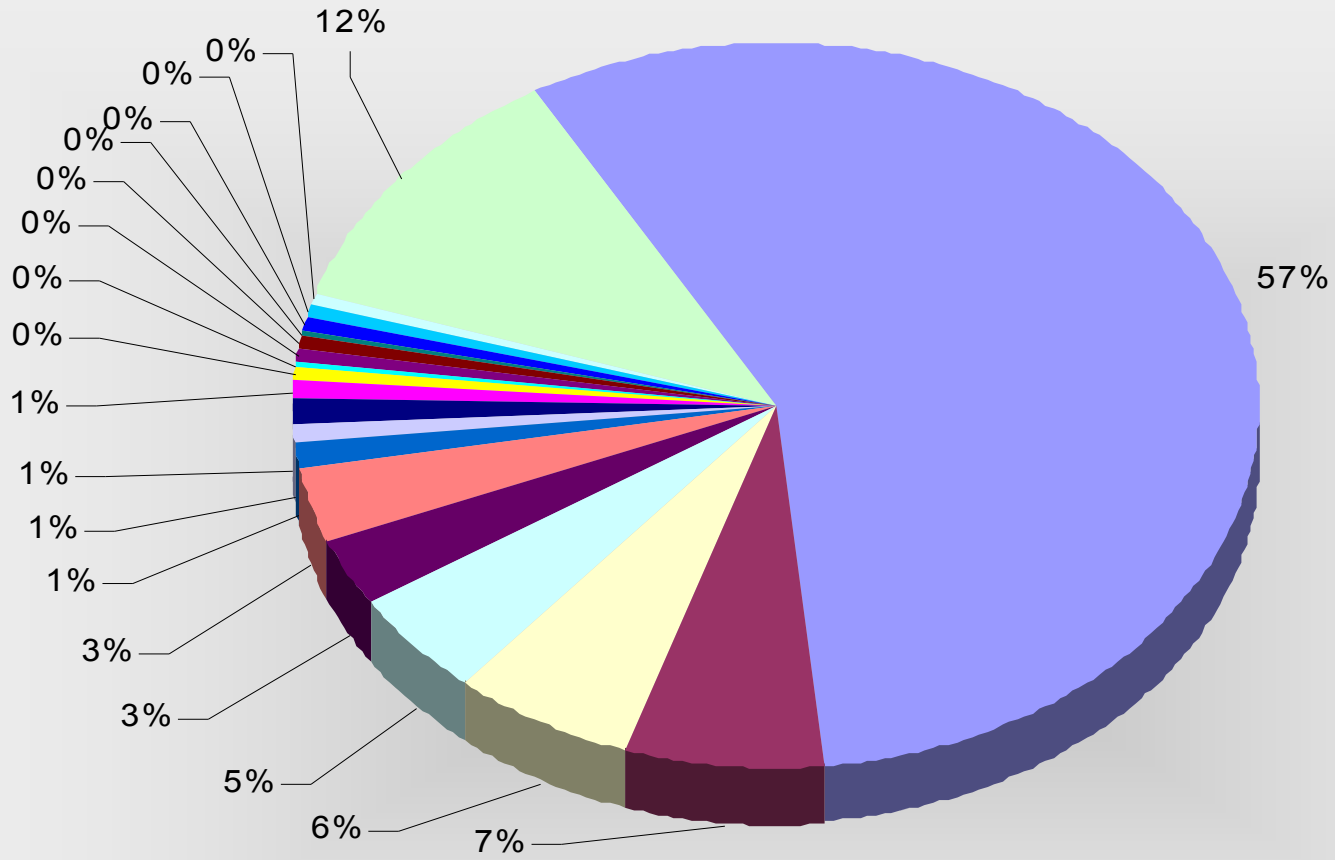
Consideraciones Muestrales

- El número de participantes este año es de 223 personas (en comparación con las 182 del 2005).
- Mayor población población de los diferentes sectores productivos sobre el tema de seguridad informática en el país.
- Considerando una población limitada (alrededor de 1400 personas que participan activamente en la lista de seguridad SEGURINFO) se ha estimado un error muestral de 7% (confianza del 93%), lo cual nos permite manejar una muestra adecuada cercana a los 178 participantes. Al contar con 223 participantes en la muestra, los resultados presentados son estadísticamente representativos

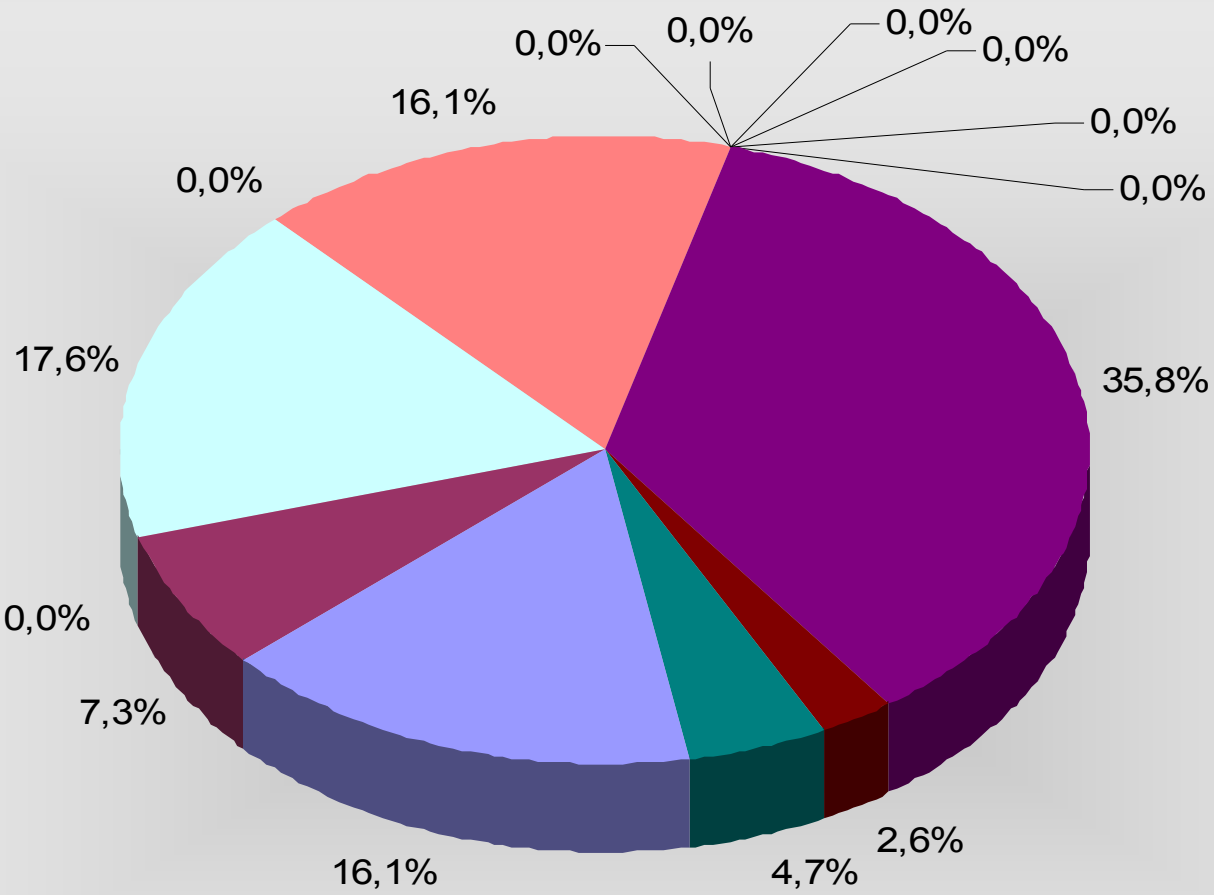
Paises Participantes



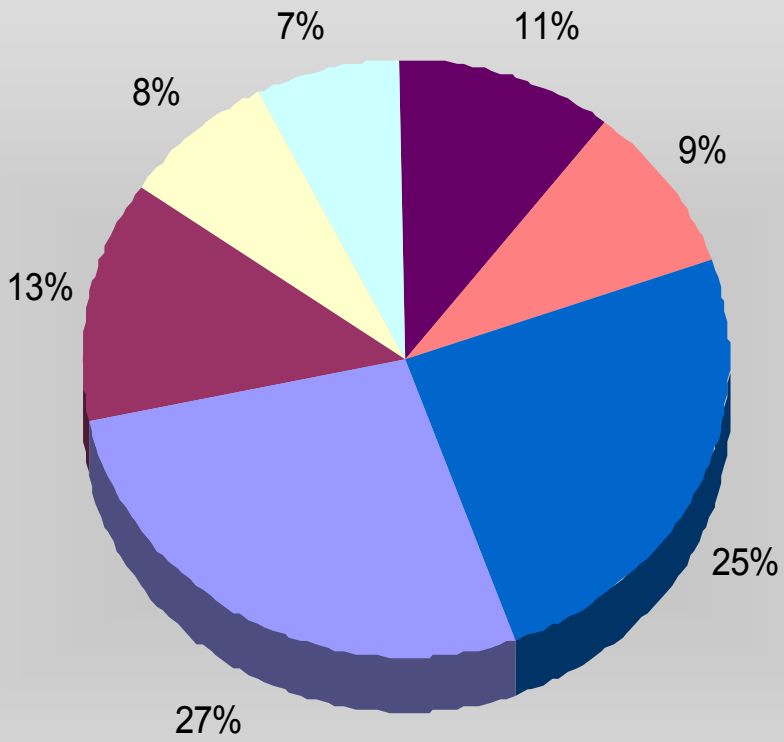
Ciudades de Colombia



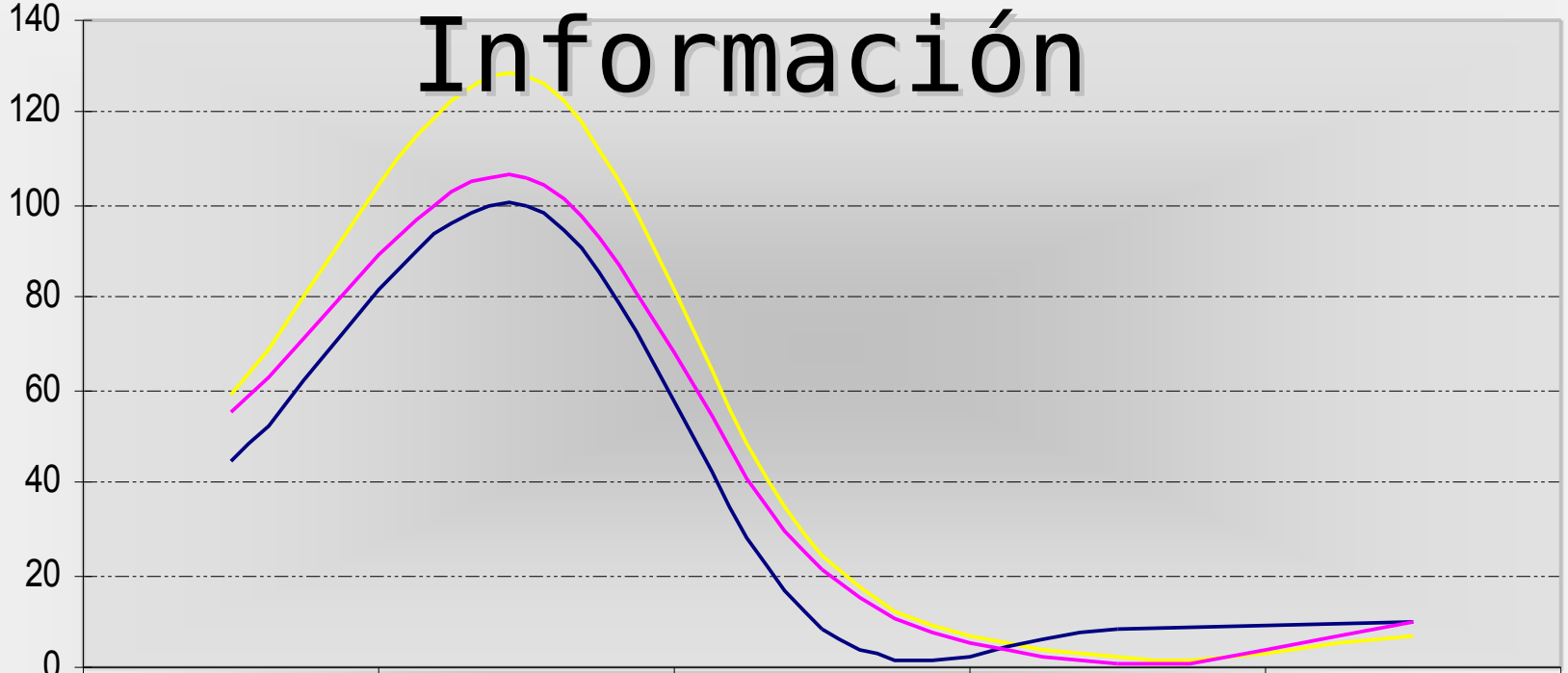
Sectores Participantes



Número de Empleados en la compañía

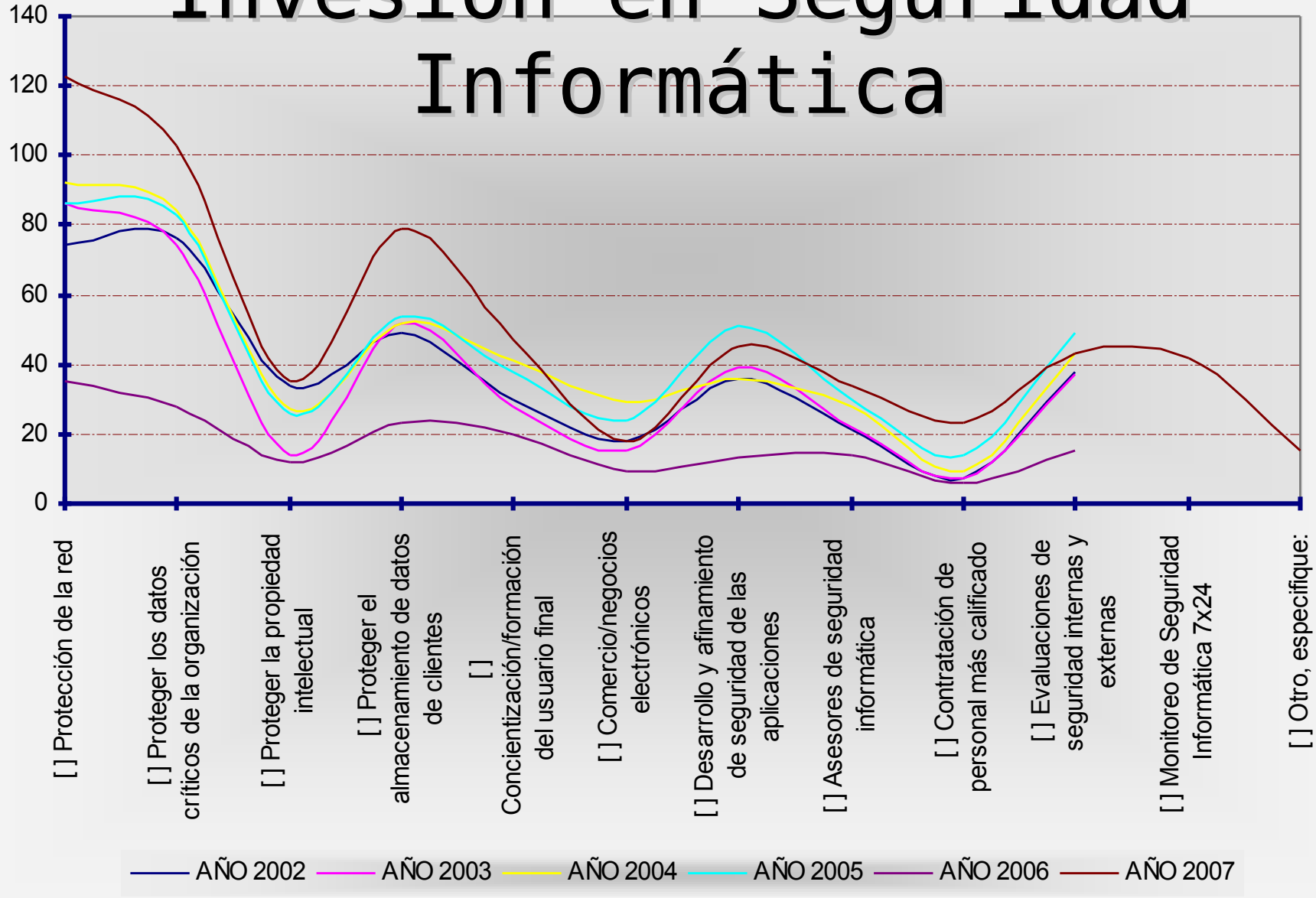


Personal de Seguridad de la Información

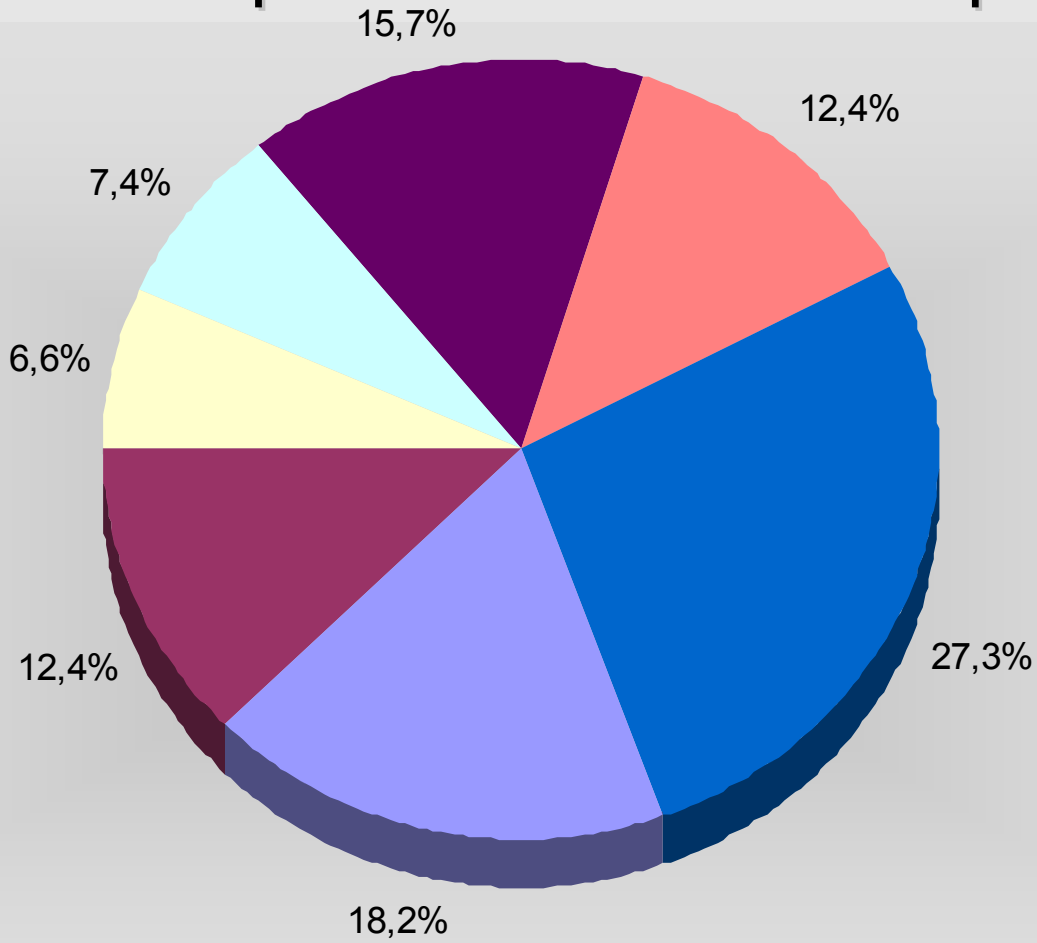


	Ninguna	1 a 5	6 a 10	11 a 15	más de 15
2004	59	128	24	2	7
2005	45	100	8	8	10
2007	55	106	21	1	10

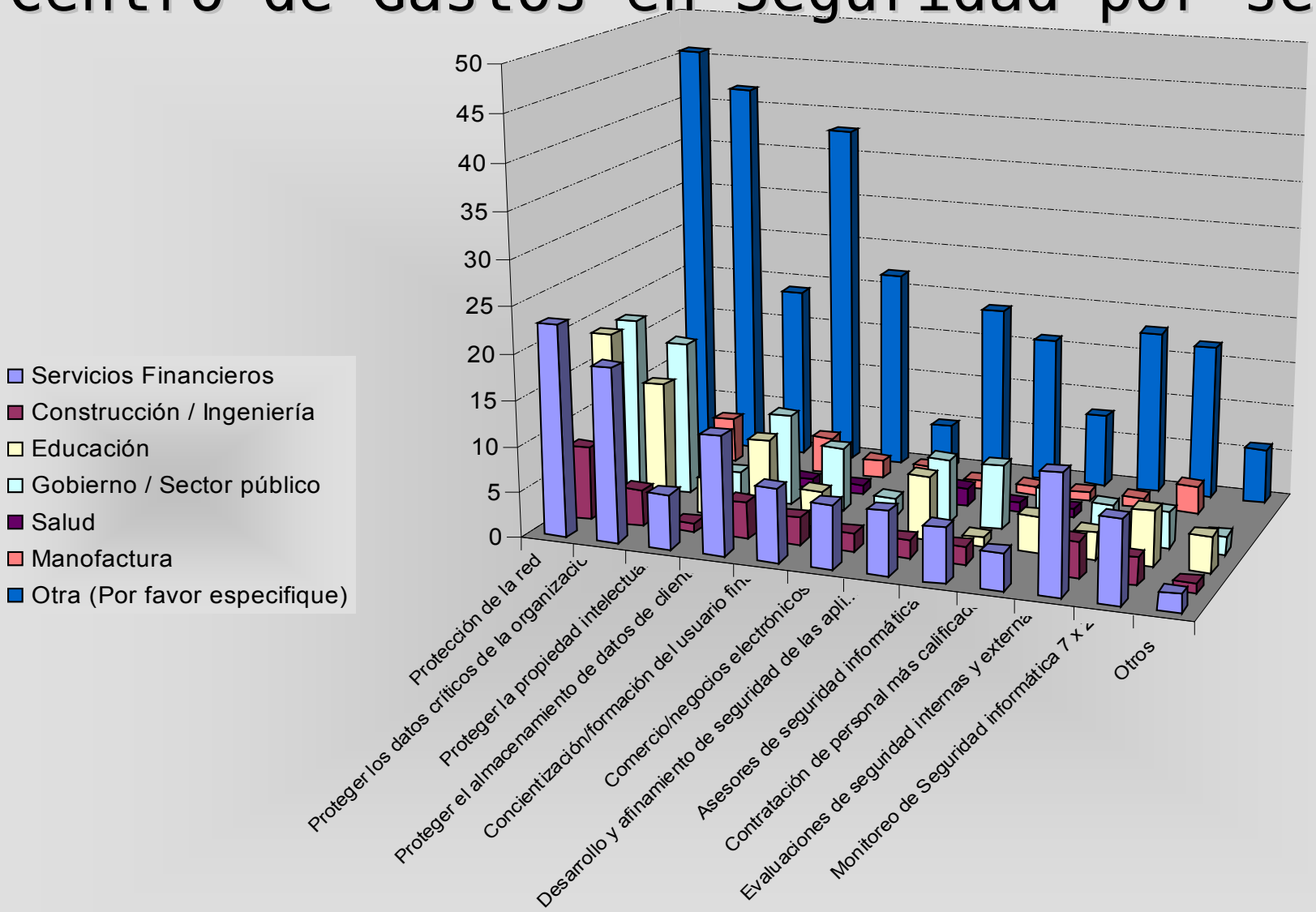
Invesión en Seguridad Informática



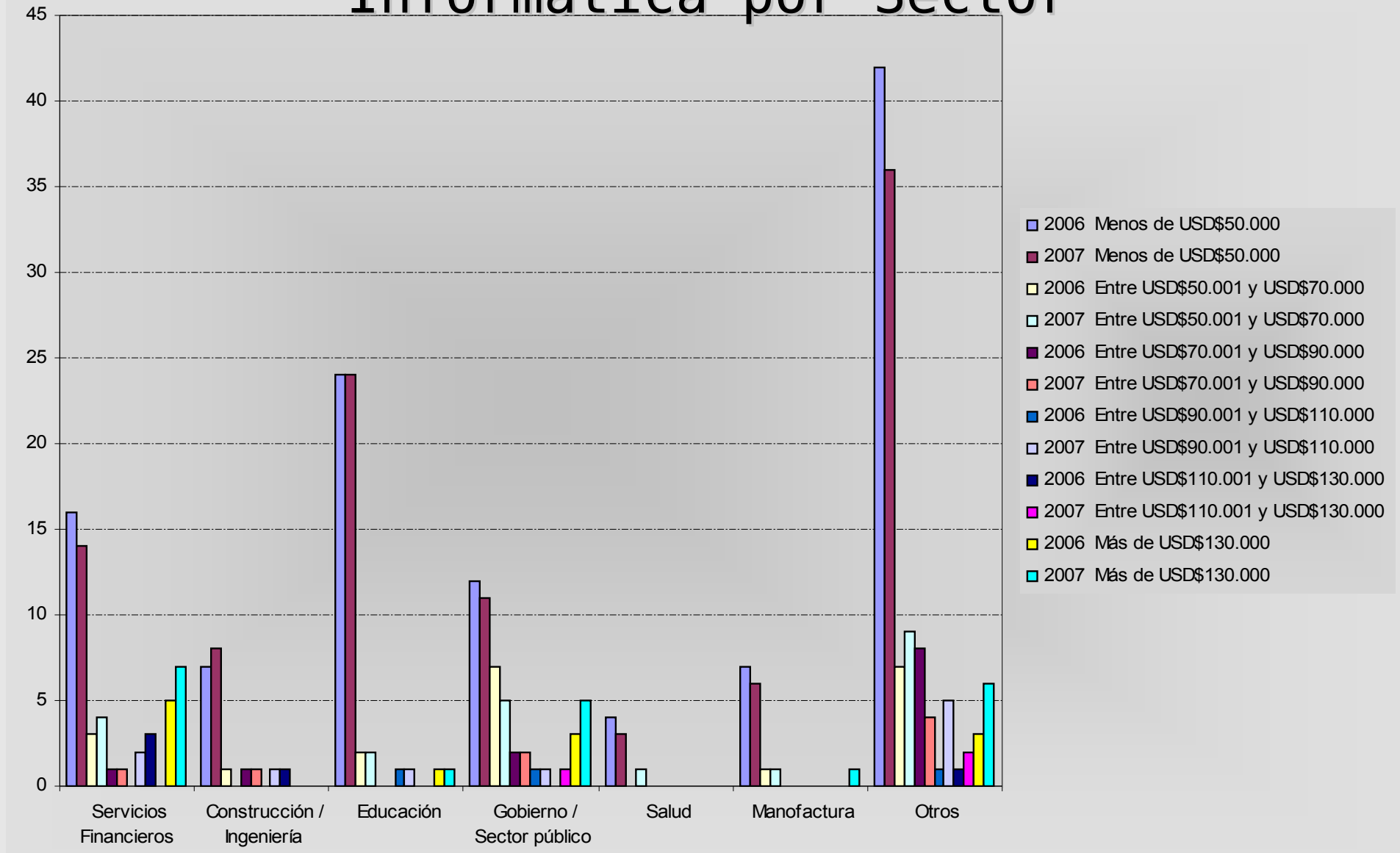
Inclusión de Tópicos en presupuestos en Seguridad por Tamaño de Empresas



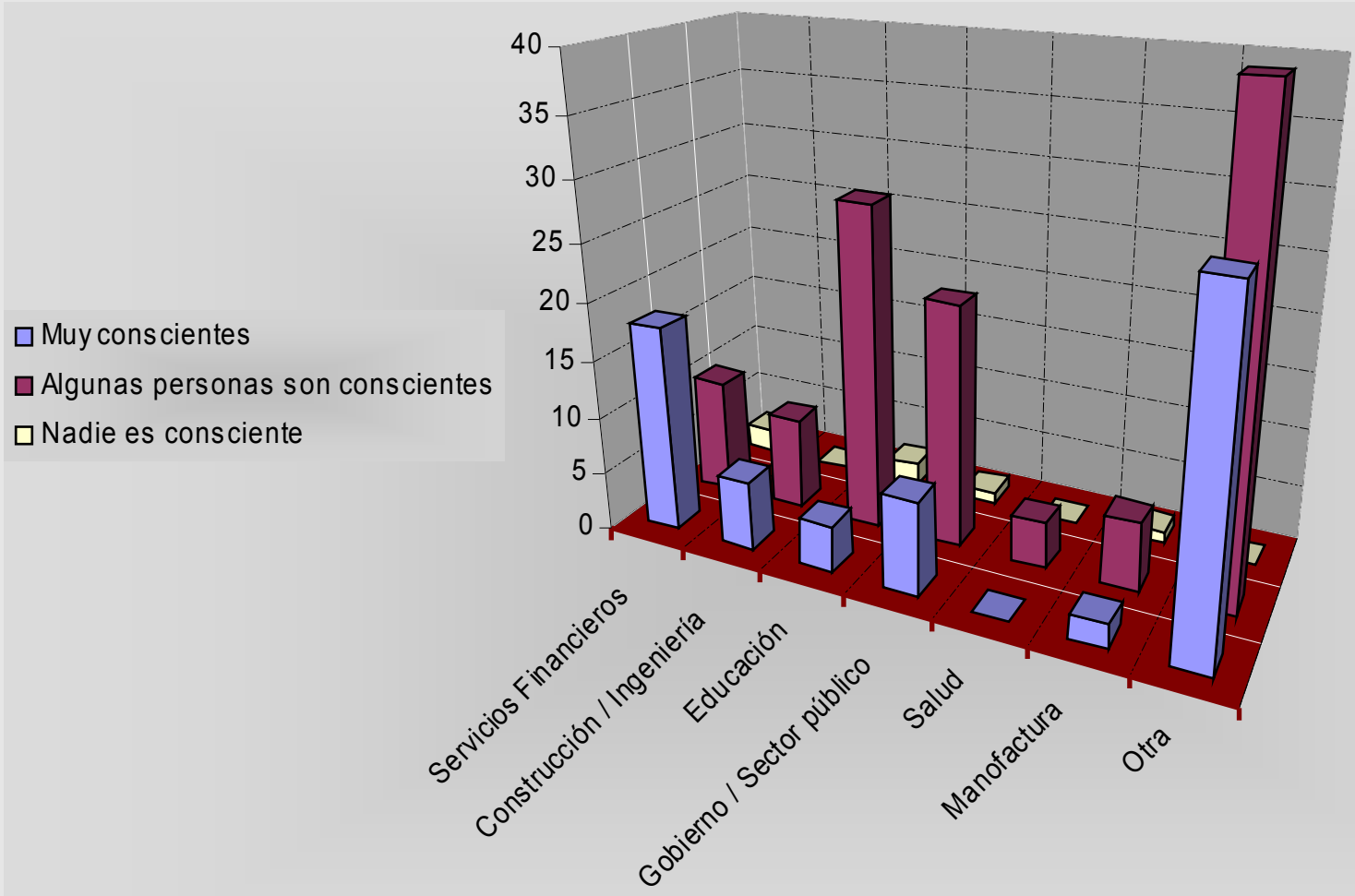
Centro de Gastos en Seguridad por sector



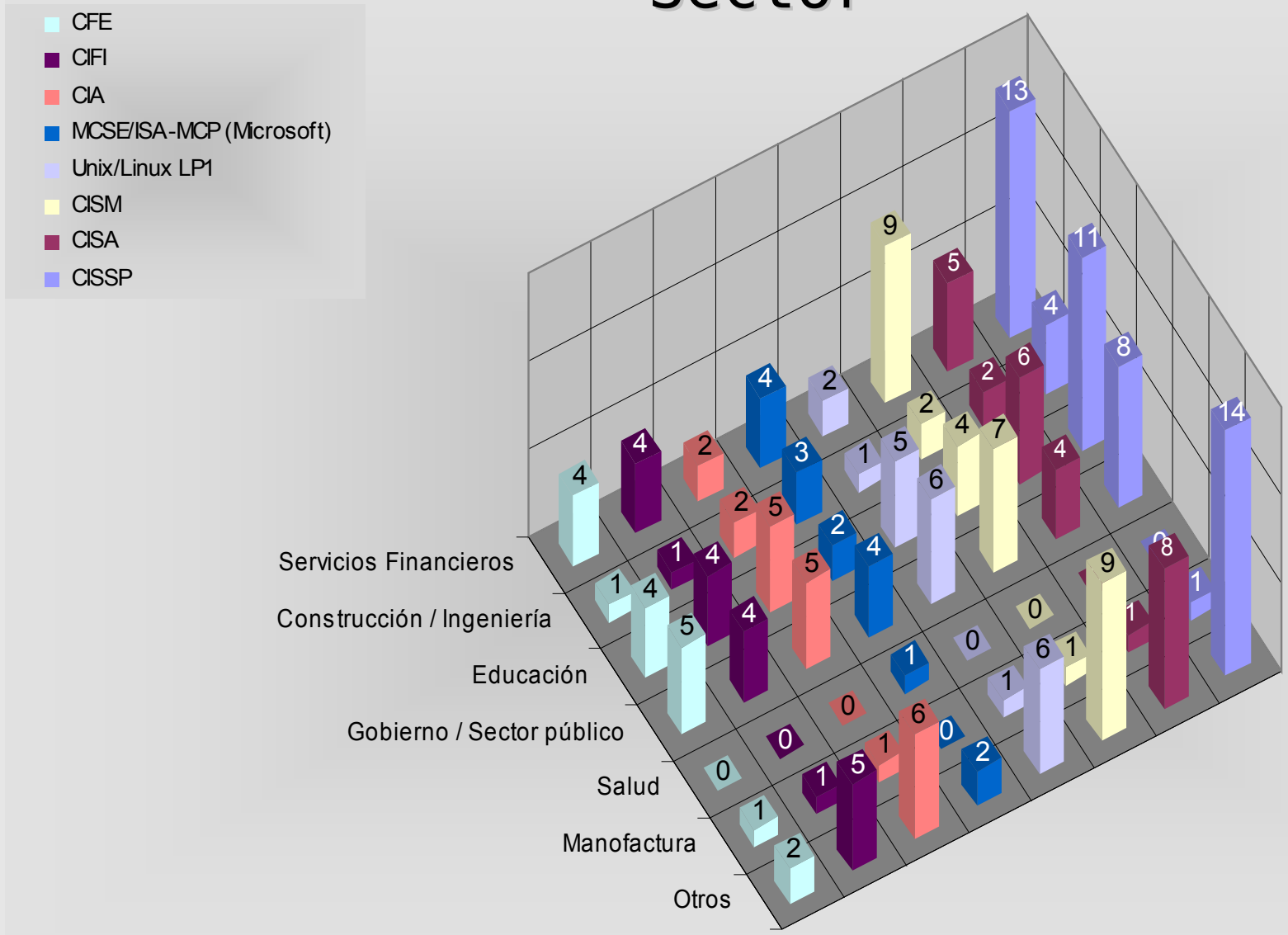
Presupuestos/Proyección en Seguridad Informática por Sector



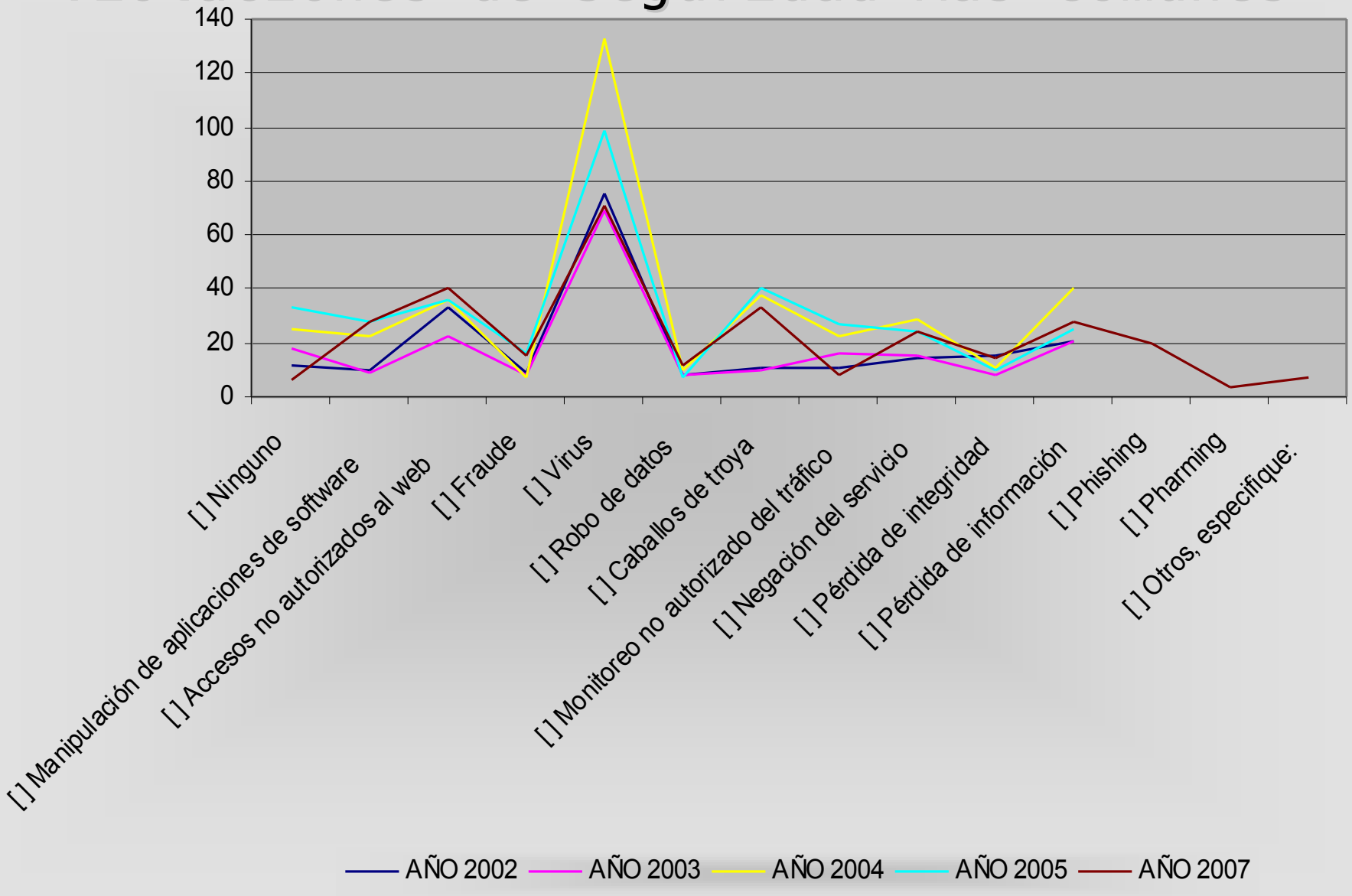
Conciencia en Seguridad Informática



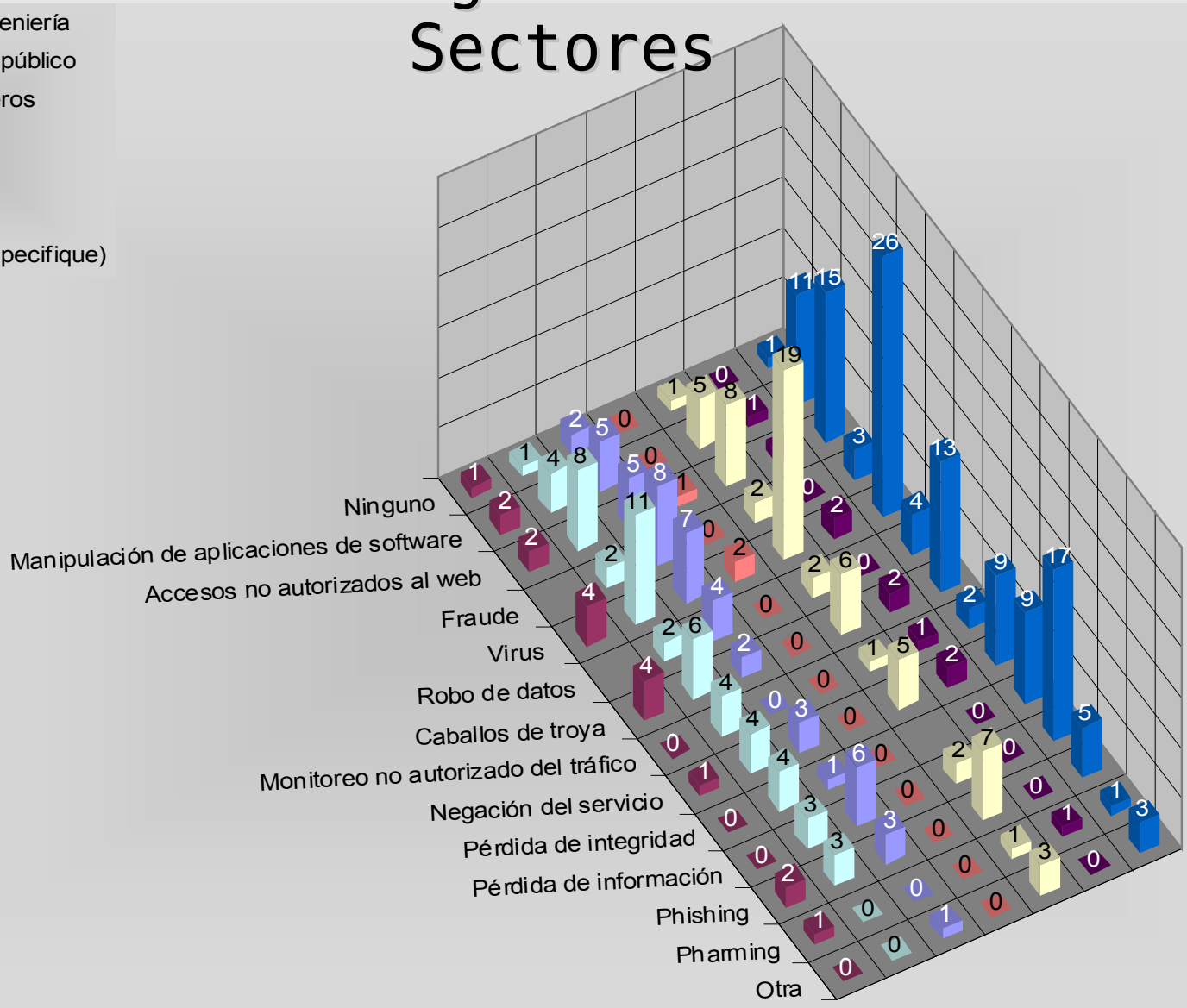
Importancia de las Certificaciones por Sector



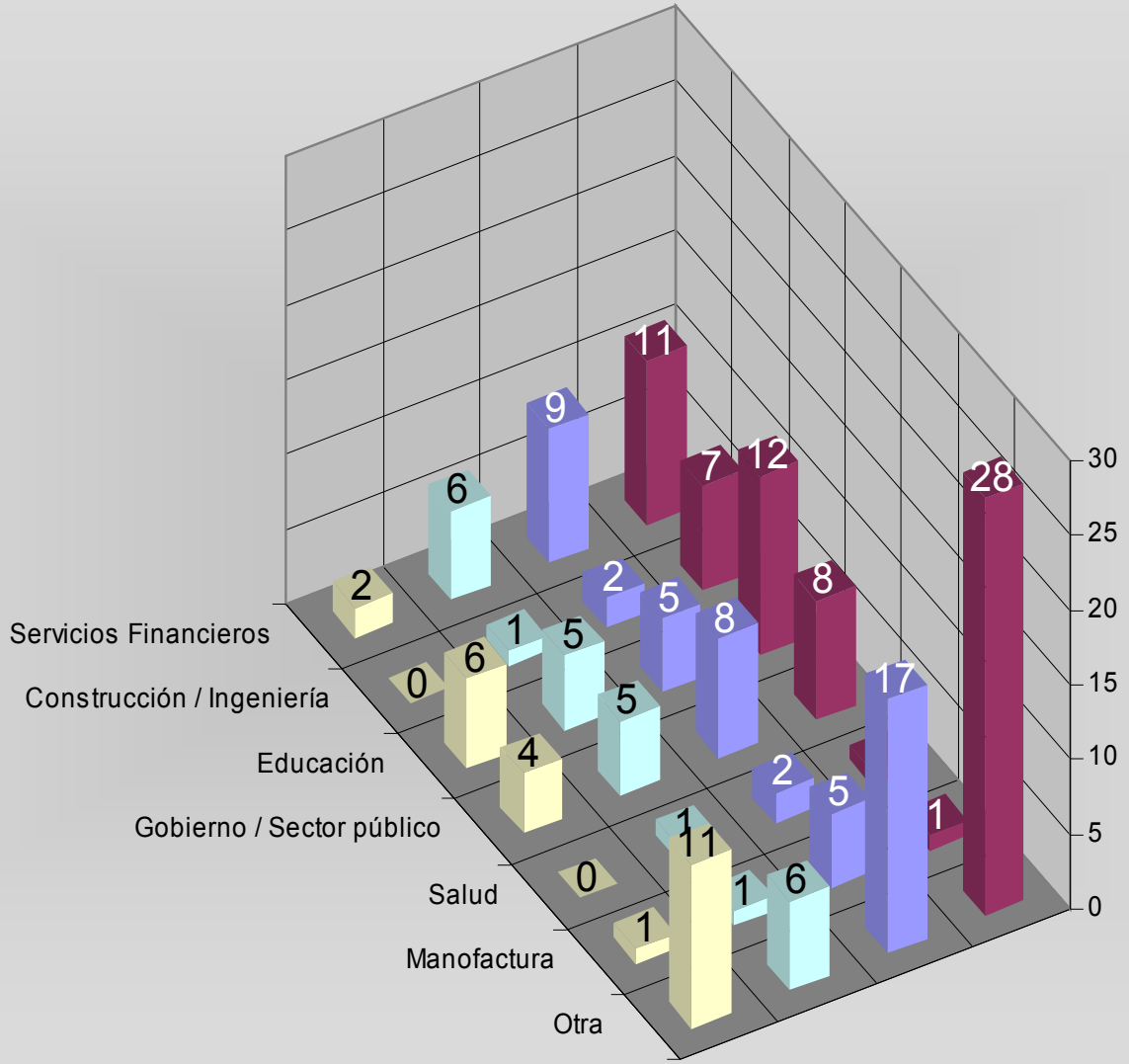
Violaciones de Seguridad Más Comunes



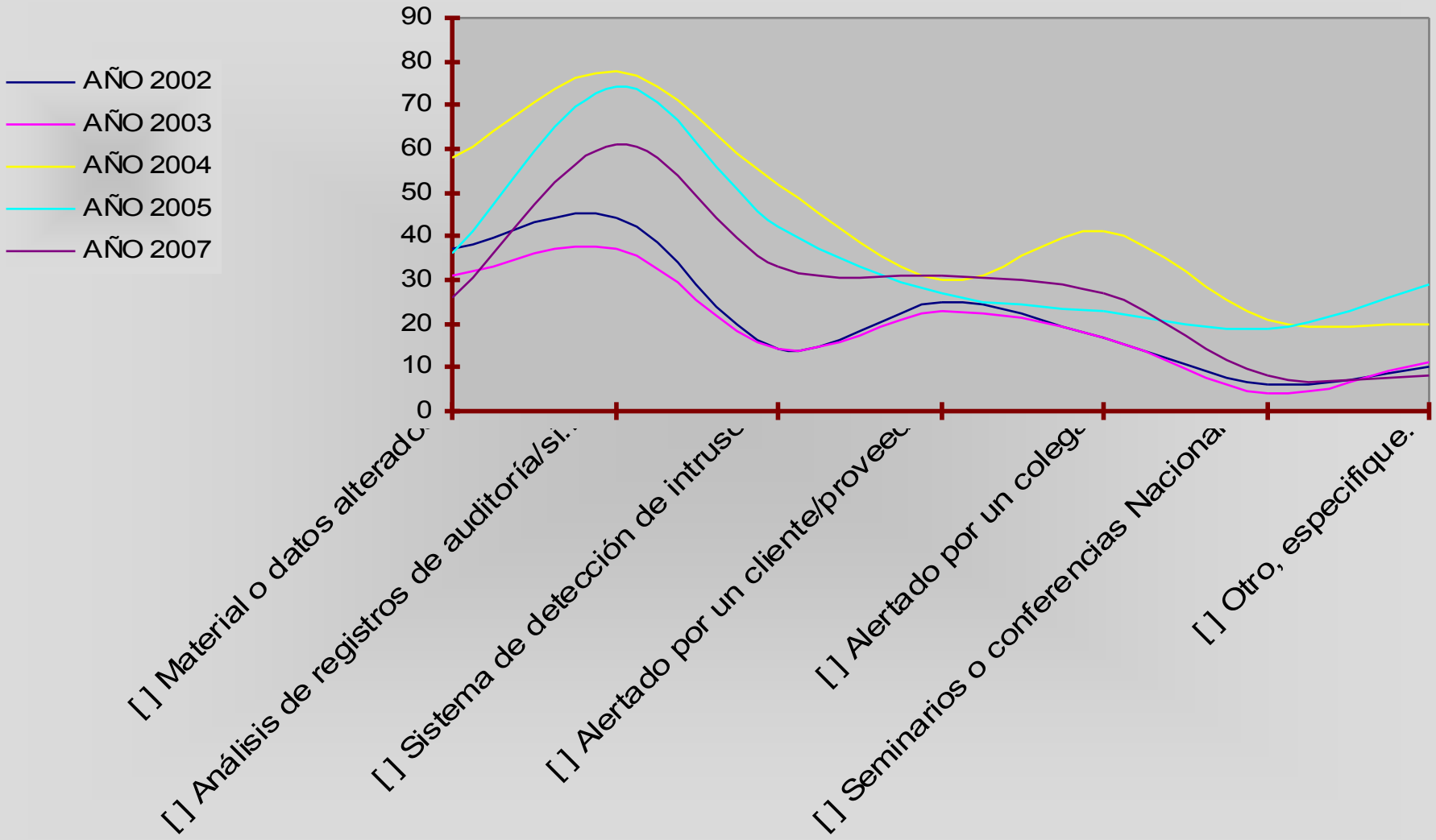
Violaciones de Seguridad Más Comunes por Sectores



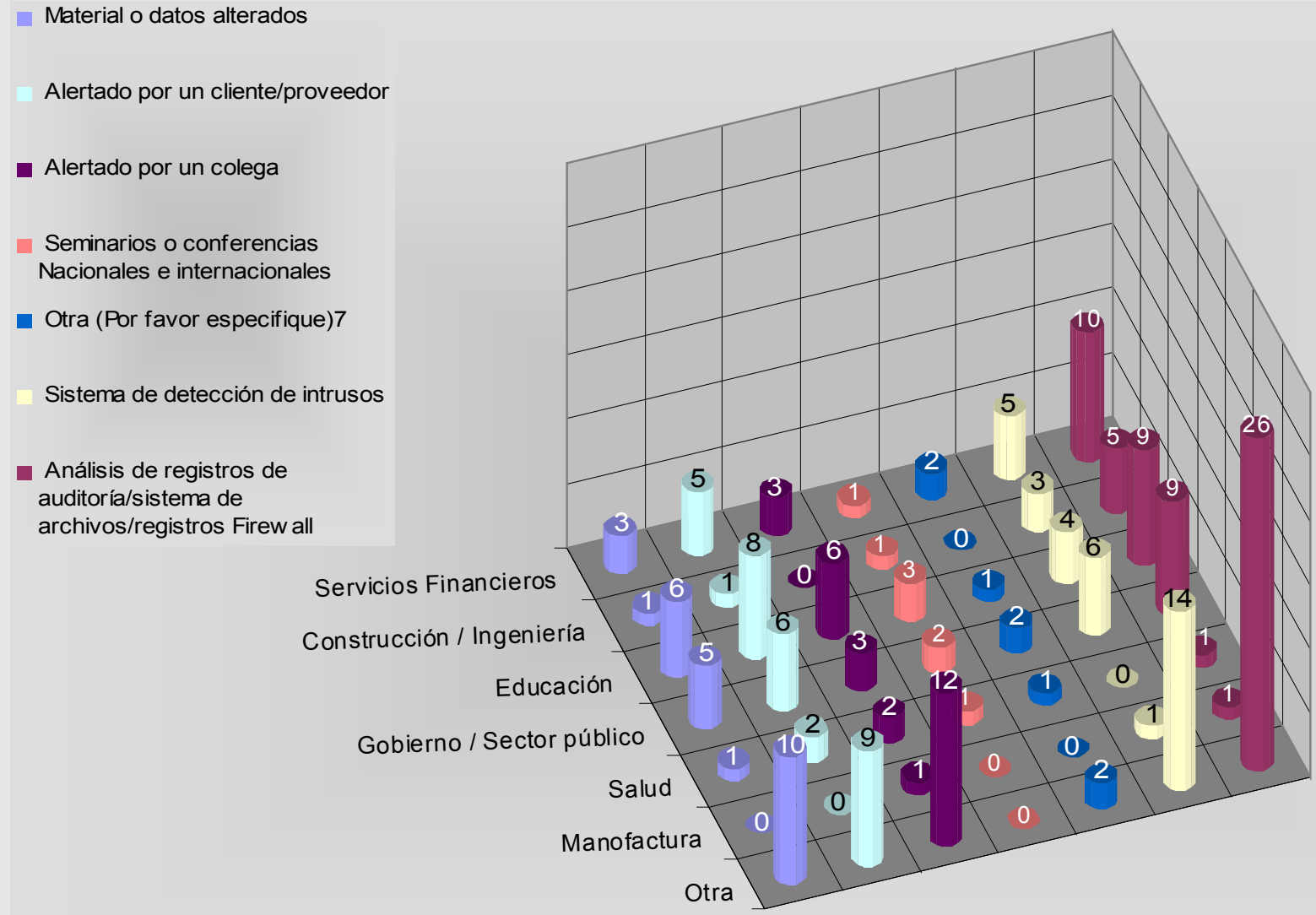
Intrusiones o Incidentes Identificados el año anterior



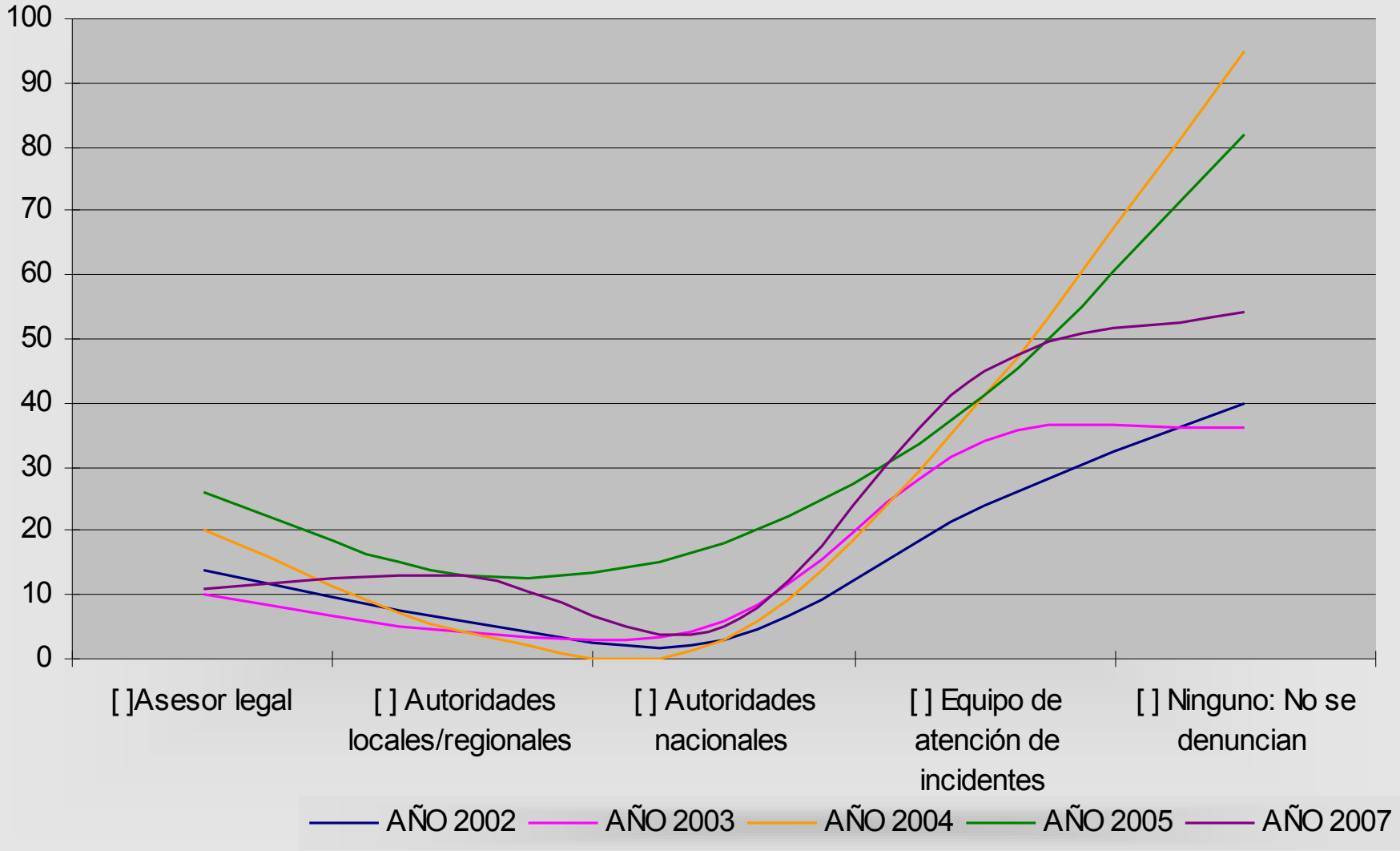
Como se entera de las violaciones de seguridad



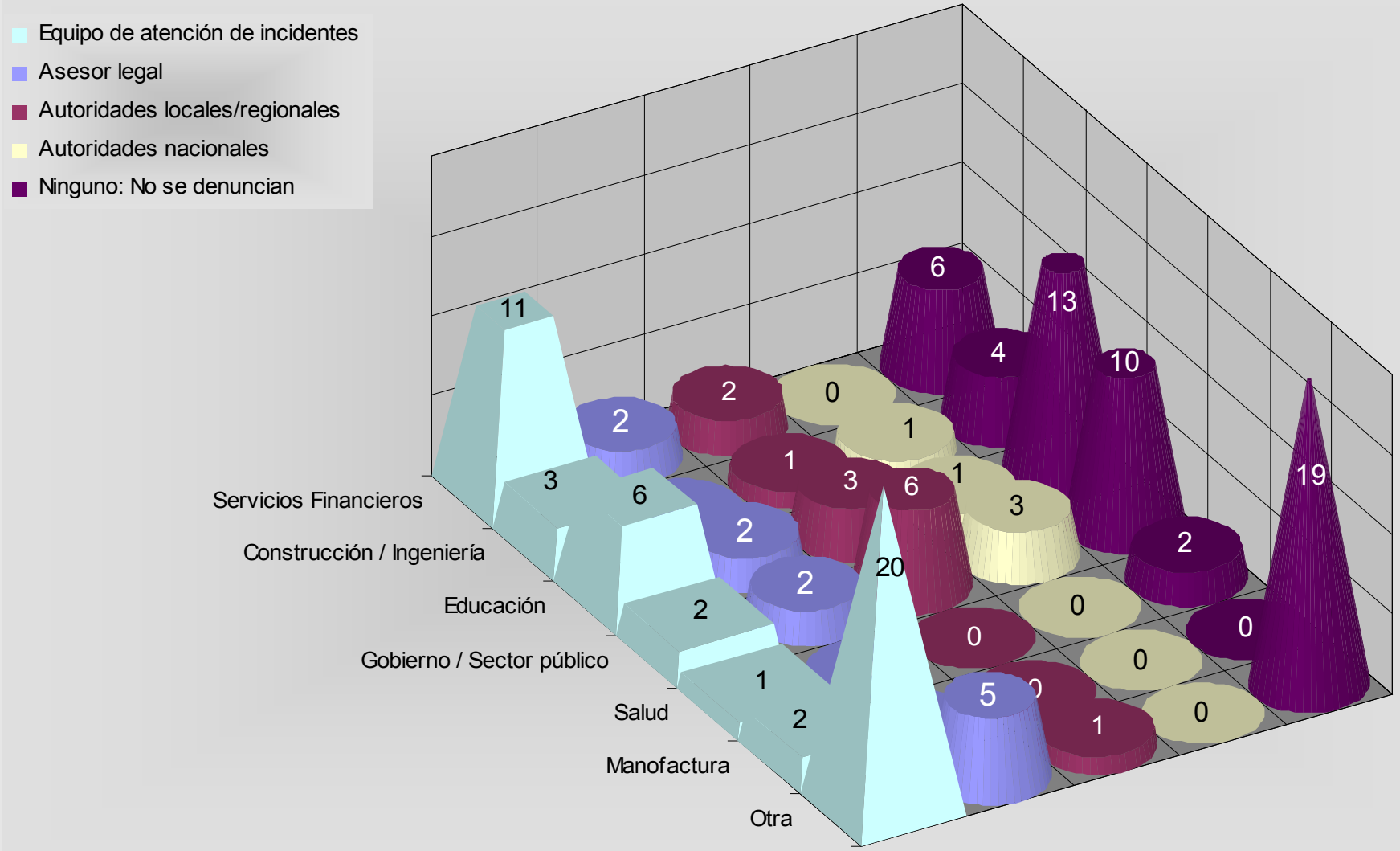
Como se entera de intrusiones



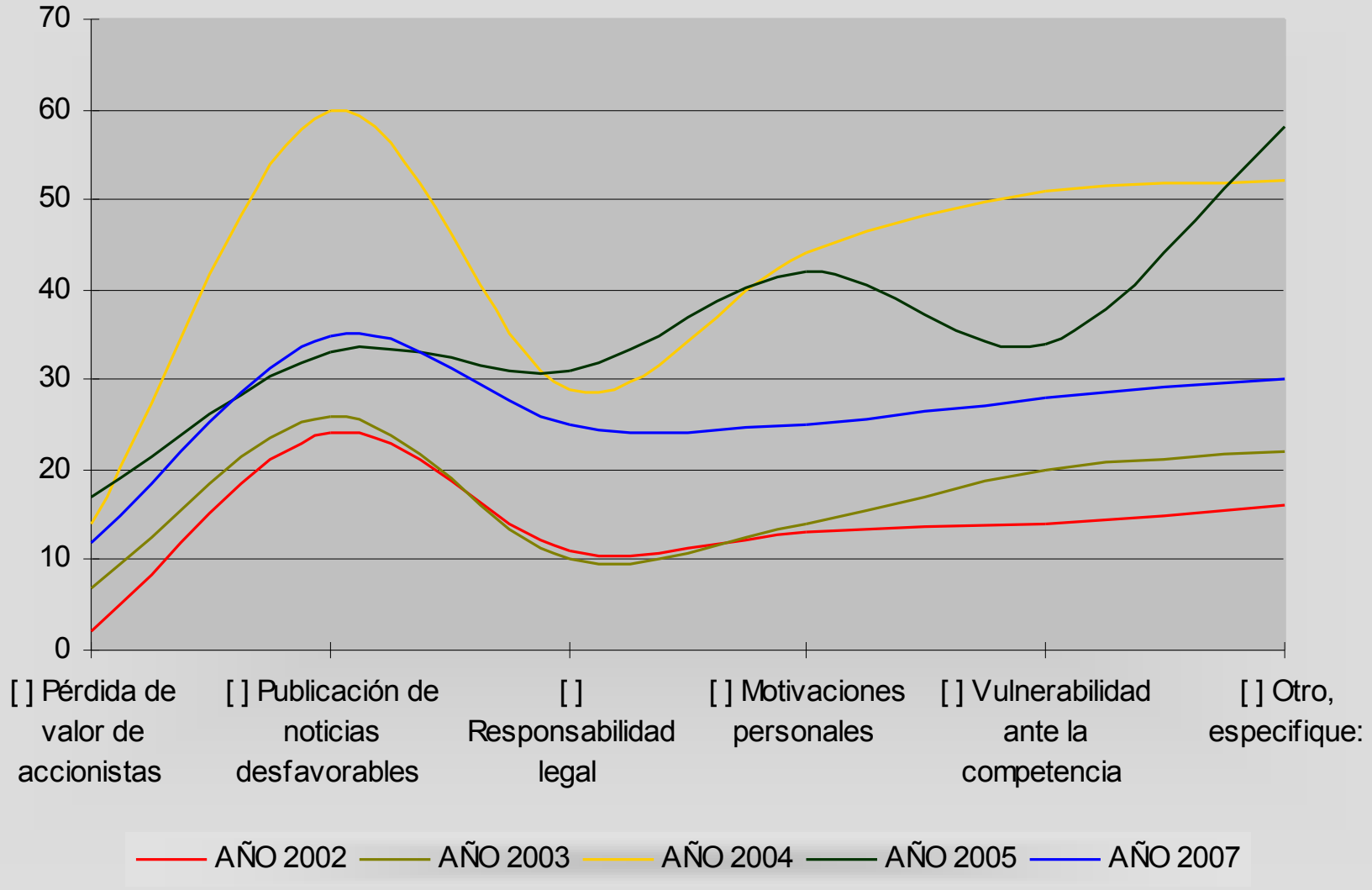
Notificación de las violaciones de seguridad



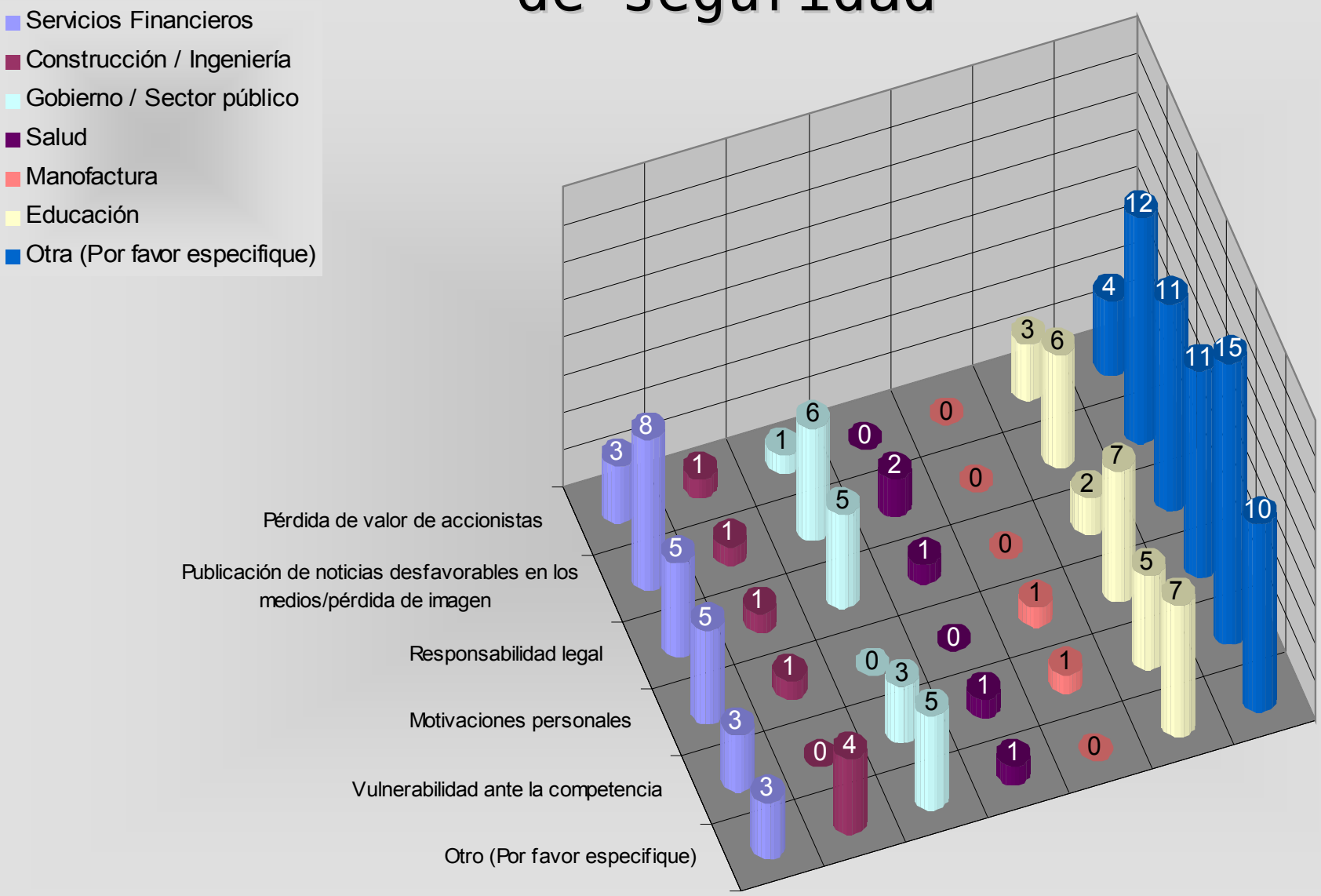
Notificación de Incidencias



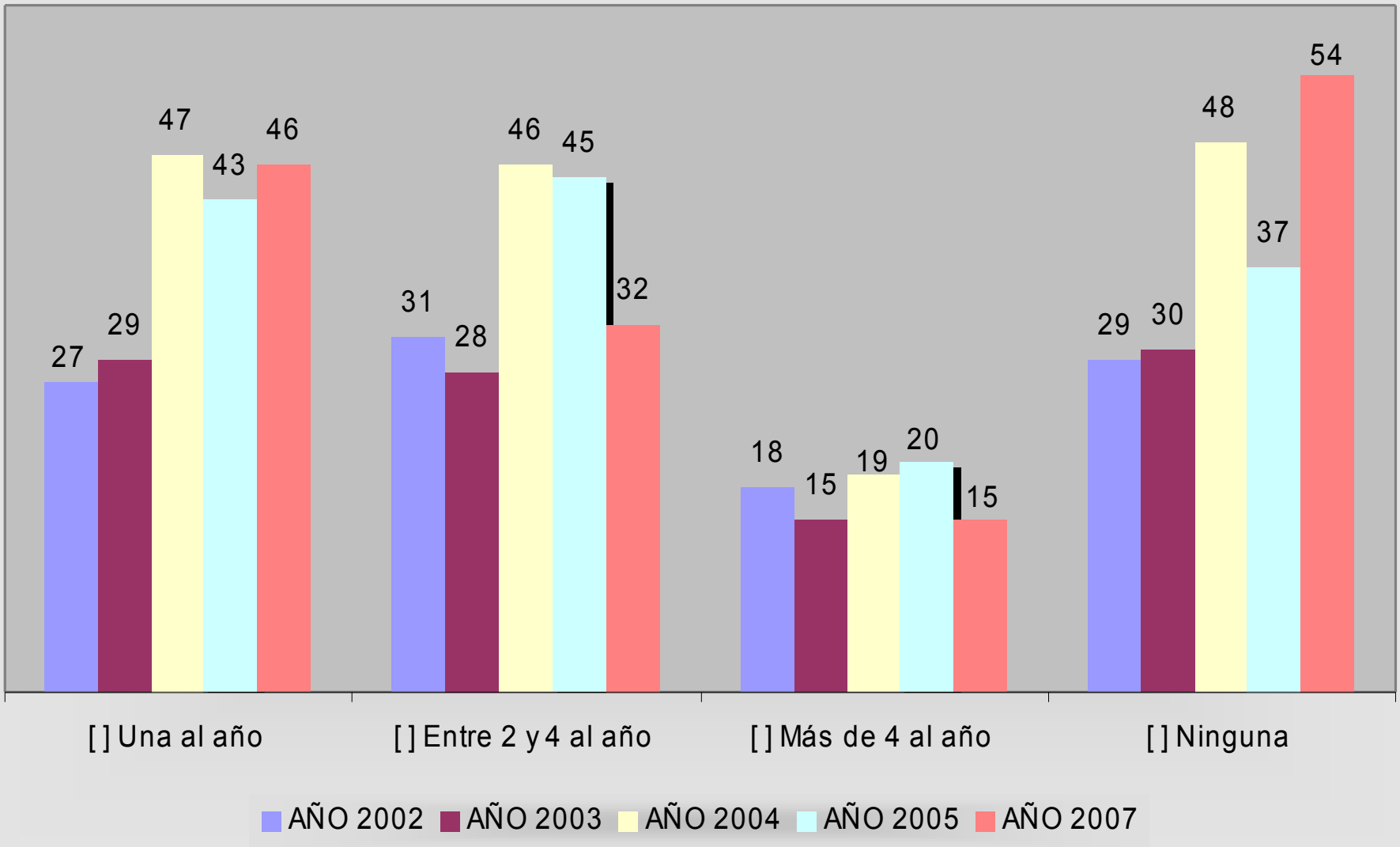
Motivos de No denunciar las violaciones de seguridad



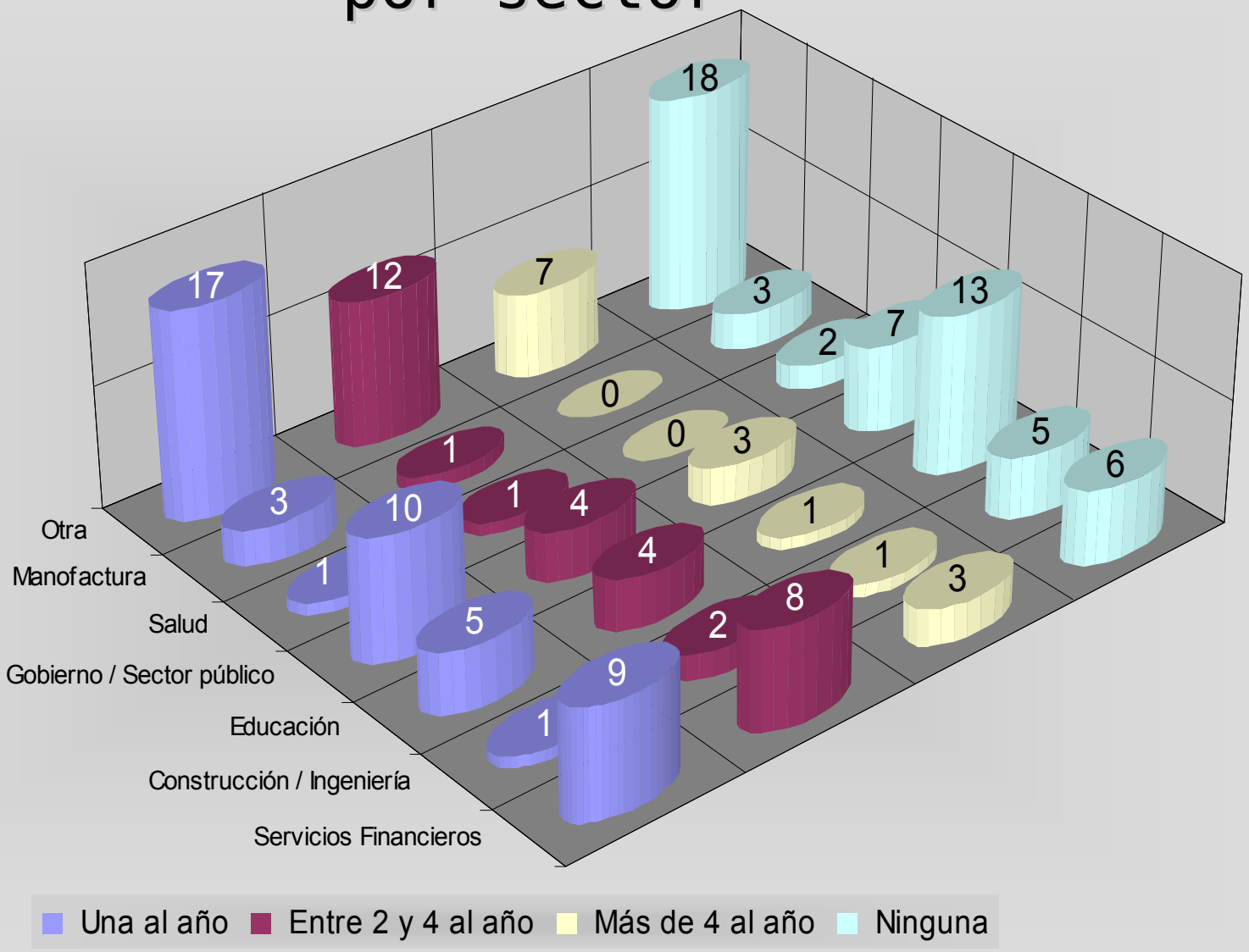
Motivos de No denunciar las violaciones de seguridad



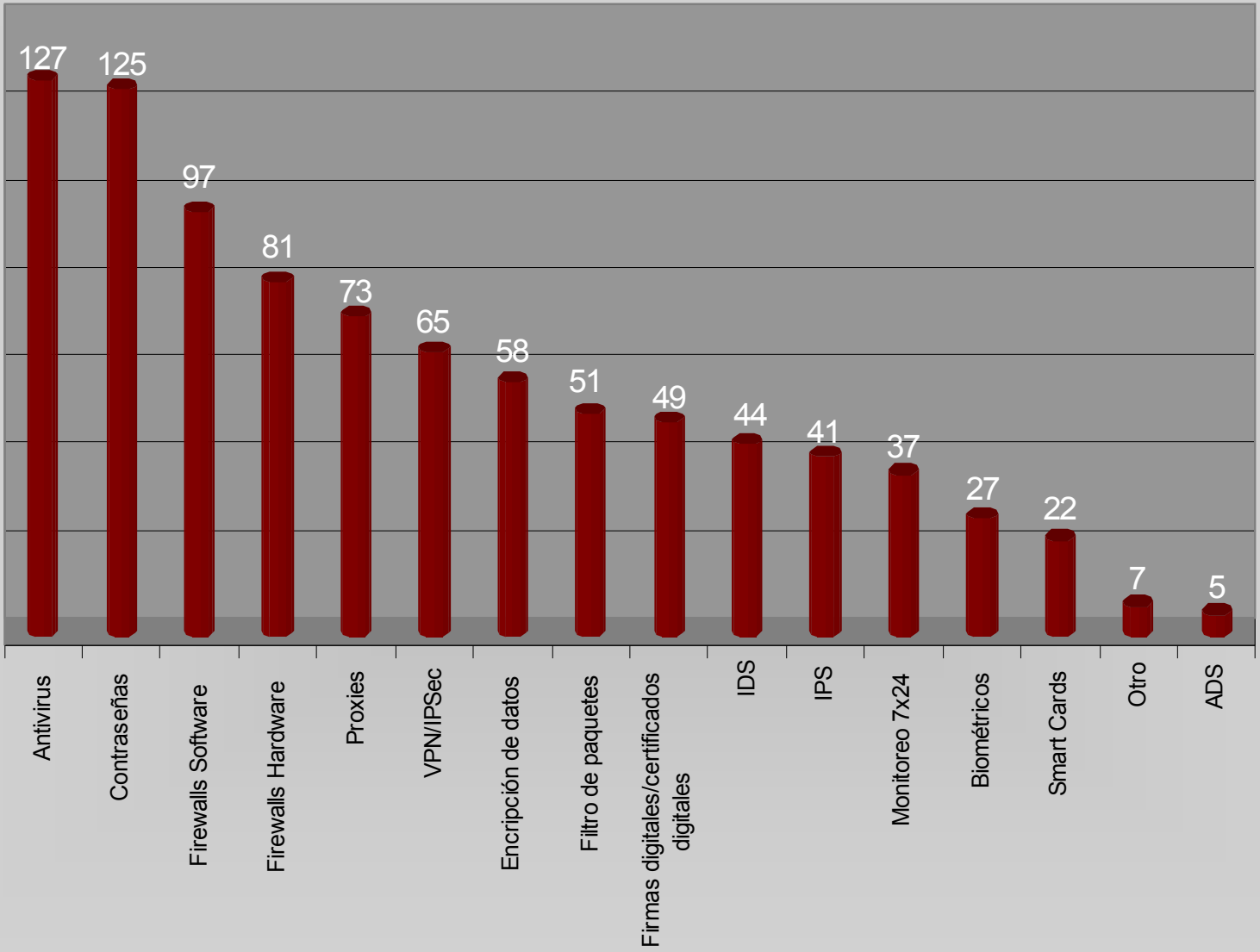
Pruebas de Seguridad Realizadas



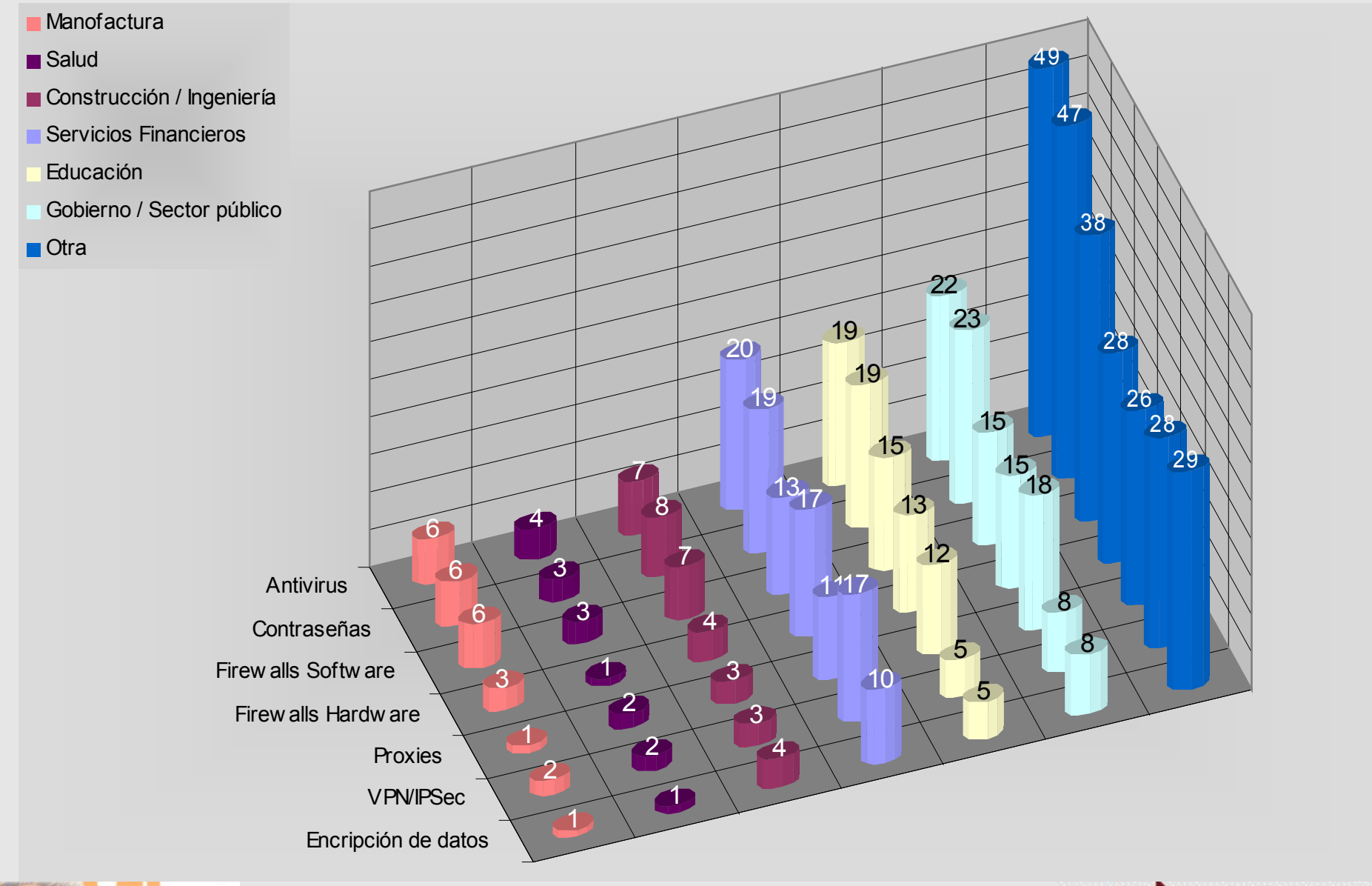
Utilización de las pruebas de seguridad por sector



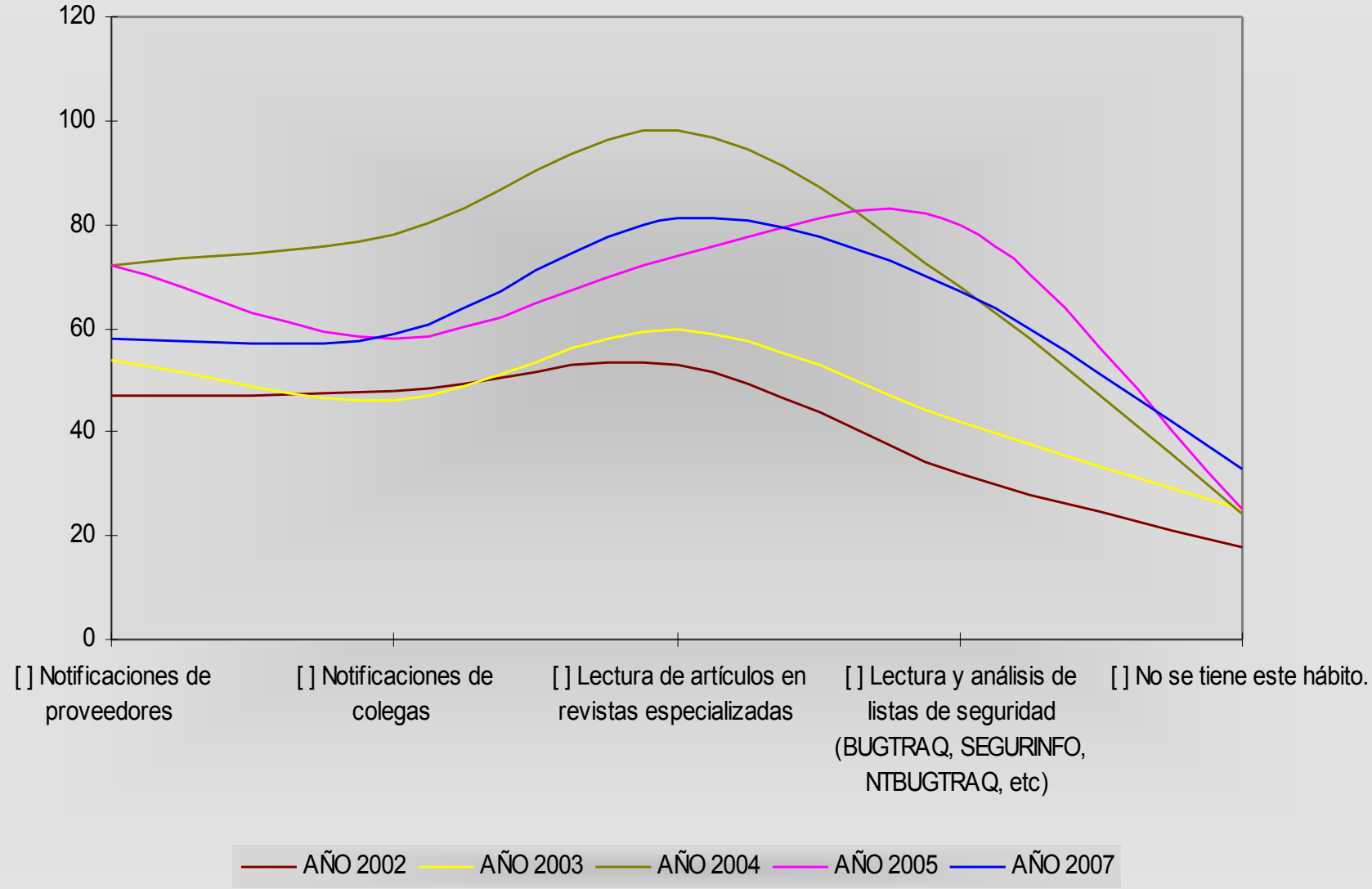
Top (10) Herramientas de Seguridad



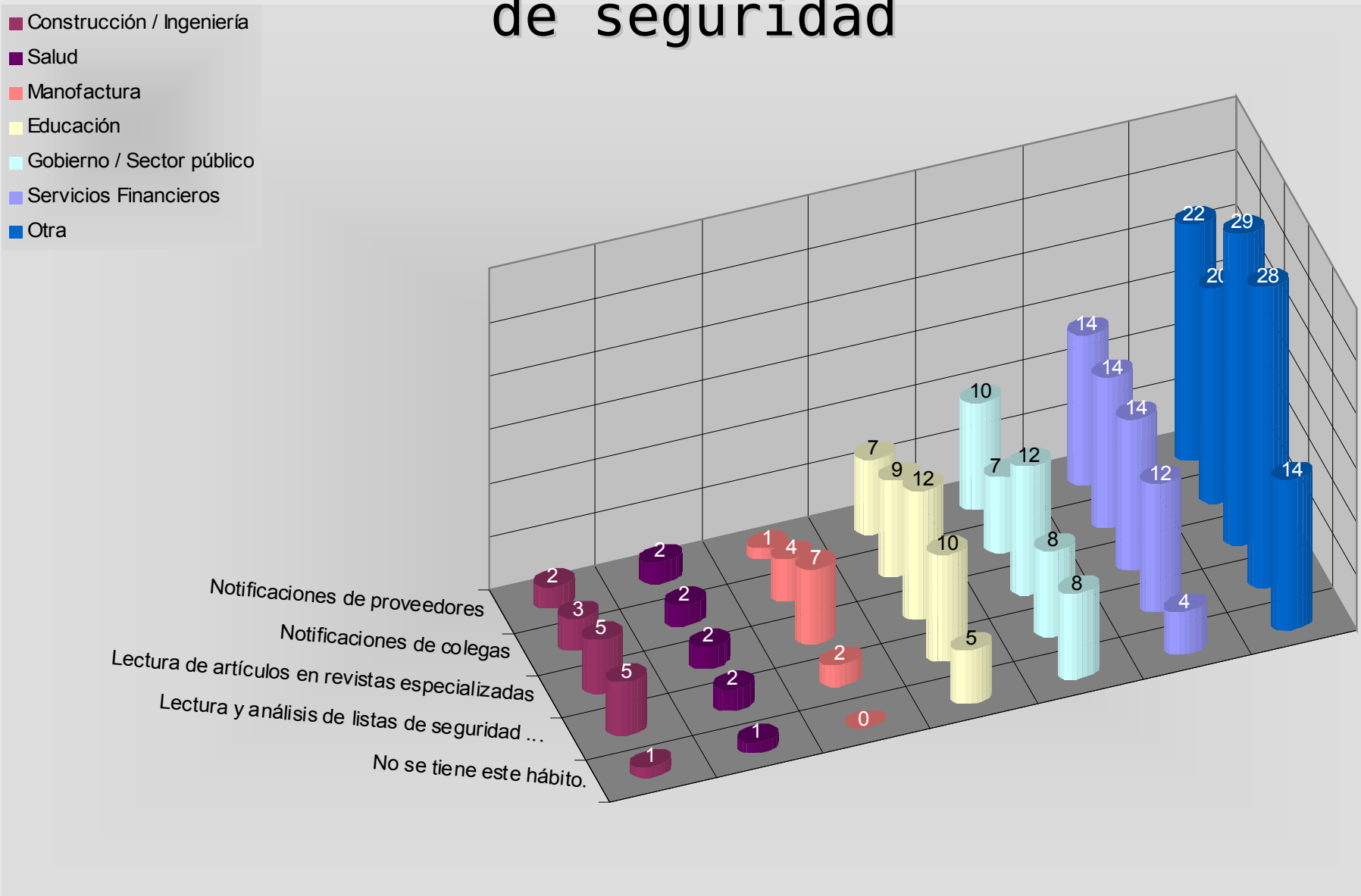
Herramientas de seguridad por sectores



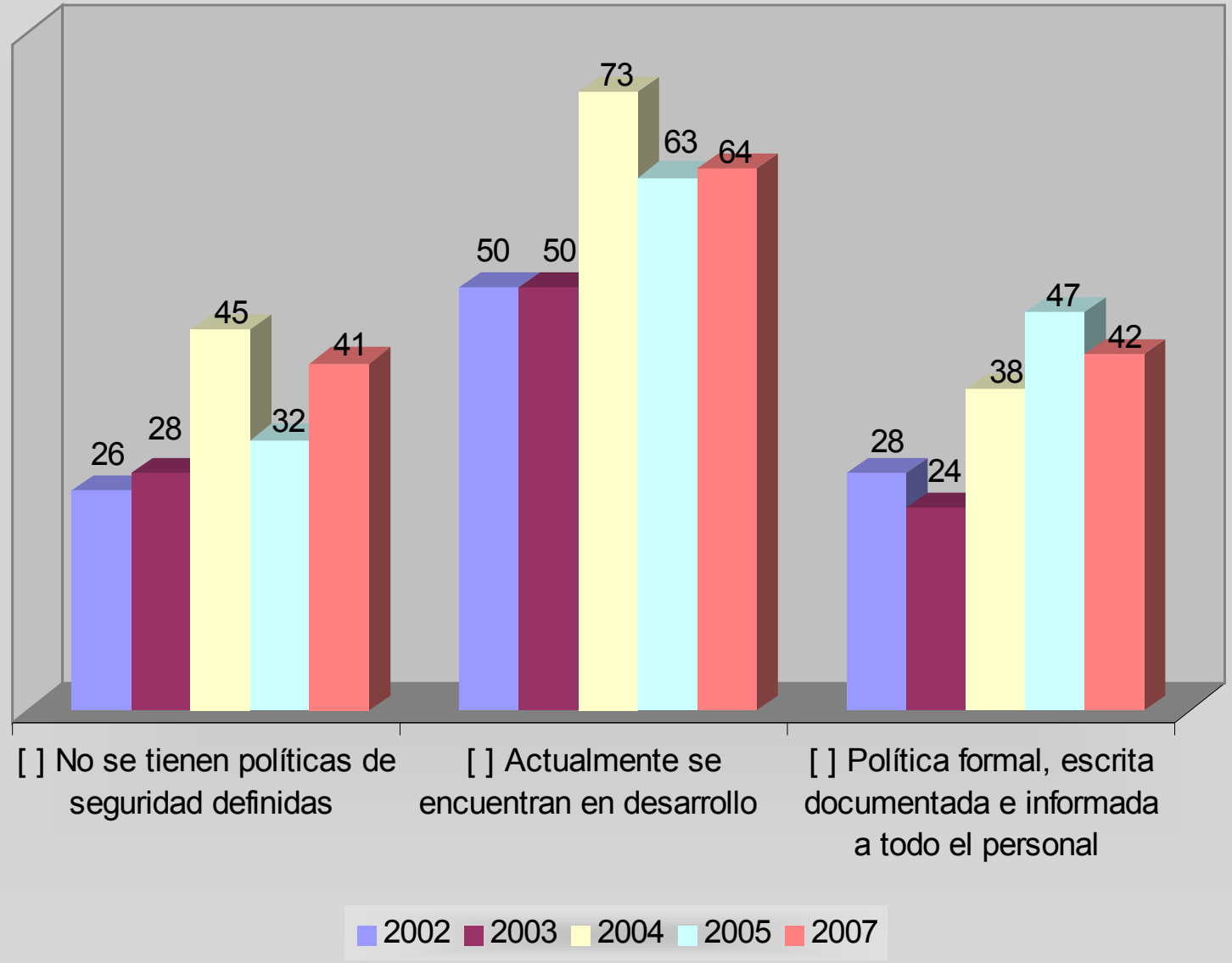
Investigación de la fallas de Seguridad



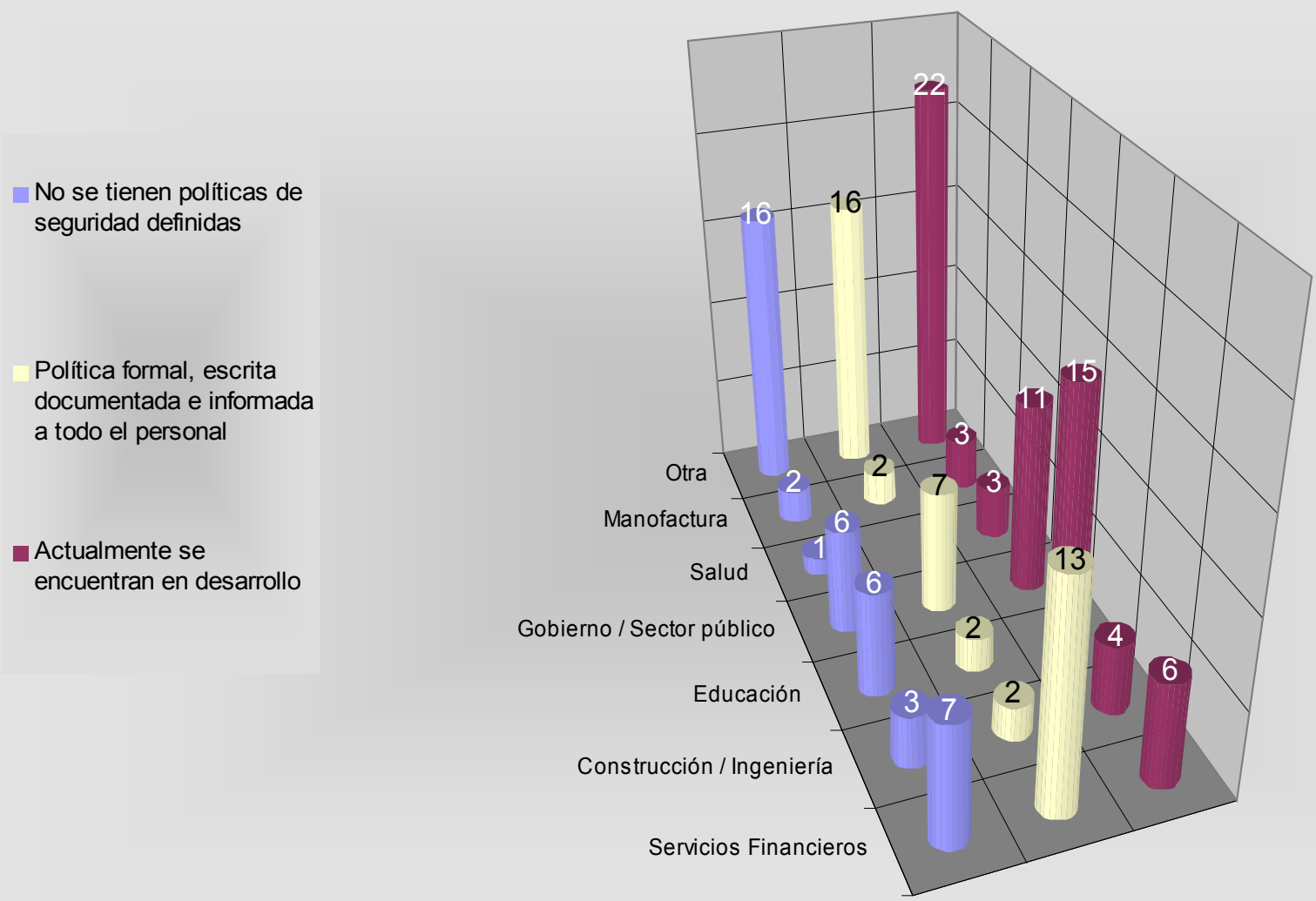
Investigacion sectorizada de las fallas de seguridad



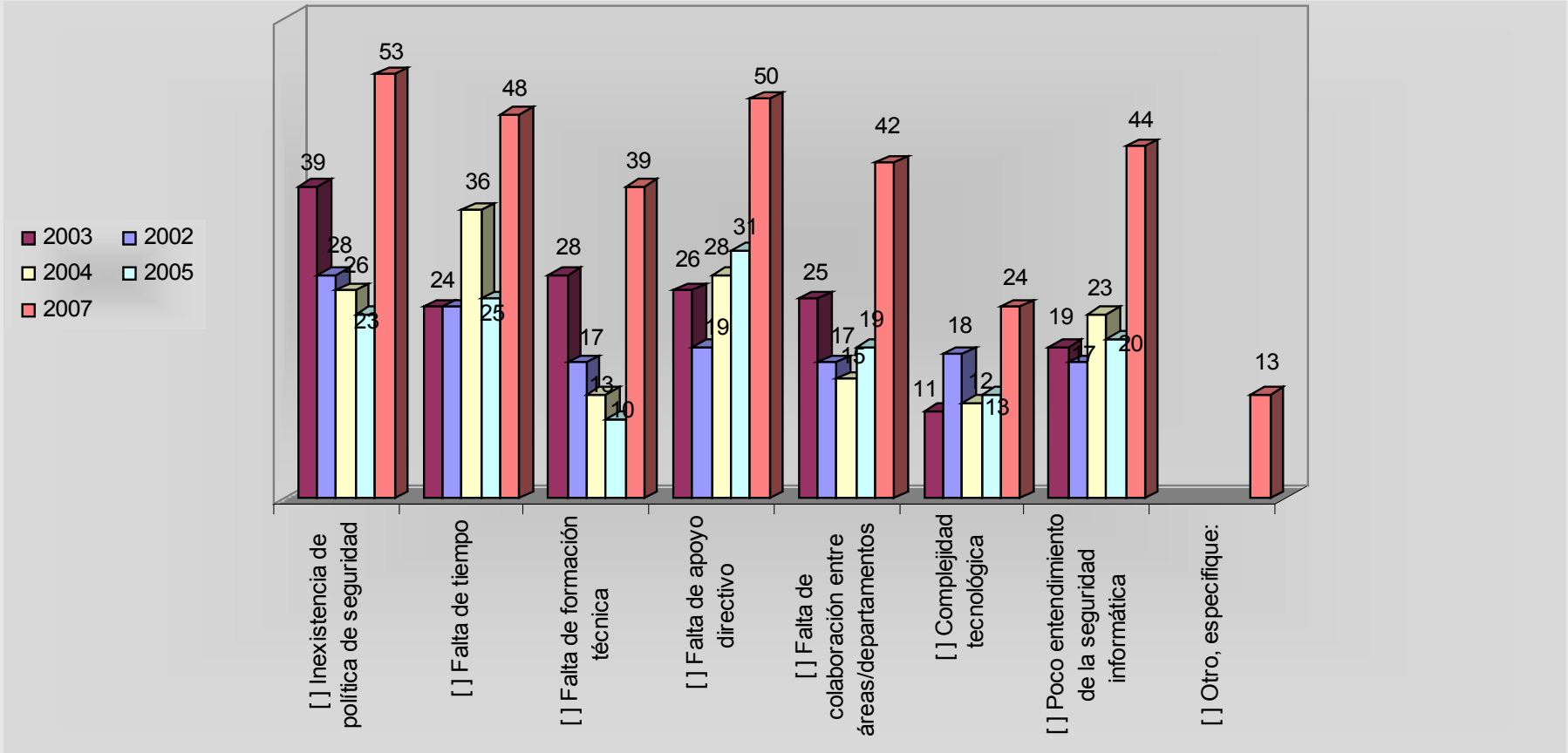
Políticas de Seguridad Informática



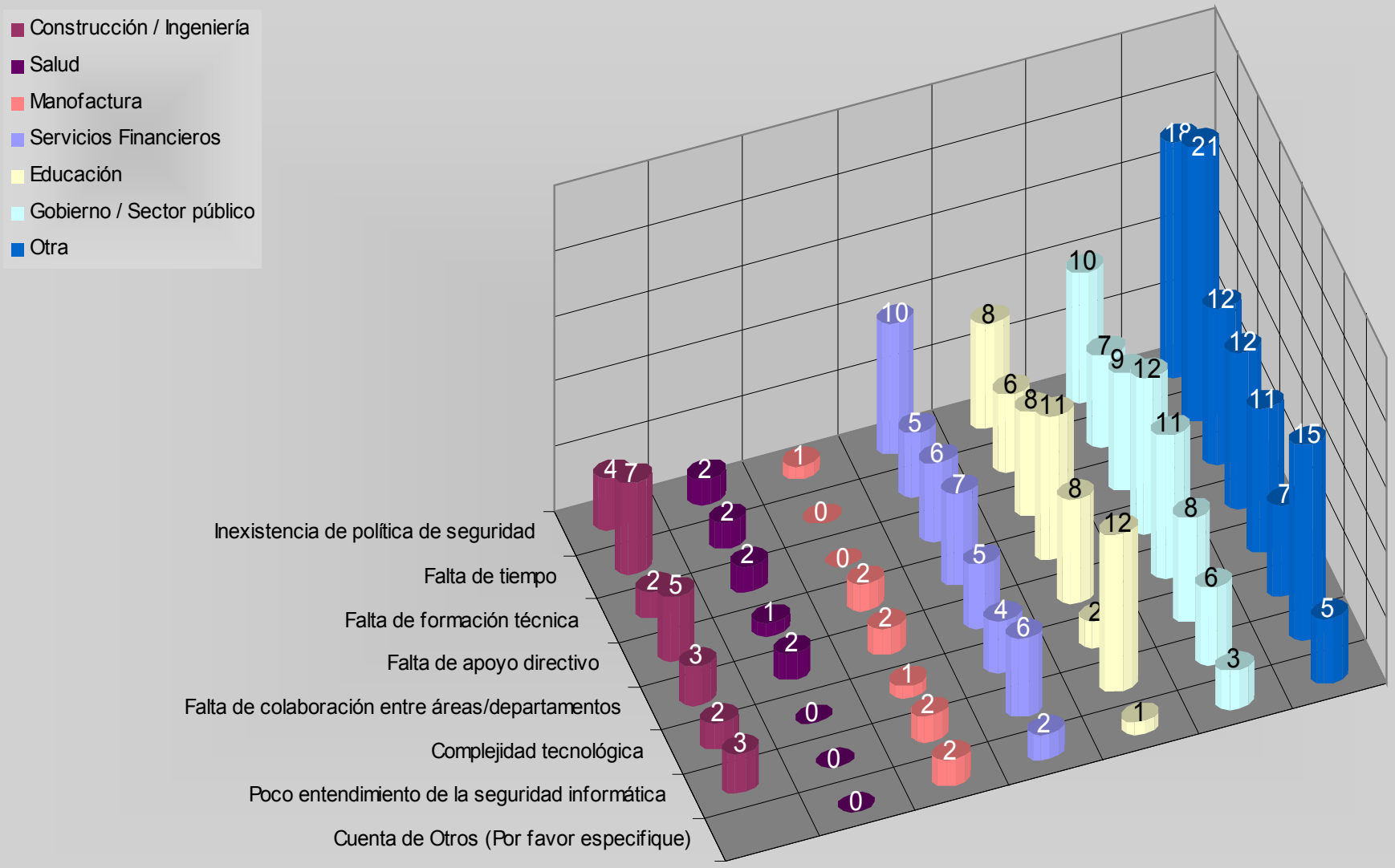
Sectorización Políticas de Seguridad Informática



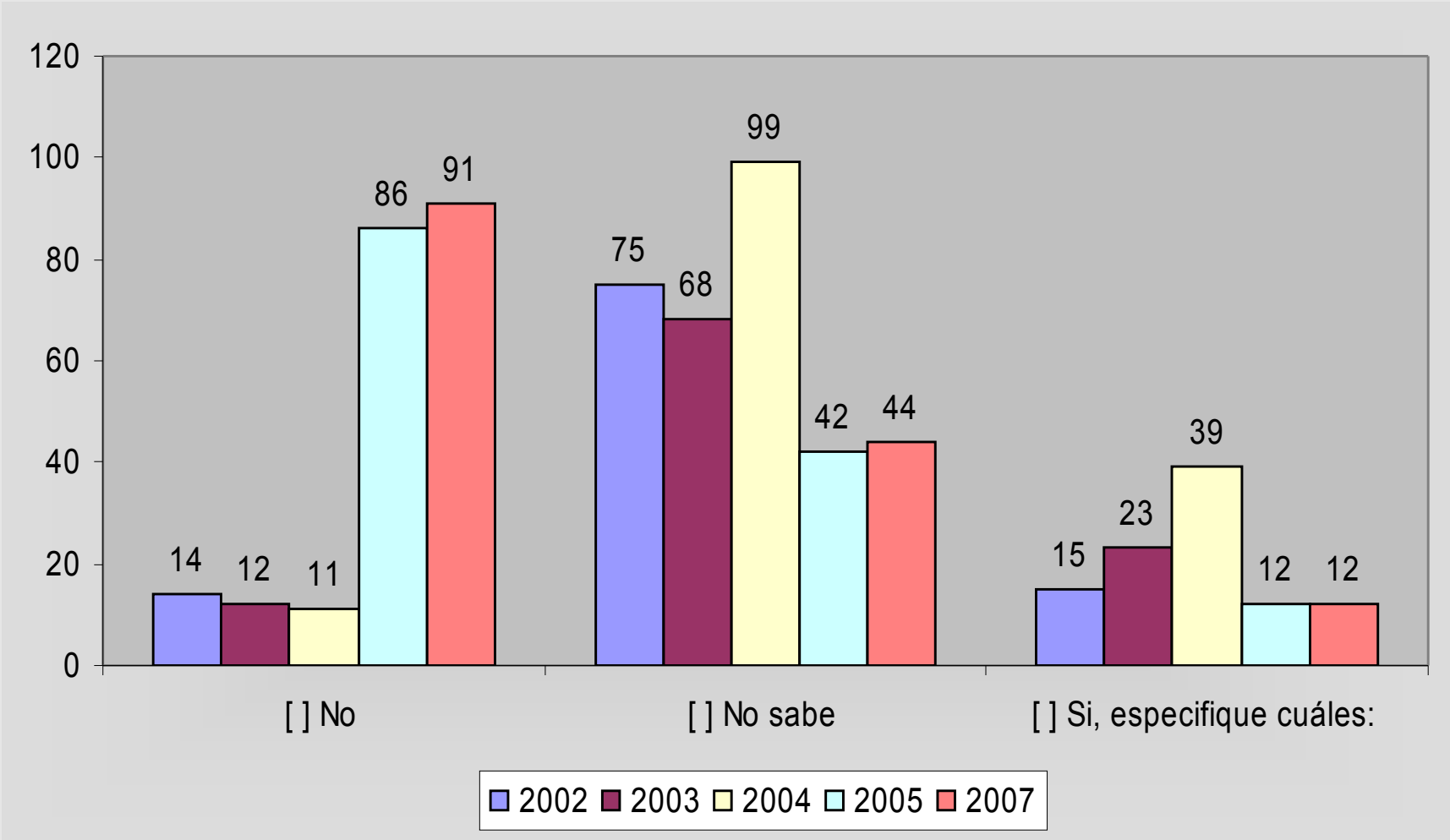
Obstaculos para una adecuada seguridad informática



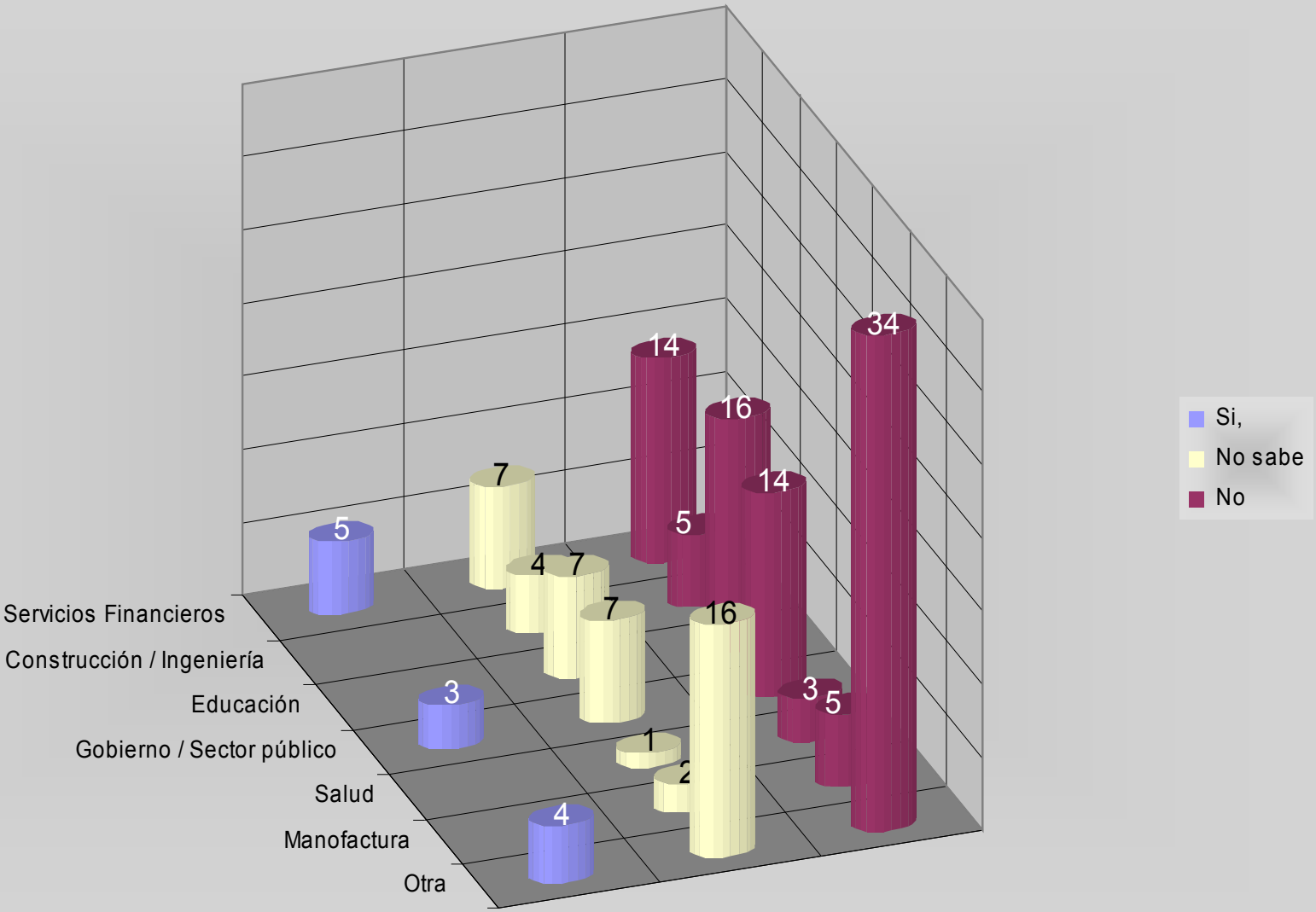
Sectorización de los obstáculos



Contactos para seguir intrusos



Contactos para seguir intrusos



Conclusiones

➔Las regulaciones nacionales e internacionales llevarán a las organizaciones en Colombia fortalecer los sistemas de gestión de la seguridad de la información, no solamente para cumplir con lo establecido en la norma ISO 27001, sino en el diseño de sistemas más resistentes y confiables para los usuarios.

➔El mercado de los profesionales de seguridad de la información demanda una formación que conjugue la práctica y experiencia verificable.

➔La formación académica (en programas de educación formal como especializaciones o maestrías) y la posesión de certificaciones generales como factores claves y atractivos para los empleadores.

Conclusiones

➔La inversión en seguridad de la información se encuentra concentrada en el perímetro de las organizaciones: redes y sistemas de comunicaciones, mientras los aspectos relacionados con la clasificación de la información y los dispositivos de almacenamiento móviles aún no son prioridad dentro de las organizaciones.

➔Mientras que las VPN, los *proxies* y *firewalls* son elementos fundamentales de los mecanismos de seguridad en las organizaciones colombianas, las herramientas forenses aún no encuentran su lugar y ni su justificación para incorporarse al discurso de la seguridad informática en Colombia.

Conclusiones

➔Si bien están tomando fuerza las unidades especializadas en delito informático en Colombia, es necesario desarrollar esfuerzos conjuntos entre la academia, el gobierno, las organizaciones y la industria, para mostrarles a los intrusos que estamos preparados para enfrentarlos.

➔La inexistencia de políticas de seguridad y la falta de tiempo, no pueden ser excusas para no avanzar en el desarrollo de un sistema de gestión de seguridad. La inversión en seguridad es costosa, pero la materialización de la inseguridad puede serlo mucho más. Ud. Decide!

➔Es hora de empezar a medir cuánto nos cuestan los incidentes de seguridad de la información para avanzar en la construcción del indicador de retorno de la inversión, como una manera de saber qué debemos fortalecer, qué debemos desaprender y a qué nos podemos comprometer en el combate de la inseguridad de la información.

Referencias

➔AUSCERT (2006) 2006 Australian Computer Crime and Security Survey. Disponible en: . (Consultado: 6/05/2007)

➔COMPUTER SECURITY INSTITUTE (2006) CSI/FBI Computer Crime and Security Survey. Disponible en: . (Consultado: 6/05/2007)

➔PRICEWATERHOUSECOOPERS – UK- DTI (2006) Information Security Breaches Survey 2006. Disponible en: . (Consultado: 6/05/2007)

➔IBM XFORCE (2006) X-Force 2006 Trend Statistics. Disponible en: . (Consultado: 6/05/2007)

➔ACIS (2007) Seguridad Informática en Colombia Tendencias 2007. Jeimy J. Cano, Ph.D, CFE