



Vulnerabilidades en mi Red



Luis Pico

Security Systems Engineer

lpico@cisco.com





Agenda

- Retos
- Lugares en la Red
- Medidas de Control
- Conclusiones
- Aclaraciones



Retos





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

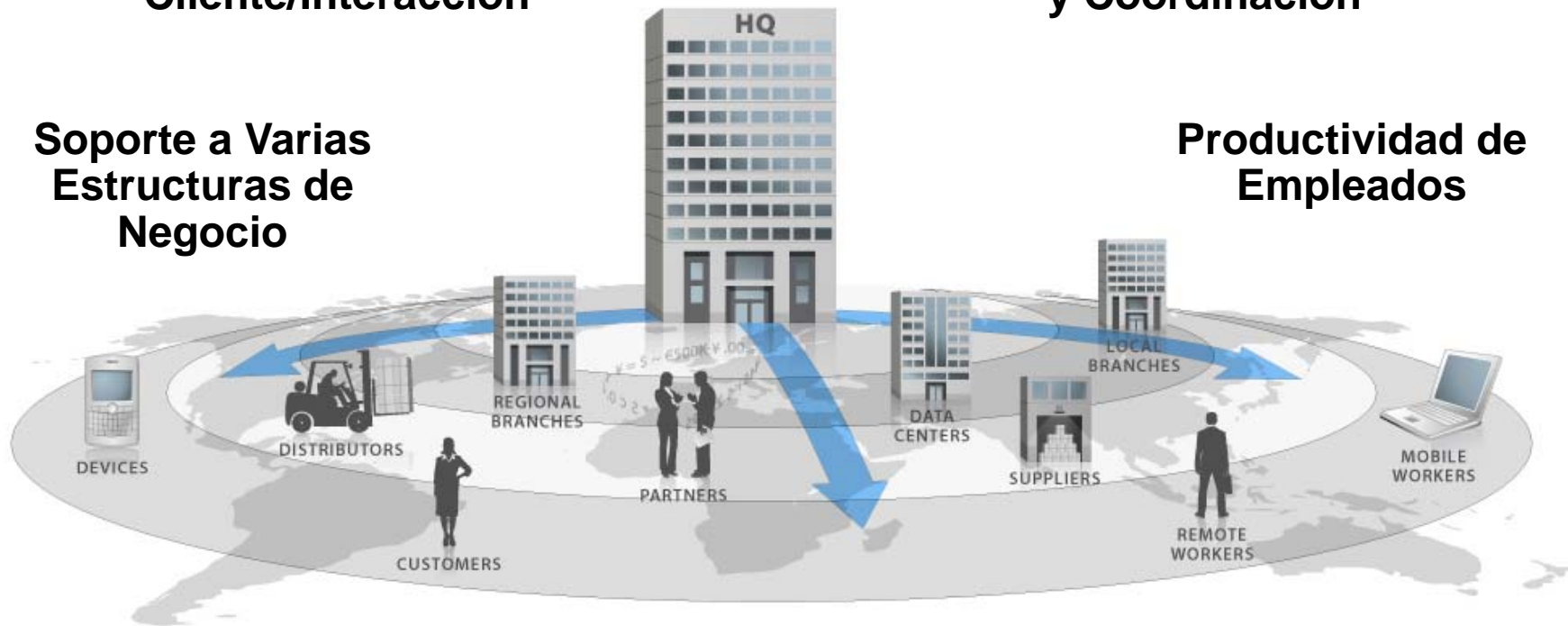
Modelos de Negocio en Constante Cambio

**Mejoramiento Servicio al
Cliente/Interacción**

**Proveer Colaboración
y Coordinación**

**Soporte a Varias
Estructuras de
Negocio**

**Productividad de
Empleados**



**Foco en el Nucleo
del Negocio**

**Mejores Desiciones
de Negocio**





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

La Empresa Competitiva Afronta Muchos Retos

Medidas contra el Riesgo

**Cumplir con multiples
requerimientos de
Cumplimiento**

**Partner / Proveedor de Seguridad
Diligente**

Vigilancia, Visibilidad y Gestión

**Tratamiento a los registros de
Seguridad**

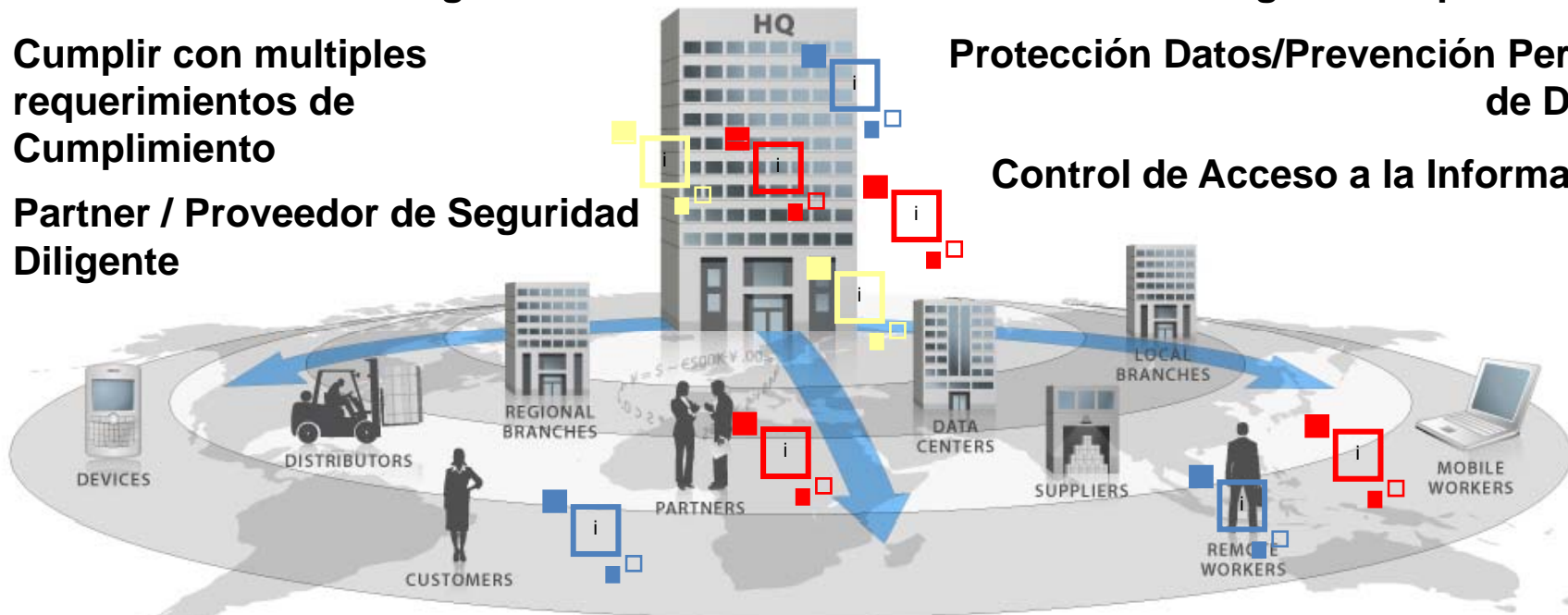
Seguridad Aplicaciones

**Protección Datos/Prevención Perdida
de Datos**

Control de Acceso a la Información

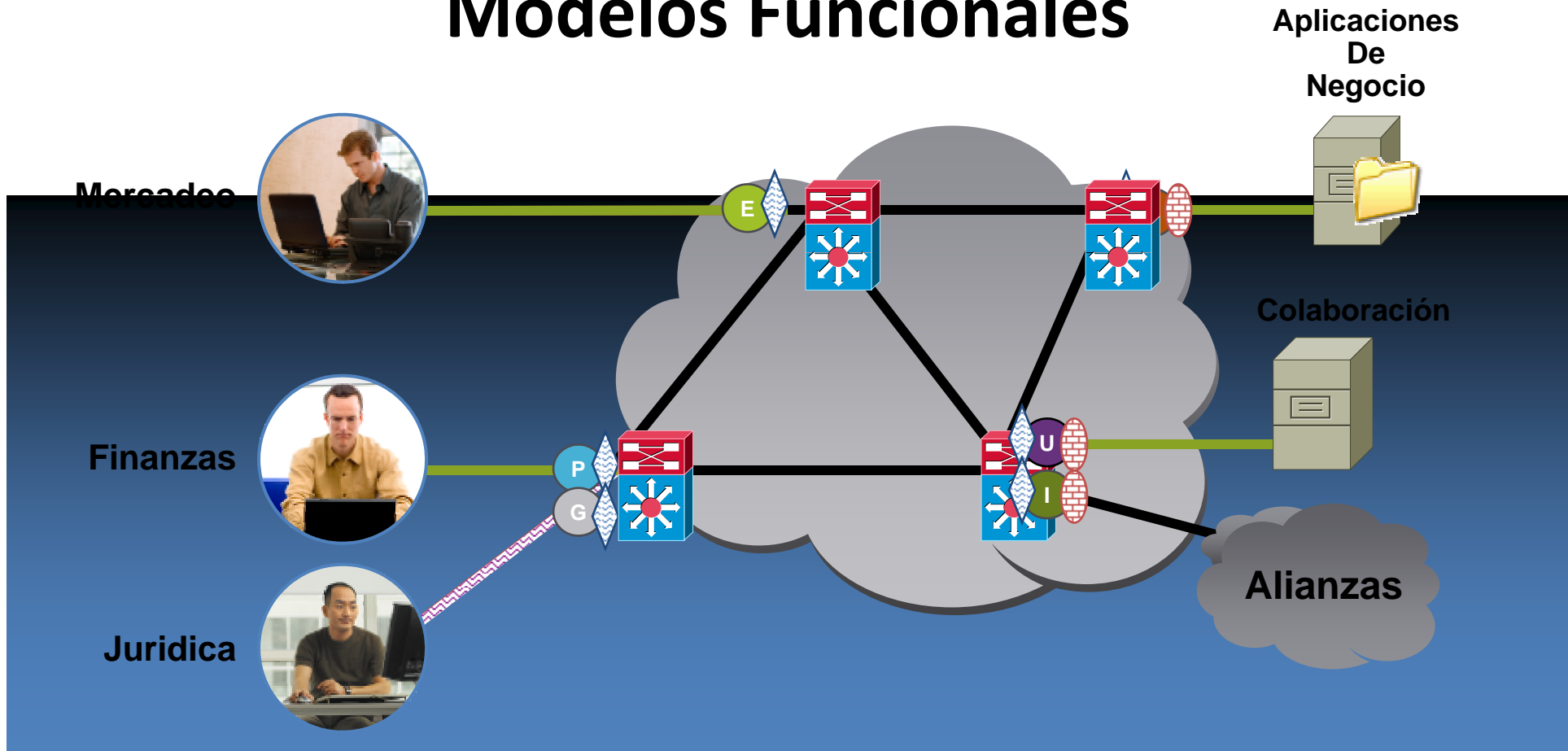
Continuidad del Negocio

Consumidor / Movilidad Empleadp





Modelos Funcionales



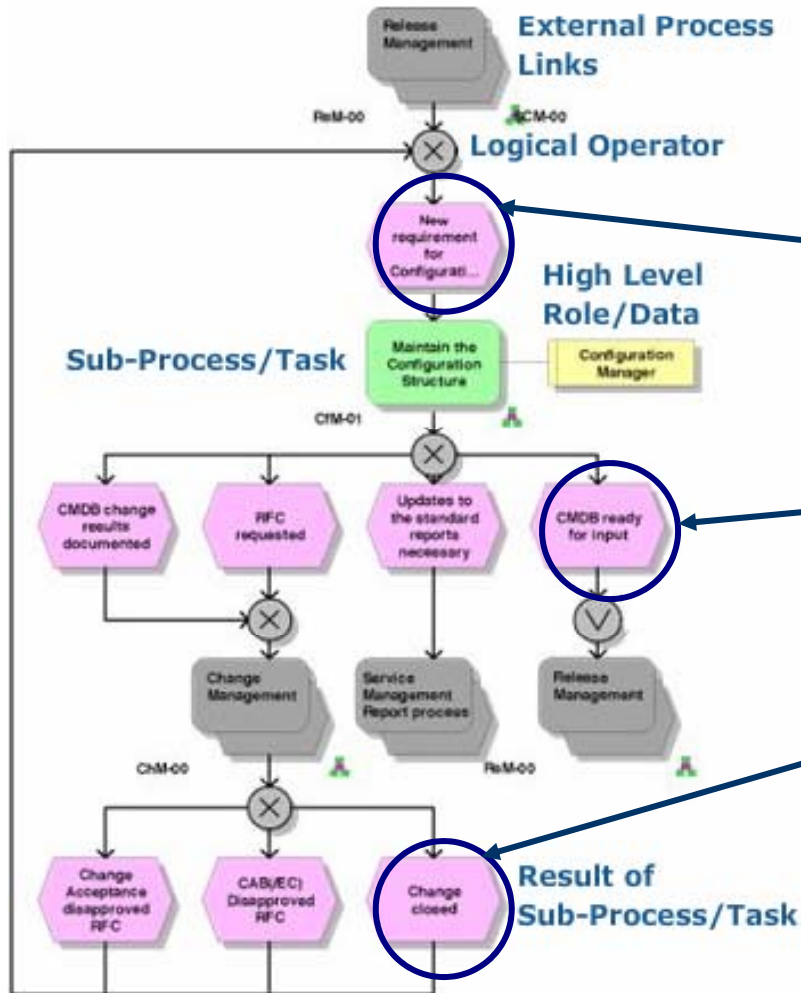
Modelos funcionales que al ser divididos en capas funcionales y bloques administrables/granulares, debe operar y ser controlado mediante la designación de un rol específico en la red.





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

Procesos de Negocio



Proceso TIC





Retos

eltiempo.com / colombia / justicia

Piratas informáticos ib millones de las gobern
Meta

eltiempo.com / colombia / justicia

Capturan a funcionaria del Ministerio de Defensa por robo de información

Pirata in internet



TECNOLOGÍA

El ciber-acoso, el robo de información principales delitos en internet: Policía

Caracol | Mayo 17 de 2009

Vote: ☆☆☆☆☆ Promedio: ☆☆☆☆☆ 0 votos

El mayor Freddy Bautista, jefe de la Unidad de Delitos Armada y la FAC. ciber-acoso es uno de los delitos más comunes, sobretodo en los menores de edad.



Foto: Néstor Gómez / EL TIEMPO

Sandra Milena Méndez fue capturada el miércoles por la Dijin.

La información contenía detalles de los sueldos, préstamos y otros datos privados de un número indeterminado de empleados del Ministerio de Defensa y miembros del Ejército, la



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

Retos



“Codigo Maligno en constante cambio”





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

Retos



“El intruso cada día es más difícil de identificar”





Necesidad de una Inspección Profunda

Es Difícil juzgar con solo una Foto o una Impresión

**Analisis inicial –
Se Observa Bien**

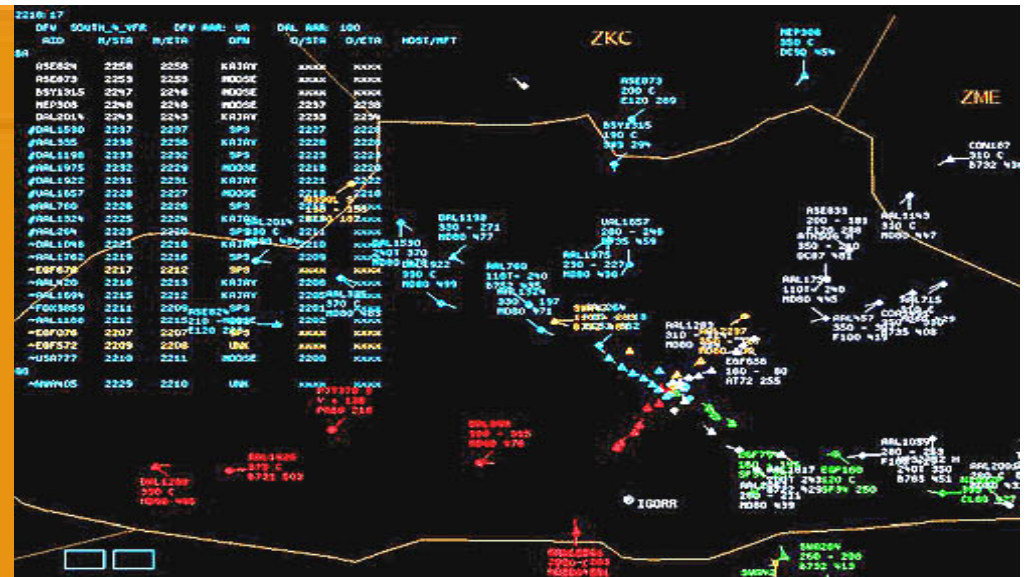




IX JORNADA de SEGURIDAD de INFORMÁTICA

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

Lugares en la Red





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

Perímetro de Red

Define las fronteras de los
lugares en la red.





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

Amenazas Plataforma de Red

- Software Malicioso
- Fuga de Información
- Daño
- Acceso no autorizado
- Correo Basura



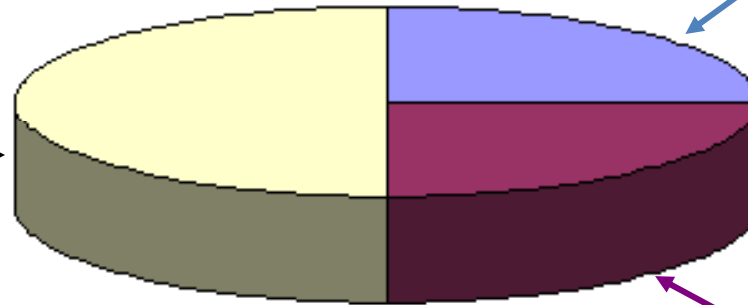
- Terrorismo
- Terremotos
- Inundación
- Infiltración
- Penetración



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

Fraude Empresarial

50% de los
empleados son
honestos de
acuerdo a los
controles



25% de los
empleados son
honestos

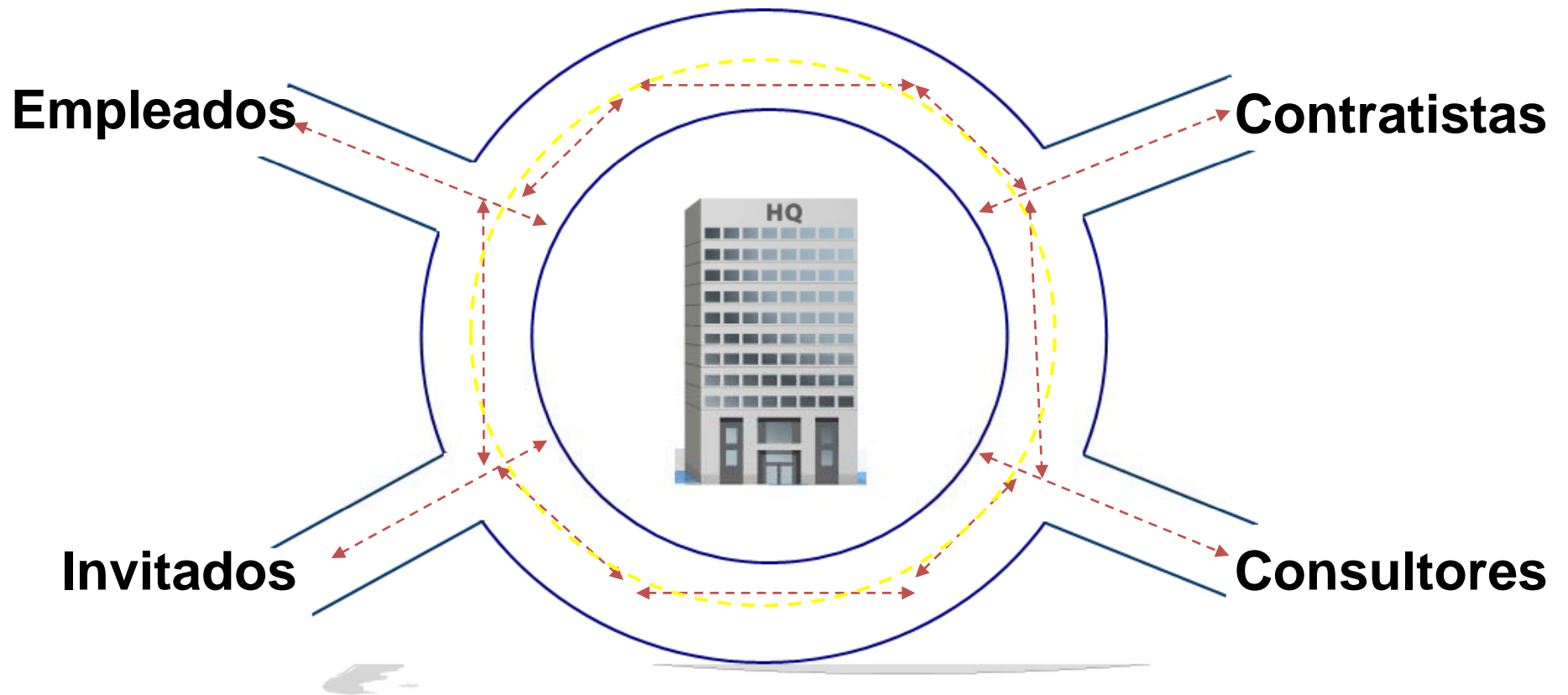
25% de los
empleados son
deshonestos

El fraude en la empresa.
Michael Comer



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

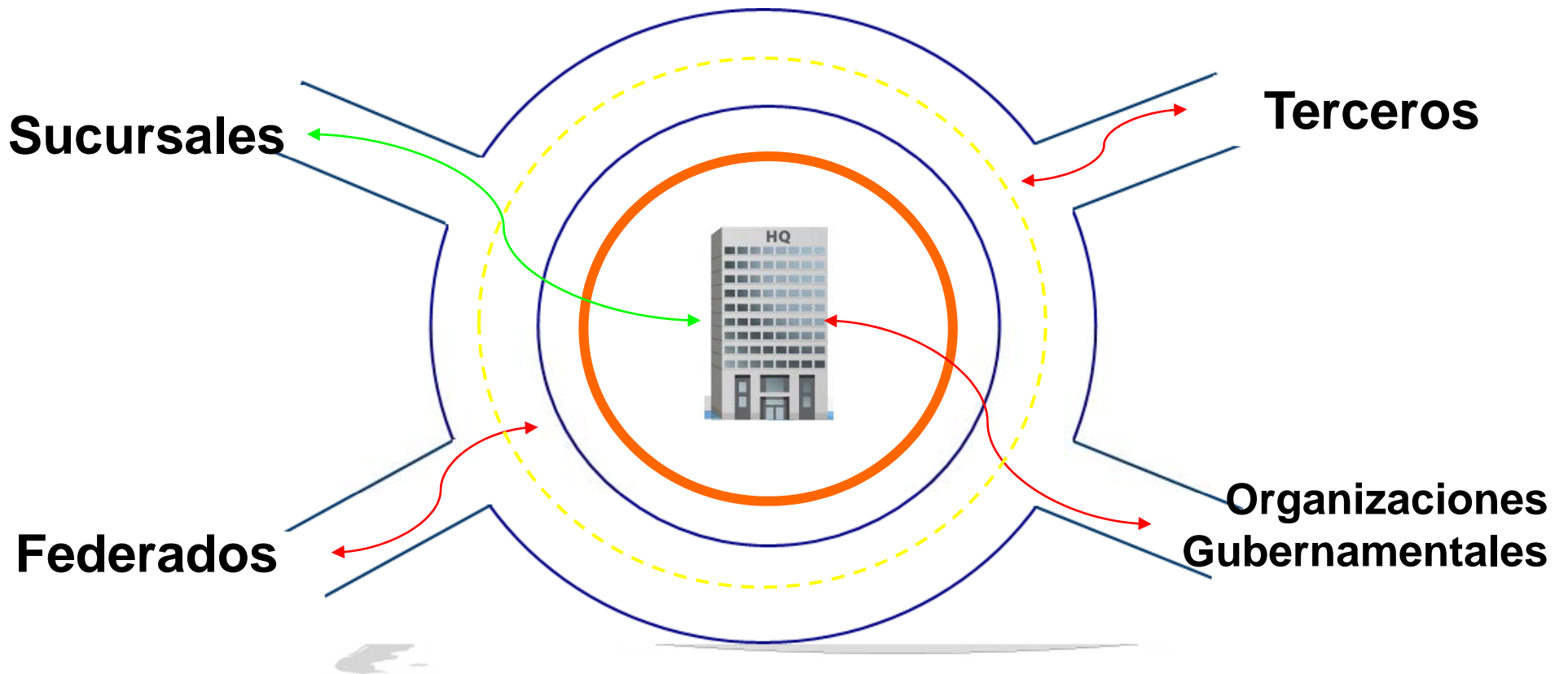
Necesidades LAN/MAN





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

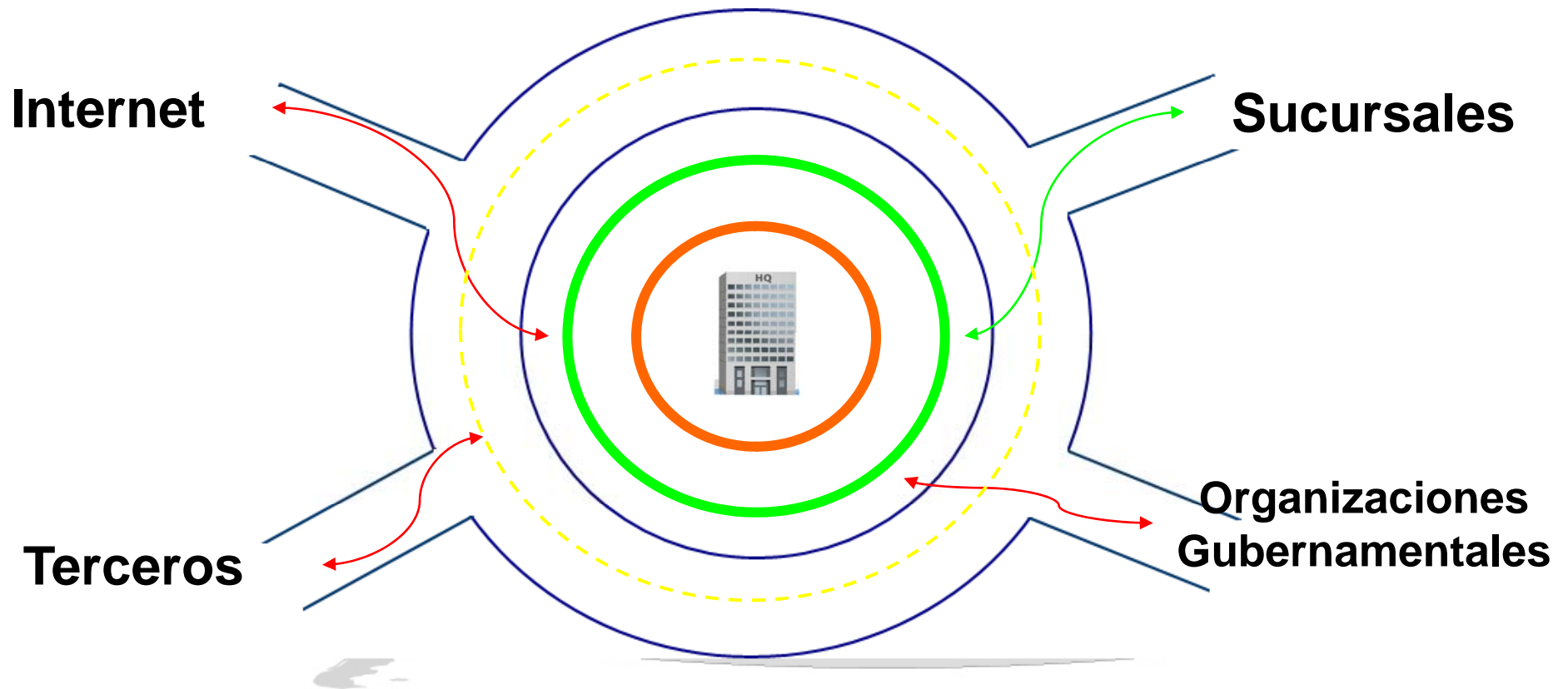
Necesidades WAN





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

Necesidades Internet/Redes Colaborativas





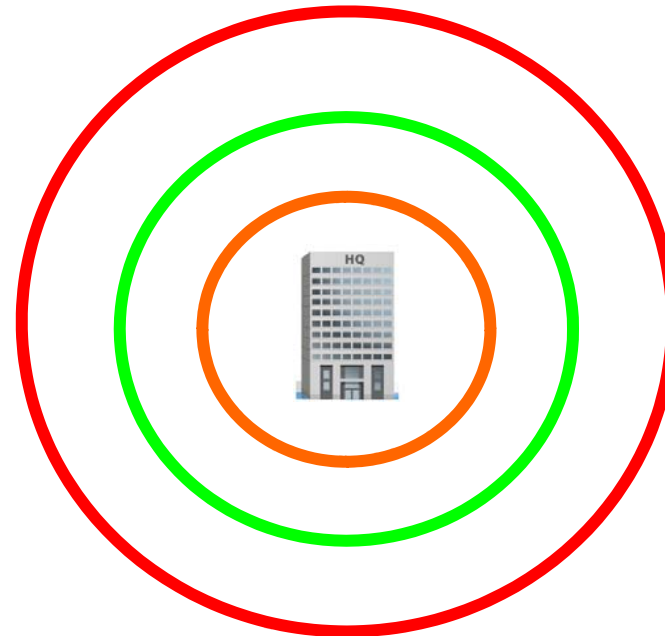
Medidas de Control





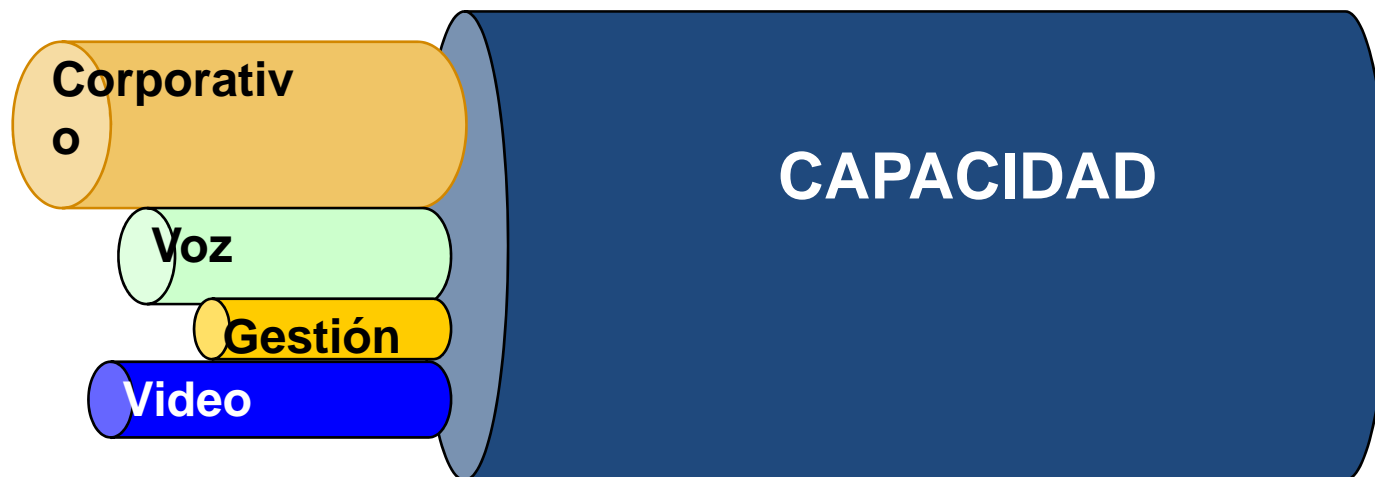
Quien accede a mi Red?

Conozco mi infraestructura de red?





Segregación de Tráfico





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

Control de Acceso a la Red

- Acceso instalaciones
- Identificación
- Escaneo de Vulnerabilidades
- Perímetro de acceso
- Permanencia
- Auditoria





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

Gestión de la Plataforma de Red

- Protocolos de Funcionamiento de la red seguros.
- Sincronización segura de hora legal.
- Información de eventos adecuados a la política de seguridad.
- Segregación de Roles y Responsabilidades
- Respaldo Configuraciones
- Documentación plataforma





Endurecimiento Dispositivos de Red

- Servicios necesarios de monitoreo
- Acceso controlado administrativo
- Protección ambiental
- Desactivación servicios vulnerables
- Protección ataques de negación de Servicio





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

Protección de Fronteras de Red

- Paredes de Fuego
- Sistemas de Prevención de Intrusos
- Control en profundidad en el flujo de protocolos vulnerables.
- Firewalls avanzados para Aplicaciones
- Autenticación fuerte
- Cifrado
- Control Fuga de Información





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

Seguridad Instalaciones

- Control de Acceso
- Video Vigilancia
- Registro
- Protección Ambiental
- Control de Incendios
- Seguridad Pública

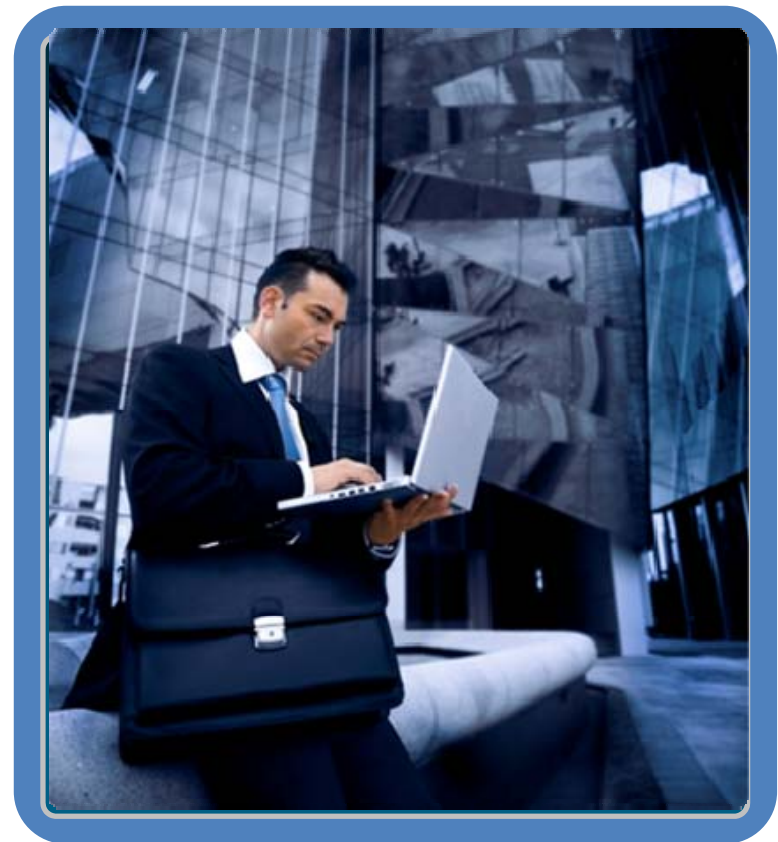




**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Participación Global

- Base de Información de Vulnerabilidades
- Colaboración Eventos
- Casuística

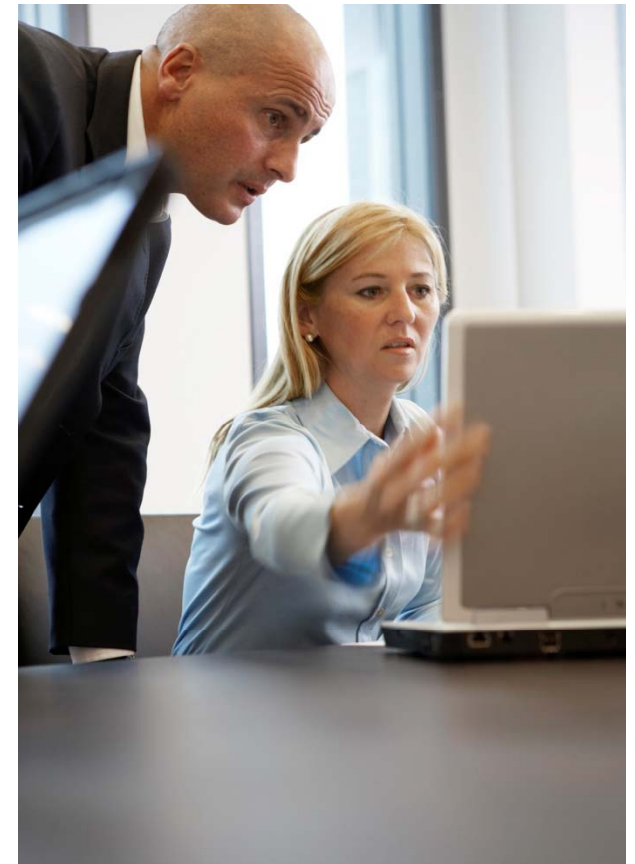




**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Medidas Procedimentales

- Gestión del Cambio
- Gestión de Incidentes
- Gestión de Problemas
- Gestión de la Capacidad
- Gestión de Parches
- Gestión de Eventos (Manifestación amenazas)
- Gestión de Vulnerabilidades
- Gestión del Riesgo





Acciones de Seguridad

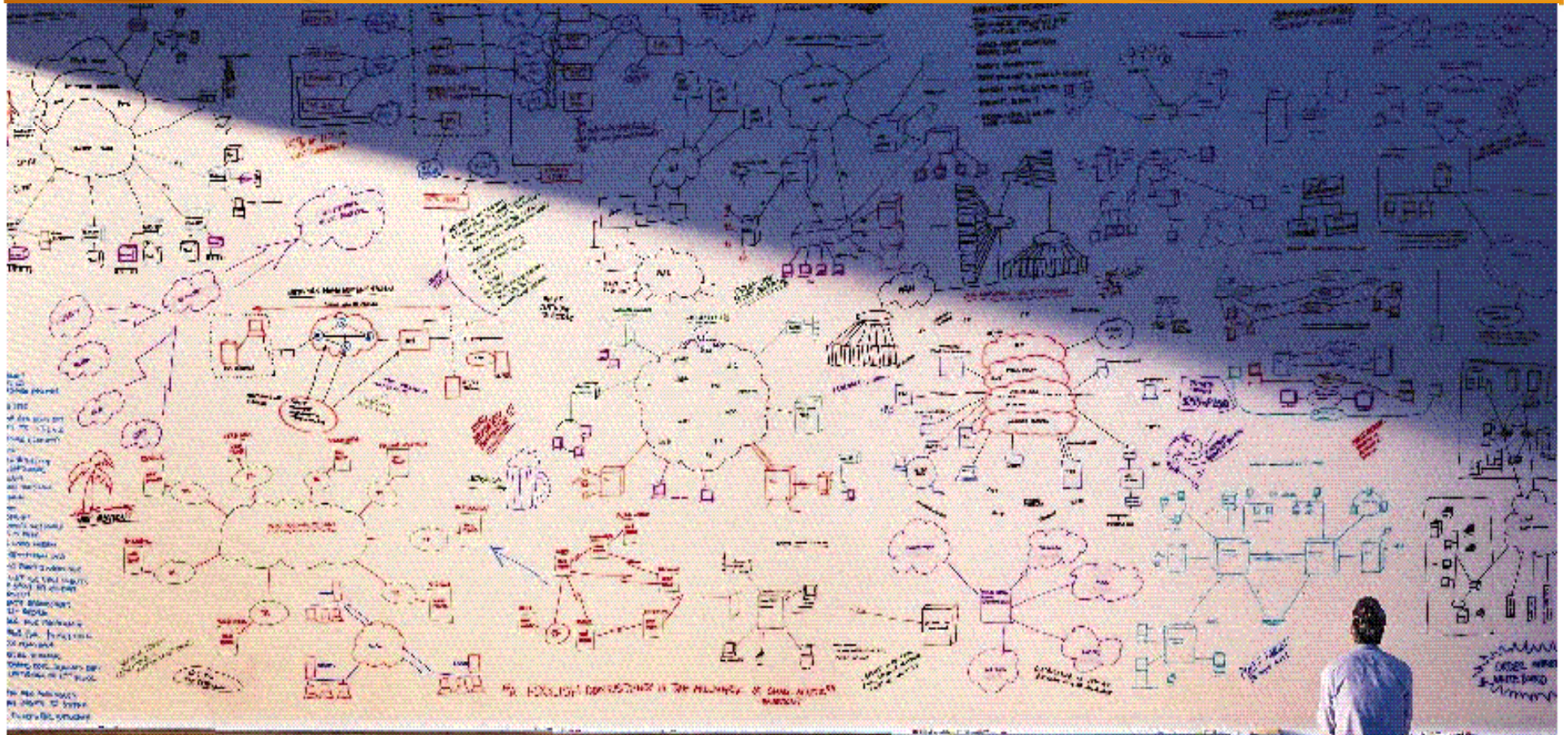
- Mayor Visibilidad
- Identificación de Amenazas
- Conocer mis Vulnerabilidades
- Reducir Falsos Positivos
- Mayor eficiencia en la Gestión de Eventos
- Determinar la severidad de los Incidentes
- Reducir el tiempo de respuesta a la gestión de Incidentes.





IX JORNADA de SEGURIDAD de INFORMÁTICA

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



Preguntas...



Gracias

Dankie Faleminderit Shukran Shur-nur-ah-gah-lem Thoinks
Eskerrik Asko Dhannyabad Blagodaria Hvala Jae Zu Din Pa De
Na som M'goy Gràcies Wado Skee Xie Xie Kia Manuia Dekuji
Tak Bedankt Dankon Aitäh Akpé Vinaka Kiitos Kpè nu wé
Merci Abarka Madlobt Danke Efharisto Aguije Abarka Aabar
Mahalo Toda Dhanyavaad Köszönöm Þakka þér fyrir Terima kasih
Moteshakeram Go raibh maith agat Grazie Arigato Matur nuwun
Dhan-ya-vaadaa Kamsa hamaida Paldies Achu Waybale Nandi
Terima Kasih Kia Manuia Na gode Takk Shakkran Soolong
Aguije Mam'noon Selamat Dziekuje Obrigado Bhala Hove
Multumesc Spasiba Fa'afetai Tapadh Leibh Dakujem Dankie
Gracias Nuhun Ahsante Tack Maururu Manjuthe Khob Khun
Kha/Krab Thuk Ji Chhe Tesekkurler Thank You Dyakuyu
Maherbani Shukria спасибо Rahmat Kam ouen Diolch Nkosi
Modupe Ngiyabonga

