



**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Conferencistas:

Jeimy J. Cano, Ph.D

jcano@uniandes.edu.co

Lista de Seguridad Informática
-SEGURINFO-

Andrés R. Almanza, Msc

andres_almanza@hotmail.com





**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Agenda

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



**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Estructura de la Encuesta

- ✓ Cuestionario compuesto por 34 preguntas sobre los siguientes temas:
 - ✓ Demografía
 - ✓ Presupuestos
 - ✓ Fallas de seguridad
 - ✓ Herramientas y prácticas de seguridad
 - ✓ Políticas de seguridad



**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Consideraciones Muestrales

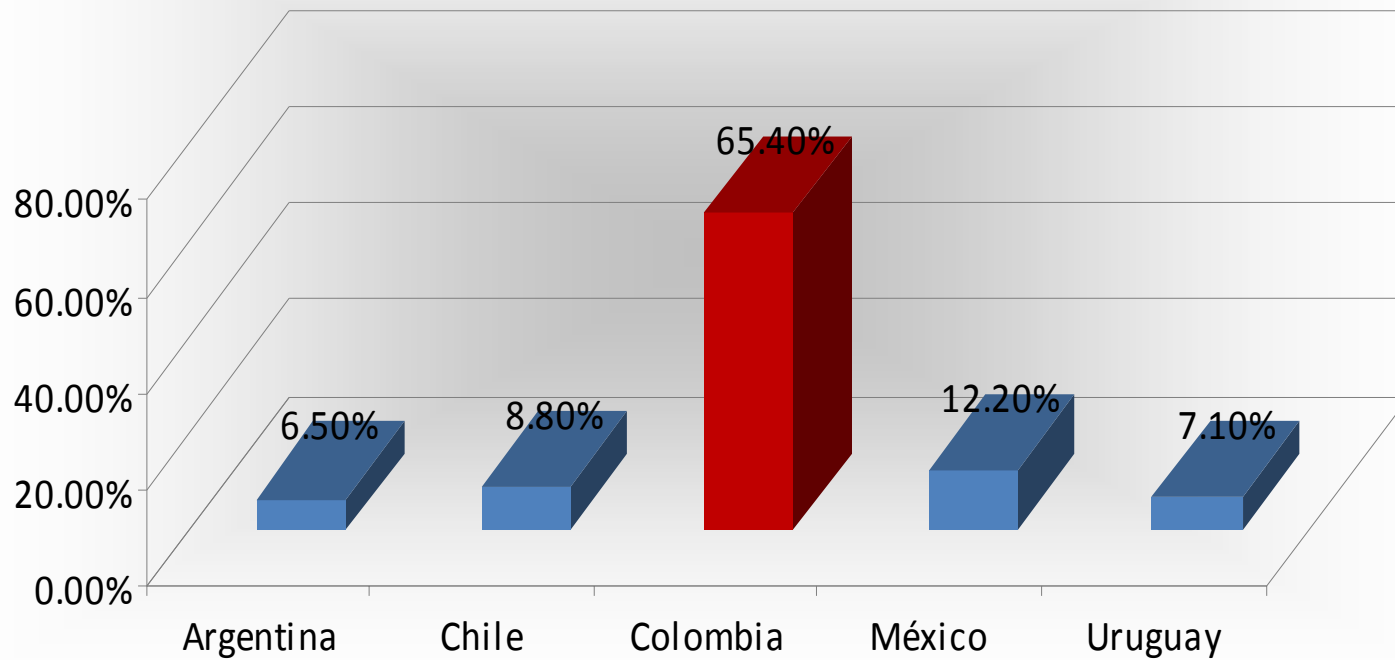
- ✓ El número de participantes este año es de 222 personas (en comparación con las 202 del 2008).
- ✓ *Considerando una población limitada (alrededor de 1800 personas que participan activamente en la lista de seguridad SEGURINFO) se ha estimado un error muestral de 7% (confianza del N), lo cual nos permite manejar una muestra adecuada cercana a los 813 participantes. Al contar con 222 participantes en la muestra, los resultados presentados son estadísticamente representativos*



IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Países Participantes

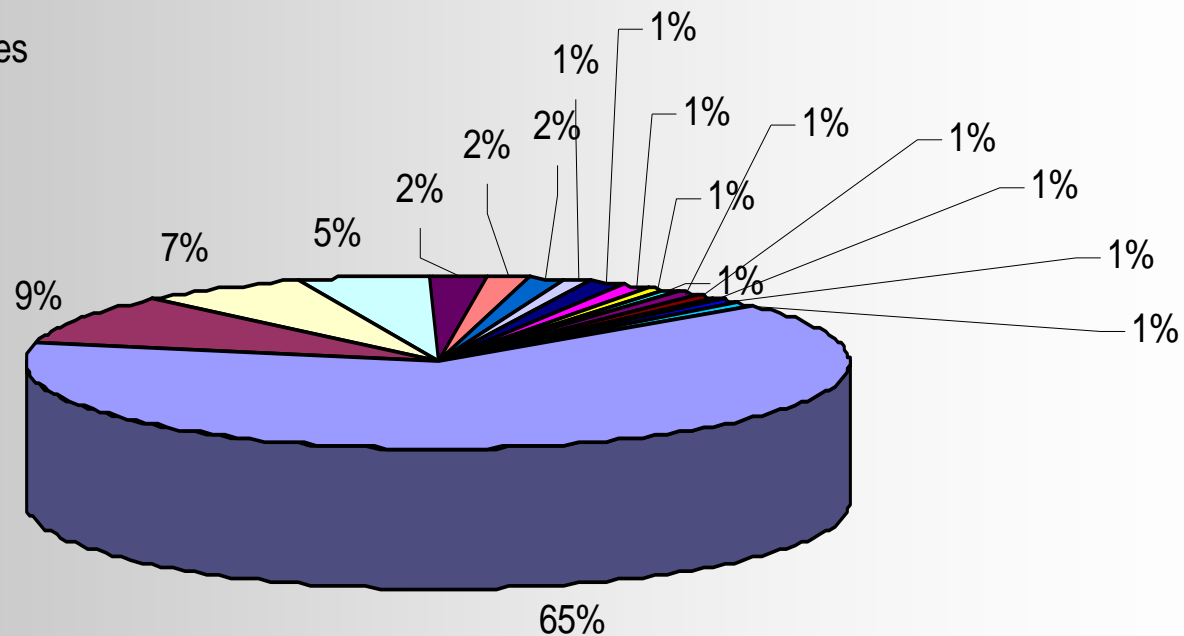




IX JORNADA de SEGURIDAD de INFORMATICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Ciudades Participantes



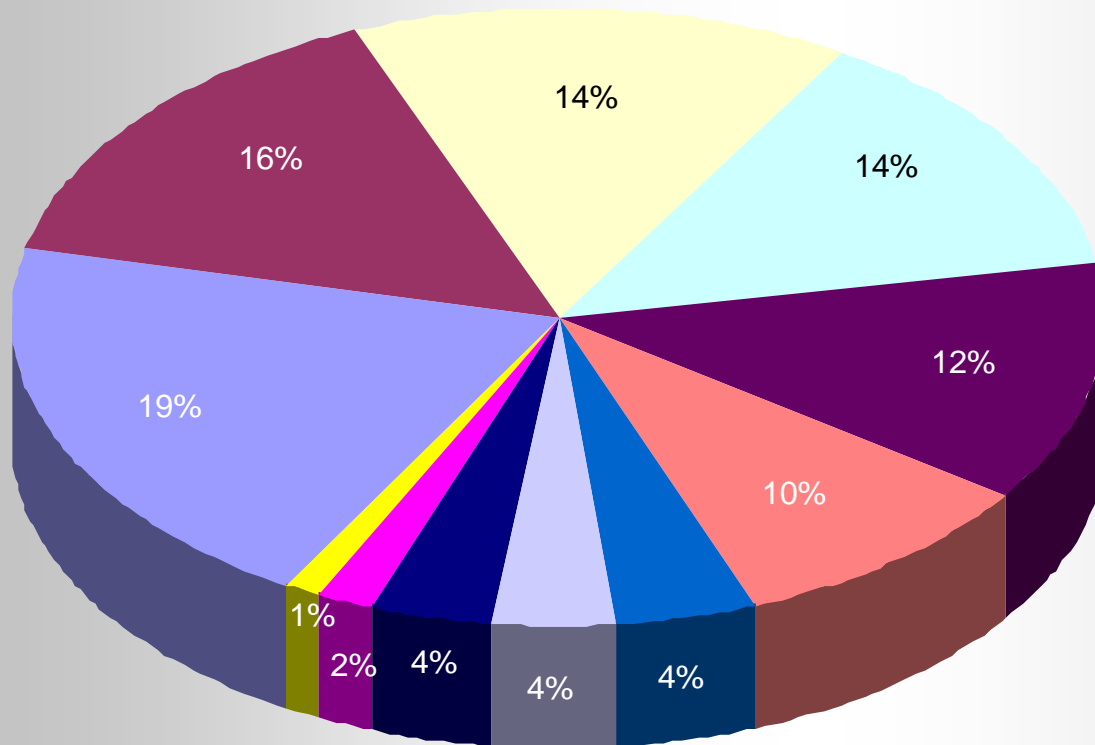
Bogotá	Medellín	Bucaramanga	cali	Barranquilla	POpayan
Cartagena	Tunja	PEREIRA	Manizales	Santiago	cucuta
Riohacha	Pasto	NEIVA	Armenia	Ibagué	



IX JORNADA de SEGURIDAD INFORMATICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Sectores Participantes



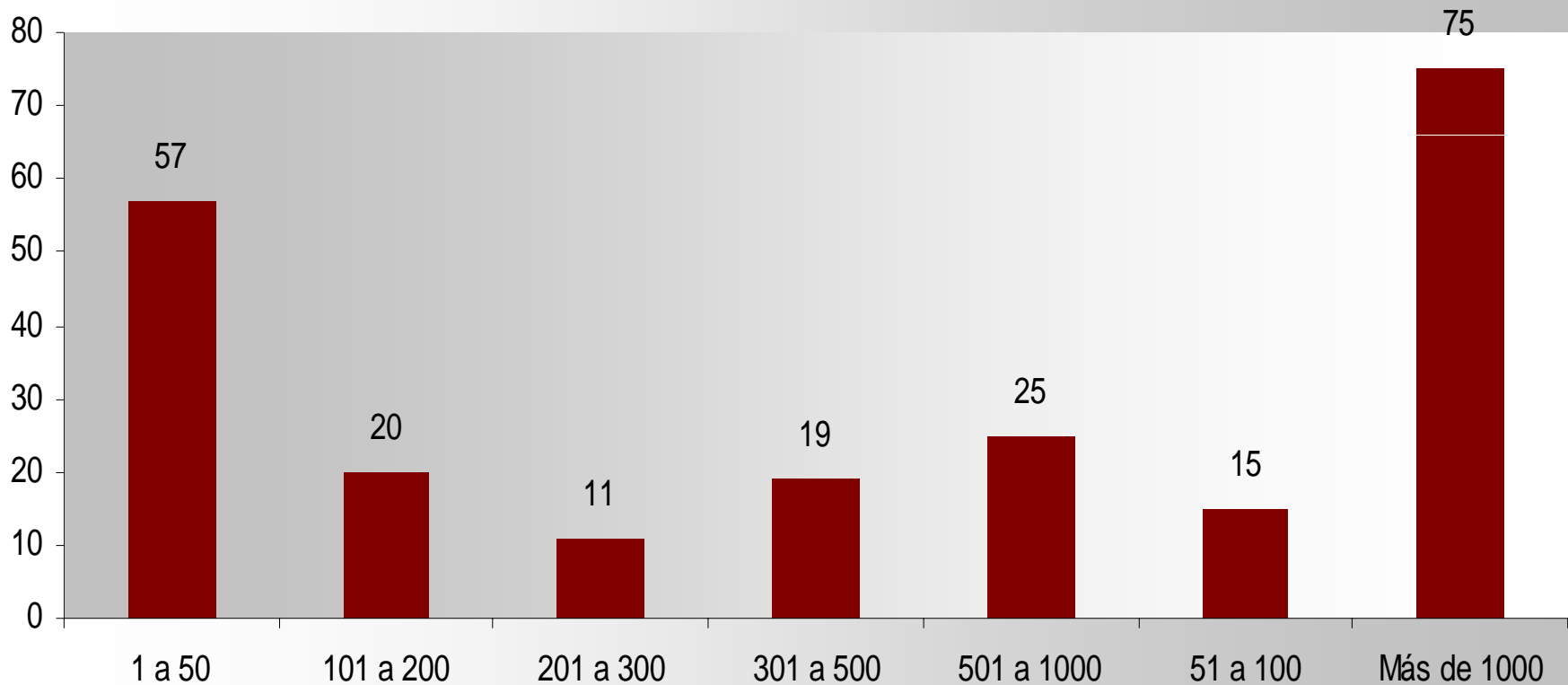
- Otra (Por favor especifique)
- Educación
- Telecomunicaciones
- Consultoría Especializada
- Gobierno / Sector público
- Servicios Financieros y Banca
- Manufactura
- Construcción / Ingeniería
- Salud
- Sector de Energía
- Alimentos



IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Cantidad de Empleados



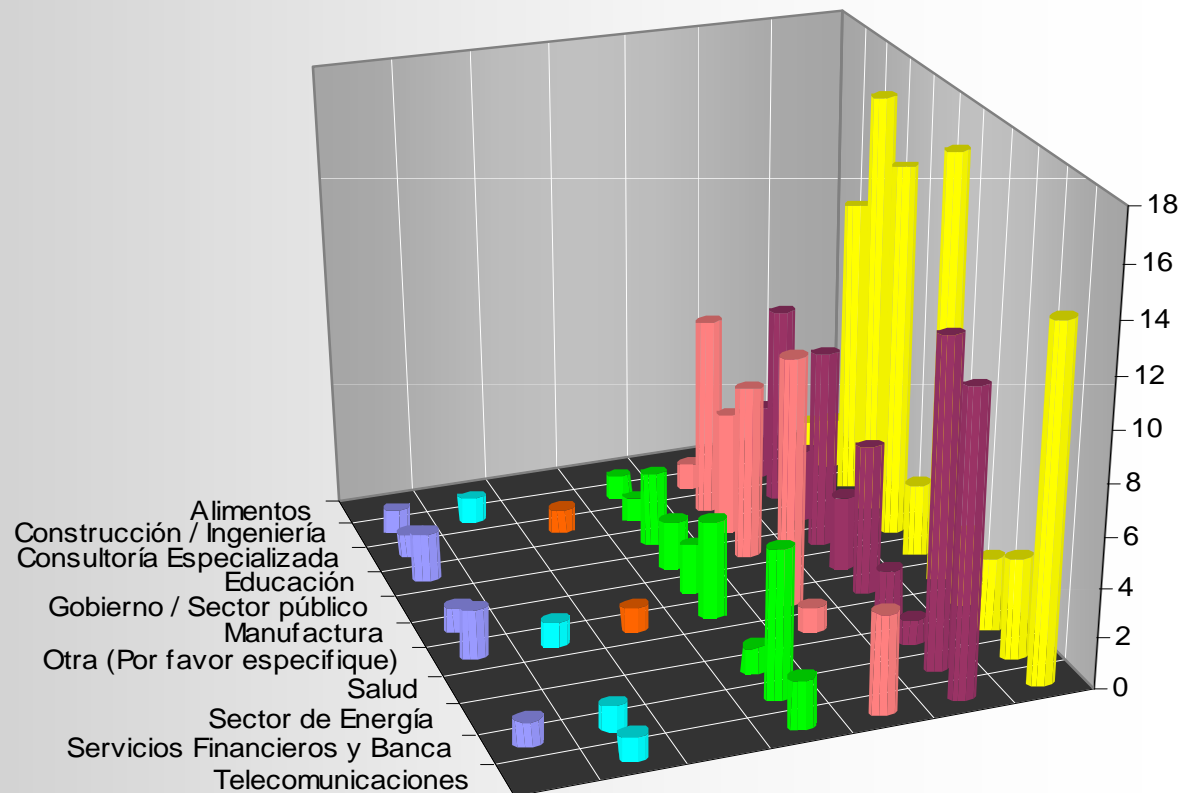


IX JORNADA de SEGURIDAD INFORMATICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Dependencia del area de Seguridad

- Auditoria interna
- Gerente de Operaciones
- Gerente Ejecutivo
- Otra
- No se tiene especificado formalmente
- Director de Seguridad Informática
- Director Departamento de Sistemas/Tecnología

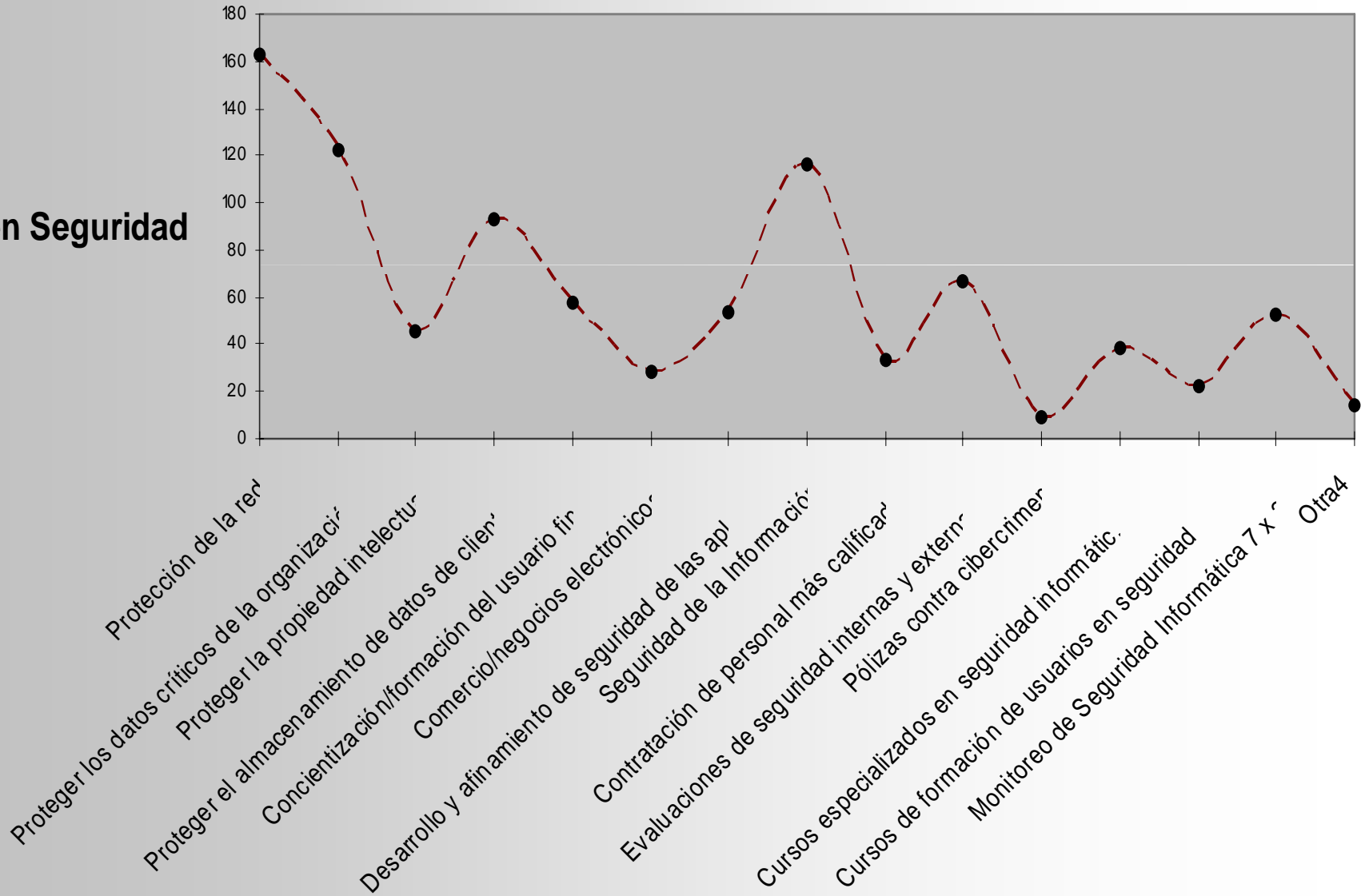




IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Gastos en Seguridad

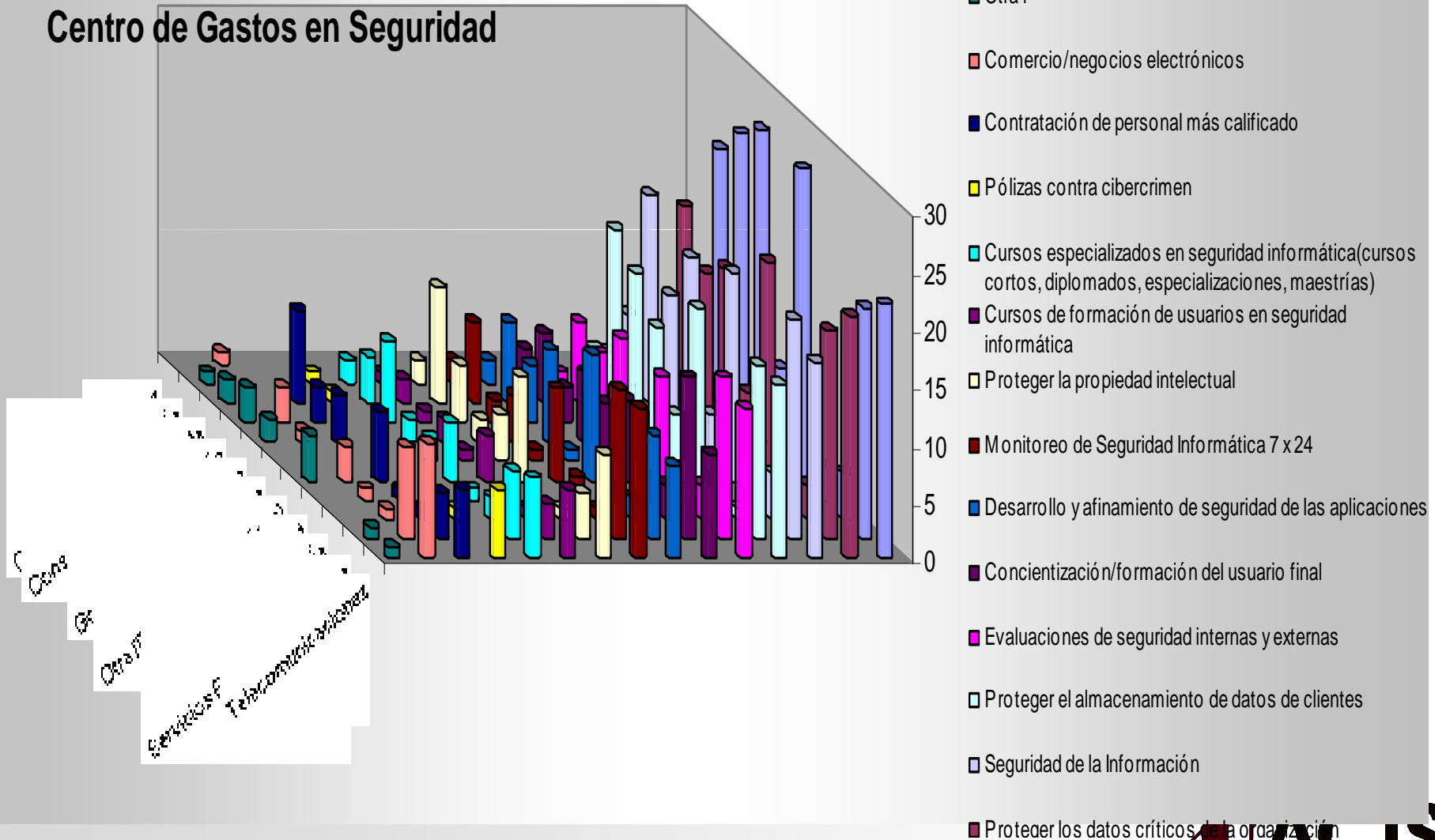




IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Centro de Gastos en Seguridad

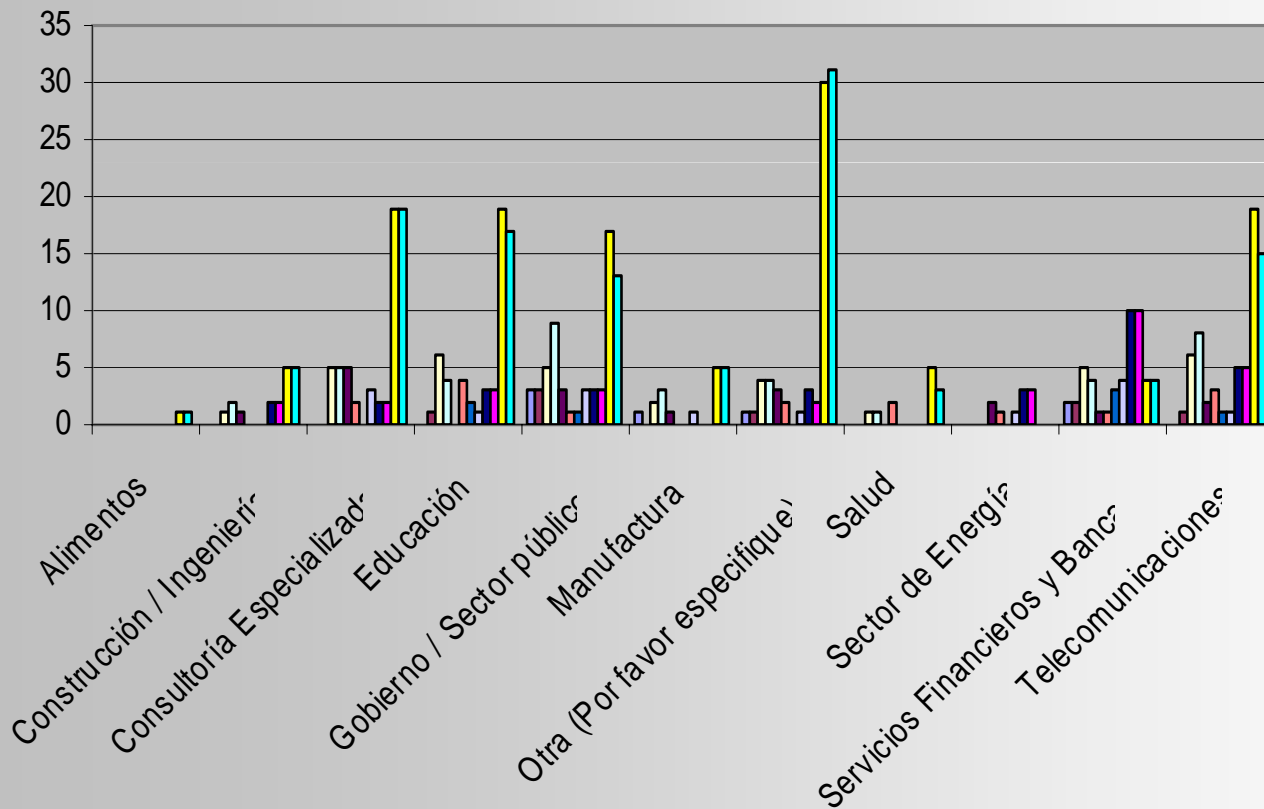




IX JORNADA de SEGURIDAD INFORMATICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Gastos/Proyecciones Seguridad



- 2008 Entre USD\$110.001 y USD\$130.000
- 2009 Entre USD\$110.001 y USD\$130.000
- 2008 Entre USD\$50.001 y USD\$70.000
- 2009 Entre USD\$50.001 y USD\$70.000
- 2008 Entre USD\$70.001 y USD\$90.000
- 2009 Entre USD\$70.001 y USD\$90.000
- 2008 Entre USD\$90.001 y USD\$110.000
- 2009 Entre USD\$90.001 y USD\$110.000
- 2008 Más de USD\$130.000
- 2009 Más de USD\$130.000
- 2008 Menos de USD\$50.000
- 2009 Menos de USD\$50.000

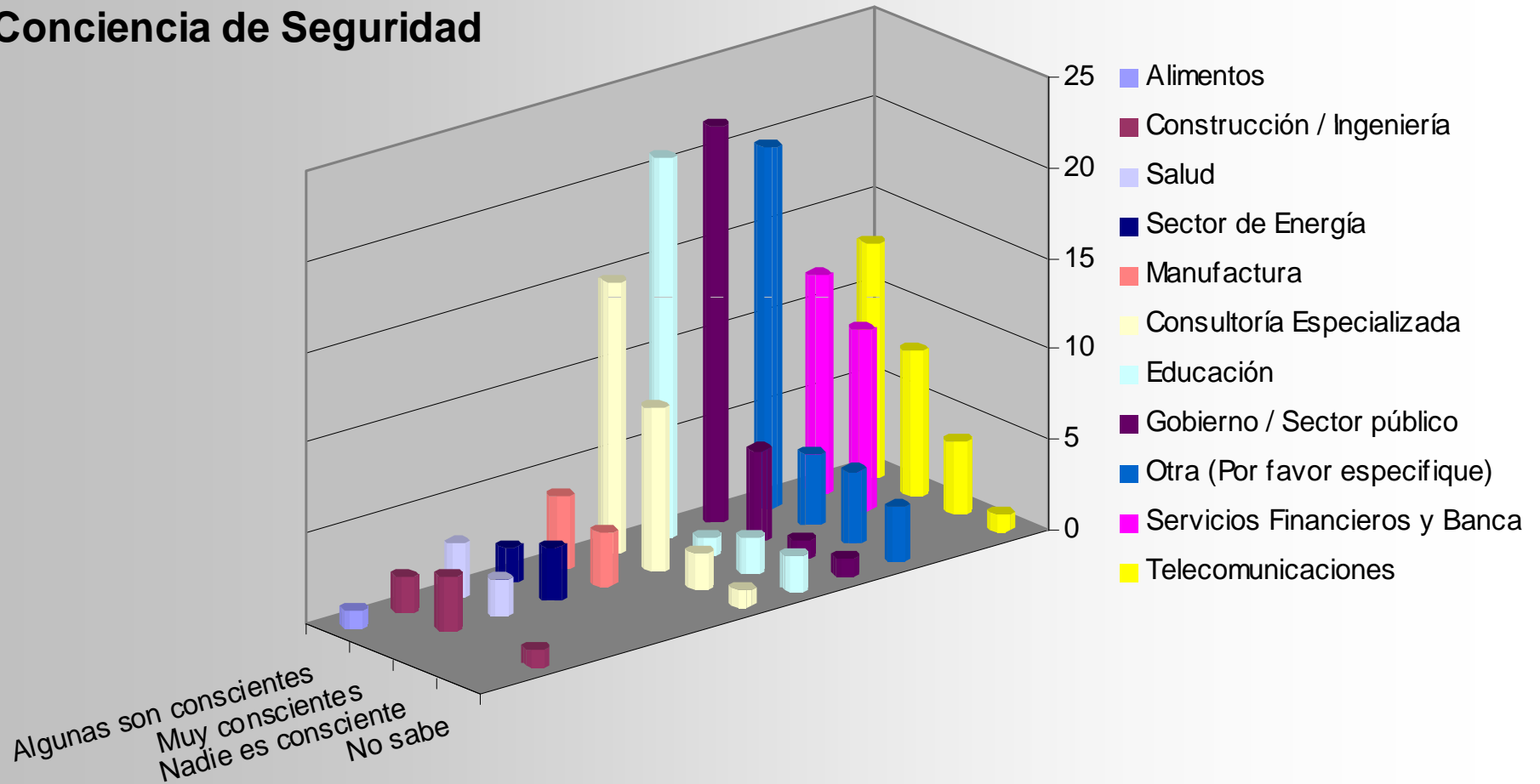




IX JORNADA de SEGURIDAD INFORMATICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Conciencia de Seguridad

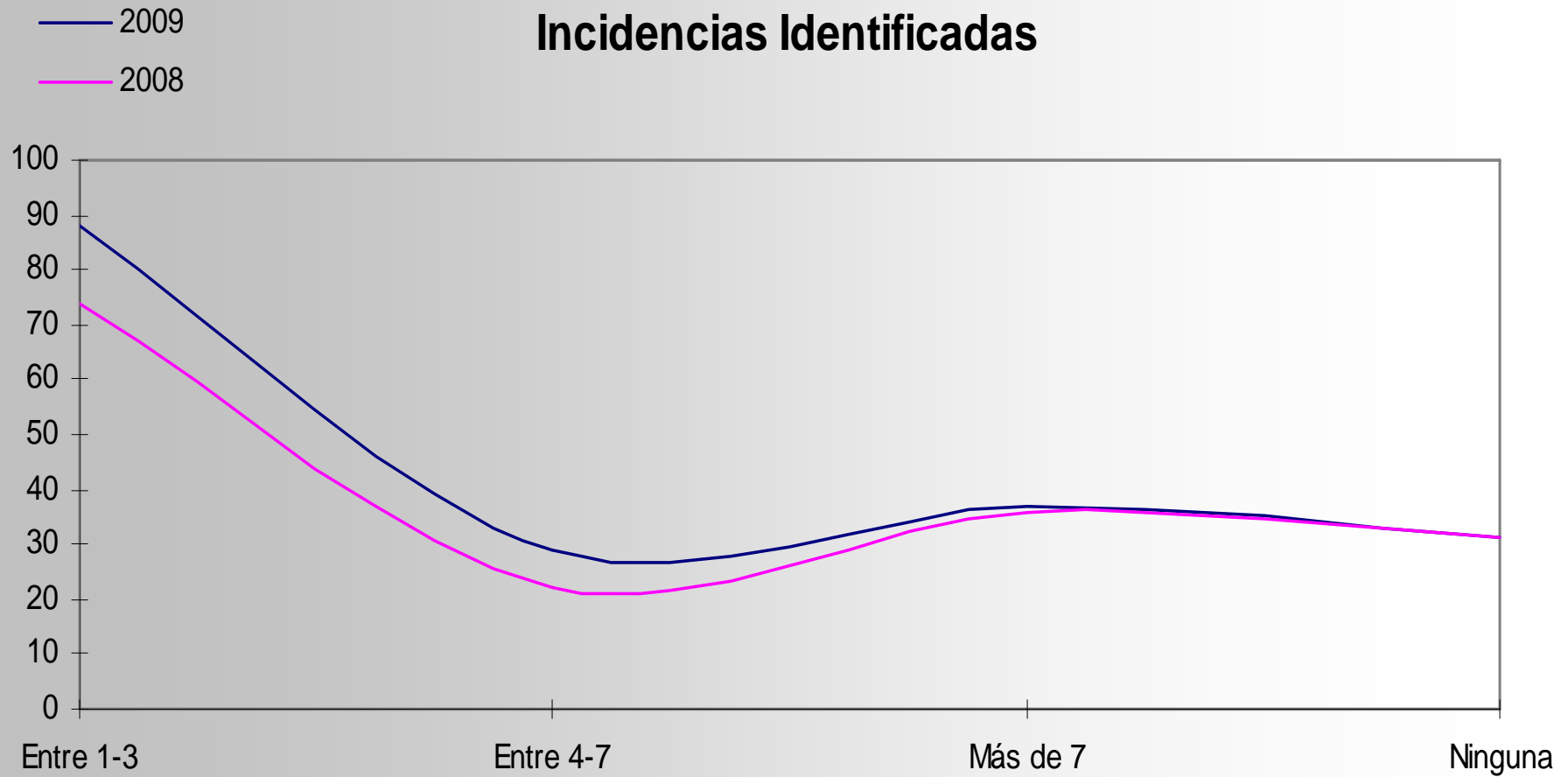




IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Incidencias Identificadas



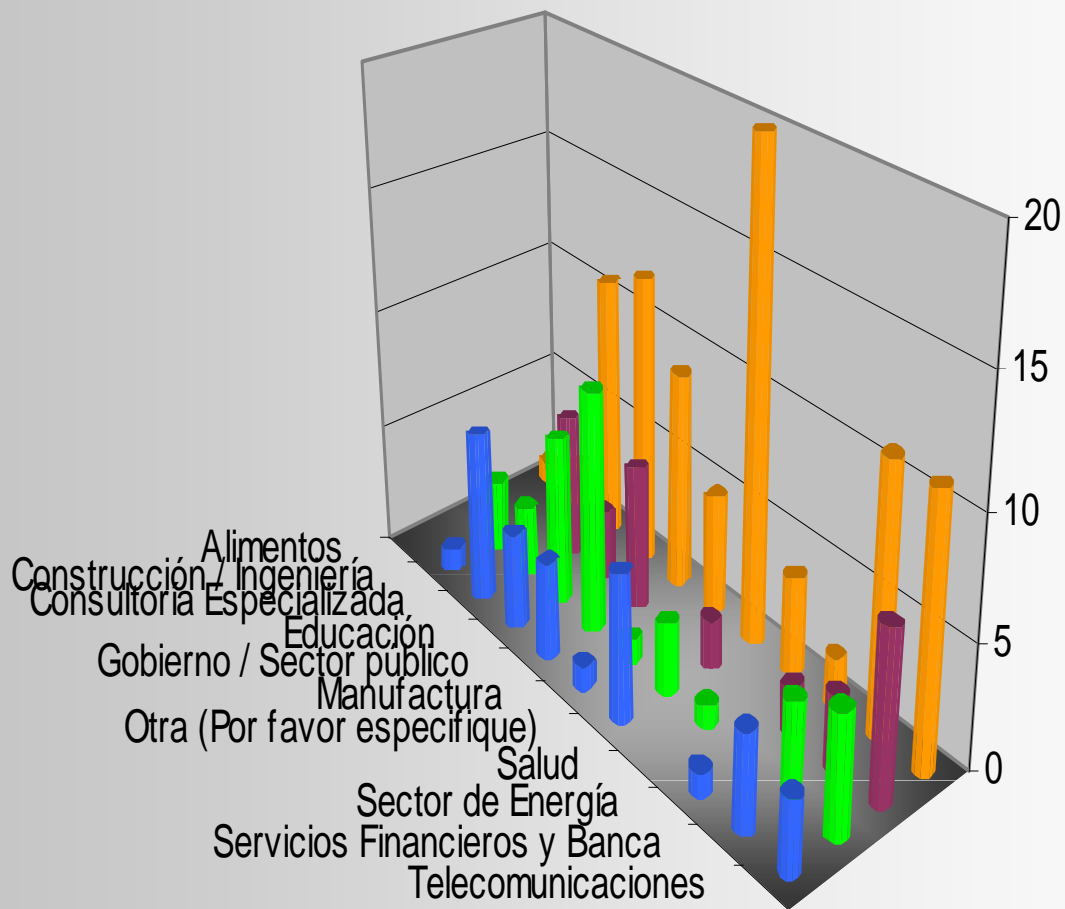


IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Identificación de Incidencias x Sectores

- Ninguna
- Más de 7
- Entre 4-7
- Entre 1-3

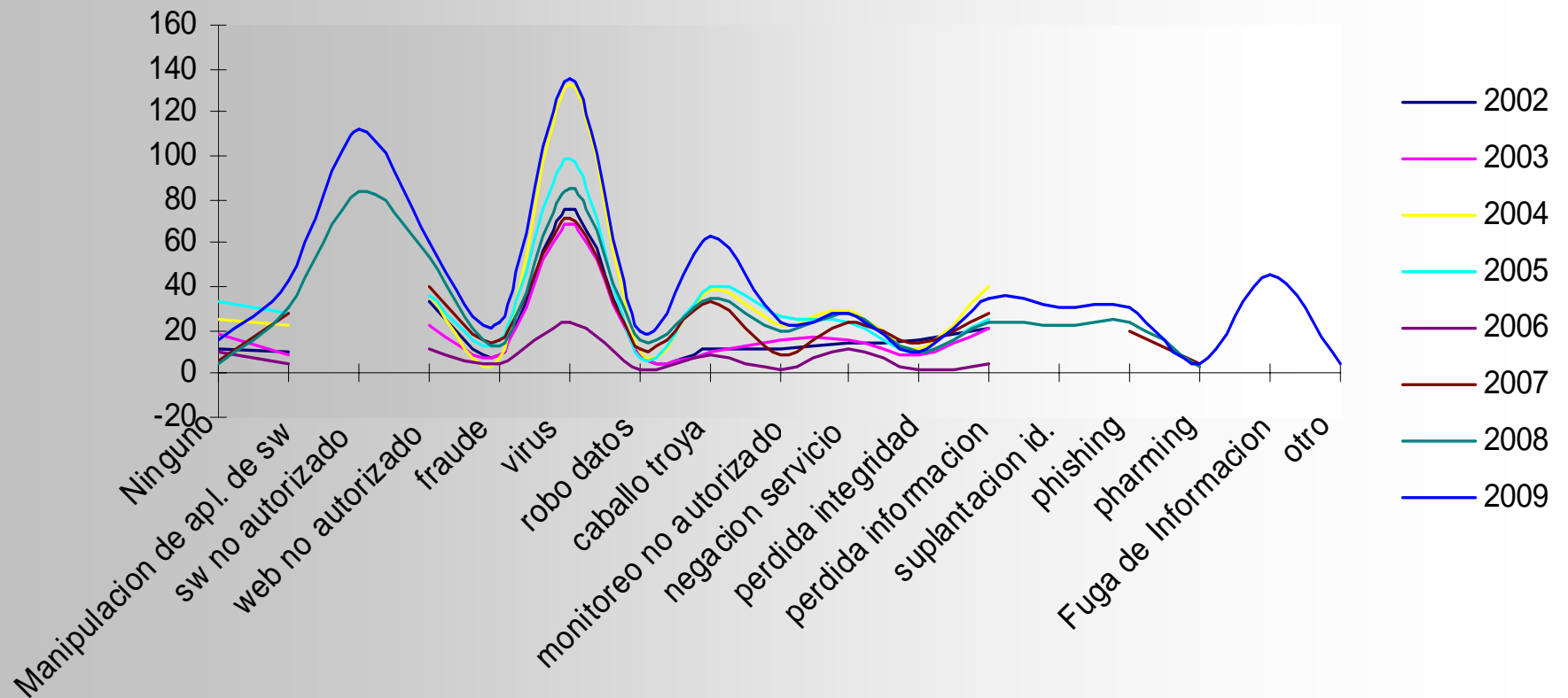




IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Evolucion de Fallas de Seguridad

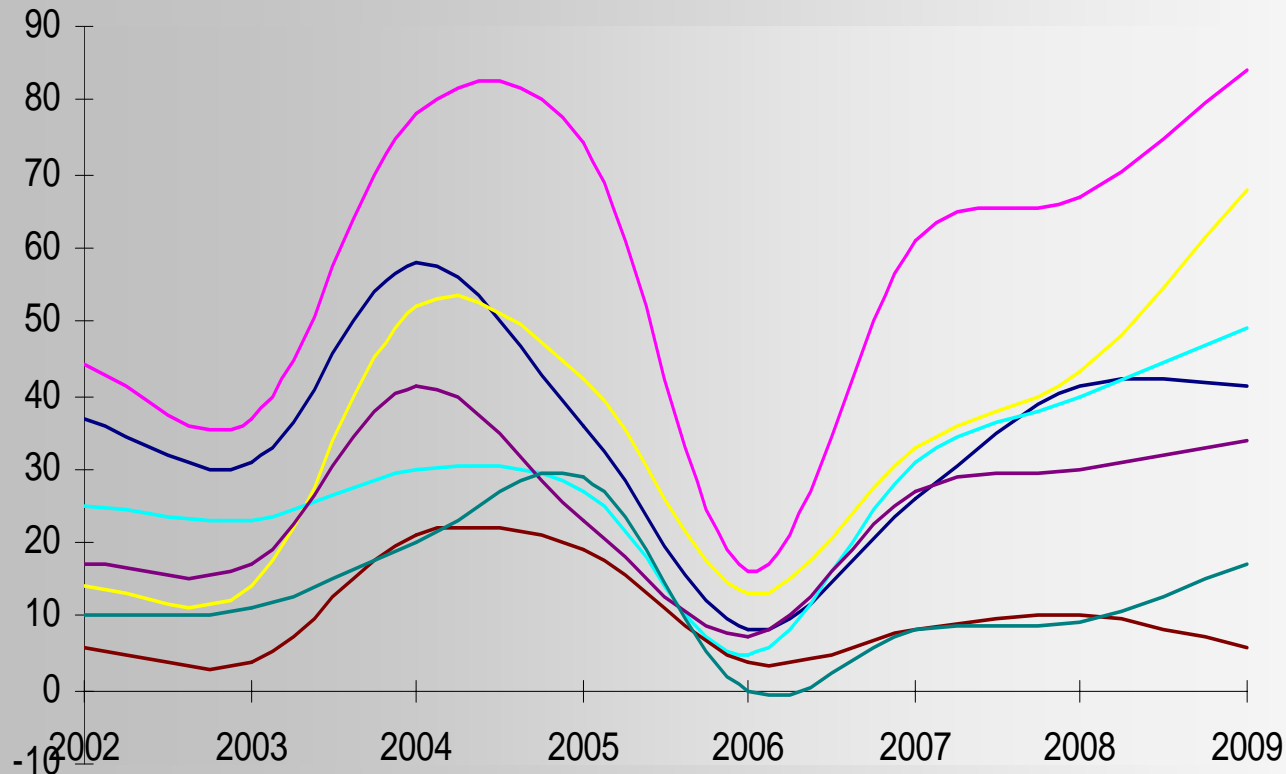




IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Identificación de las Fallas



- Material o datos alterados
- Analisis de registros
- sistema deteccion intrusos
- alertado cliente
- alertado colega
- seminarios
- otro
- Notificación de un empleado

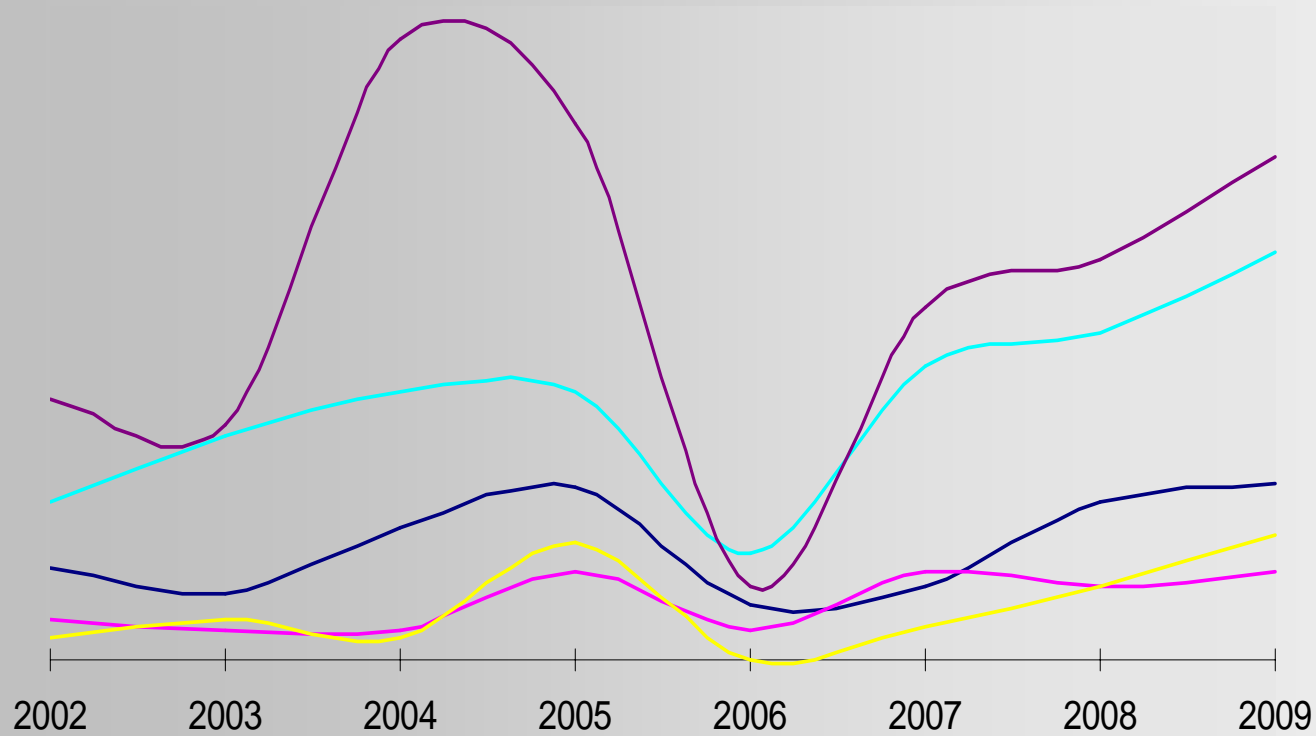


IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Notificación de Fallas

- Asesor legal
- Autoridades locales/regionales
- Autoridades nacionales
- Equipo de atención de incidentes
- Ninguno: No se denuncian

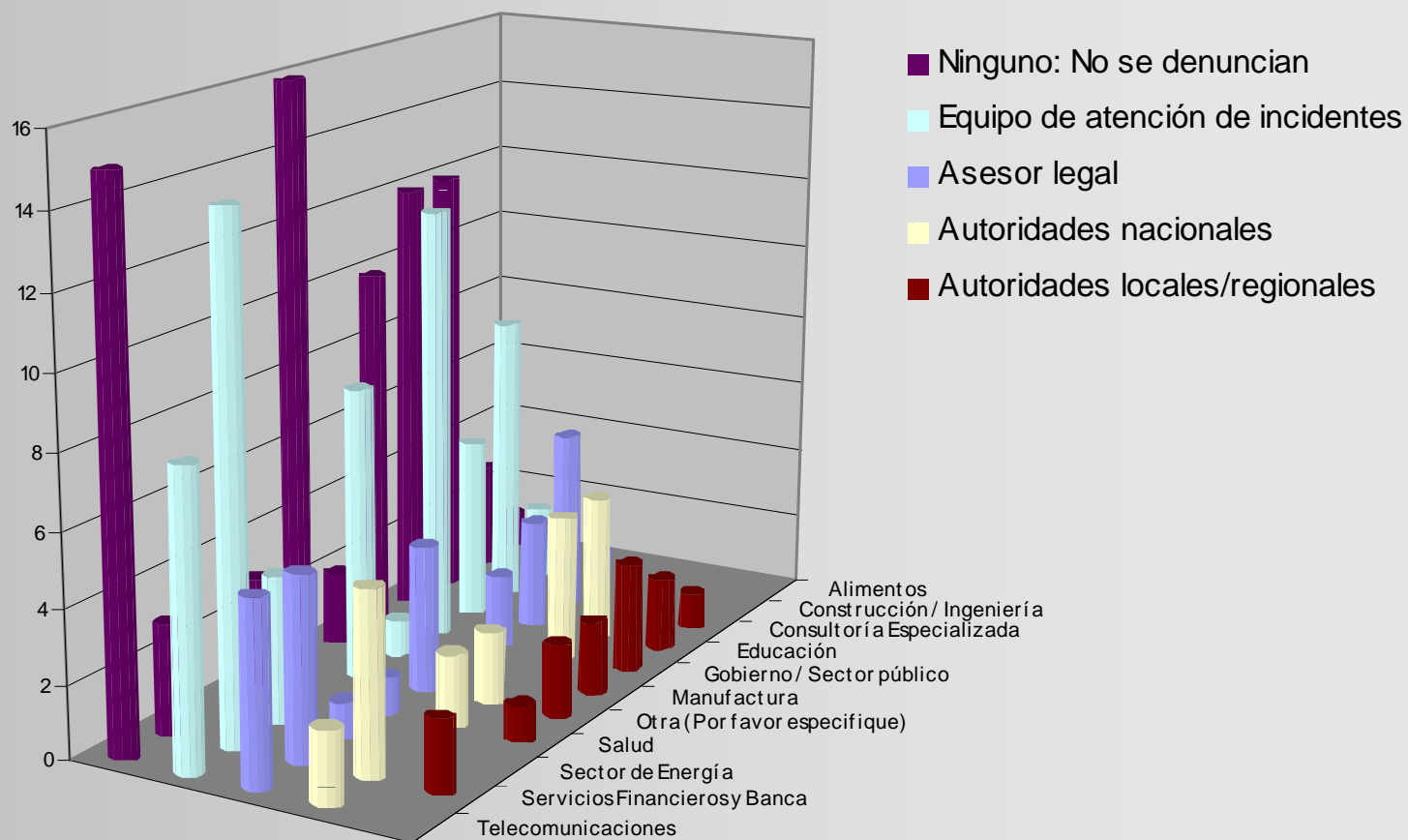




IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Notificación x Sector

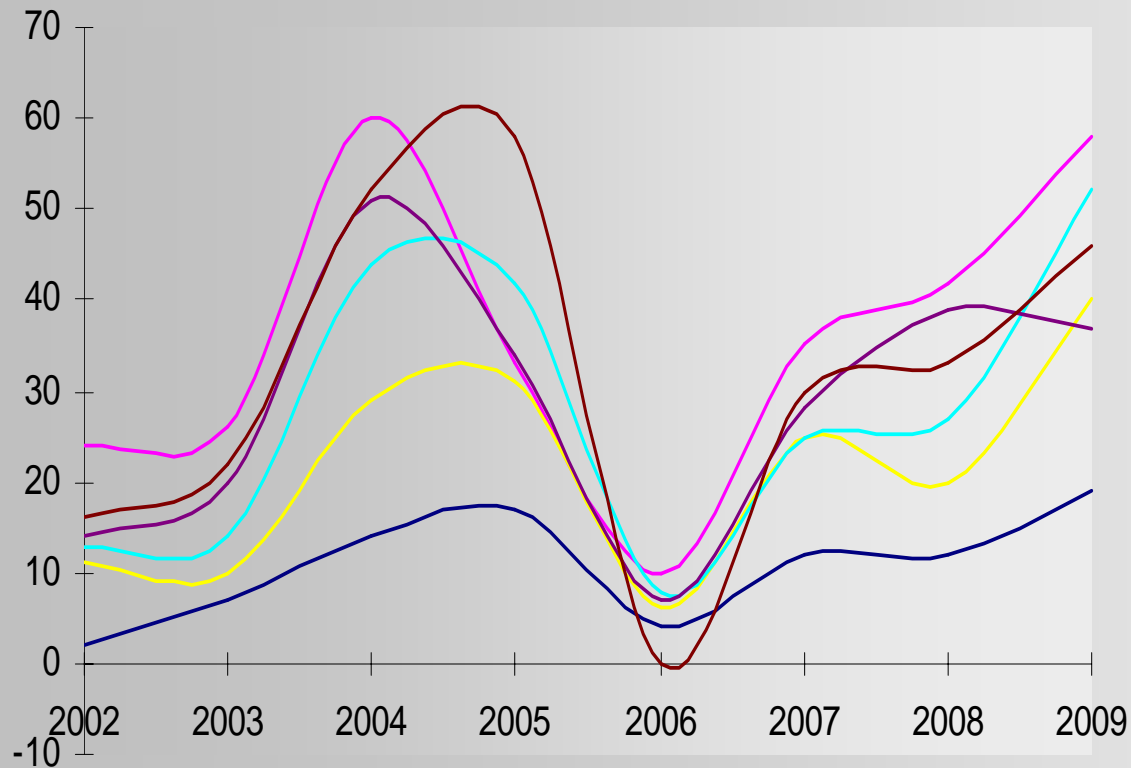




IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Motivos para no Denunciar



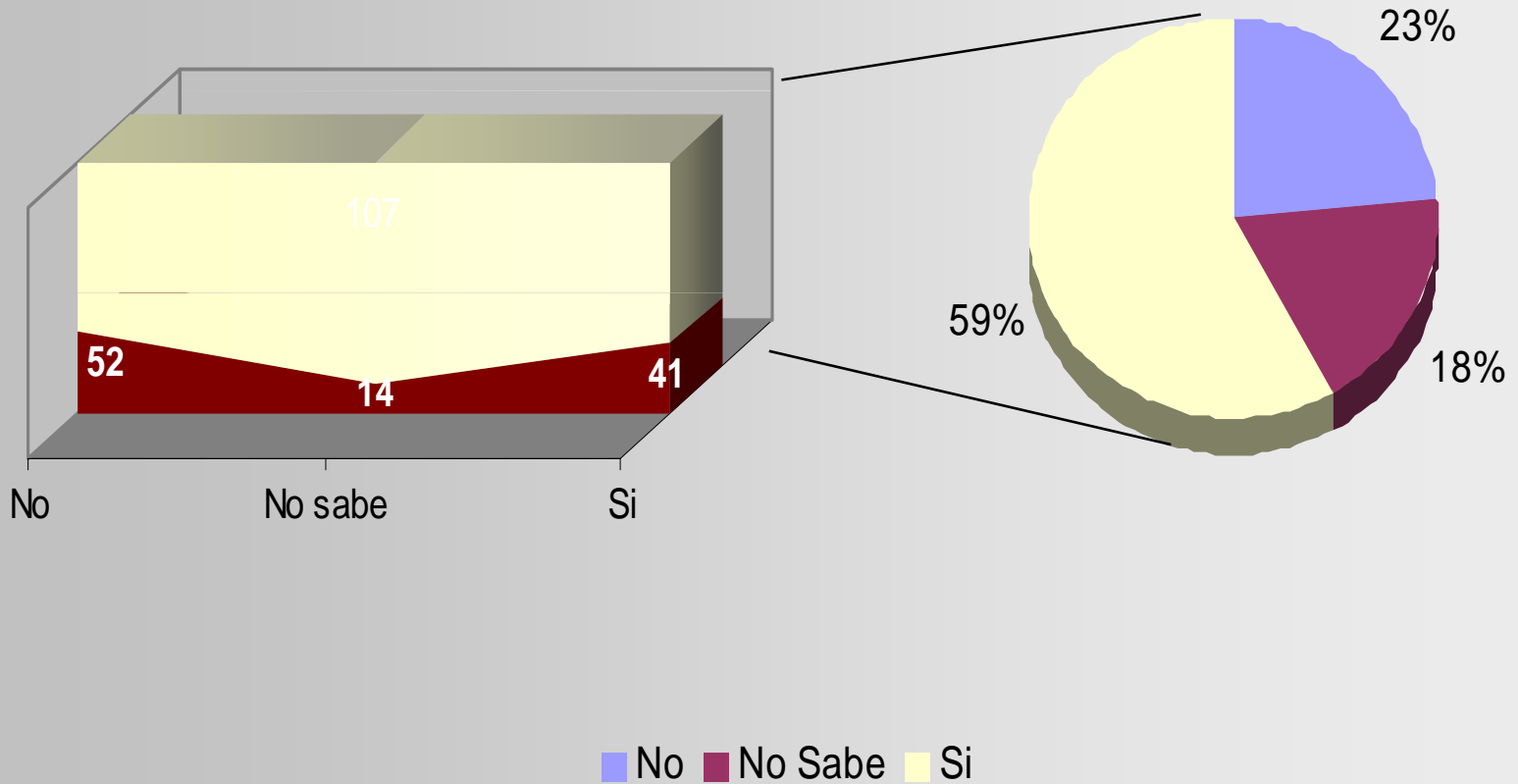
- Pérdida de valor de accionistas
- Publicación de noticias desfavorables
- Responsabilidad legal
- Motivaciones personales
- Vulnerabilidad ante la competencia
- Otro, especifique:



IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Conciencia de Evidencia Digital

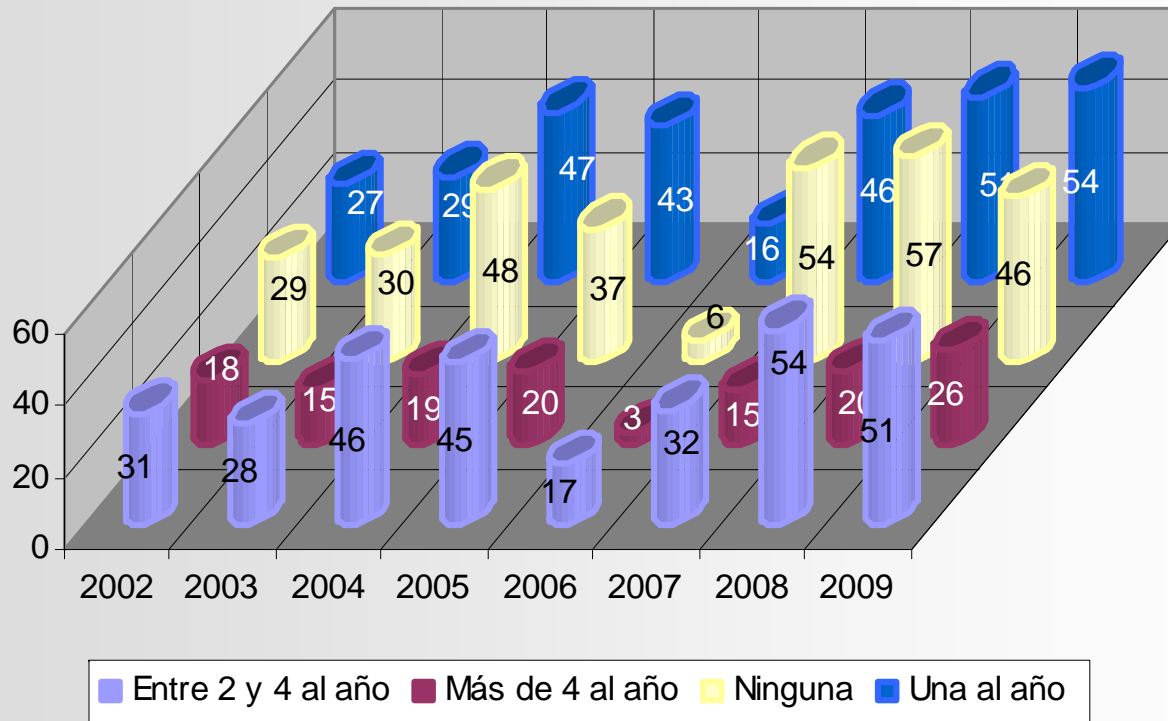




IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Pruebas de Intrusión X Año

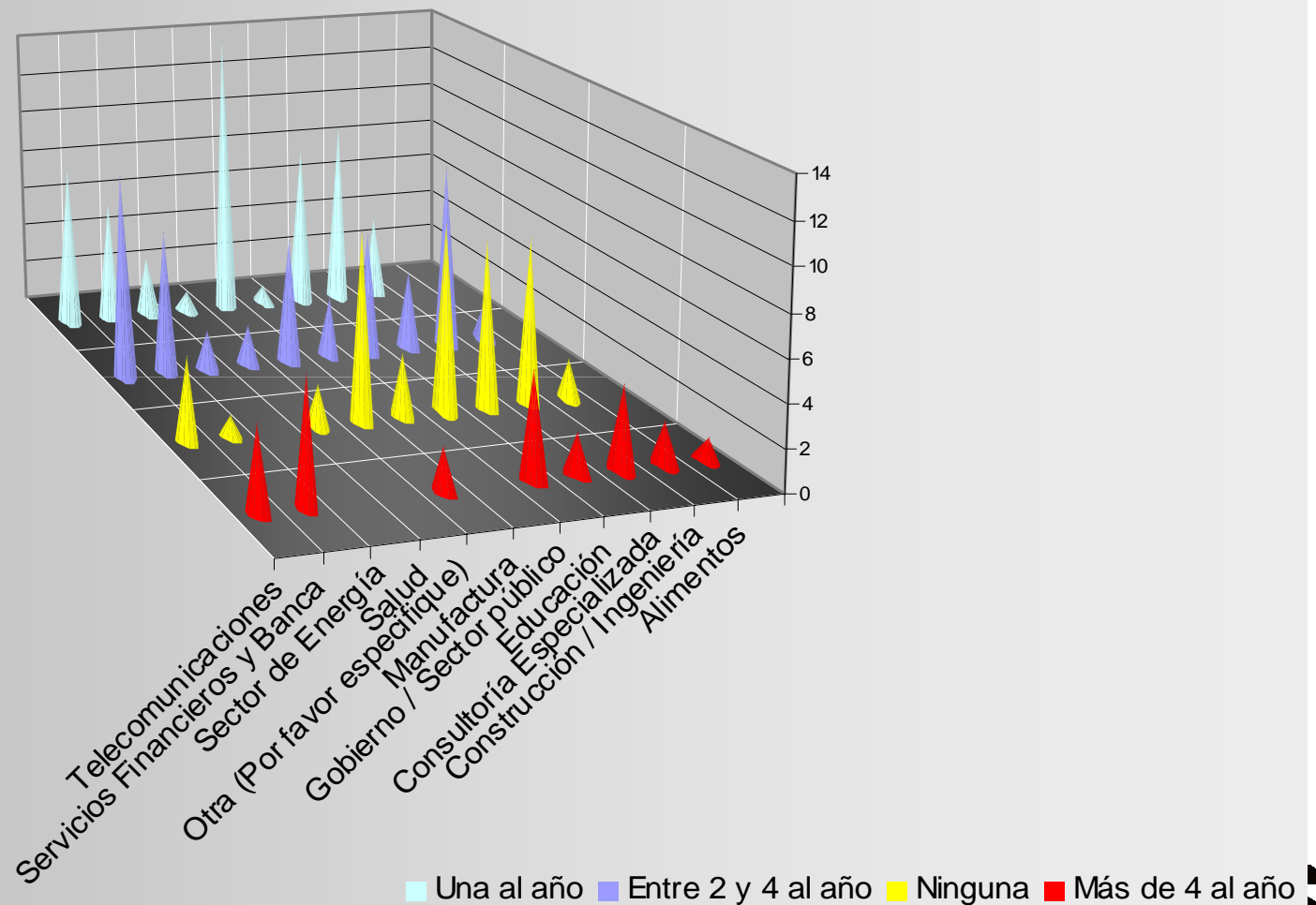




IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Pruebas de Seguridad x Sector



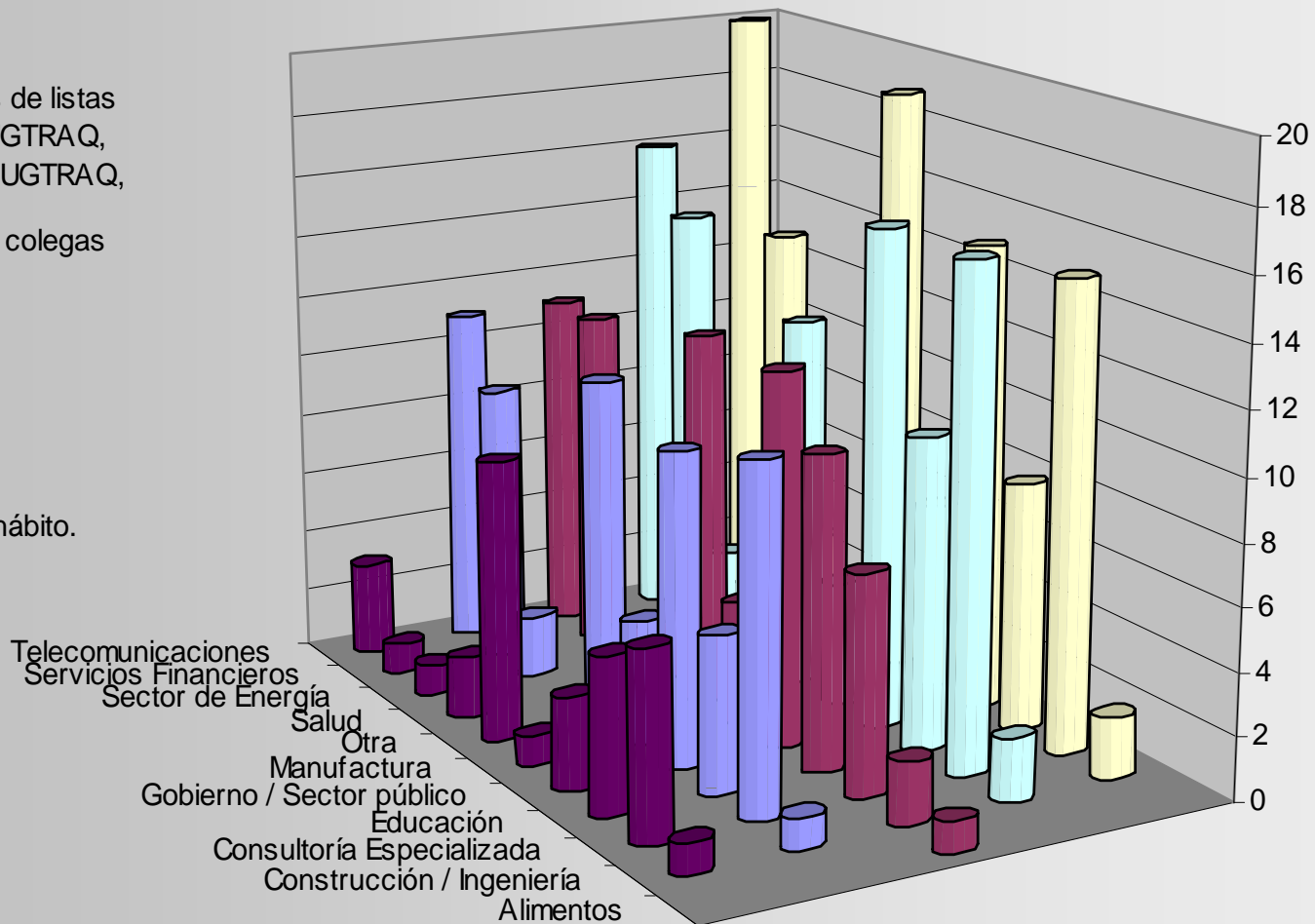


IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Notificación x Industria

- Lectura de artículos en revistas ializadas
- Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NBUGTRAQ, etc)
- Notificaciones de colegas
- Notificacion de Proveedores
- No se tiene este hábito.

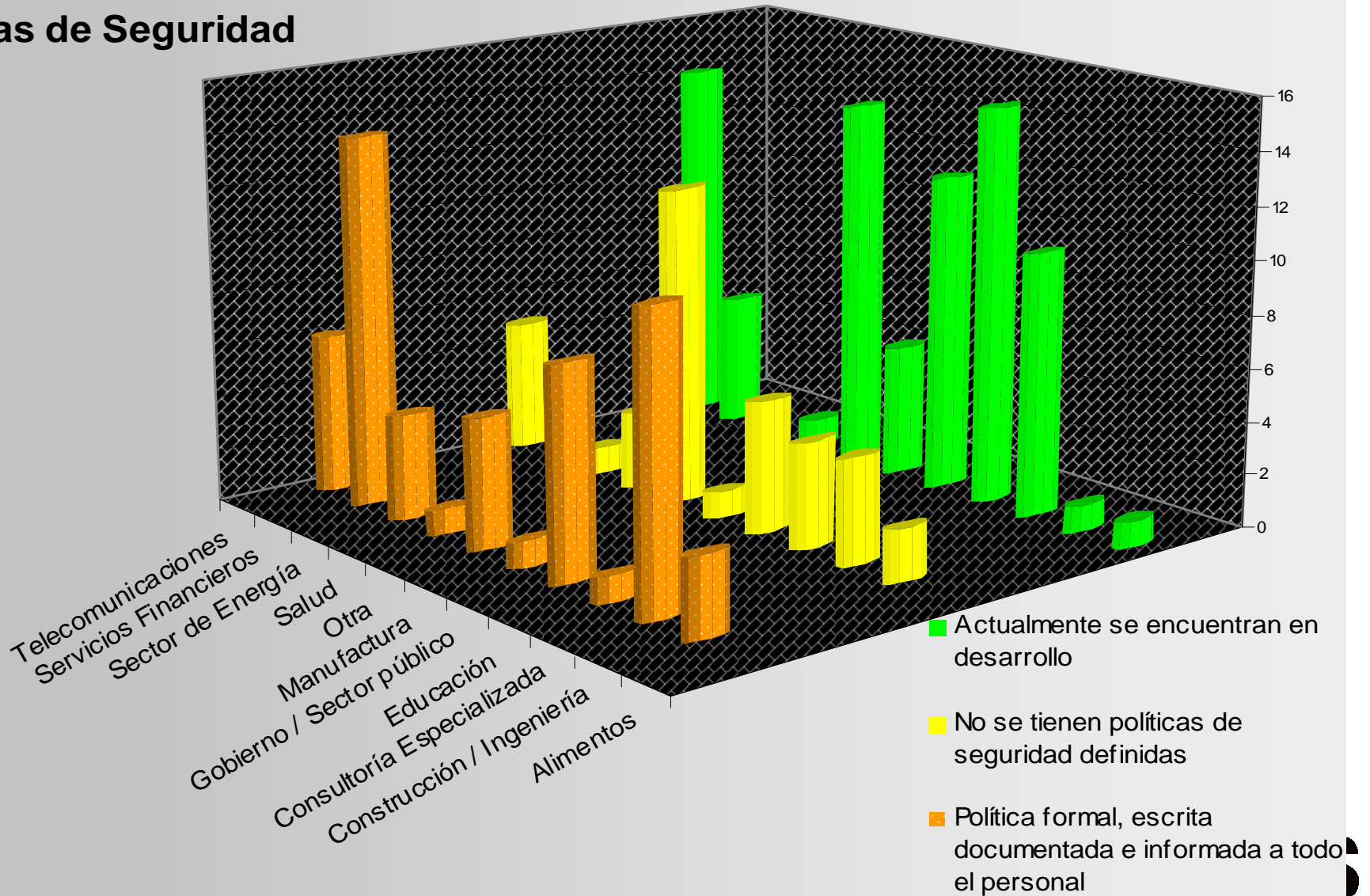




IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Políticas de Seguridad



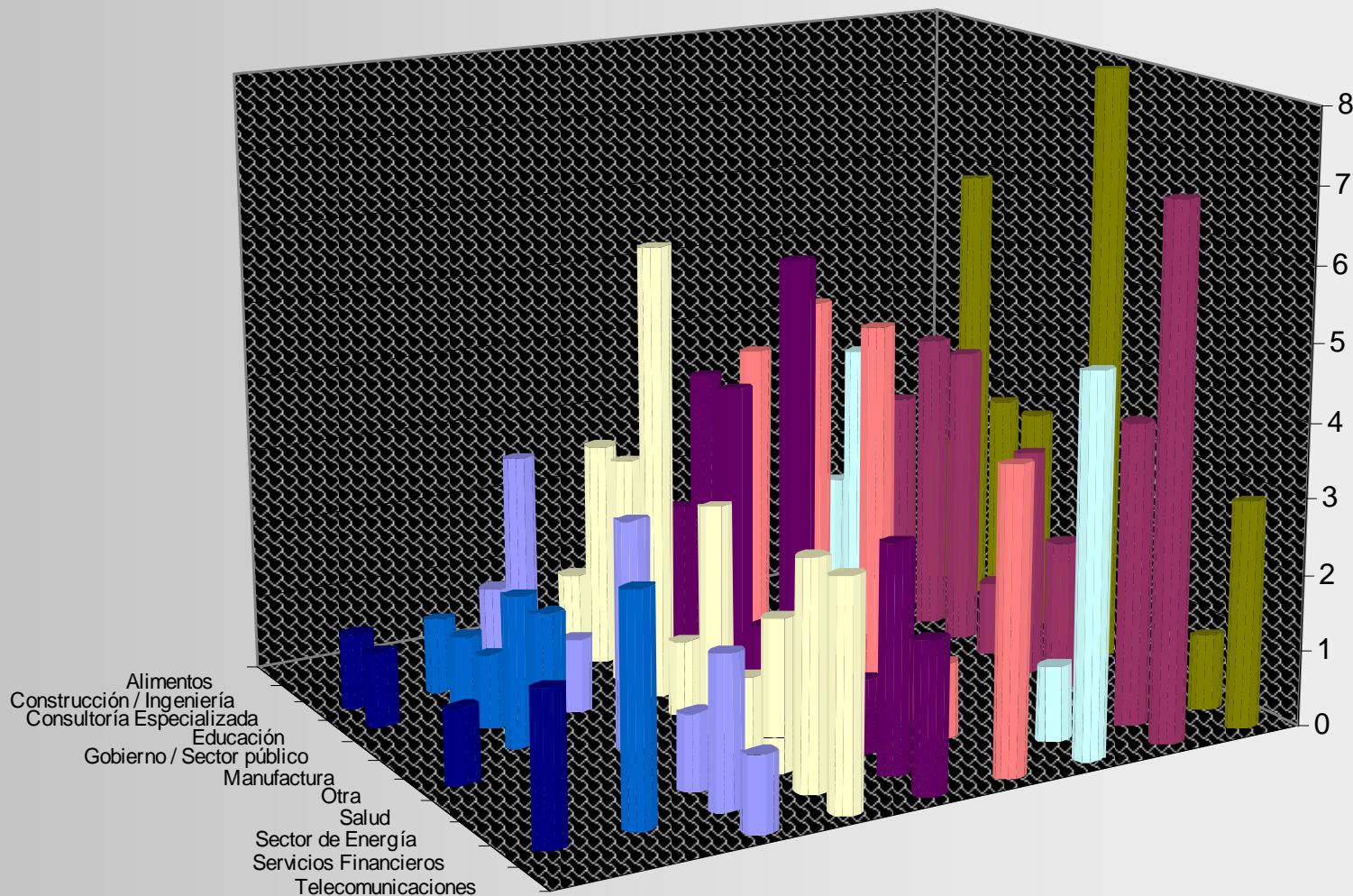


IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Obstaculos en Seguridad

- Poco entendimiento de los flujos de la información en la organización
- Otros (Por favor especifique)
- Complejidad tecnológica
- Falta de colaboración entre áreas/departamentos
- Falta de tiempo
- Inexistencia de política de seguridad

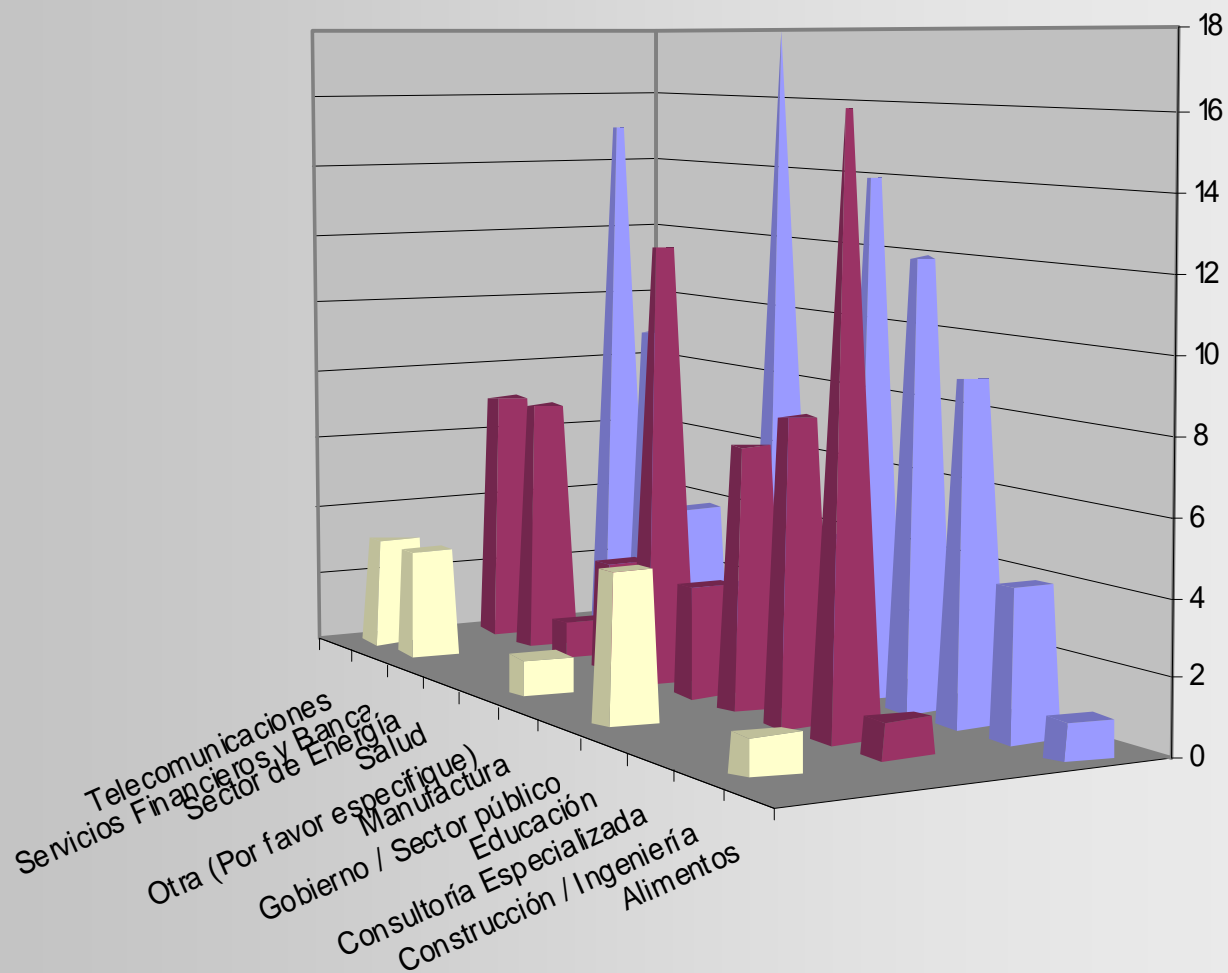




IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

- No
- No sabe
- Si



Contactos para seguir intrusos



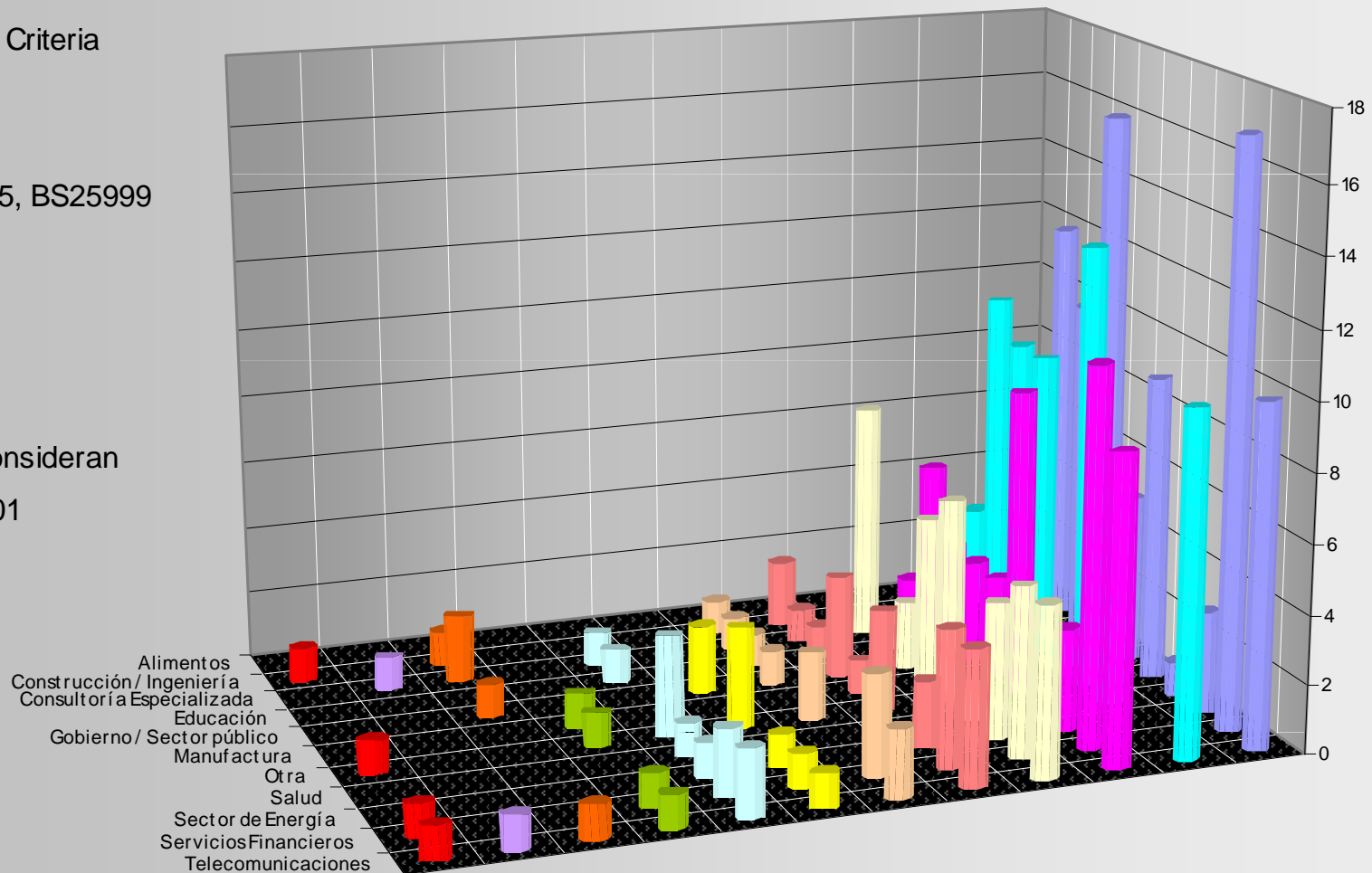


IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Estandares usados

- ISM3
- SANS
- Common Criteria
- Octave
- Magerit
- ISO27005, BS25999
- OSSTM
- NIST
- Cobit 4.1
- ITIL
- No se consideran
- ISO 27001



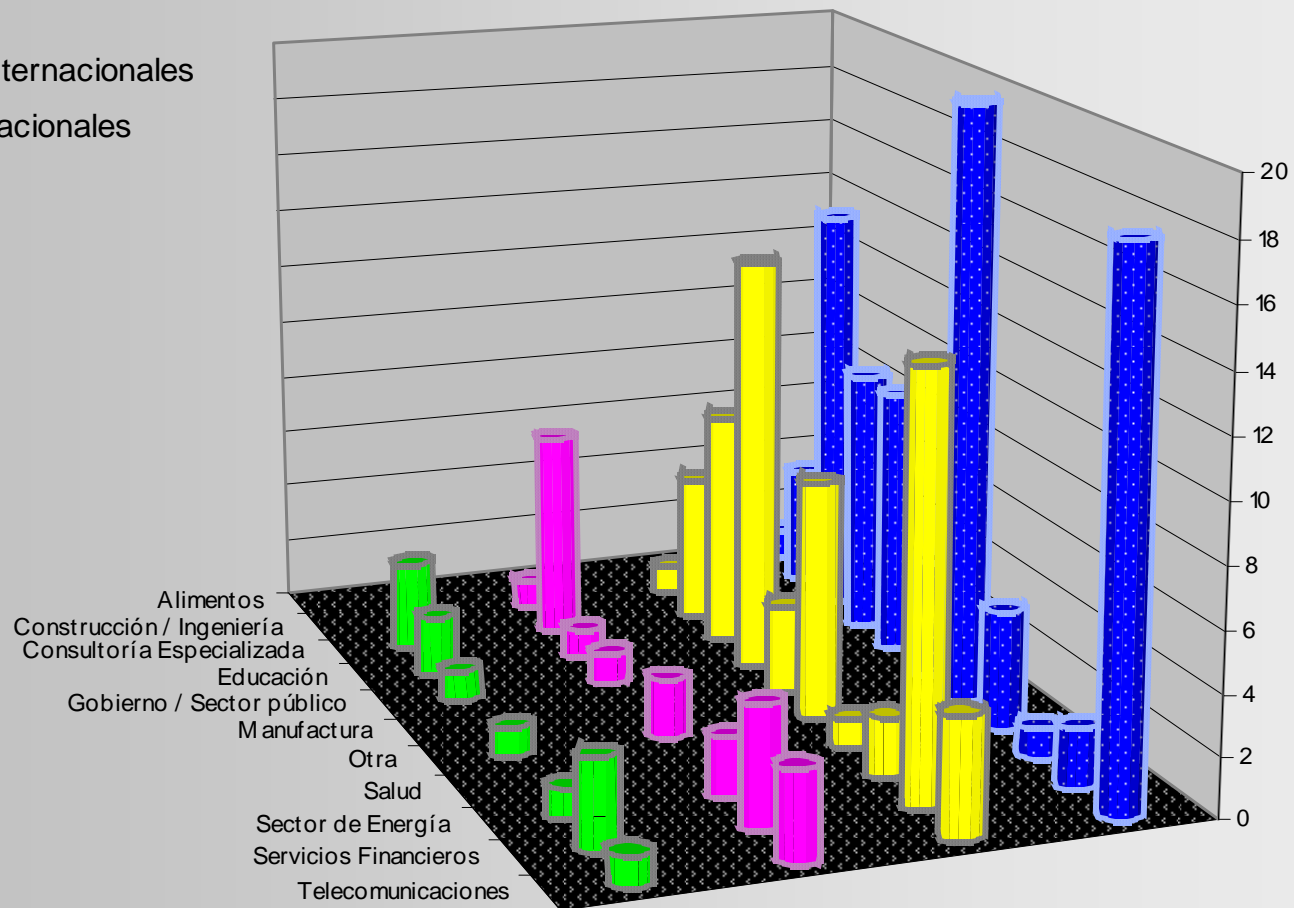


IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Regulaciones

- Otras
- Regulaciones internacionales
- Regulaciones nacionales
- Ninguna

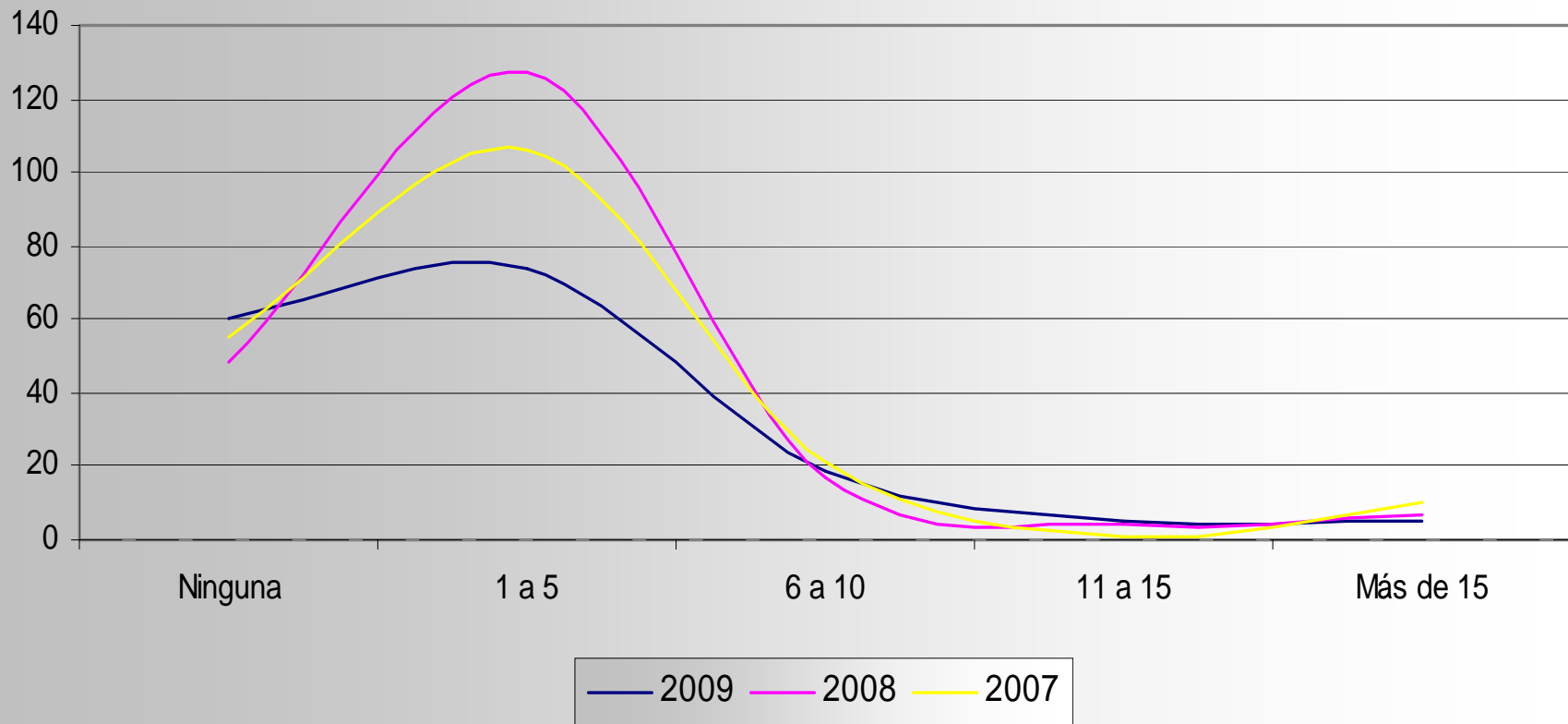




IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Dedicacion de Tiempo del Personal a Seguridad



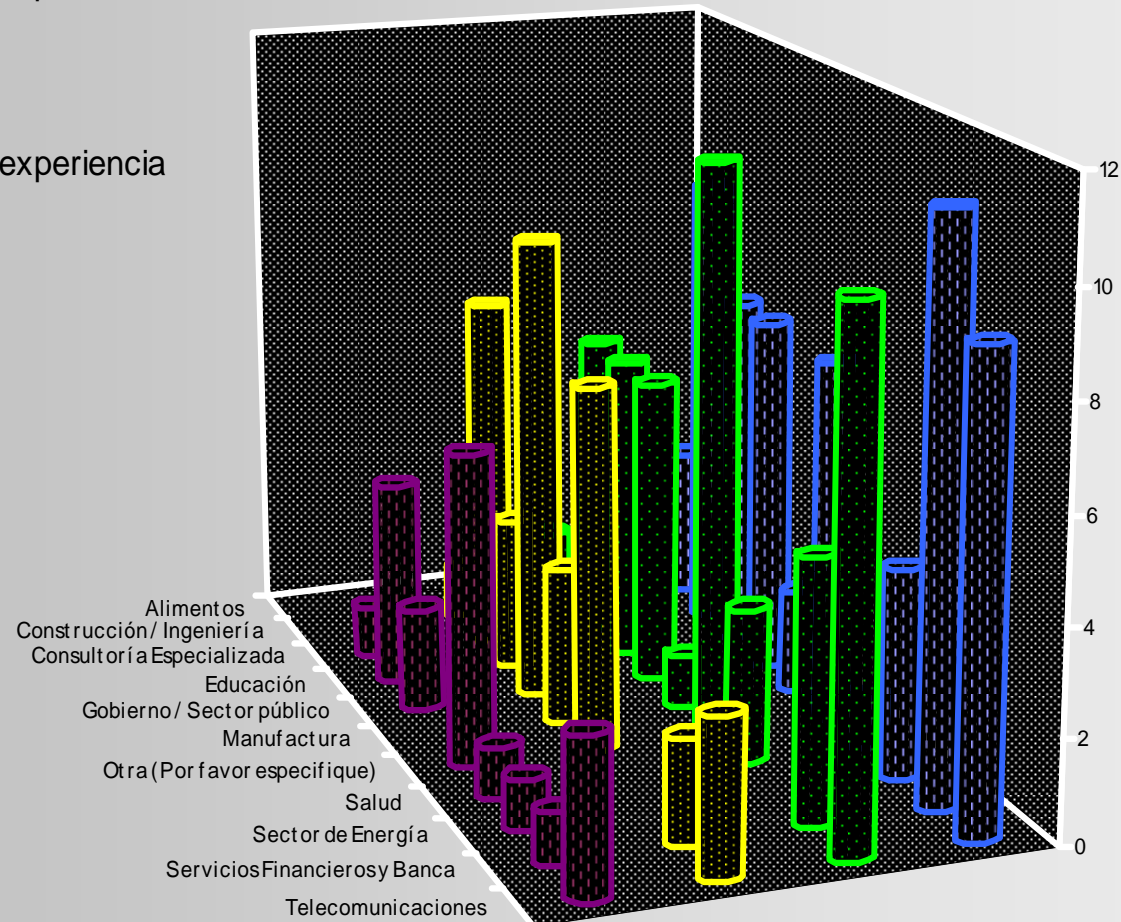


IX JORNADA de SEGURIDAD de INFORMÁTICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Experiencia de Expertos

- Menos de un año de experiencia
- Ninguno
- Uno a dos años
- Más de dos años de experiencia

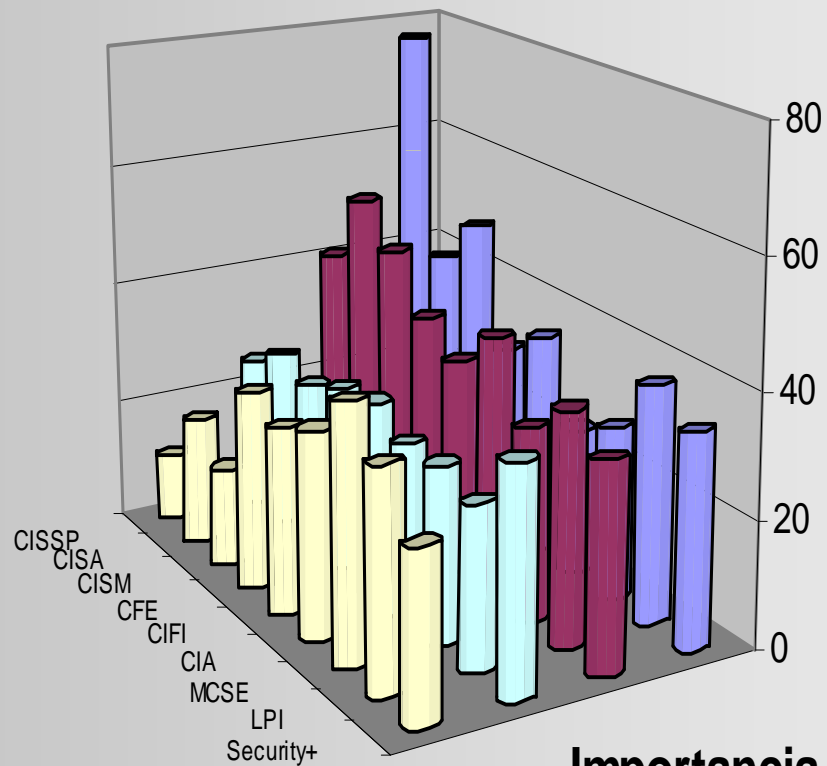




IX JORNADA de SEGURIDAD de INFORMATICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

- No Importante
- No sabe
- Importante
- Muy Importante



Importancia de las Certificaciones



IX JORNADA de SEGURIDAD INFORMATICA Monitoreo y Evolución de la Inseguridad Informática Junio 17, 18 y 19 de 2009

Retos y Conclusiones

- Las regulaciones nacionales e internacionales llevarán a las organizaciones en Colombia fortalecer los sistemas de gestión de la seguridad de la información.
- Las certificaciones CISSP, CISM y CISA, son las mas valoradas por el mercado, y son las cartas de presentación profesional a tener en cuenta en la ejecución de proyectos de seguridad.
- Estándares como ISO 27000, ITIL COBIT y NIST son los estándares mas usados para la gestión de la seguridad.
- La inversión en seguridad de la información se encuentra concentrada en el perímetro de las organizaciones: redes y sistemas de comunicaciones, así como la protección de los datos del cliente, aparece un nuevo escenario que son las pólizas de cibercrimen
- Es necesario mencionar que se debe reforzar el tema de conciencia en los temas de seguridad, adicional a temas de manejo de evidencias digitales y su formalizacion dentro de las organizaciones.



IX JORNADA de SEGURIDAD INFORMATICA Monitoreo y Evolución de la Inseguridad Informática Junio 17, 18 y 19 de 2009

Retos y Conclusiones

- Se debe continuar los esfuerzos desde el gobierno, la academia, la empresa y la industria, para afrontar los posibles ataques de los intrusos.
- Se debe decidir si se desea que se materialice la inseguridad, por lo tanto es necesario desarrollar y fortalecer los temas de políticas dentro de la organización
- Se ve que las organizaciones realizan cada vez mas mas cantidades de pruebas de seguridad, es importante por que muestra que se preocupan por la seguridad de las plataformas tecnologicas
- Aumenta de manera importante que la responsabilidad de seguridad frente a otros anos crece con respecto a las areas de seguridad de la informacion o informatica, asi como se nota que hay mayores aumentos frente a las inversiones de seguridad.
- Se debe insistir en que es necesario denunciar las intrusiones, dado que es un mecanismo de control que ayuda en el mejoramiento de la seguridad.



Bibliografía

- COMPUTER SECURITY INSTITUTE (2008) CSI/FBI. Computer Crime and Security Survey 2007
- PRICEWATERHOUSECOOPERS-UK (2008) Information Security Breaches Survey 2008
- PRICEWATERHOUSECOOPERS (2008) Global State of Information Security Study
- DELOITTE & TOUCHE (2007) 2008 Privacy and data protection survey.