

Oficial de Seguridad Información : Coordinador de la gestión

Oh... y ahora quien
podrá ayudarnos...

- ✓ 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 gestionar

Propósitos

- ➔ Introducción
 - ➔ Consideraciones y estadísticas
- ➔ Definiciones Generales
 - ➔ Evolución de la seguridad
 - ➔ CISO, CSO, o Que...
 - ➔ Que Hace.....
- ➔ Utópico Esta en la organización
 - ➔ Infraestructura corporativa
 - ➔ Modelo de trabajo
 - ➔ Enfoques de trabajo
- ➔ Retos y Conclusiones
- ➔ Referencias Bibliográficas

Altos volúmenes de información

Grandes retos para proteger la información

Regulaciones, leyes

Mayores interrelaciones entre procesos, tecnología y gente

Personalización y apropiación de la seguridad

Interrelaciones entre visual de negocio y riesgo

Múltiples fuentes de amenazas (Internas, Externas)

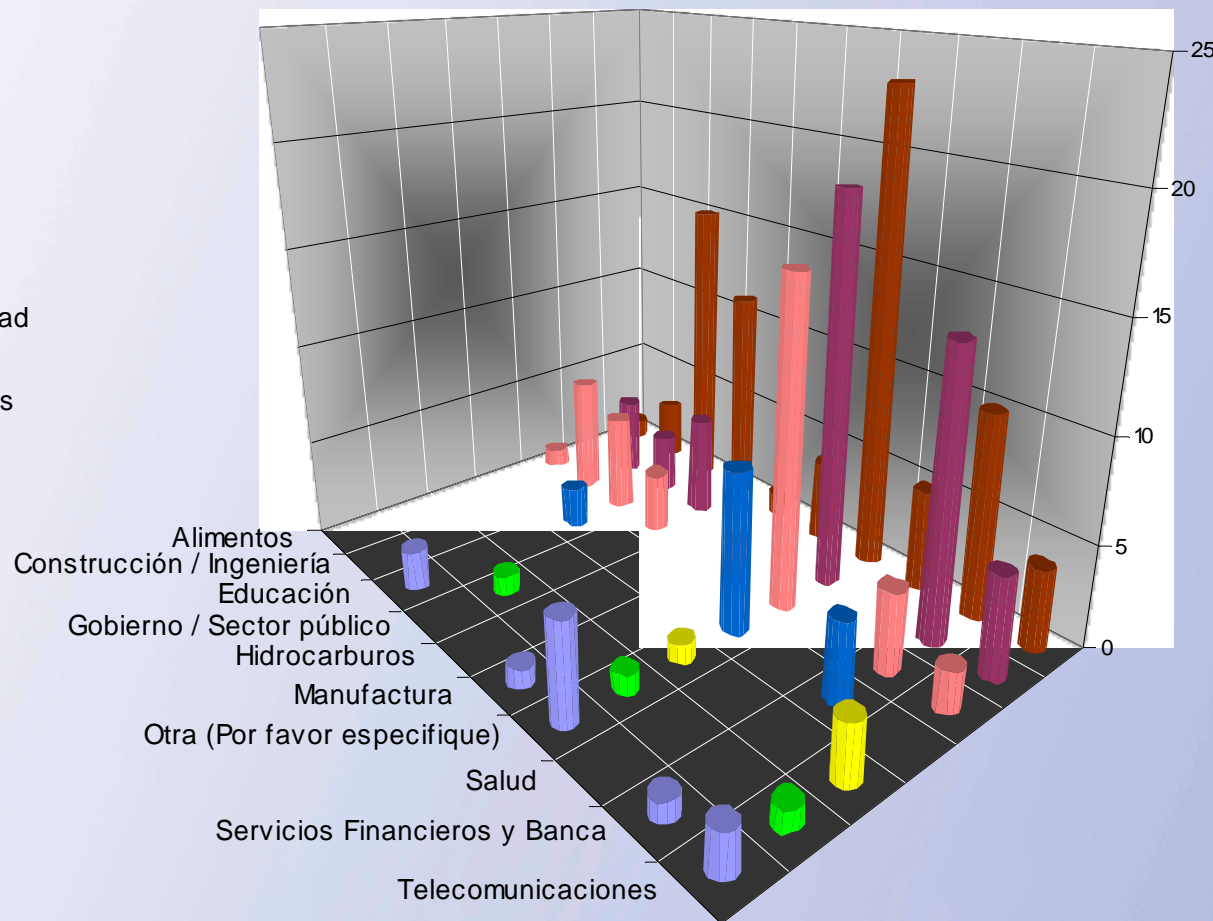
Introducción

VIII Jornada Nacional de Seguridad Informática



Áreas de Responsabilidad de la Seguridad

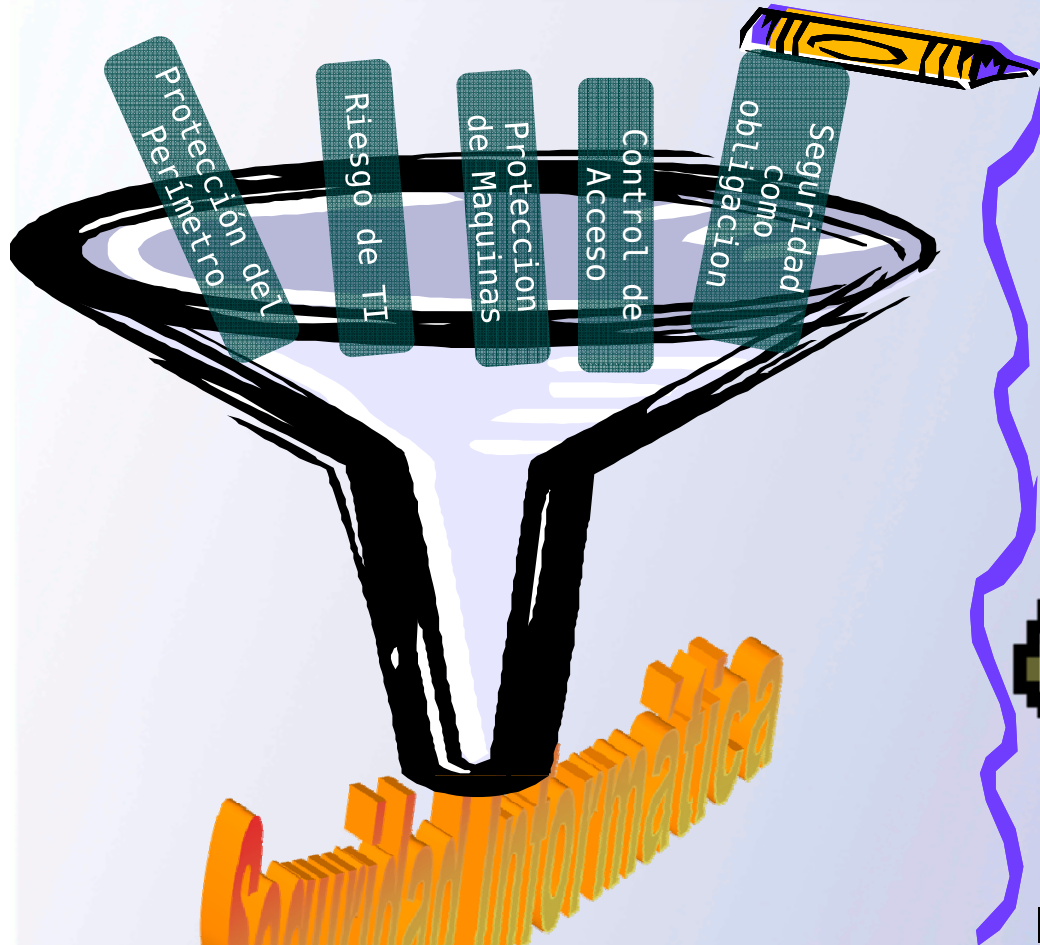
- Auditoria interna
- Gerente de Operaciones
- Gerente Ejecutivo
- Otra
- No especificado
- Director de Seguridad Informática
- Director de Sistemas



Introducción

Andrés R. Almanza, Ms(c)
andres_almanza@hotmail.com

VIII Jornada Nacional de Seguridad Informática



Seguridad Informática

Definiciones Generales

VIII Jornada Nacional de Seguridad Informática



Hoy se habla de
CISO/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.....”

Orquestador

Andrés R. Almanza, Ms(c)
andres_almanza@hotmail.com

VIII Jornada Nacional de Seguridad Informática



Gobierno



Gestión

Ejecución

Estratégico

Táctico

Operativo

Roles

Responsabilidades

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

Influenciar a la alta dirección

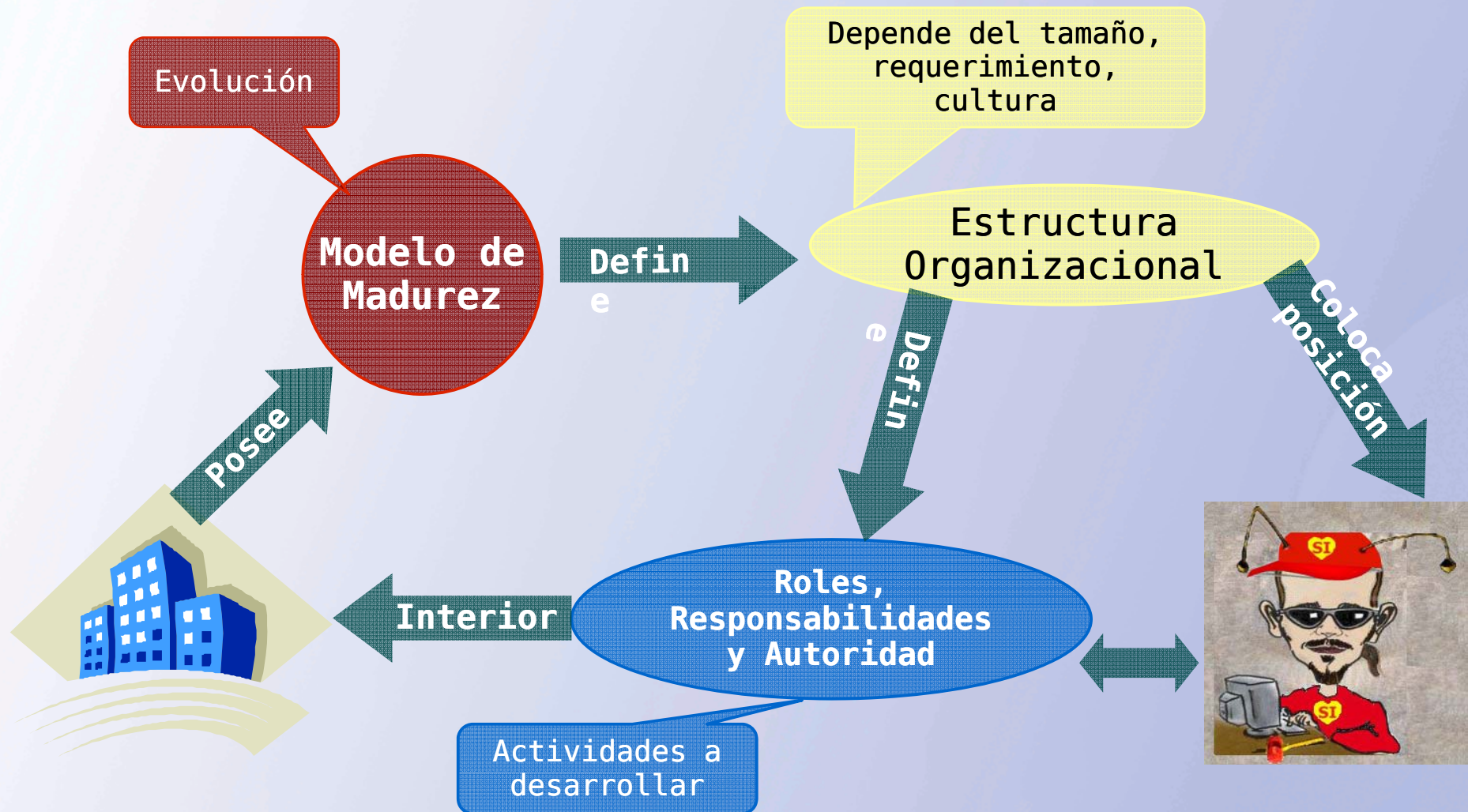


Interacción con Usuarios y áreas de TI

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

Competencias



Interrelaciones

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



Donde está la empresa?

Excelencia

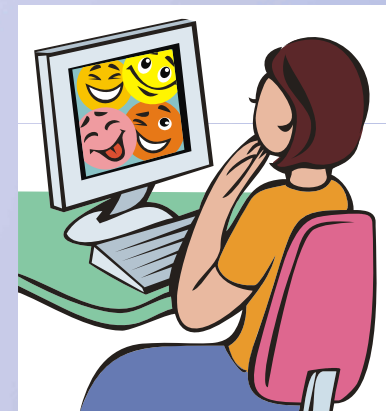
- ✓ Cultura organizacional, involucra la seguridad
- ✓ Seguridad orientada a ser un servicio del negocio
- ✓ Mejoramiento continuo, basado en las mediciones, métricas, indicadores y metas
- ✓ Se entiende el riesgo corporativa
- ✓ Se acepta el riesgo residual
- ✓ Programa organizacional de seguridad,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



Donde está la empresa?

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
 - ✓ Seguridad en el desarrollo



Donde está el responsable?

Andrés R. Almanza, Ms(c)
andres_almanza@hotmail.com

Enfoque Técnico



Donde está el responsable?

Enfoque Técnico

RoI/ 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



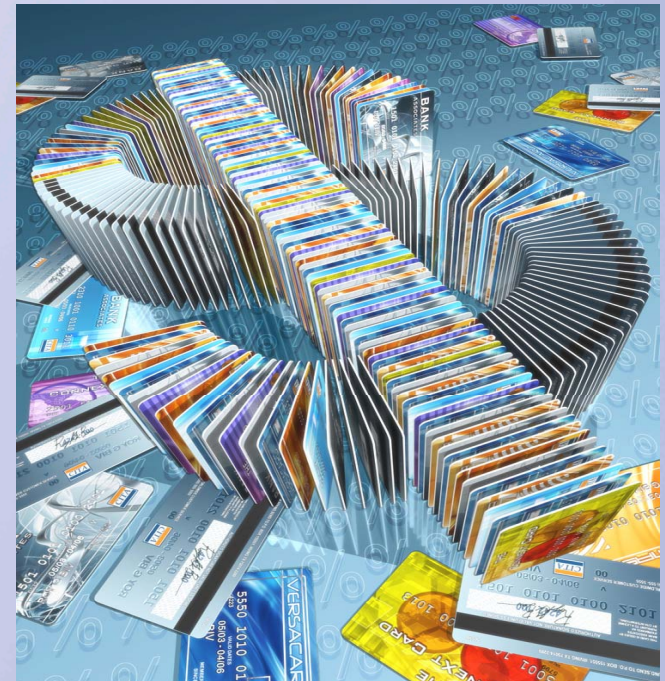
Funciones

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

RoI, Autoridad, Funciones

Enfoque Técnico/Administración

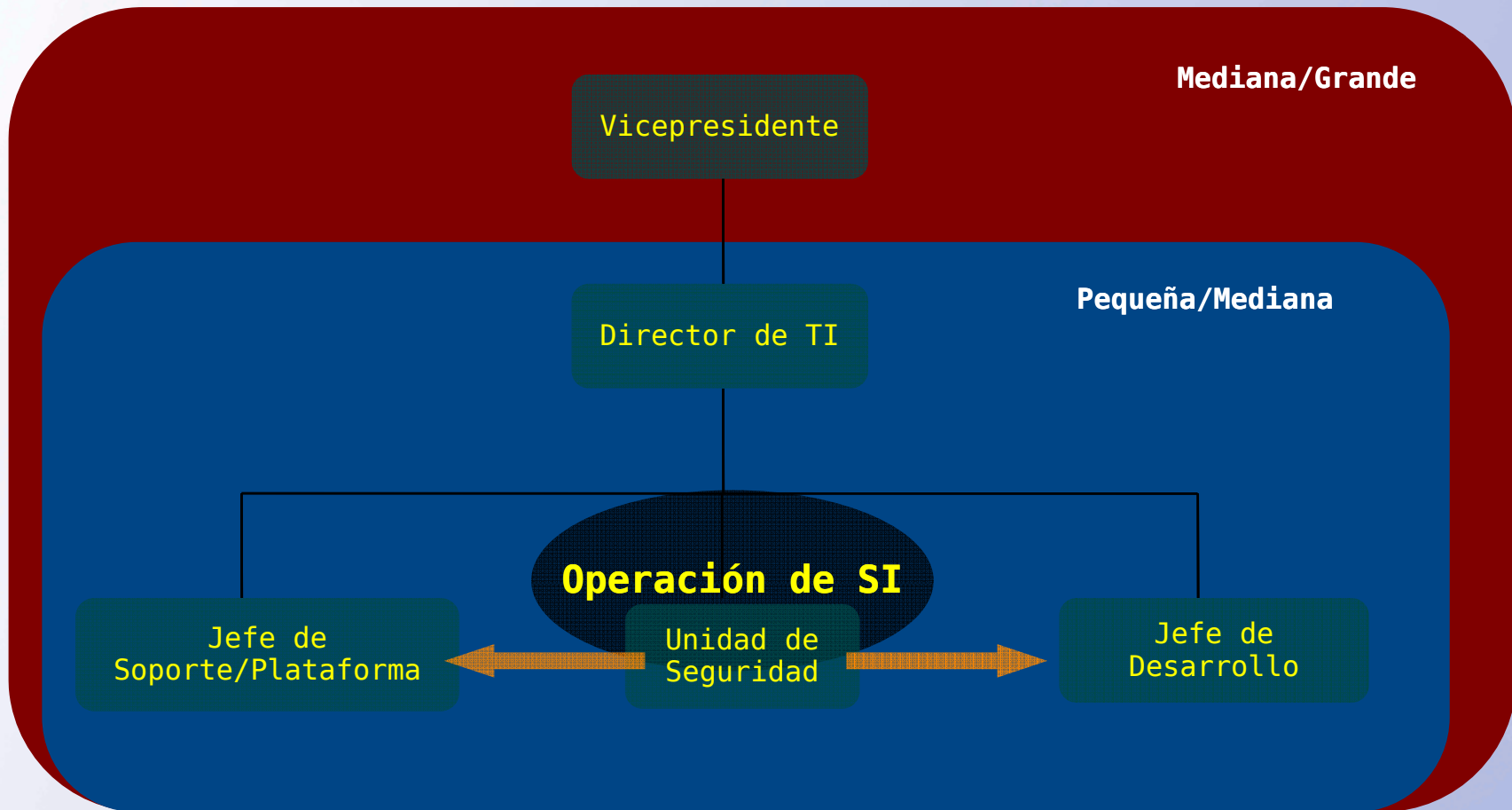
- ✓ Existe un responsable de seguridad
- ✓ Reportes son realizados en áreas
 - ✓ Operacionales o TI
- ✓ Las labores están enfocadas en
 - ✓ Seguridad operacional. Alto porcentaje
 - ✓ Gestión y Administración. Bajos porcentajes
 - ✓ Estrategia. Bajos porcentajes



Donde está el responsable?

Andrés R. Almanza, Ms(c)
andres_almanza@hotmail.com

Enfoque Técnico/Administración



Donde está el responsable?

Enfoque Técnico/Administración

RoI/ Autoridad

- ✓ Rol mixto técnico-gestión
- ✓ 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

- ✓ 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
- ✓ 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
- ✓ Romper con las premisas, como la que dice "...debo estar en la cima para dirigir...."
- ✓ 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.

Retos y Conclusiones

- ✓ Su responsabilidad y sentido de compromiso y pasión por lo que hacen son sometidos a prueba todo el tiempo.
- ✓ Tolerancia absoluta a la incertidumbre y las respuestas que no desean escuchar.
- ✓ 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.

Retos y Conclusiones

VIII Jornada Nacional de Seguridad Informática



✓ Chief Security Officer. Guideline (2004). ASIS International. URL. 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?](http://www.unc.edu/cause05/presentations/mccoy/mccoy.ppt). Disponible en: www.unc.edu/cause05/presentations/mccoy/mccoy.ppt

✓ Chief Information Security Officer. URL http://en.wikipedia.org/wiki/Chief_information_security_officer.

✓ Chief Information Security Officer. URL <http://www.chiefinformationsecurityofficer.com/>

✓ [¿Qué tipo de CISO ser?](http://www.bsecure.com.mx/articulos.php?id_sec=59&id_art=6561). URL

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

✓ Quien es el líder de la inseguridad informática?. URL.

http://www.eltiempo.com/participacion/blogs/default/un_articulo.php?id_blog=3516456&id_recurso=450008547&random=688

✓ "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 Bibliograficas

Andrés R. Almanza, Ms(c)
andres_almanza@hotmail.com

VIII Jornada Nacional de Seguridad Informática



- ✓Wyllder J. (2004) *Strategic Information Security*. Addison Wesley. John Wyllder
- ✓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-officer/>
- ✓ 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
- ✓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.
- ✓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
- ✓The Changing Role Of The CISO?. URL
http://www.informationweek.com/blog/main/archives/2008/02/the_changing_ro.html

Referencias Bibliograficas

Andrés R. Almanza, Ms(c)
andres_almanza@hotmail.com

VIII Jornada Nacional de Seguridad Informática



- ✓Are We Ready for a Chief Information Security Officer. Jack McCoy. URL. 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
- ✓Germain, J. (2005, October 13). *Your next job title: CISO?* Retrieved November 2, 2005 from the Newsfactor Magazine Web site http://www.cio-today.com/story.xhtml?story_title=Your_Next_Job_Title_CISO_&story_id=38430
- ✓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/pub0002.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>

Referencias Bibliograficas

Andrés R. Almanza, Ms(c)
andres_almanza@hotmail.com