



# IV Encuesta Nacional de Seguridad Informática

ACIS 2004

Jeimy J. Cano, Ph.D

Lista de Seguridad Informática

**-SEGURINFO-**

# Estructura

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

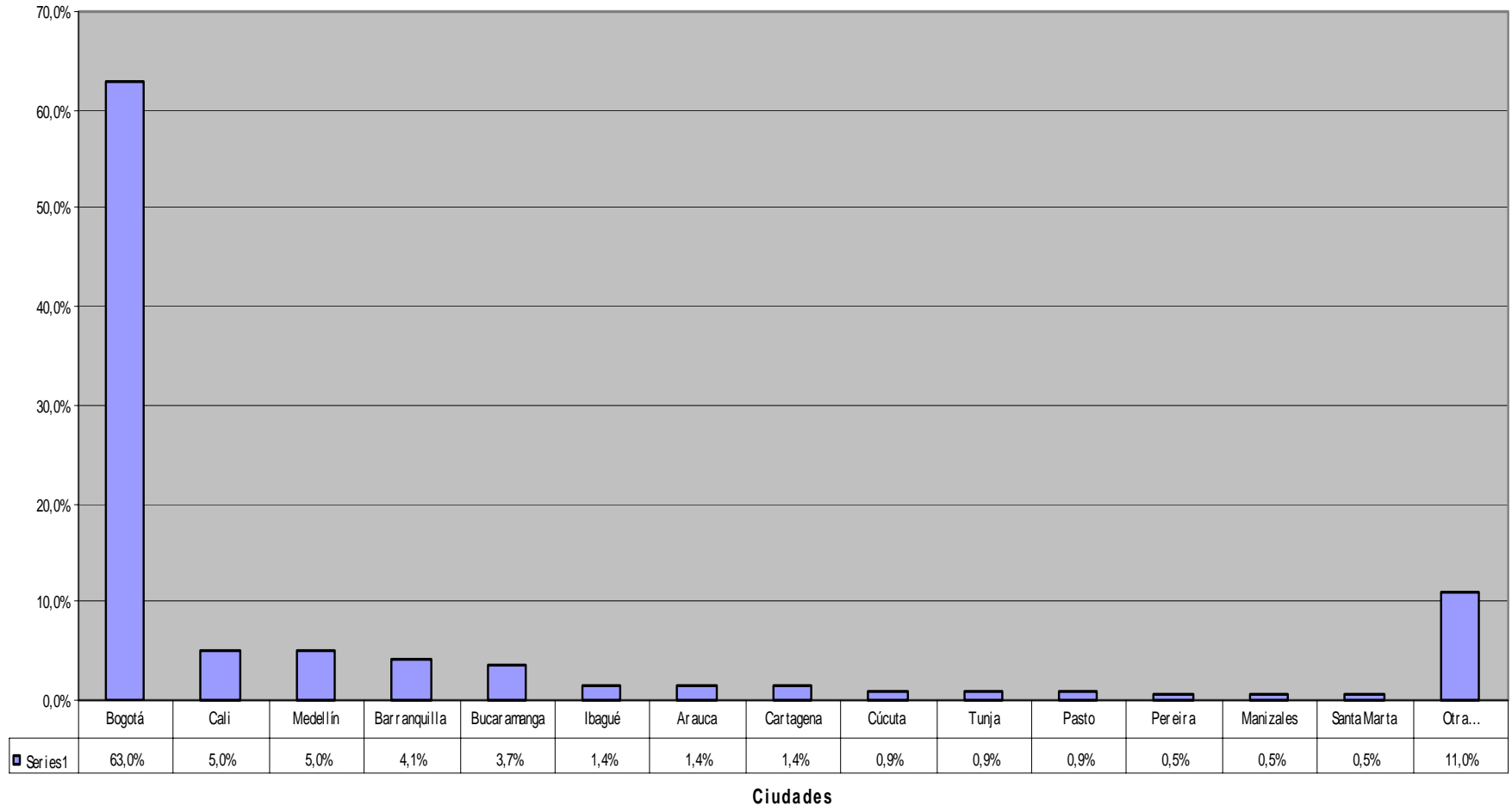
# Consideraciones Muestrales

- Considerando una población limitada (alrededor de 800 personas que participan activamente en la lista de seguridad SEGURINFO) se ha estimado un error muestral de 8% (confianza del 92%), lo cual nos permite manejar una muestra adecuada cercana a los 130 participantes.
- Al contar con 149 participantes en la muestra, los resultados presentados son estadísticamente representativos.

# Ciudades

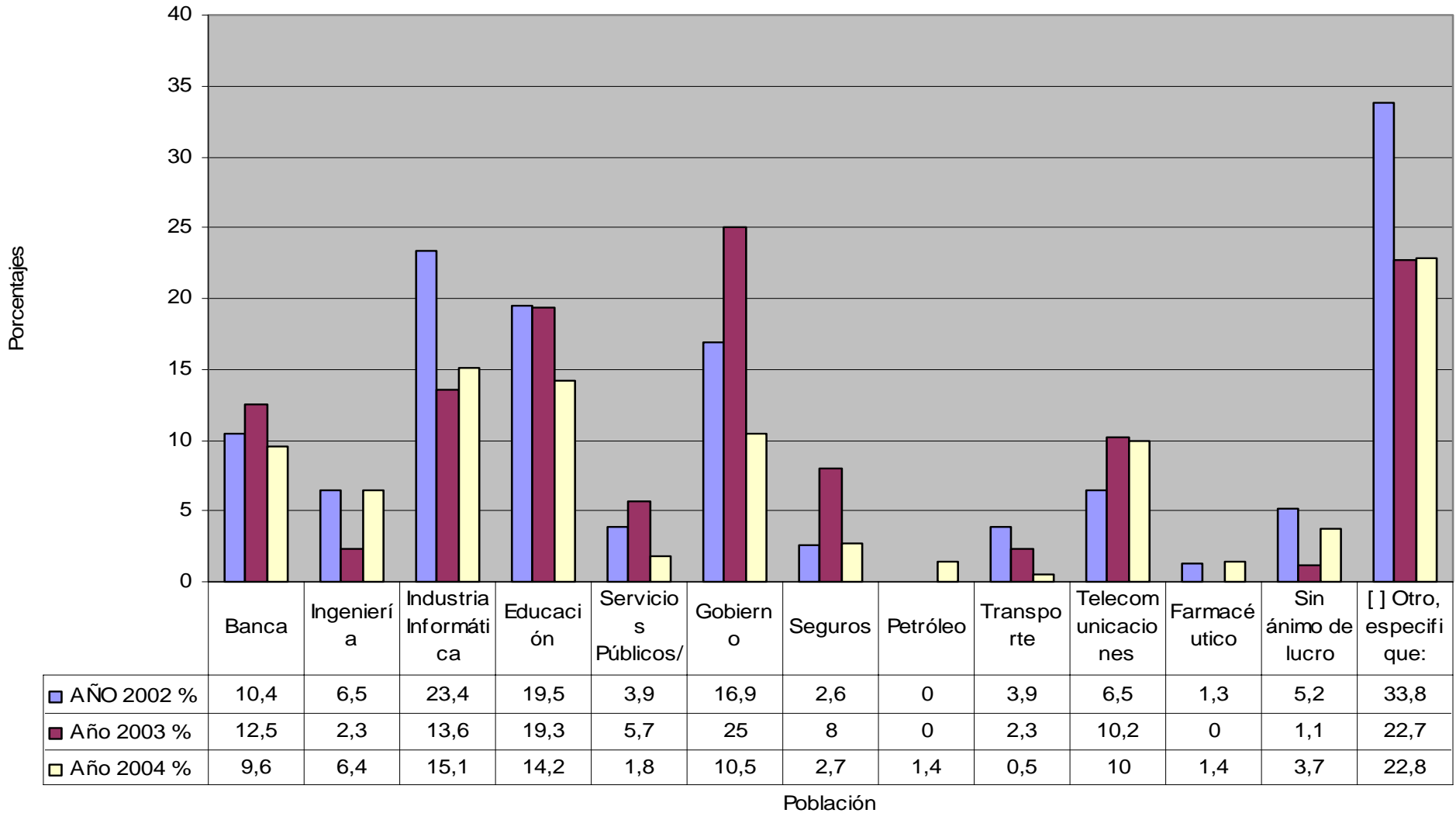


## Participación por Ciudades



# SECTOR

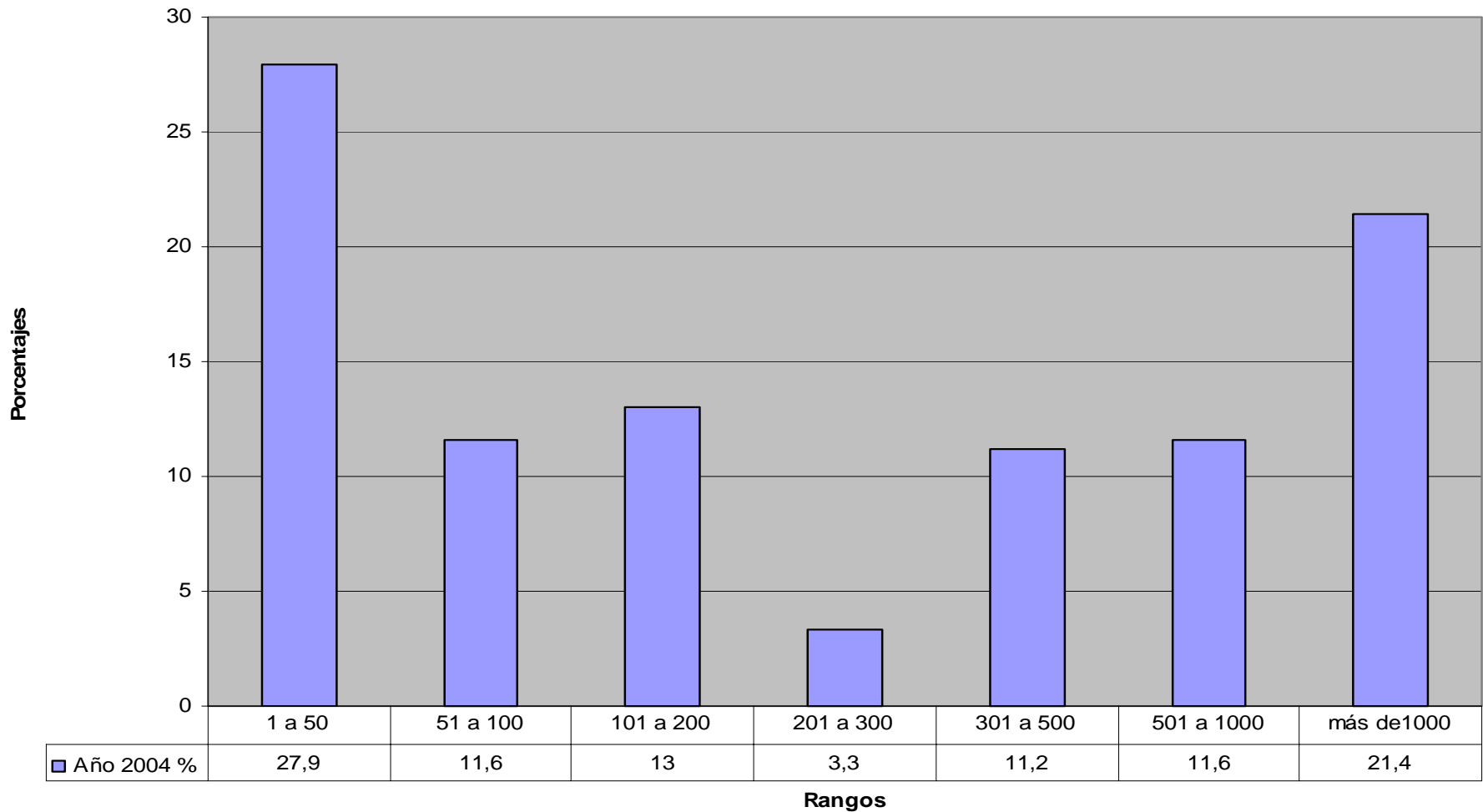
DEMOGRAFIA



# No. Empleados en la compañía



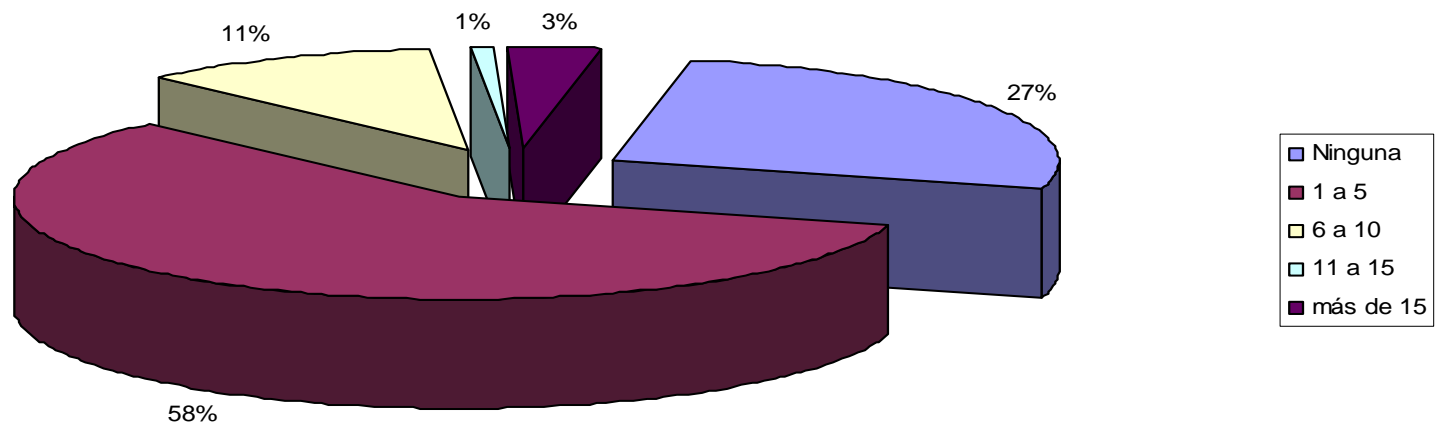
No. Empleados



# No. Personas dedicadas a Seguridad Informática

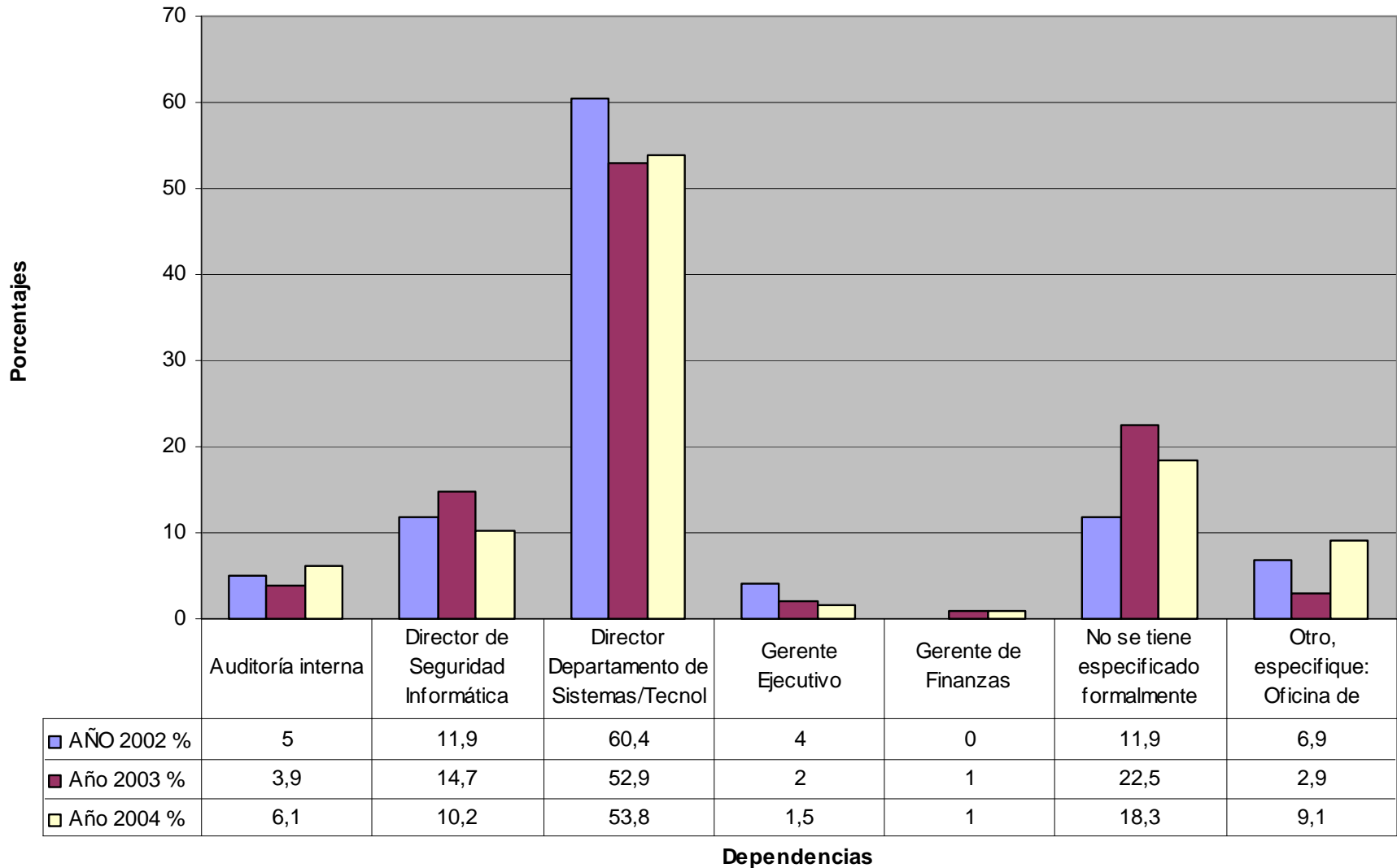


No. Personas Dedicadas a Seg. Inf.



# Dependencia del Área de Seguridad Informática

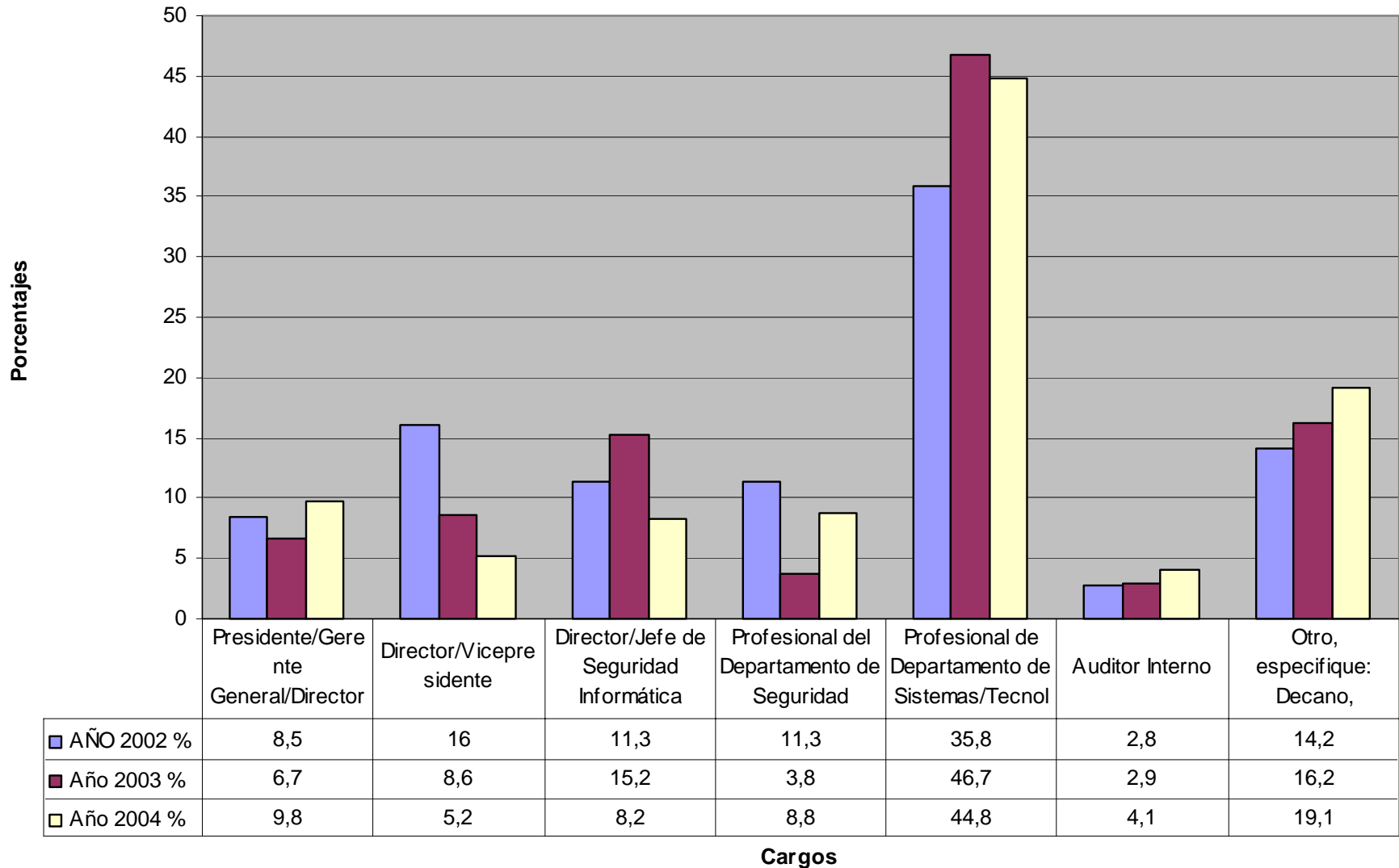
Dependencia Area Seguridad Informática



# Cargos que Respondieron la encuesta

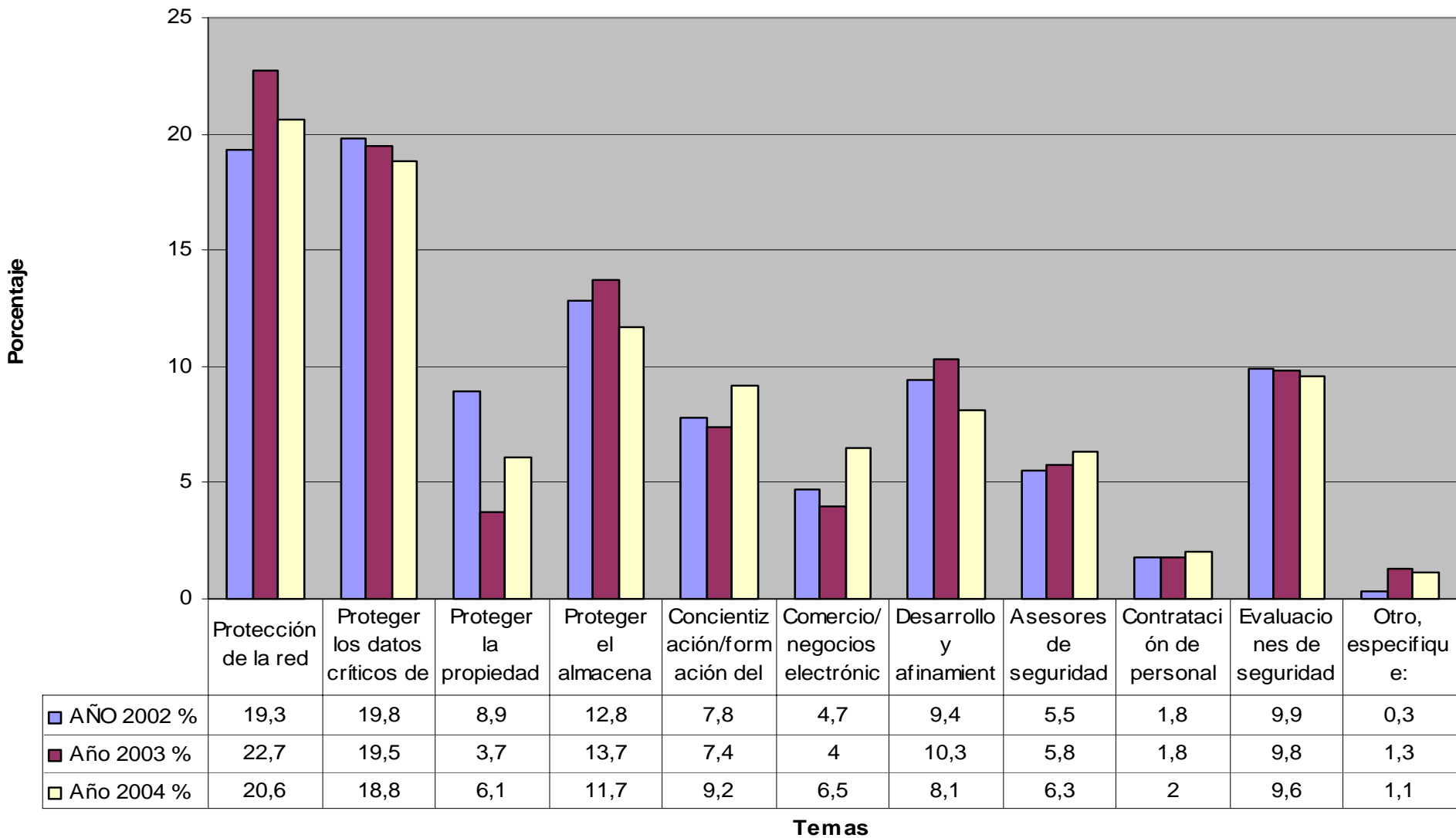


## Perfil Partipantes



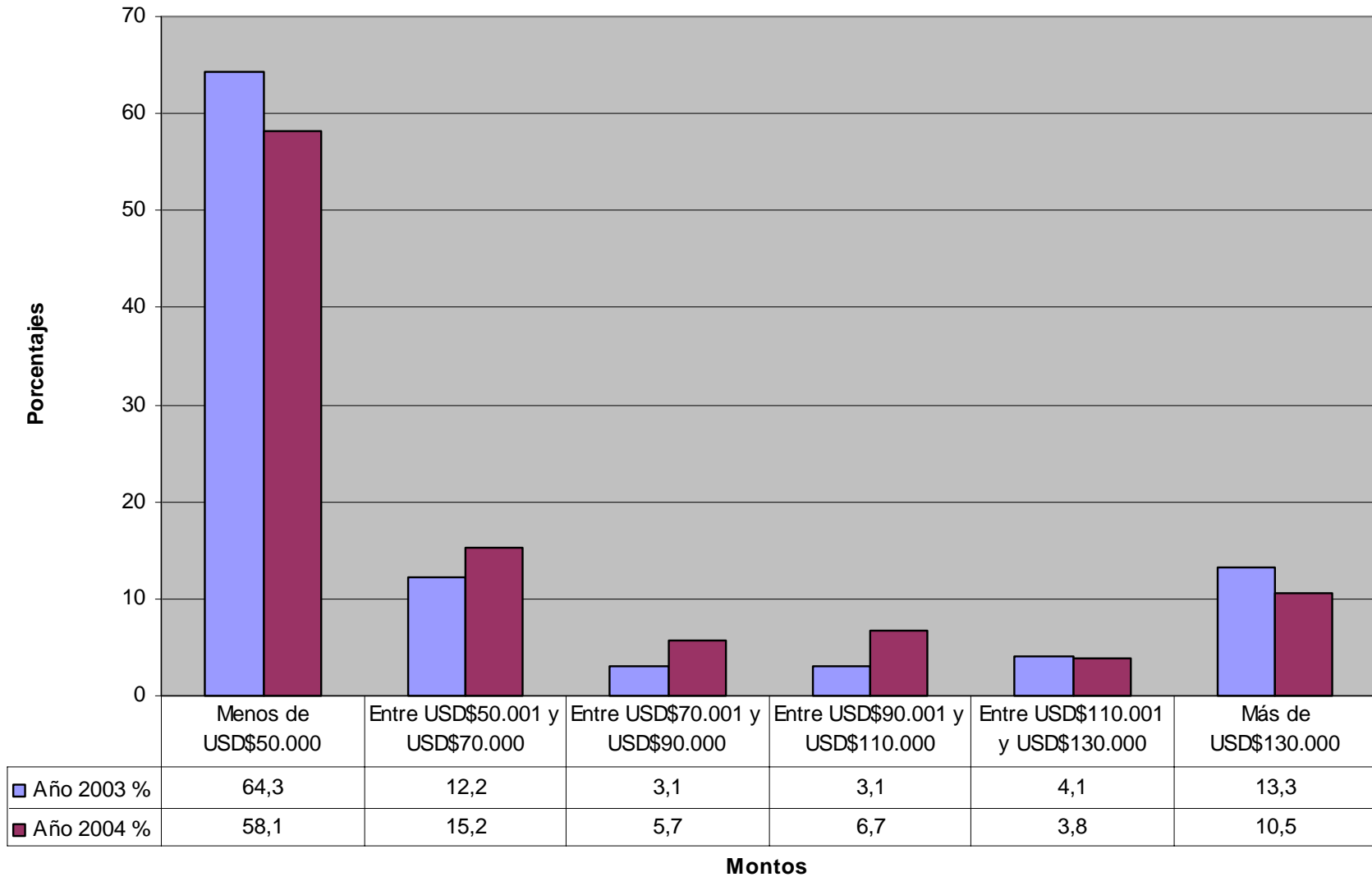
# Inversión en Seguridad Informática

## Temas de Inversión



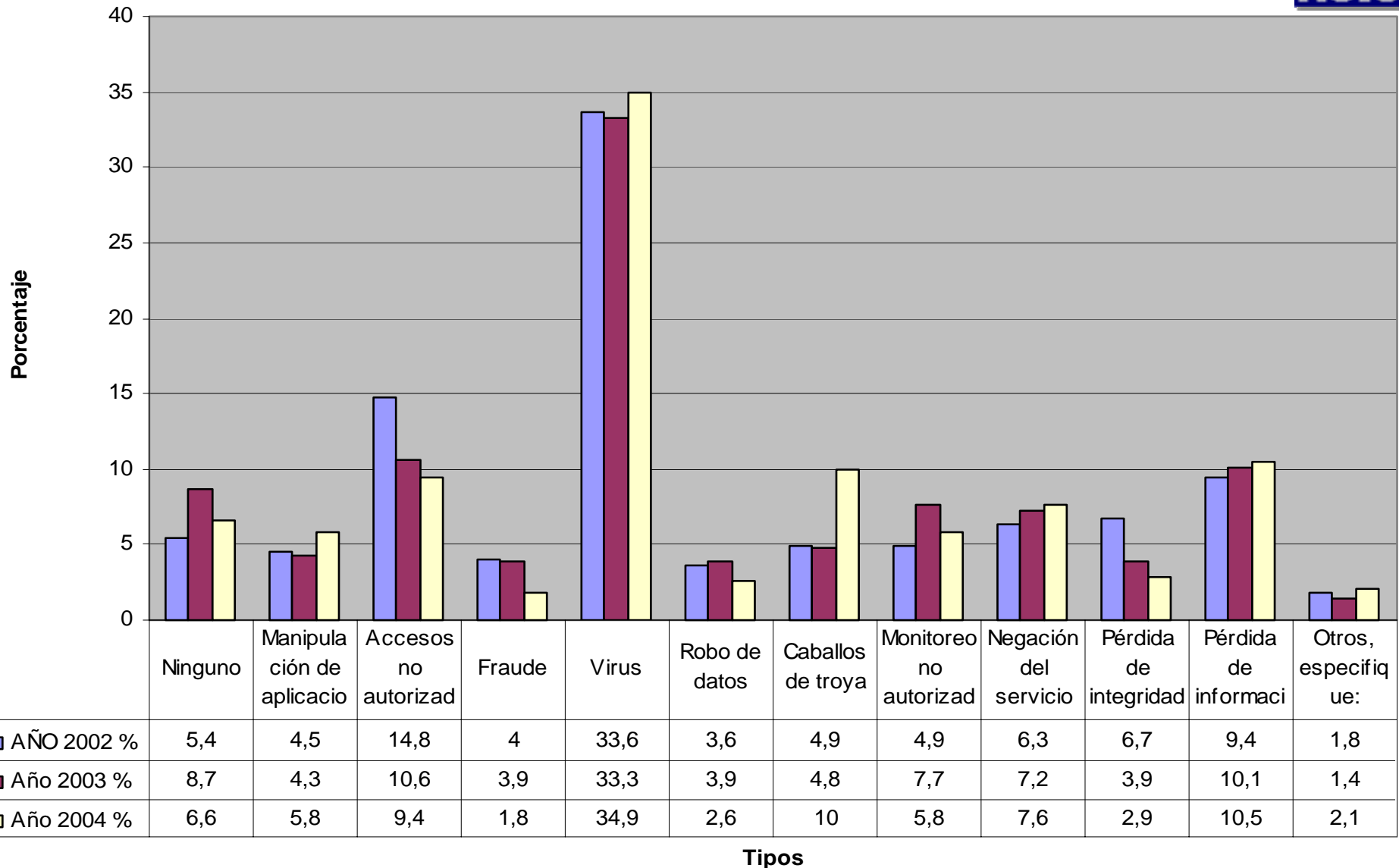
# Inversión en Seguridad Informática

## Inversión en Seguridad Informática



# Violaciones de Seguridad

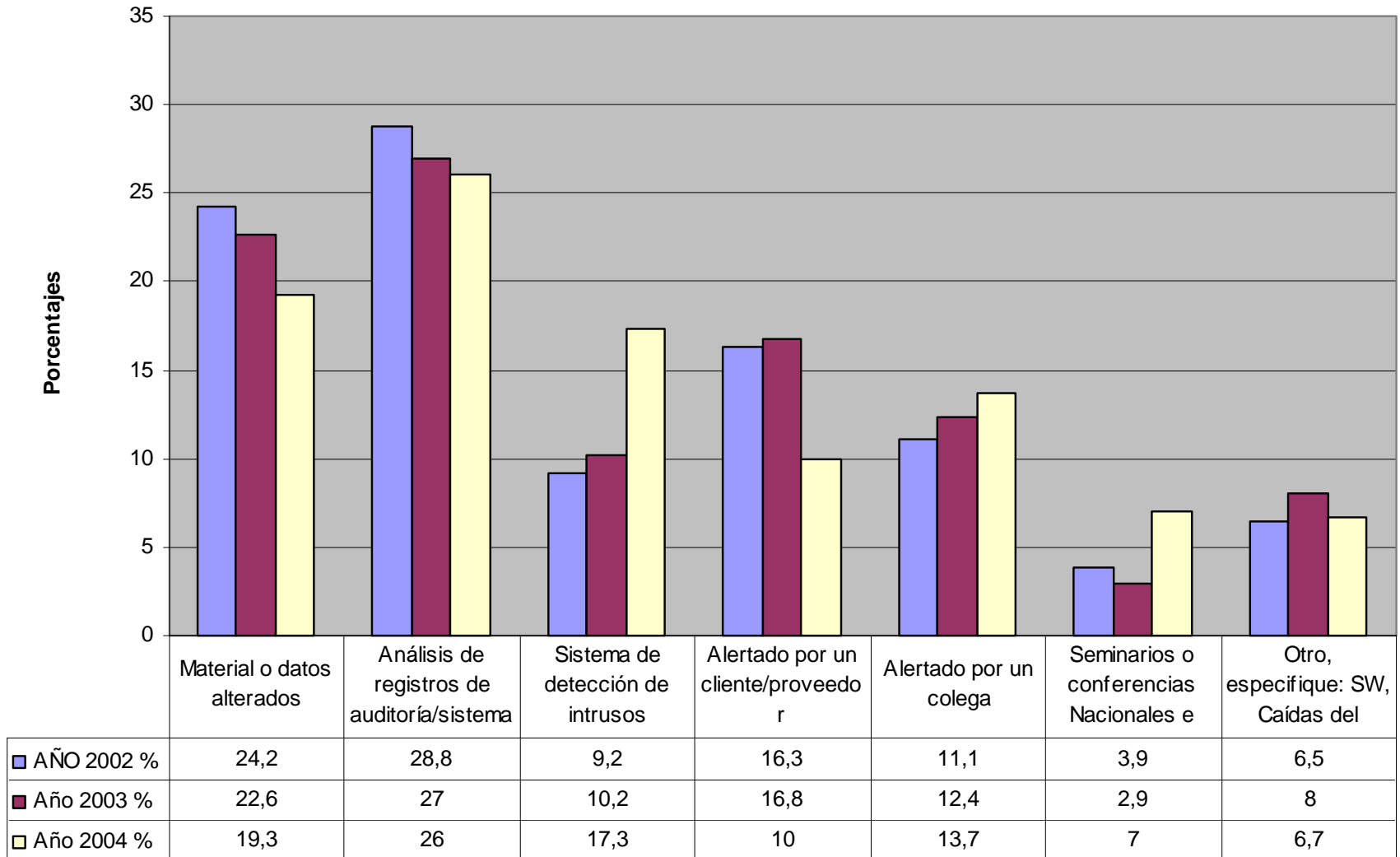
## Fallas de Seguridad



# Cómo se entera de las Violaciones de Seg.



Identificación de Fallas

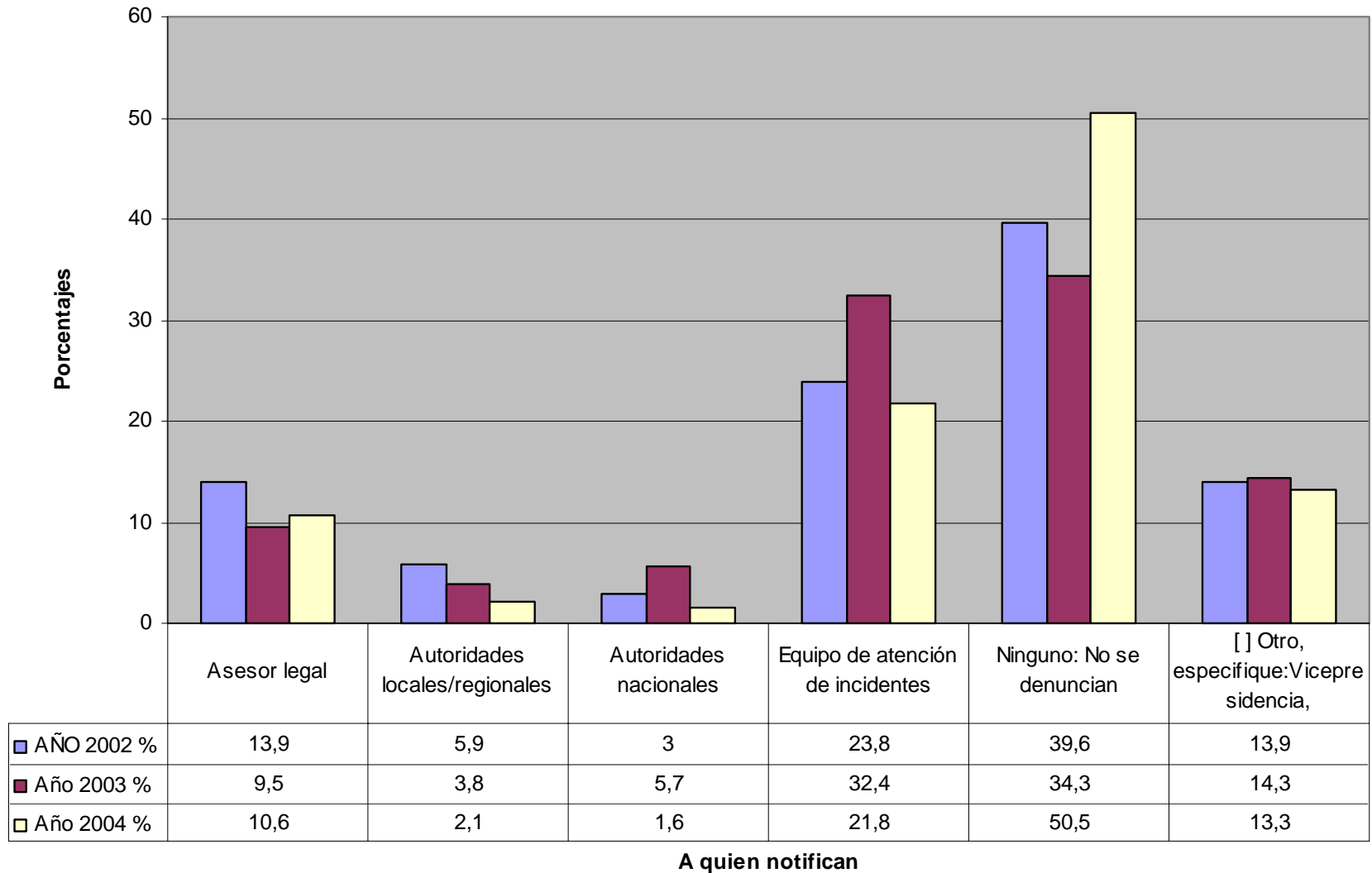


Estrategia

# A quien se notifica de una Violación de Seg.



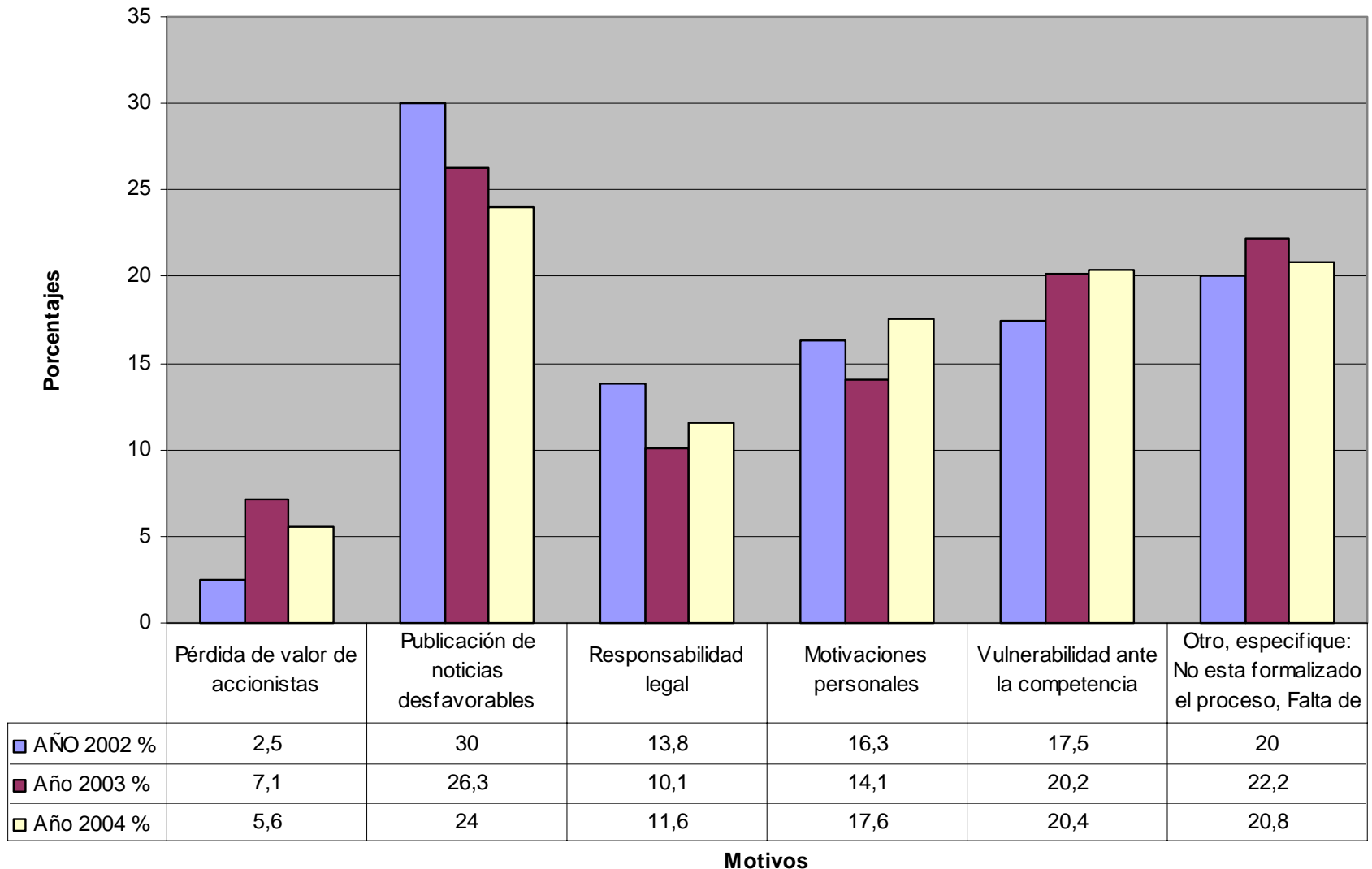
## Notificación de Incidentes



# Motivos de No denuncia - Violación de Seg.



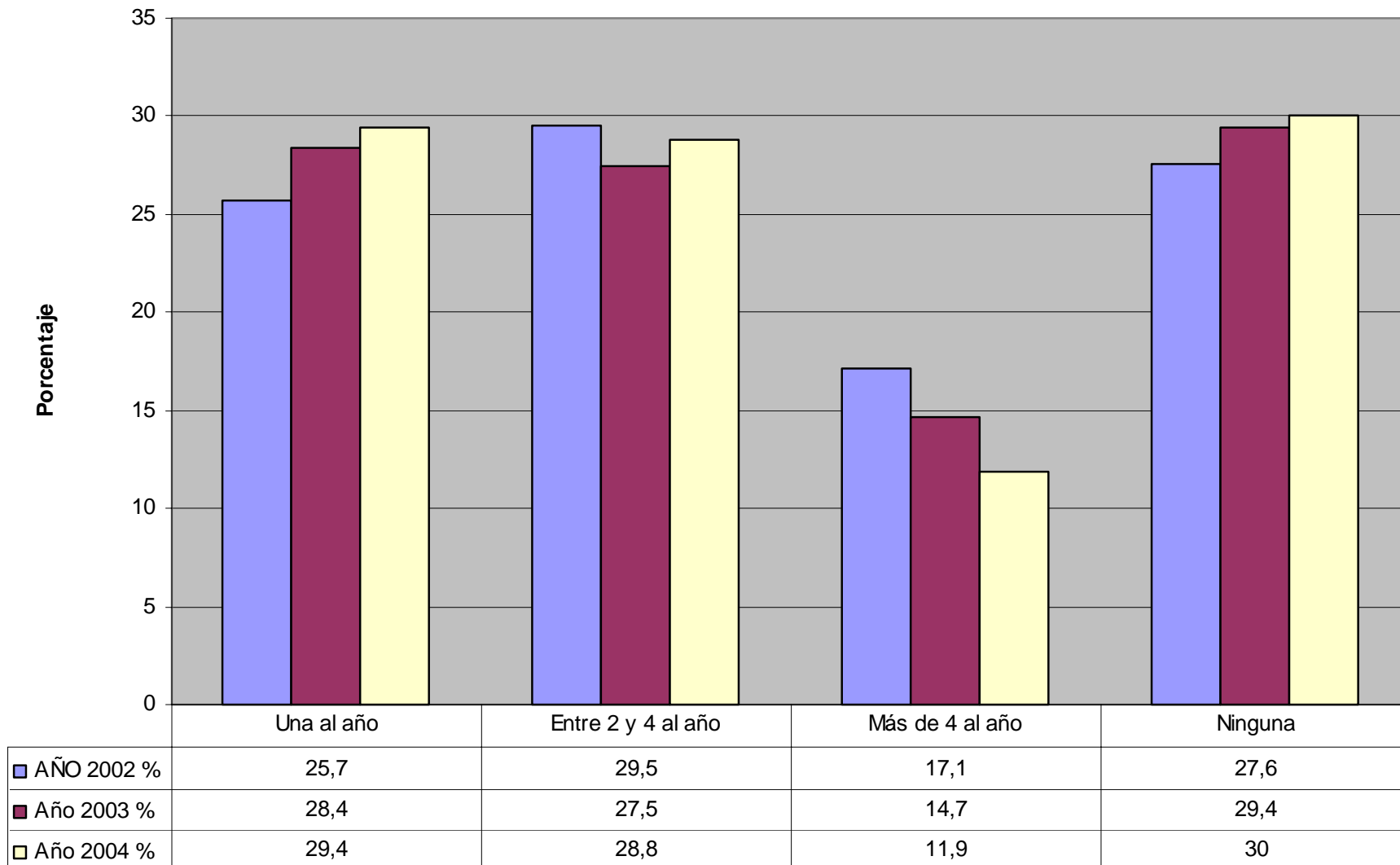
## No Denuncia Incidentes de Seguridad Informática



Motivos

# Pruebas de Seguridad Realizadas

Evaluaciones de Seguridad

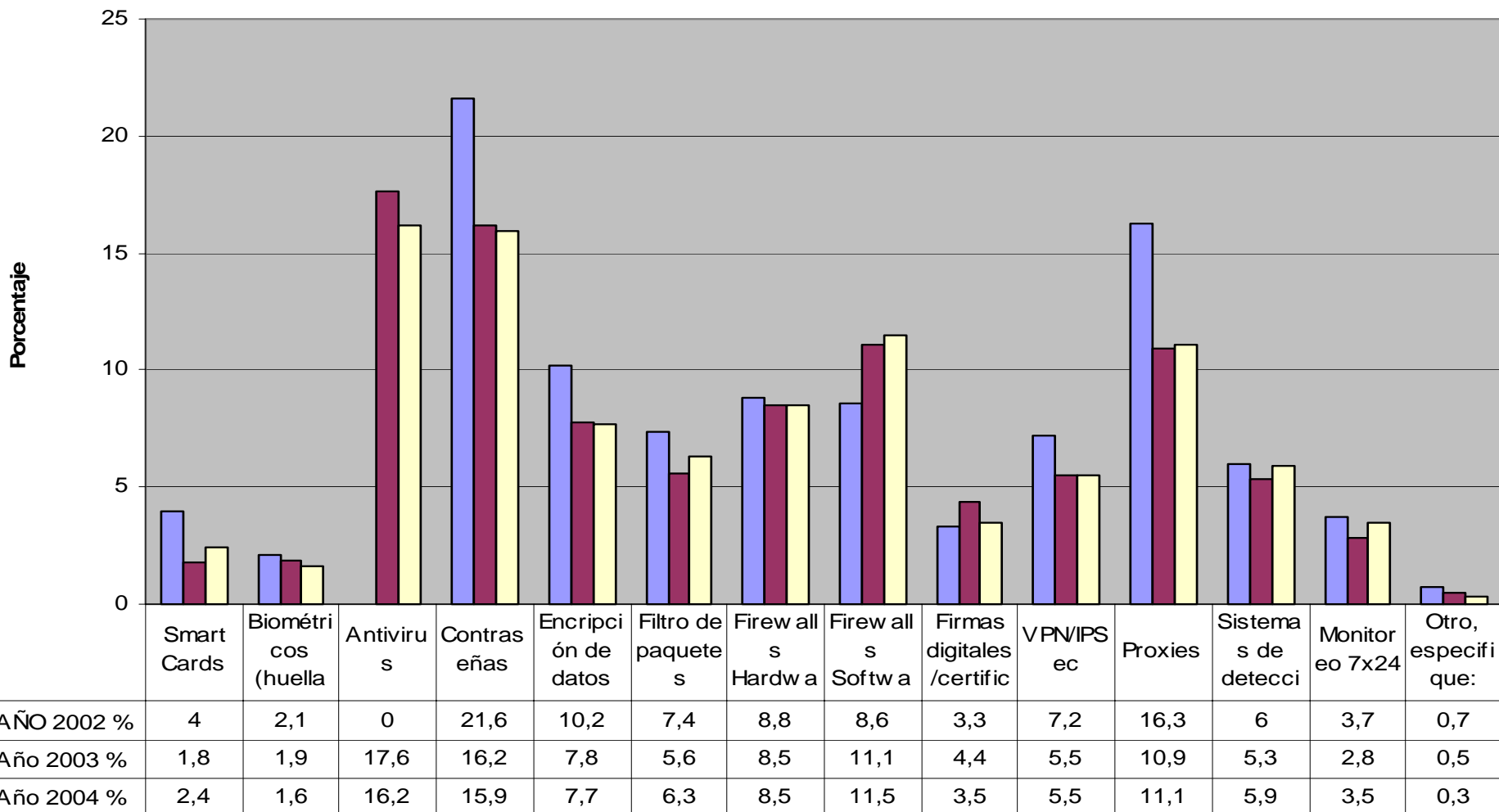


No. Pruebas realizadas

# Mecanismos de Seguridad Informática



## Tecnología de Seguridad Informática

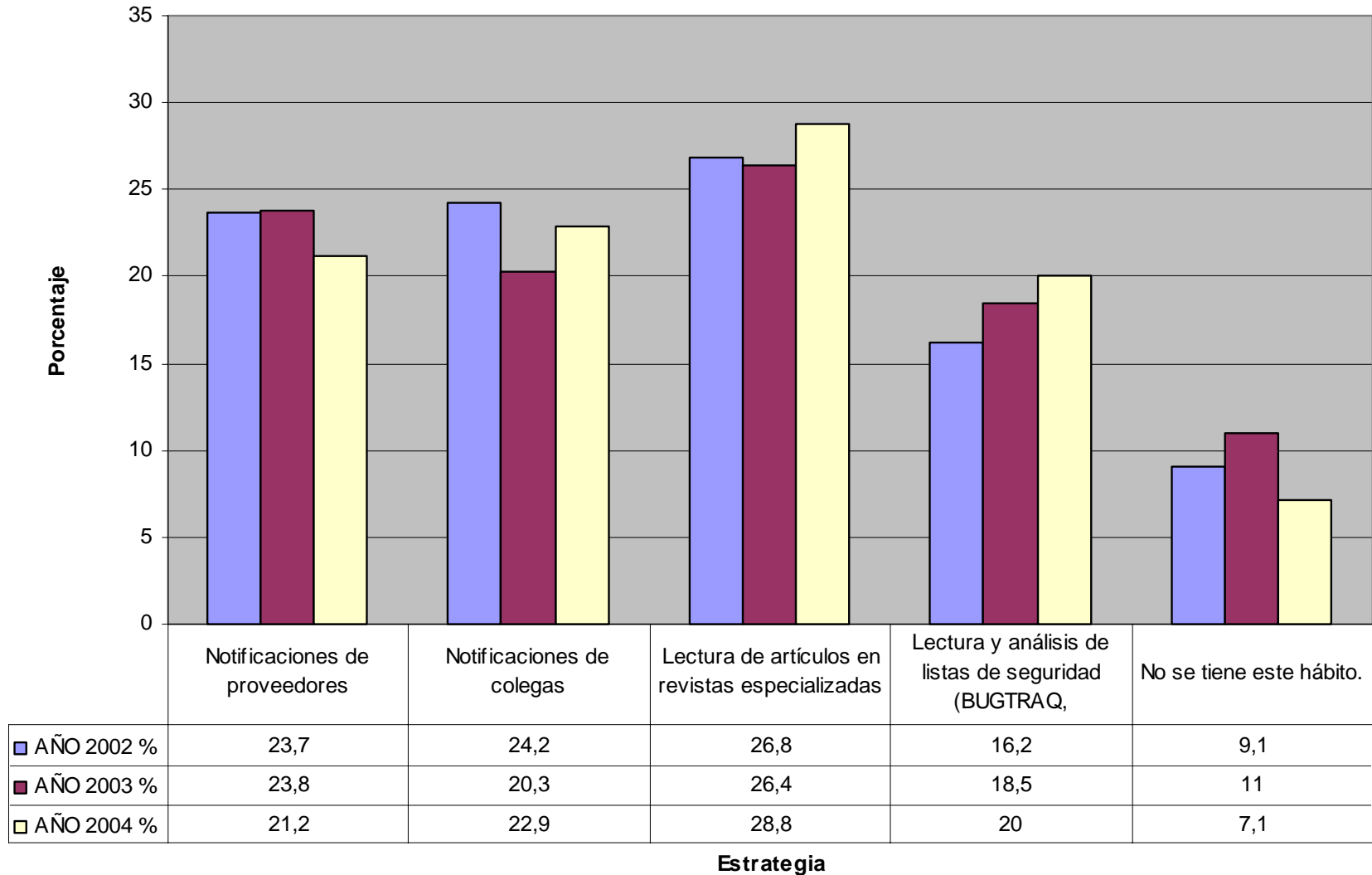


### Mecanismos

# Cómo se entera de fallas de Seguridad?



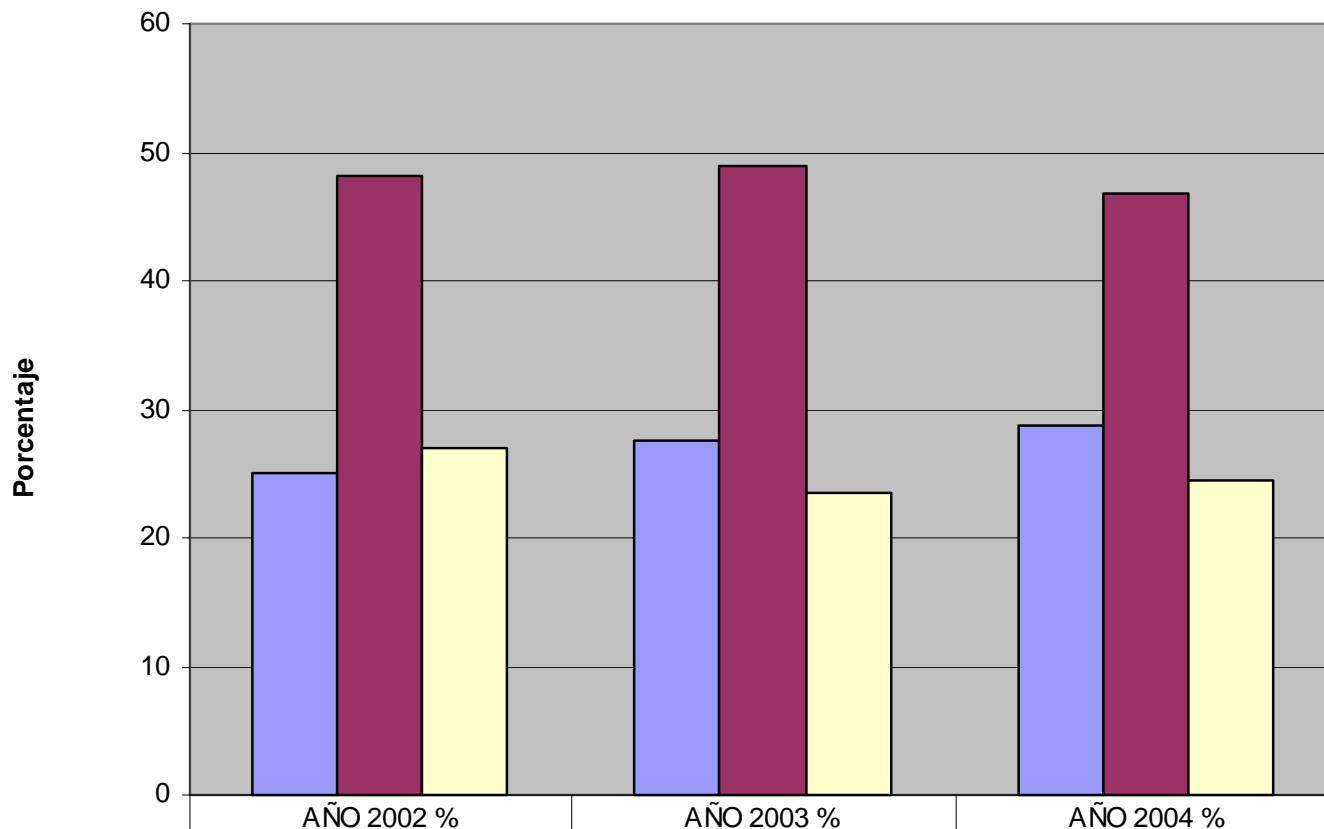
¿Cómo se entera de las fallas de seguridad?



# Políticas de Seguridad Informática



## Políticas de Seguridad Informática



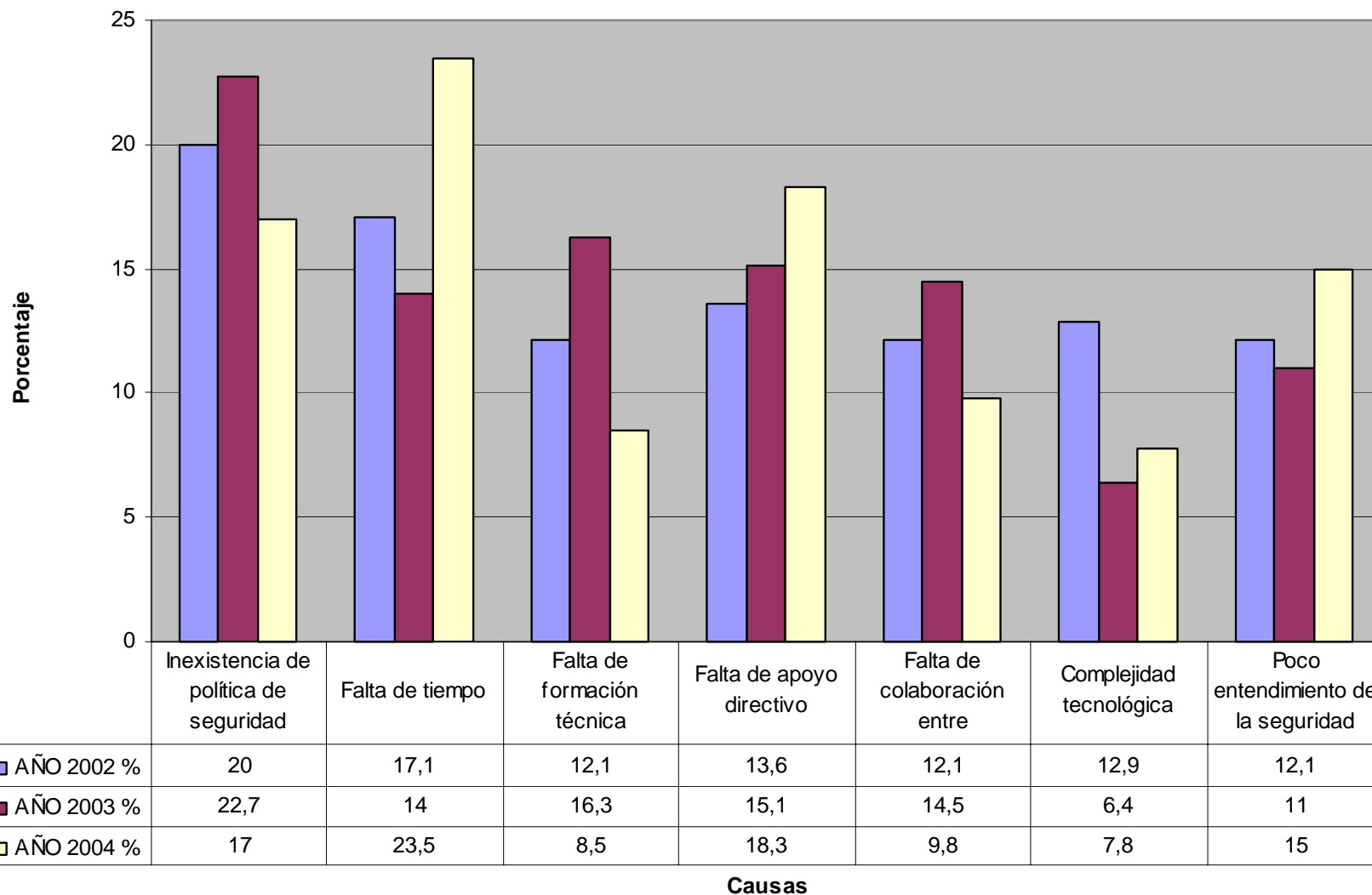
■ No se tienen políticas de seguridad definidas	25	27,5	28,8
■ Actualmente se encuentran en desarrollo	48,1	49	46,8
■ Política formal, escrita documentada e informada a todo el personal	26,9	23,5	24,4

Años

# Obstáculos para contar con una adecuada Seguridad Informática

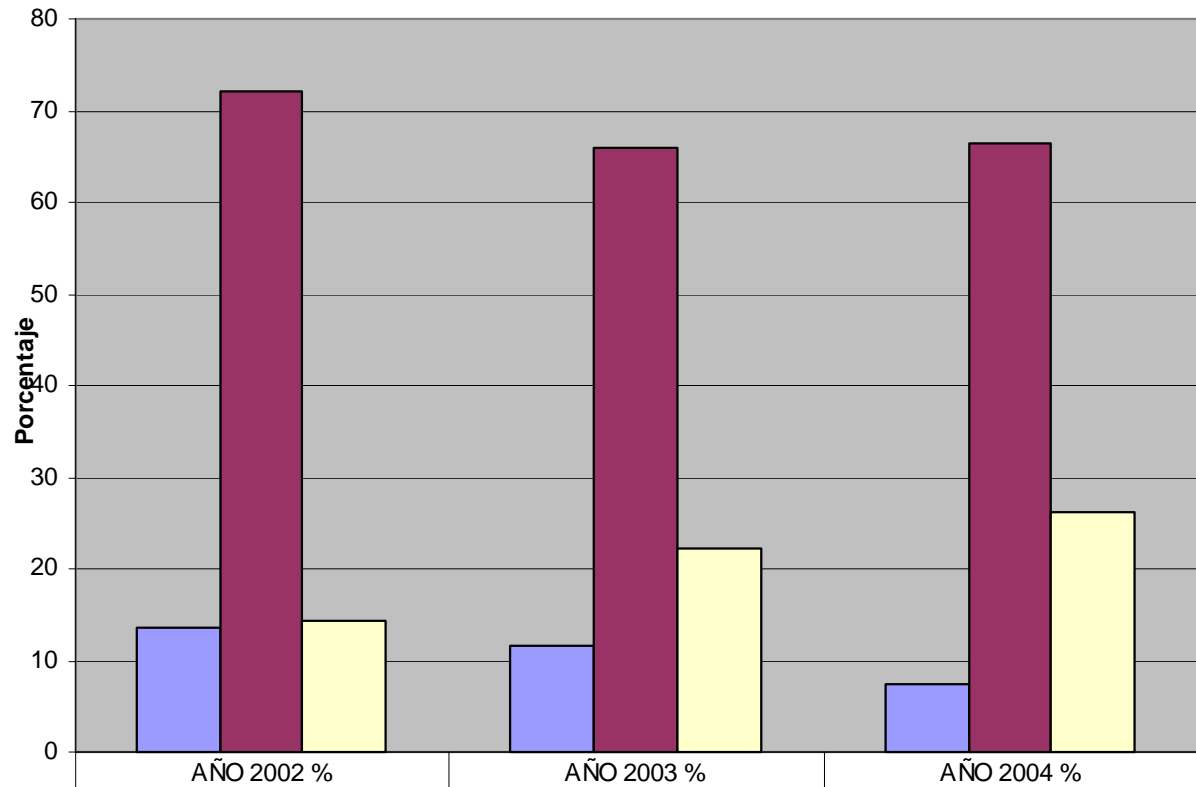


Obstáculos Seguridad Informática



# Contactos para Seguir Intrusos

Contactos para notificar un incidente



■ Si, especifique cuáles: DAS, Fiscalía, Grupos de Linux, Interpol, ISP, ISS

■ No

■ No sabe

Años

# Conclusiones Generales



1. La mediana empresa considera **al tema de seguridad informática un insumo estratégico** de negocio para fortalecer sus estrategias de negocios electrónicos y diferenciación de productos.
2. Las áreas de seguridad informática mientras **continúen dentro del dominio del Departamento de Sistemas o Tecnología**, estarán compitiendo en prioridades con los aspectos de tecnología informática aplicado a los negocios, restringiendo su participación clave en la construcción de una manera diferente de entenderla, más allá de la visión eminentemente técnica.
3. Es necesario adelantar **estudios y prácticas comparativas de los costos** que se derivan de los incidentes de seguridad informática para construir una base sistemática de análisis que permita a las organizaciones estimar y proponer modelos de inversión en seguridad informática acordes con su realidad de negocios y el escenario cambiante de la seguridad informática.
4. Las tecnologías de seguridad como los **antivirus, las VPN, los sistemas de detección de intrusos, los firewalls y los certificados digitales** son elementos mandatorios en las infraestructuras de cómputo en las organizaciones colombianas.
5. Se requiere establecer un **canal oficial de reporte, análisis y orientación de las tendencias de la seguridad informática**, así como para **atender y canalizar investigaciones sobre intrusos** en los sistemas informáticos en Colombia, que genere un espacio coherente y formal para fortalecer la cultura de seguridad informática en el país.

# Conclusiones Generales



6. El **poco entendimiento de la seguridad informática** en las organizaciones, como obstáculo más sobresaliente para la implementación de este tema, debe ser el incentivo tanto de las áreas de negocio como de las áreas de tecnología como una oportunidad para repensar las estrategias corporativas con una visión sistémica, es decir integral.
7. Reconociendo **a los individuos como el eslabón más importante en el sistema de seguridad informática**, es preciso informarlo y entrenarlo para que se convierta en el ente que retroalimente dicho sistema y procure su regulación y adaptación permanente.

# Referencias



- PRICEWATERHOUSECOOPERS and DEPARTMENT OF TRADE AND INDUSTRY – UK (2004) Information Security Breaches Survey 2004.  
[http://www.dti.gov.uk/industries/information\\_security/downloads.html](http://www.dti.gov.uk/industries/information_security/downloads.html)
- AUSCERT (2004) 2004 Australian Computer Crime and Security Survey.  
<http://www.auscert.org.au/crimesurvey>.
- SCHNEIER, B. (2004) Security and Compliance. *IEEE Security and Privacy*.  
Abril-Mayo