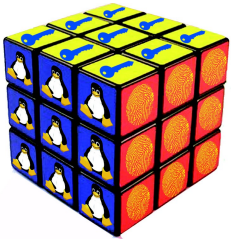




# Oficial de (in)Seguridad de la Información : Coordinador de la gestión

Octubre 2008



Oh, y ahora ¿quien podrá ayudarnos?

*En Cantv ahora la seguridad es Integral*

Andrés R. Almanza, Ms(c)  
[andres\\_almanza@hotmail.com](mailto:andres_almanza@hotmail.com)

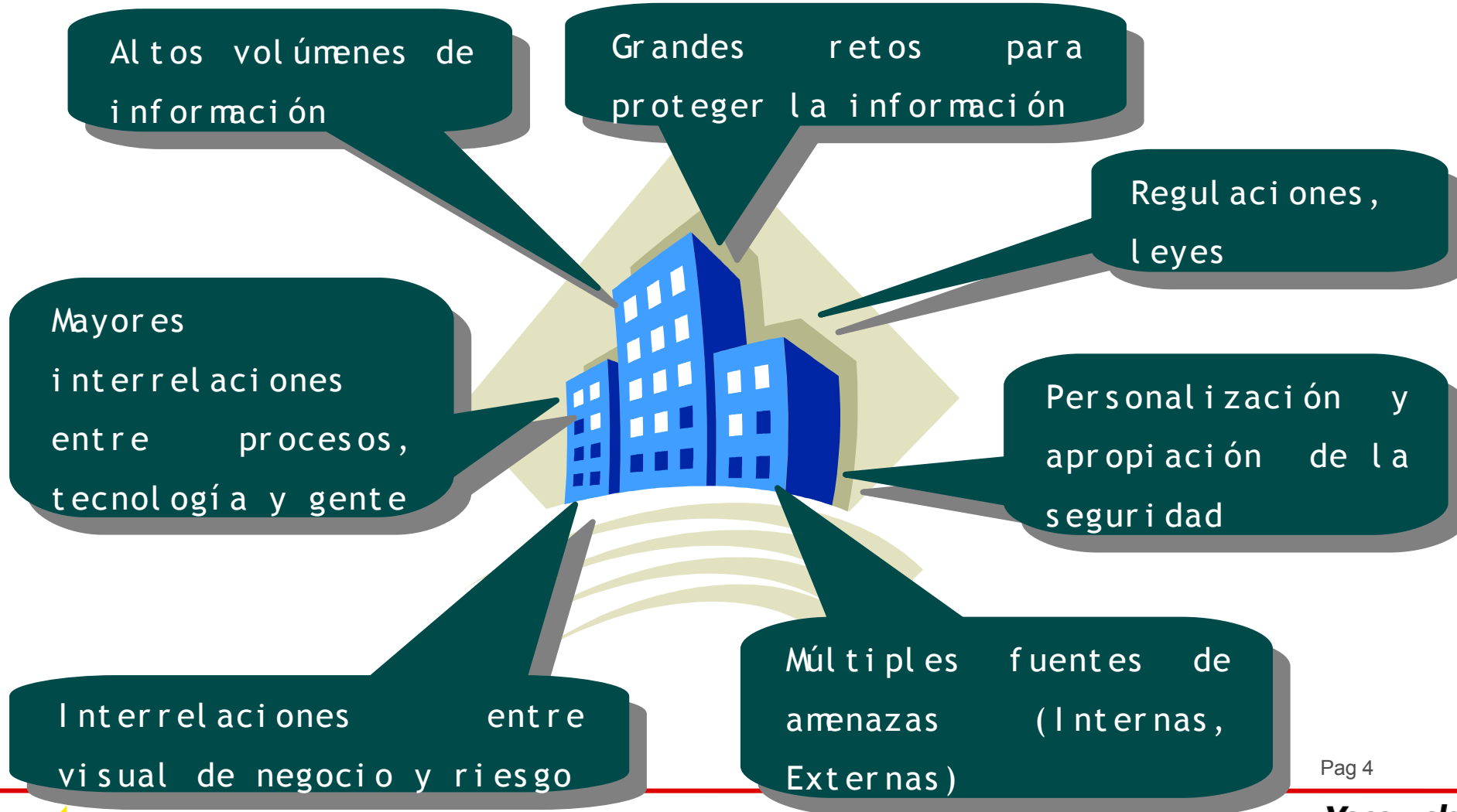
- ✓ Reflexión consiente de la forma en como es vista la seguridad de la información en la organización
- ✓ Quien puede liderar un proceso de seguridad y algunas consideraciones para hacerlo
- ✓ Que hace el líder de seguridad de la información en la organización
- ✓ Por que se puede desistir en el intento de gestionarumento

# Agenda

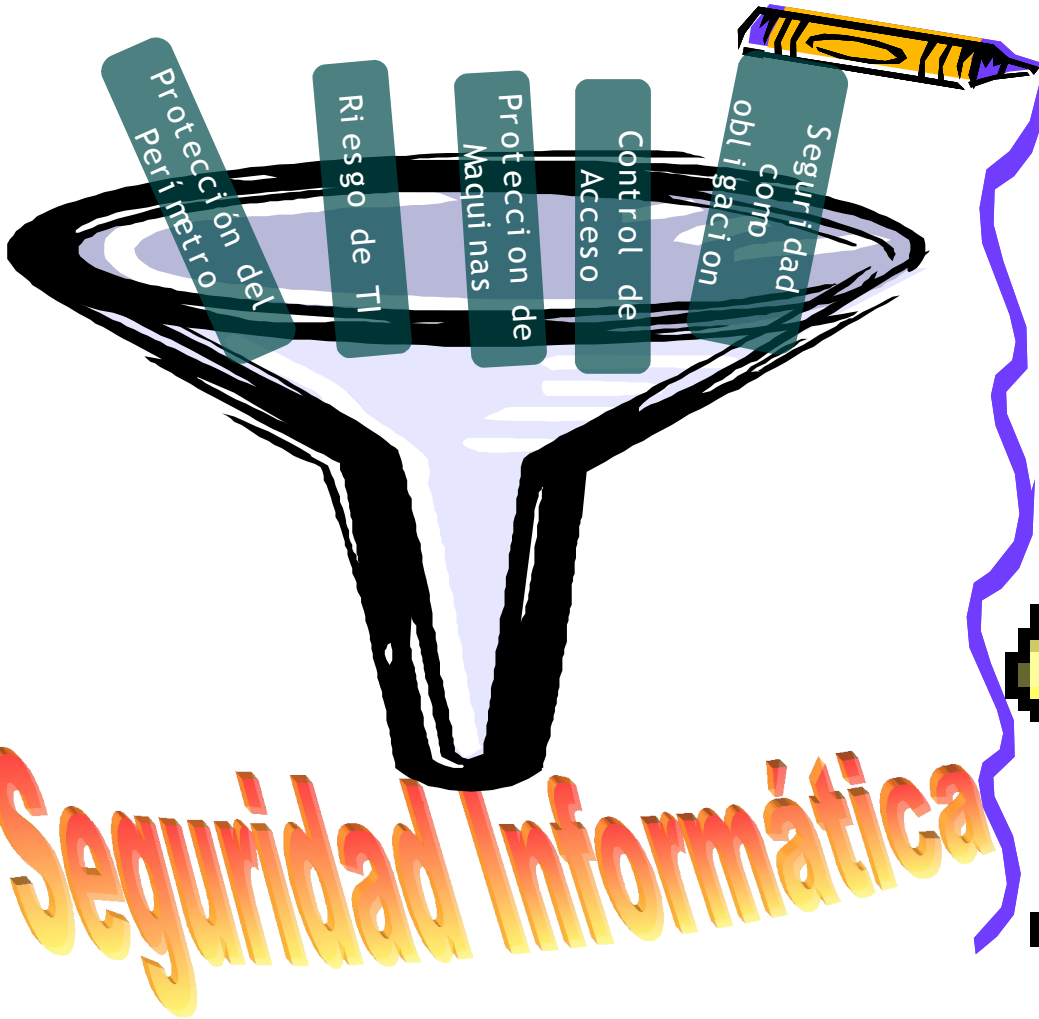


- ➔ Introducción
  - ➔ Consideraciones
- ➔ Definiciones Generales
  - ➔ Evolución de la seguridad
  - ➔ CISO, CSO, o Que...
  - ➔ Que Hace.....
- ➔ Donde esta en la organización?
  - ➔ Infraestructura corporativa
  - ➔ Modelo de trabajo
  - ➔ Enfoques de trabajo
- ➔ Realidad Local
- ➔ Retos y Conclusiones
- ➔ Referencias Bibliográficas

# Introducción



# Definiciones Generales



# Orquestador . . . . .

Hoy se habla de  
CI SO/CSO/ISO/OSI .

Hoy se ve un enfoque  
✓ Informática  
✓ Información



“..... Es el líder que posee las habilidades y destrezas necesarias para identificar, materializar, gestionar, acoplar y personalizar las necesidades en materia de seguridad y protección de la organización, buscando crear una postura de inseguridad adecuada. Para ello se valdrá de las herramientas, metodologías, y enfoques necesarios, para involucrar la seguridad y protección en la perspectiva del negocio.....”

# Rol y Responsabilidades



# Competencias

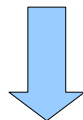
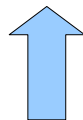


## Conductuales

- ✓ Habilidades de comunicación.
- ✓ Diplomacia y buenas relaciones
- ✓ Autonomía, disciplina
- ✓ Buen Juicio, motivación
- ✓ Integridad, honestidad, responsabilidad
- ✓ Fortalezas de un “nerd”, Instintos de un policía
- ✓ Vencer el paradigma de la “cima....”
- ✓ LIDERAZGO DE NIVEL MEDIO

de

Influenciar a la alta dirección

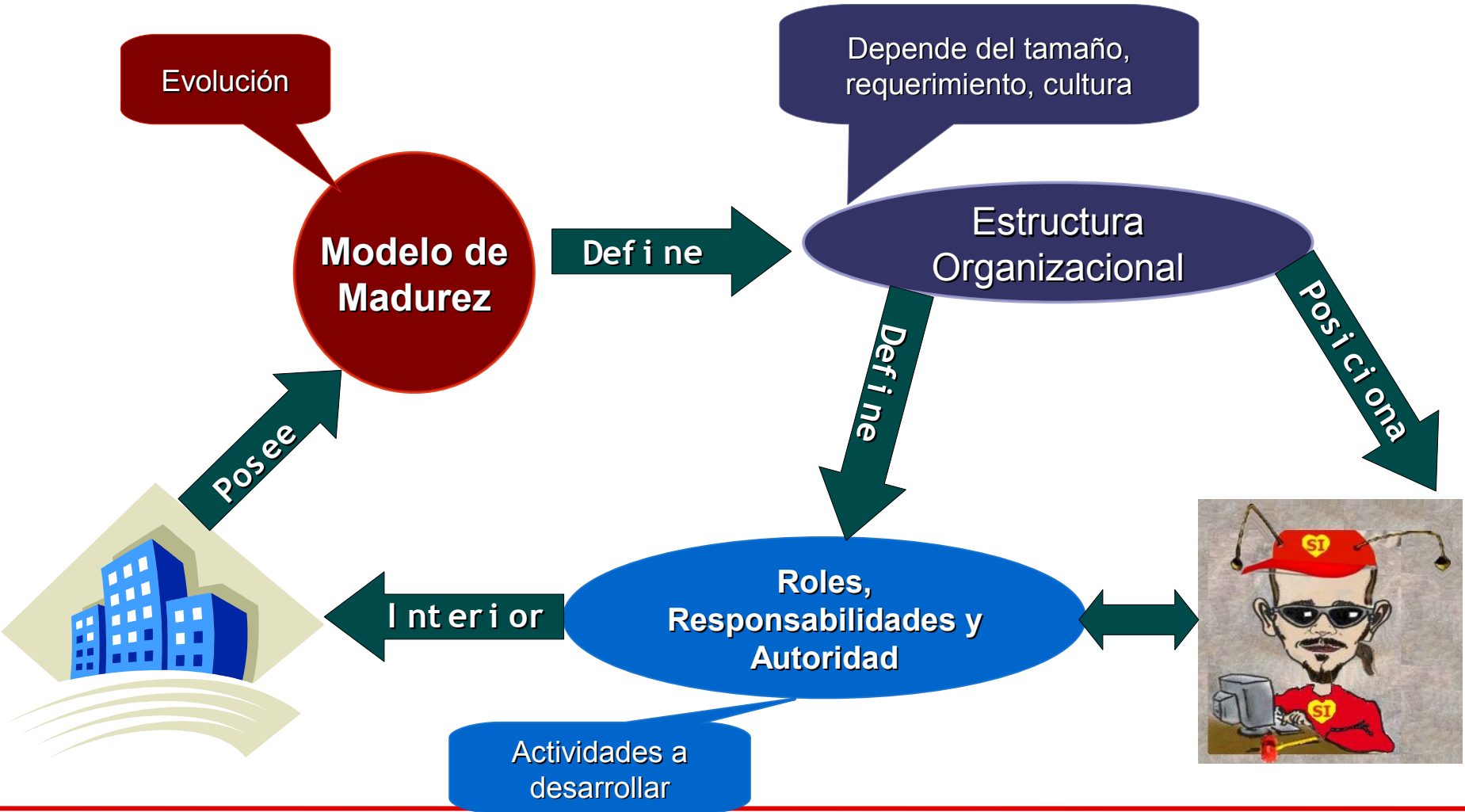


Interacción con Usuarios y áreas de TI

## Técnicas

- ✓ Formación y experiencia en SI
  - ✓ Gestión del riesgo
  - ✓ Seguridad en red
  - ✓ Normativas y estándares de seguridad
  - ✓ Experiencia (2 a 4 años)
  - ✓ Pruebas de intrusión
  - ✓ Pruebas de vulnerabilidad
  - ✓ Gestión de incidentes
  - ✓ Gestión de Proyectos

# Interrelaciones



# Donde está la empresa?



## Ignorancia Total

- ✓ Políticas desactualizadas
- ✓ Sin entrenamiento del personal
- ✓ Poca comunicación entre
  - ✓ Seguridad
  - ✓ Negocio
  - ✓ TI
- ✓ Convicción de que todo de por sí es seguro
- ✓ No se reportan las fallas de seguridad
- ✓ No existe gestión, ni medición
- ✓ Seguridad reactiva



# Donde está la empresa?



## Conciencia

- ✓ Iniciativas no continuas en conciencia de seguridad a la organización
- ✓ Iniciativa no completada de un equipo de seguridad
- ✓ Enfoque sobre la política y su revisión
- ✓ Creencia en que la política es lo único
- ✓ Fácil para volver a la ignorancia
- ✓ Desarrollo de las relaciones entre TI, negocio, y seguridad
- ✓ Desarrollo inicial de visión y misión de la seguridad en la organización



# Donde está la empresa?



## Funcional

- ✓ Programa estratégico de seguridad
- ✓ Orientación a procesos, en torno a:
  - ✓ Seguridad
  - ✓ Riesgos
  - ✓ Gobierno
- ✓ Necesidades de negocio embebidas en las políticas
- ✓ Inicio de mediciones y reportes
- ✓ Comunicaciones con la alta gerencia
- ✓ Diseño de la arquitectura de seguridad



# Donde está la empresa?



## Excelencia

- ✓ Cultura organizacional, involucra la seguridad
- ✓ Seguridad orientada a ser un servicio del negocio
- ✓ Mejoramiento continuo, basado en las mediciones, métricas, indicadores y metas
- ✓ Se entiende el riesgo corporativa
- ✓ Se acepta el riesgo residual
- ✓ Programa organizacional de seguridad, seguido por la alta dirección
- ✓ Mejoramiento continuo



# Donde está el responsable?



## Enfoque Técnico

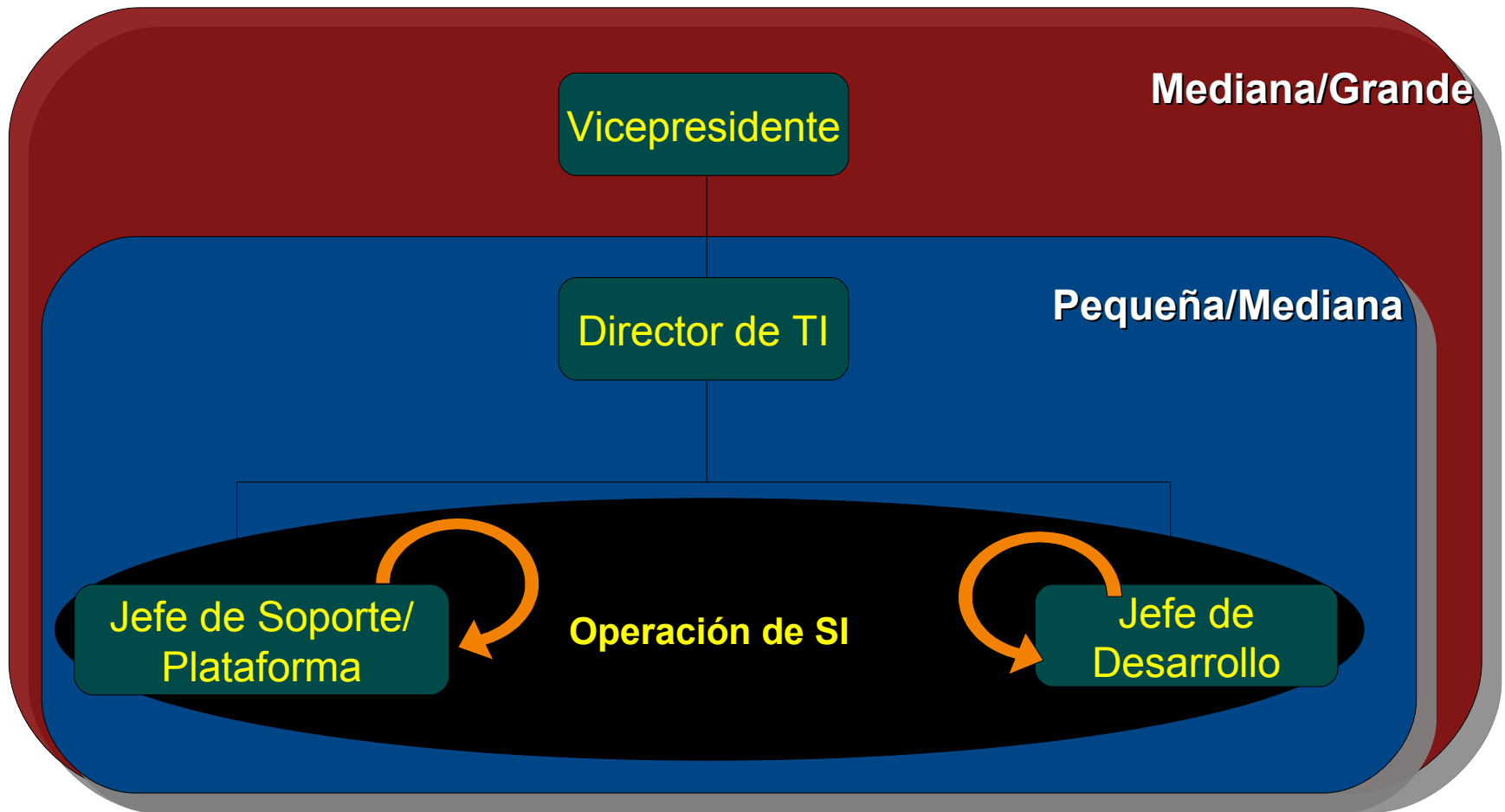
- ✓ No existe una función formal de seguridad
- ✓ Asumida por la operación de TI
- ✓ Reportes son realizados en áreas
  - ✓ Operacionales o TI
- ✓ Las labores están enfocadas en
  - ✓ Seguridad en la red
  - ✓ Seguridad en la operación
  - ✓



# Donde está el responsable?



## Enfoque Técnico



# Donde está el responsable?



## Enfoque Técnico

### Rol / Autoridad

- ✓ Rol netamente técnico
- ✓ Autoridad relegada, y aislada a sus funciones
- ✓ Poca influencia en toma de decisiones
- ✓ Se escucha solo cuando algo se tenga que cumplir



### Funciones

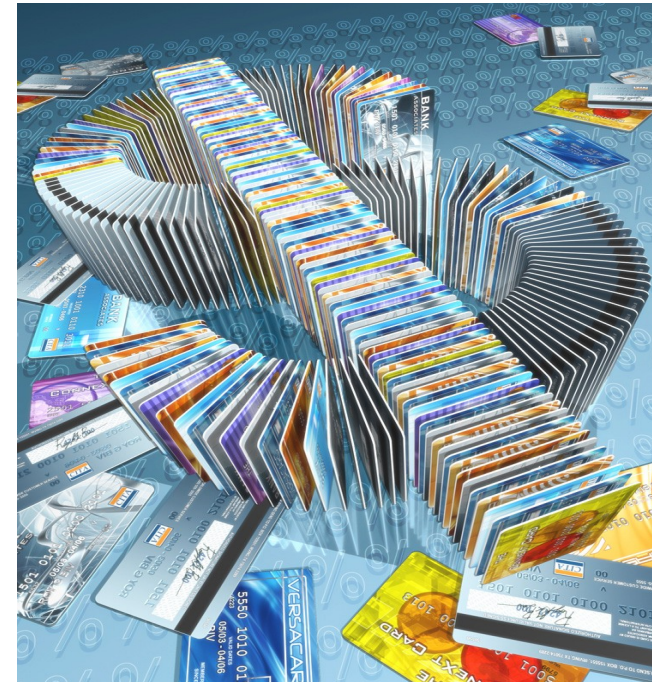
- ✓ Administración del firewall
- ✓ Control de acceso
- ✓ Pruebas de vulnerabilidad
- ✓ Monitoreo de red
- ✓ Servicios de red. Correo, Intranet.
- ✓ Instalación y configuración de servidores y servicios

# Donde está el responsable?



## Enfoque Técnico/Administración

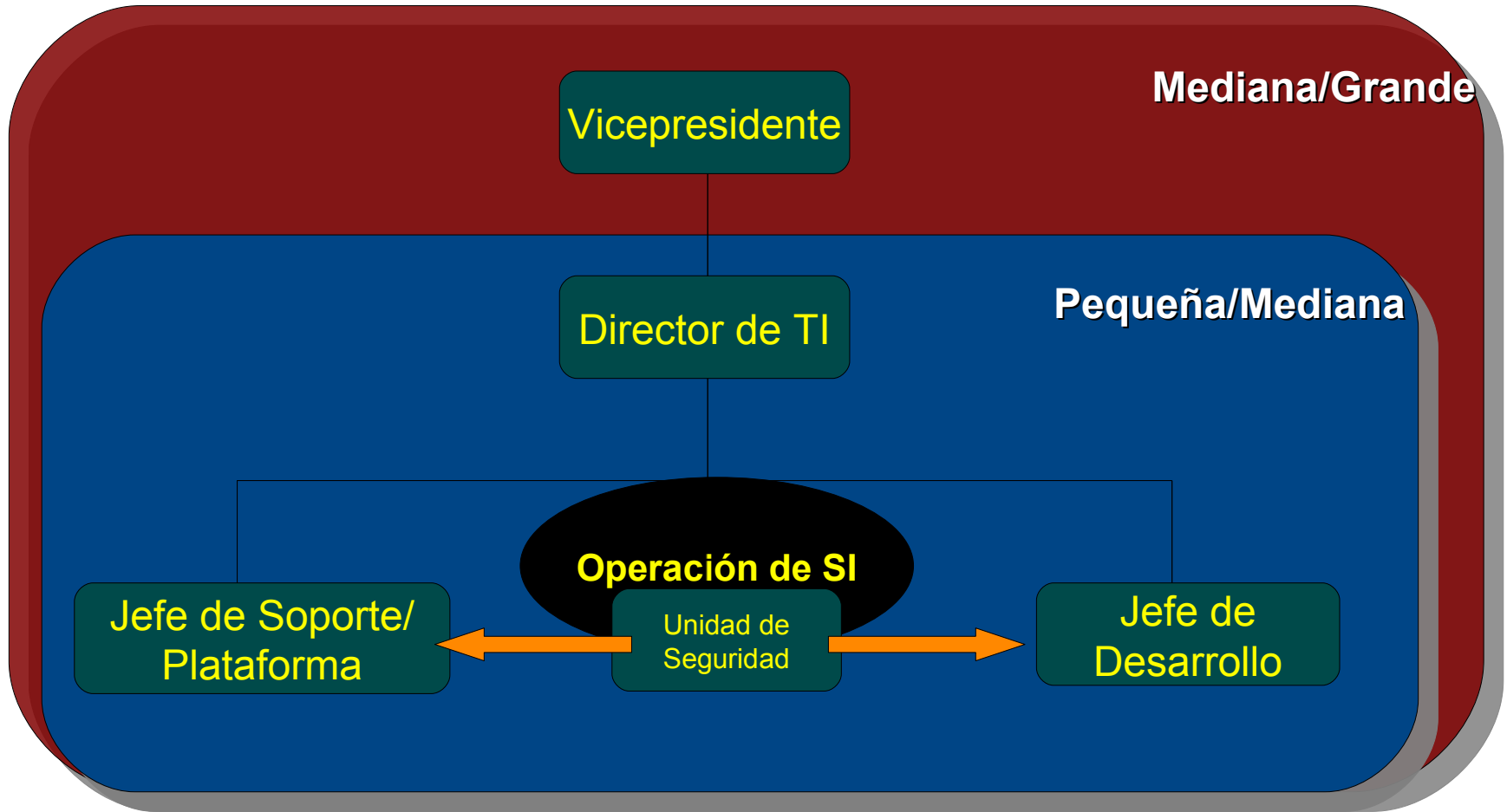
- ✓ Existe un responsable de seguridad
- ✓ Reportes son realizados en áreas
  - ✓ Operacionales o TI
- ✓ Las labores están enfocadas en
  - ✓ Seguridad operacional. Alto porcentaje
  - ✓ Gestión y Administración. Bajos porcentajes
  - ✓ Estrategia. Bajos porcentajes



# Donde está el responsable?



## Enfoque Técnico/Administración



# Donde está el responsable?



## Enfoque Técnico/Administración

### Rol / Autoridad

- ✓ Rol mixto técnico-gestión. (Coordinador)
- ✓ Autoridad mas visible,
- ✓ Poca influencia en toma de decisiones
- ✓ Se escucha en su interrelación con las áreas de su mismo nivel



### Funciones

- ✓ Definición de políticas estándares y procedimientos
- ✓ Seguridad en la infraestructura
  - ✓ Servidores
  - ✓ Parches
  - ✓ Malware
  - ✓ IDS/IPS/Firewall
- ✓ Gestión de riesgo de TI

# Donde está el responsable?



## Enfoque Administración

- ✓ Existe un responsable de seguridad
- ✓ Existe un equipo multidisciplinario responsable de la seguridad
- ✓ Administración de la infraestructura de seguridad
- ✓ Revisión de la seguridad desde un entorno corporativo
- ✓ Las responsabilidades de seguridad son dirigidas o supervisadas sobre las áreas



# Donde está el responsable?



# Donde está el responsable?



## Enfoque Administración

### Rol / Autoridad

- ✓ Rol enfocado a la gestión. (Asesoría)
- ✓ Autoridad mas visible,
- ✓ Interacción e influencia sobre otras áreas
- ✓ Influencia en toma de decisiones
- ✓ Comité consultor de seguridad.



### Funciones

- ✓ Definición de políticas estándares y procedimientos
- ✓ Gestión de riesgo de riesgo corporativo
- ✓ Gestion de incidentes
- ✓ Entrenamiento y concientización
- ✓ BCM/BCP
- ✓ Estandares de gestion de seguridad

# Donde está el responsable?



## Enfoque Gerencial

- ✓ Existe un responsable de seguridad
- ✓ Existe un equipo multidisciplinario responsable de la seguridad
- ✓ Crea un gobierno alrededor de la seguridad
- ✓ La cultura organizacional adopta la seguridad como suya
- ✓ La seguridad operacional es devuelta a los directos responsables
- ✓ Mediciones exactas y claras acerca de la seguridad

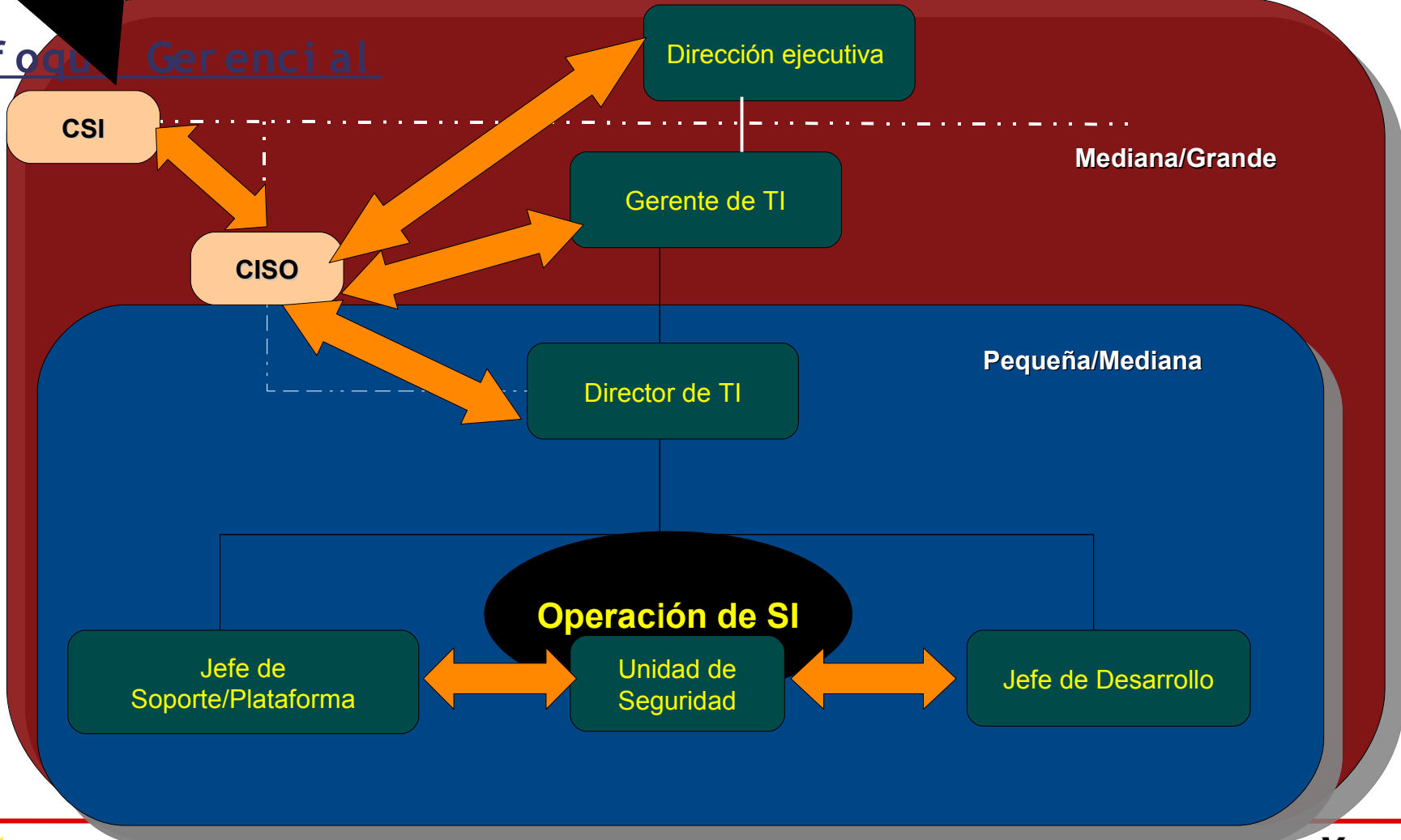


# el responsable?



Enfoque Gerencial

- Auditoria
- RRHH
- TI (Soporte/Desarrollo)
- Seguridad (Física/ Electronica)
- Juridica



# Donde está el responsable?



## Enfoque Gerencial

### Rol / Autoridad

- ✓ Rol enfocado a la gestión y gobierno. (Socio estratégico. Gerente)
- ✓ Autoridad y consultoría
- ✓ Interacción e influencia sobre otras áreas
- ✓ Orientación al negocio
- ✓ Comité consultor de seguridad.
- ✓ Interacción con entes externos



### Funciones

- ✓ Definición de políticas estándares y procedimientos
- ✓ Gestión de riesgo de riesgo corporativo
- ✓ BCM/BCP
- ✓ Métricas y mediciones
- ✓ Planeación estratégica de la seguridad
- ✓ Procesos de seguridad
- ✓ Cumplimiento de regulaciones y leyes



# Ventajas / Desventajas



Dentro de TI

Fuera de TI

Ventajas

- ✓ Iniciativas de cambio dentro de TI
- ✓ Fortalecimiento del Director / Gerente de TI.
- ✓ Conciencia de seguridad a los niveles jefes

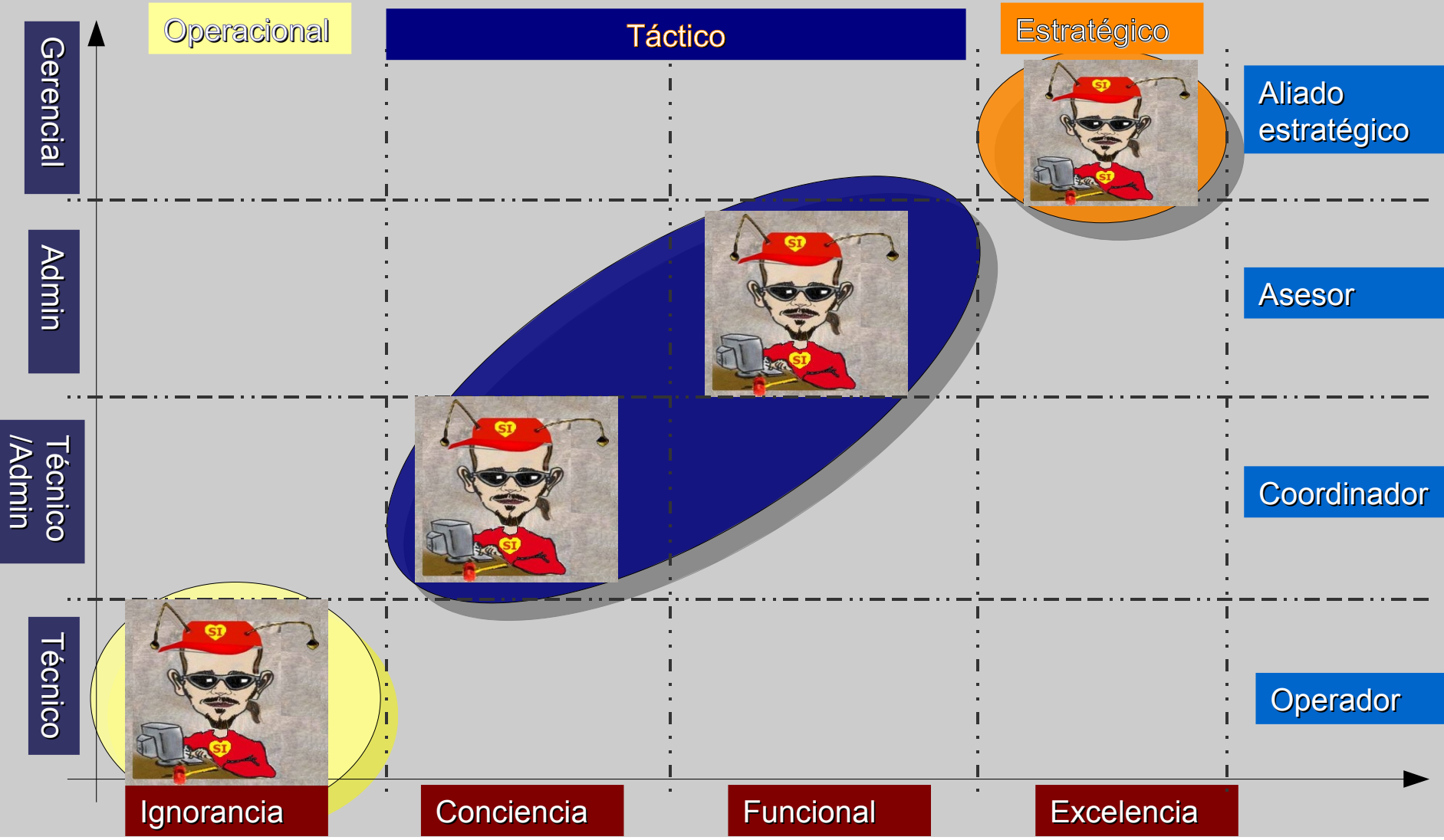
- ✓ Actividad de tiempo completo
- ✓ Mayor de nivel de autoridad y visibilidad
- ✓ Entrega de resultados a niveles de la alta dirección
- ✓ Equipo de trabajo ( A, SI, TI )

Desventajas

- ✓ Carga adicional a los niveles directivos de TI
- ✓ Conflictos de intereses entre seguridad y servicios de TI
- ✓ Seguridad se convierte en actividades de tiempo parcial.
- ✓ Afectada la imparcialidad en investigaciones en TI

- ✓ Choques de trenes entre TI y Seguridad
- ✓ Posibilidad de convertirse en prosa
- ✓ Poca profundidad en investigación
- ✓ Rendición de cuentas requiere de autoridad.

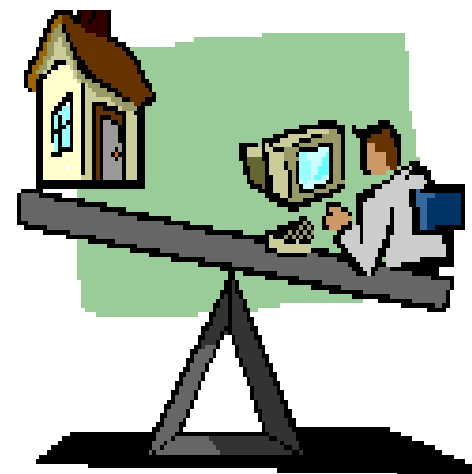
# Mezclando . . . .



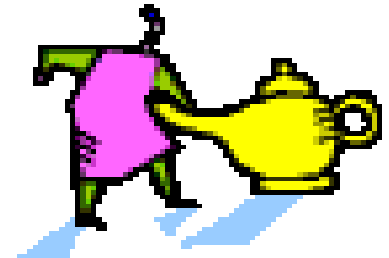
# Hábitos buenos ...



- ✓ Estructura moral y ética altamente desarrollada
- ✓ Ser diligente y ágil para la ejecución del trabajo
- ✓ Gestionar seguridad como un negocio
- ✓ Paciencia como virtud
- ✓ Hacer y hacer y hacer....
- ✓ Trabajo de la cultura organizacional entorno a la seguridad.
- ✓ Recopilación de datos y saber como



- ✓ Mito de la posición “..No se puede dirigir sino se esta en la cima..”
- ✓ Mito de la influencia. “...No se puede influir por no estar en la cima..”
- ✓ Superar el síndrome del todologo...
- ✓ No utilizar el factor MID, para vender sus ideas
- ✓ Enfoque autoritario, para justificar su trabajo.
- ✓ Pocas relaciones por ser de seguridad.

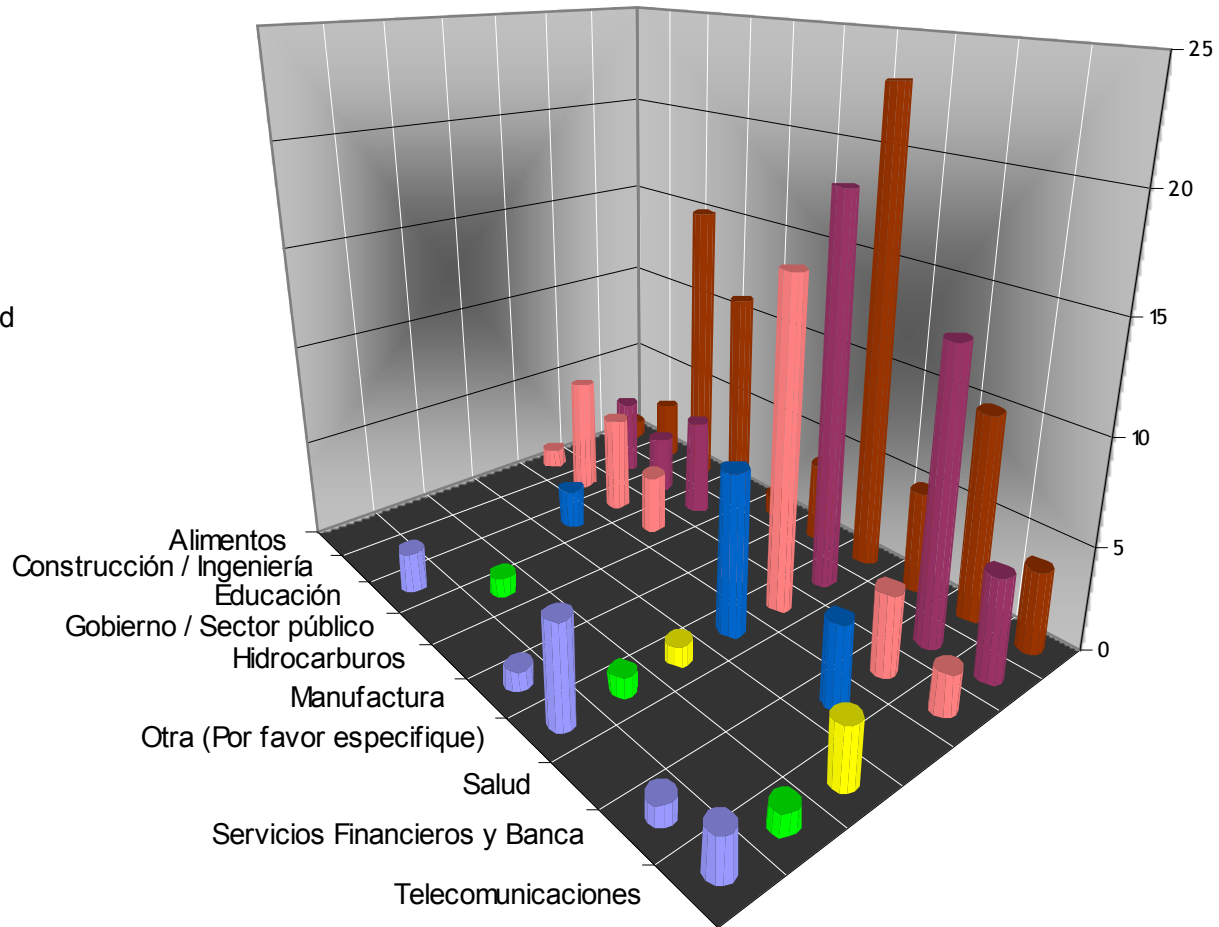


# Encuesta Nacional de Seguridad (Colombia-Mexico)



## Areas de Responsabilidad de la Seguridad

- Auditoria interna
- Gerente de Operaciones
- Gerente Ejecutivo
- Otra
- No especificado
- Director de Seguridad Informática
- Director de Sistemas



# Retos y Conclusiones



- ✓ Es necesario un responsable de seguridad por:
  - ✓ Ambientes complejos y con distintas variables
  - ✓ Cantidad de requerimientos de las partes interesadas que deben atenderse
  - ✓ Alguien debe gobernar, gestionar y dirigir
  - ✓ Debe garantizar la personalización de la seguridad de la información
- ✓ Su interacción con los elementos de la organización (alta dirección, usuarios, TI), lo define como una persona multifuncional que debe dominar los lenguajes de las partes interesadas.
- ✓ La seguridad de la información se ve en la actualidad como un elemento estratégico del negocio, que es manejado a través del proceso de la gestión del riesgo.

# Retos y Conclusiones



- ✓ Las organizaciones deben realizar un autodiagnostico que les permita determinar donde se encuentran y con ello su responsable en seguridad tendrá claro lo que la organización desea y hasta donde desea llegar
- ✓ Debe buscar definir su arquitectura de seguridad que como objetivo principal sea alinearse con el negocio. (Misión - Visión)
- ✓ Cada vez mas encontramos que los responsables de la seguridad de la información participan en las decisiones estratégicas de la organización y reportan a la gerencia
- ✓ El líder de la inseguridad en la organización, debe tener claro que su disciplina, constancia, y dedicación son las herramientas validas para dirigir el proceso.

# Retos y Conclusiones



- ✓ Su responsabilidad y sentido de compromiso y pasión por lo que hace son sometidos a prueba todo el tiempo.
- ✓ Tolerancia absoluta a la incertidumbre y las respuestas que no desean escuchar.
- ✓ Romper con las premisas, como la que dice "...debo estar en la cima para dirigir...."
- ✓ La diplomacia es una de las características mas importante que debe desarrollar nuestro responsable de seguridad en pro de la integración de las partes interesadas.



Gracias...

¿.....?

# Referencias Bibliográficas



- ✓ Chief Security Officer. Guideline (2004). ASIS International. URL. [www.asisonline.org/guidelines/guidelineschief.pdf](http://www.asisonline.org/guidelines/guidelineschief.pdf)
- ✓ JOHNSON M. ERIC, GOETZ ERIC . (2007) Embedding Information Security into the Organization. *Security & Privacy*. Pp 16-24.
- ✓ Jack McCoy. (2004) Are We Ready for a Chief Information Security Officer?. Disponible en: [www.unc.edu/cause05/presentations/mccoy/mccoy.ppt](http://www.unc.edu/cause05/presentations/mccoy/mccoy.ppt)
- ✓ Chief Information Security Officer. URL [http://en.wikipedia.org/wiki/Chief\\_information\\_security\\_officer](http://en.wikipedia.org/wiki/Chief_information_security_officer).
- ✓ Chief Information Security Officer. URL <http://www.chiefinformationsecurityofficer.com/>
- ✓ ¿Qué tipo de CISO ser?. URL [http://www.bsecure.com.mx/articulos.php?id\\_sec=59&id\\_art=6561](http://www.bsecure.com.mx/articulos.php?id_sec=59&id_art=6561)
- ✓ The Changing Role Of The CISO?. URL [http://www.informationweek.com/blog/main/archives/2008/02/the\\_changing\\_ro.html](http://www.informationweek.com/blog/main/archives/2008/02/the_changing_ro.html)
- ✓ Quien es el líder de la inseguridad informática?. URL. [http://www.eltiempo.com/participacion/blogs/default/un\\_articulo.php?id\\_blog=3516456&id\\_](http://www.eltiempo.com/participacion/blogs/default/un_articulo.php?id_blog=3516456&id_)
- ✓ A Current View of the State CISO: A National Survey Assessment” NASCIO, September 2006. URL. <http://www.nascio.org/publications/documents/NASCIO-CISOsurveyReport.pdf>

# Referencias Bibliográficas



- ✓Wyl der J. (2004) *Strategic Information Security*. Addison Wesley. John Wyl der
- ✓Kovacich G. (2003) *The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program, Second Edition*. Butterworth Heinemann
- ✓The Global State of Information Security - 2007. PwC, September 2007
- ✓El rol del CISO: Chief Information Security Officer. URL.  
<http://criadoindomable.wordpress.com/2007/11/14/el-rol-del-ciso-chief-information-security>
- ✓ 10 principales razones por las cuales el CISO renunciará en el 2008 . URL.  
[http://cxo-community.com.ar/index.php?option=com\\_content&task=view&id=229&Itemid=30](http://cxo-community.com.ar/index.php?option=com_content&task=view&id=229&Itemid=30)
- ✓What is a Chief Security Officer?. URL. <http://www.csoonline.com/article/print/221739>
- ✓Chief Information Security Officer. URL  
[http://en.wikipedia.org/wiki/Chief\\_information\\_security\\_officer](http://en.wikipedia.org/wiki/Chief_information_security_officer).
- ✓Chief Information Security Officer. URL  
<http://www.chiefinformationsecurityofficer.com/>
- ✓¿Qué tipo de CISO ser?. URL  
[http://www.bsecure.com.mx/articulos.php?id\\_sec=59&id\\_art=6561](http://www.bsecure.com.mx/articulos.php?id_sec=59&id_art=6561)
- ✓The Changing Role Of The CISO?. URL  
[http://www.informationweek.com/blog/main/archives/2008/02/the\\_changing\\_ro.html](http://www.informationweek.com/blog/main/archives/2008/02/the_changing_ro.html)

# Referencias Bibliográficas



- ✓ Are We Ready for a Chief Information Security Officer. Jack McCoy. URL. [www.unc.edu/cause05/presentations/mccoy/mccoy.ppt](http://www.unc.edu/cause05/presentations/mccoy/mccoy.ppt)
- ✓ Gartner (2005, September 15). *Gartner highlights the evolving role of CISO in the new security order*. Retrieved November 2, 2005 from the Gartner Web site [http://www.gartner.com/press\\_releases/asset\\_135714\\_11.html](http://www.gartner.com/press_releases/asset_135714_11.html)
- ✓ Germain, J. (2005, October 13). *Your next job title: CISO?* Retrieved November 2, 2005 from the Newsfactor Magazine Web site [http://www.ci-o-today.com/story.xhtml?story\\_title=Your\\_Next\\_Job\\_Title\\_\\_CISO\\_&story\\_id=38](http://www.ci-o-today.com/story.xhtml?story_title=Your_Next_Job_Title__CISO_&story_id=38)
- ✓ Kobus, W. S. (2005, November 1). *Security management*. Presented at the ISSA Triangle InfoSeCon conference on November 1, 2005 in Cary, NC. URL. <http://www.tess-llc.com/Security%20Management.pdf>
- ✓ Hawkins, B. L., Rudy, J. A., & Nicolich, R. (2004). *EDUCAUSE core data report: 2004 summary report*. Retrieved November 2, 2005 from the EDUCAUSE Web site <http://www.educause.edu/ir/library/pdf/pub8002.pdf>
- ✓ Boni, W. (2005, April 5). *The role of the CSO: An industry perspective*. Presented at the EDUCAUSE Security Professionals Conference 2005. Washington, DC. Retrieved November 2, 2005 from the EDUCAUSE Web site. <http://www.educause.edu/LibraryDetailPage/666?ID=SPC0528>

