

Introducción a la Gestión de Redes

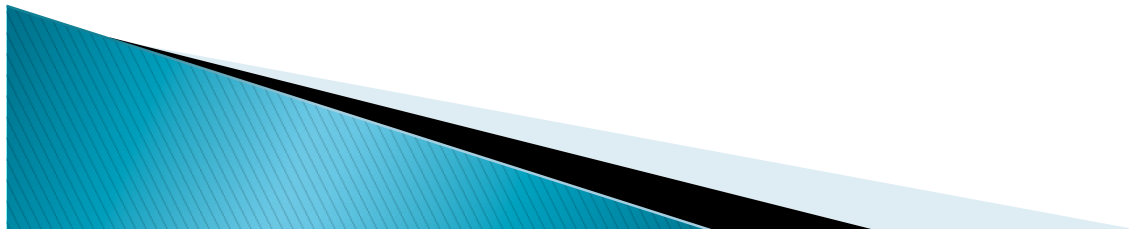
Hervey Allen

hervey@nsrc.org



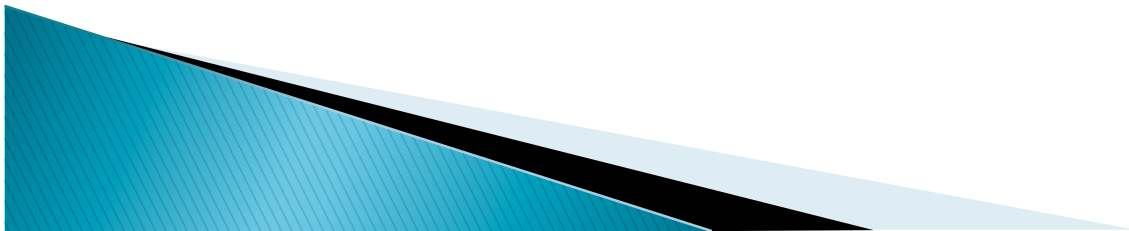
Carlos Armas

carmas@roundtripnetworks.com



¿Qué es la Gestión de Redes?

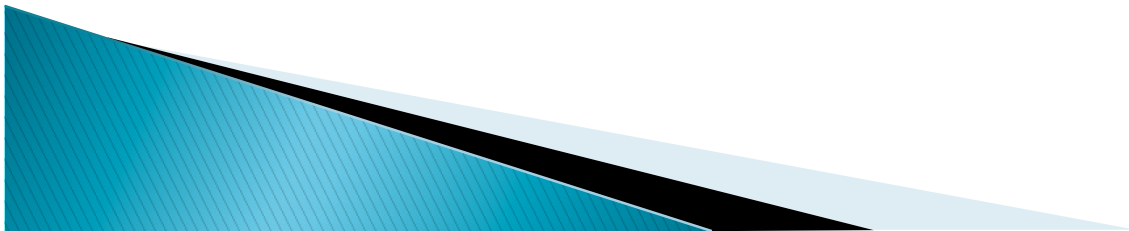
- ▶ Muchas definiciones, pero en esencia:
 - **Seguridad:** Proteger en contra de uso no autorizado
 - **Desempeño:** Eliminar limitaciones (“cuellos de botella”)
 - **Confiabilidad:** Asegurar que la red este’ disponible, respondiendo rapidamente a incidentes (averías, fallas)



Areas de Gestión de Redes

- Control de configuraciones/cambios
- Gestión de rendimiento
- Análisis y resolución de fallas
- Medición de uso (contabilidad)
- Gestión de seguridad

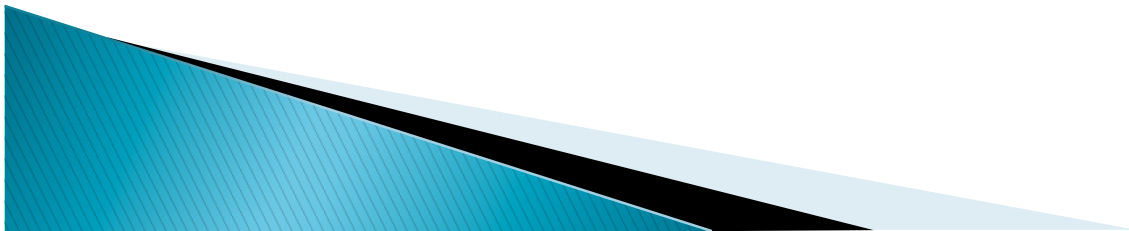
Analicemos estas areas en detalle...



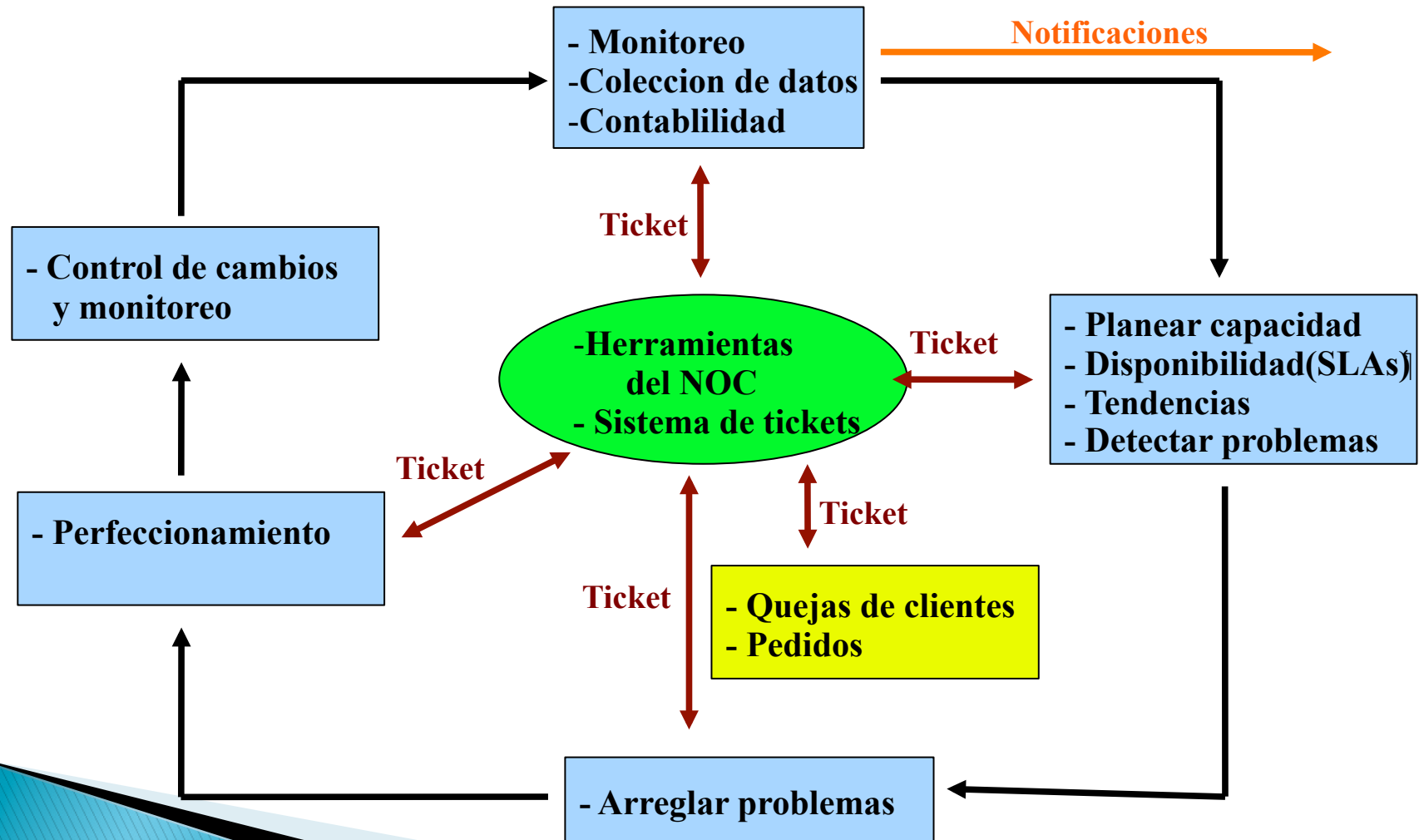
¿Qué es un NOC?

Network Operations Center
(Centro de Operaciones de Red)

- ▶ Desde donde se administra la red:
 - Disponibilidad actual, histórica y futura
 - Monitoreo de estado y estadísticas de operación
 - Gestión y resolución de fallas



Generalizando....



Control de Configuración

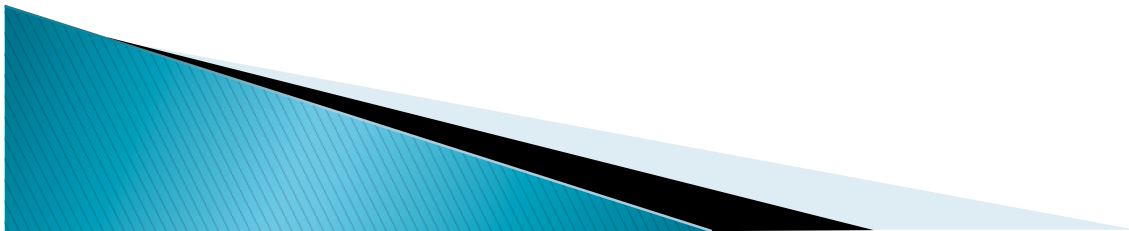
Conocer configuración de dispositivos de la red, y detectar cambios



Control de Configuración II

► Inventario, y estado actual

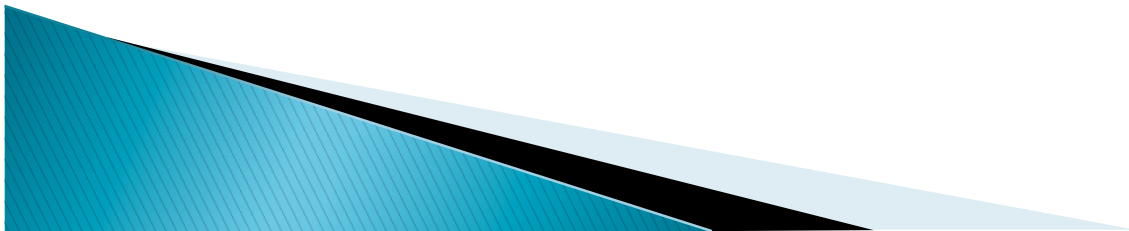
- **Qué está instalado?**
- **Dónde está instalado?**
- **Cómo está conectado?**
- **Quiénes son responsables por el dispositivo?**
- **Cómo contactarlos?**
- **Cual es el estado actual de cada elemento?**



Gestión del Rendimiento

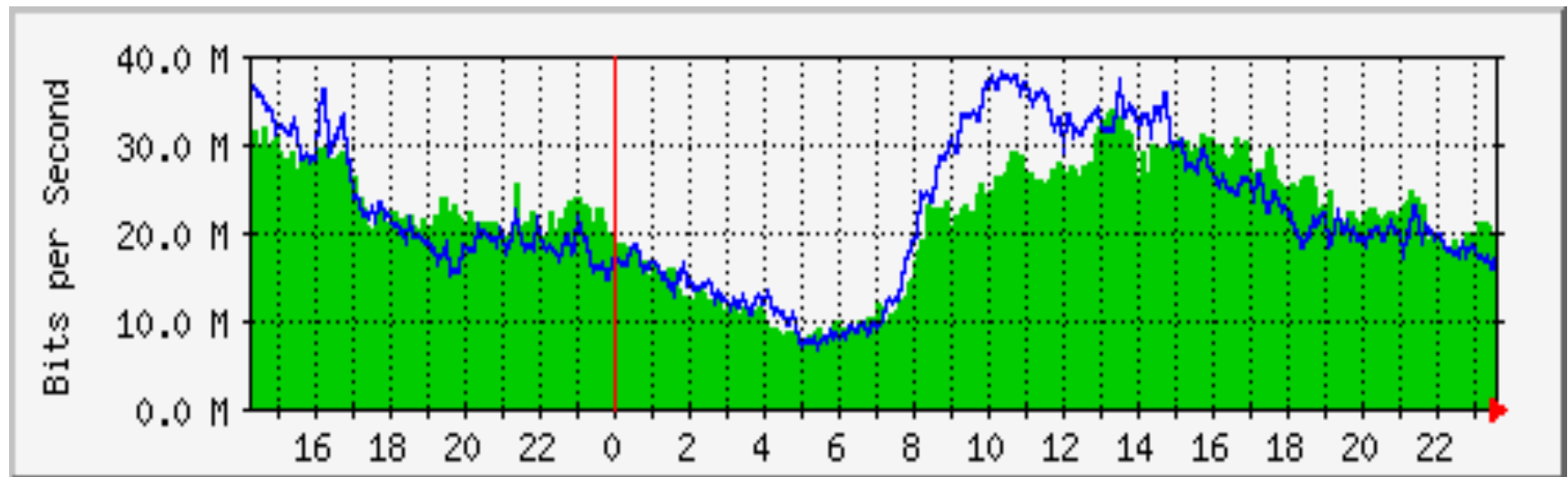
Objetivo: Garantizar un nivel de rendimiento consistente

- ▶ Colección de datos
 - Estadísticas de interfaces, y tráfico
 - Tasas de error
 - Utilización del canal y/o dispositivo
 - Disponibilidad
- ▶ Análisis de datos:
 - niveles límite de rendimiento
 - Planificación de capacidad futura



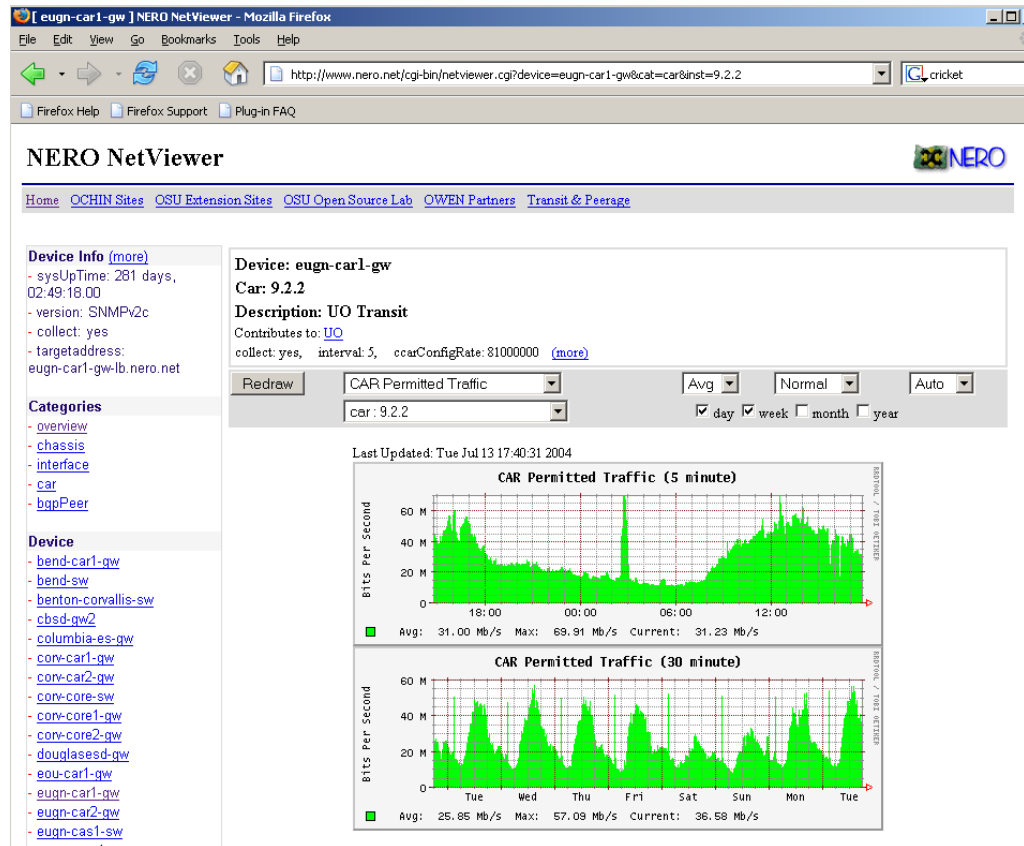
Ejemplo: MRTG

Herramienta de colección y visualización de tráfico

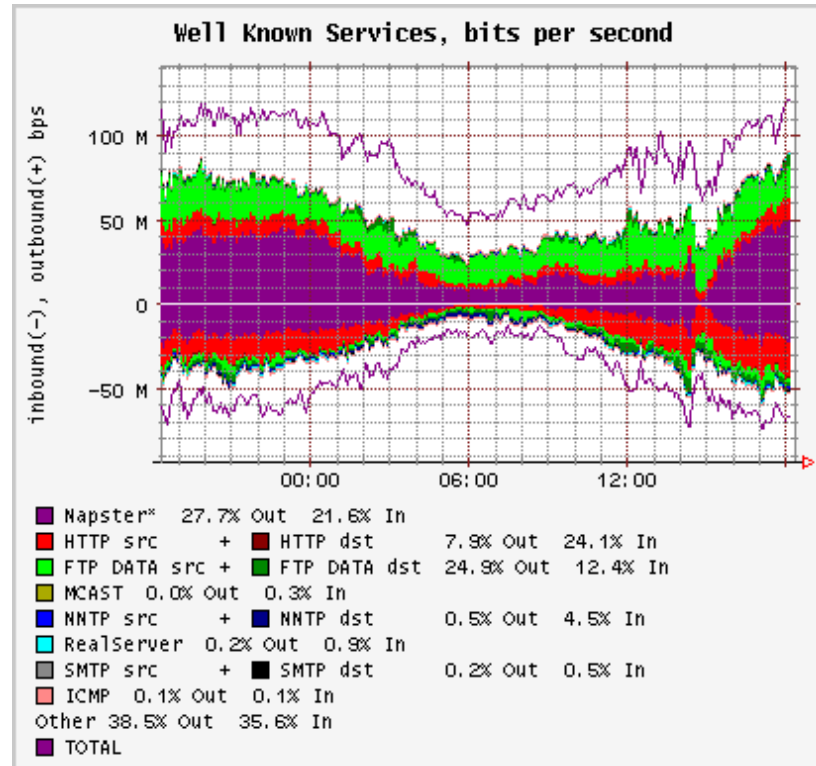


Ejemplo: Cacti

- ▶ Cacti (www.cacti.net)



Ejemplo: Flowscan



Gestión de fallas

► Identificación

- Sondeo regular de los elementos de la red
- Notificación <- importante!

► Diagnostico y aislamiento de falla

- Establecer el “dominio de fallo” consume mucho tiempo.
- Documentación es esencial!

► Reacción

- Proceso pre-establecido :
 - A quien se asigna la tarea de recuperación,
 - Pasos a seguir

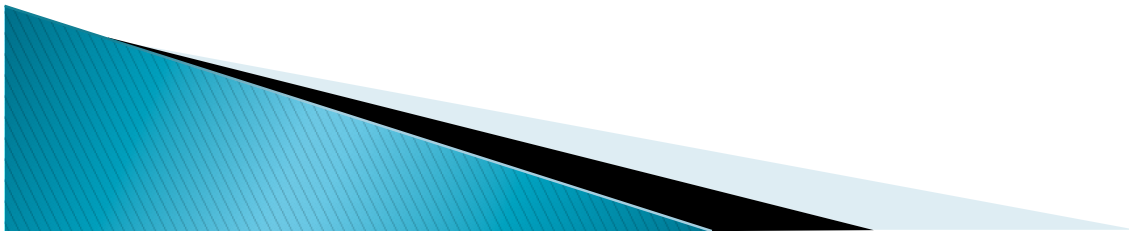
► Resolución

- Resolver, o escalar
- Notificación al cliente y demás partes interesadas



Requisitos para tener un buen sistema de gestión de fallas

- ▶ **Establecer procedimientos de notificación:**
 - Notificación al personal técnico del NOC
 - Notificación a clientes , gerentes u otro personal de acuerdo a protocolo pre-establecido
- ▶ **Tener un buen sistema de monitoreo y alarma**
 - Sistema Automático (Nagios, Cacti, otros)
- ▶ **Establecer procedimientos de reparación/recuperación**
 - Documentar procedimientos estándares (SOP)
 - Entrenar al personal técnico,
- ▶ **Mantener un sistema de manejo de incidencias (ticketing system)**
 - Conocer cantidad, prioridad, y estado de resolución de cada problema
 - Excelente base de conocimiento, datos históricos
 - Regla de 80-20: 80% del tiempo se emplea en diagnóstico
 - Administrar carga de trabajo de ingenieros
 - Ejemplo: RT (Request Tracker)



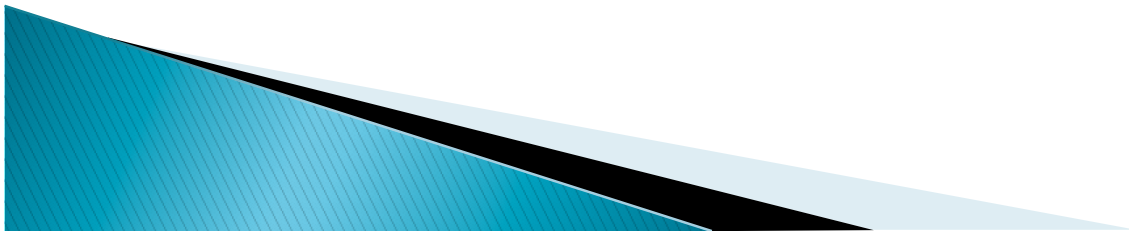
Detección y Gestión de Fallas

¿Quién detecta un problema en la red?

- Idealmente, sistema de monitoreo
- Ingenieros del NOC durante chequeo regular
- Llamada de cliente (¡mejor que no! :)

Que' pasos se deben tomar?

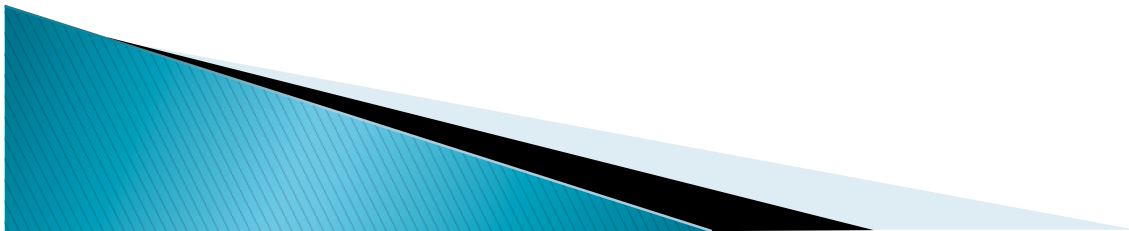
- Crear un un caso en el sistema de gestión
- Diagnosticar y aislar la falla(usualmente 80% del tiempo)
- Punto de decisión:
 - Asignar un ingeniero al caso o escalar la incidencia
 - Notificar a partes interesadas de acuerdo con el protocolo de notificación



Gestión de Fallas: Sistema de Control de Incidencias

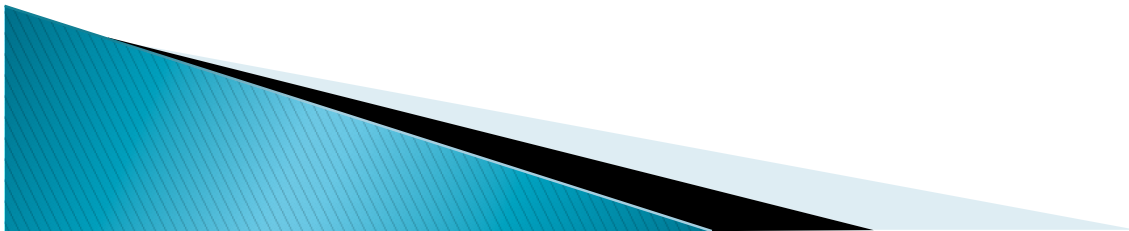
► El sistema provee:

- Programación y asignación de tareas
- Registro de la notificación
- Registro de tiempo de notificación y otros pasos
- Comentarios, escalamiento, notas técnicas
- Análisis estadístico
- Supervisión y delimitación de responsabilidades (quién hizo qué, y por qué)



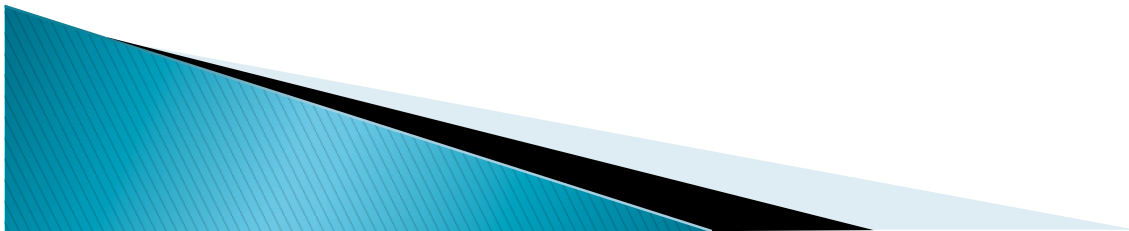
Gestión de fallas: guía de acción

- ▶ Crear un caso por cada incidente detectado
- ▶ Crear un caso por cada mantenimiento programado
- ▶ Enviar copia del caso a quién reporta, y a una lista de distribución
- ▶ El caso transita a través de una “máquina de estado”
 - abierto => asignado => en_progreso => resuelto (o escalado) => cerrado
- ▶ Quién creó el caso determina cuándo debe ser cerrada la incidencia



Gestión de contabilidad

- ▶ ¿Qué se necesita contabilizar?
 - La utilización de la red y los servicios que provee
- ▶ Los datos de contabilidad afectan los modelos de negocio
 - ¿Facturar la utilización?
 - ¿Facturar via tarifa plana?

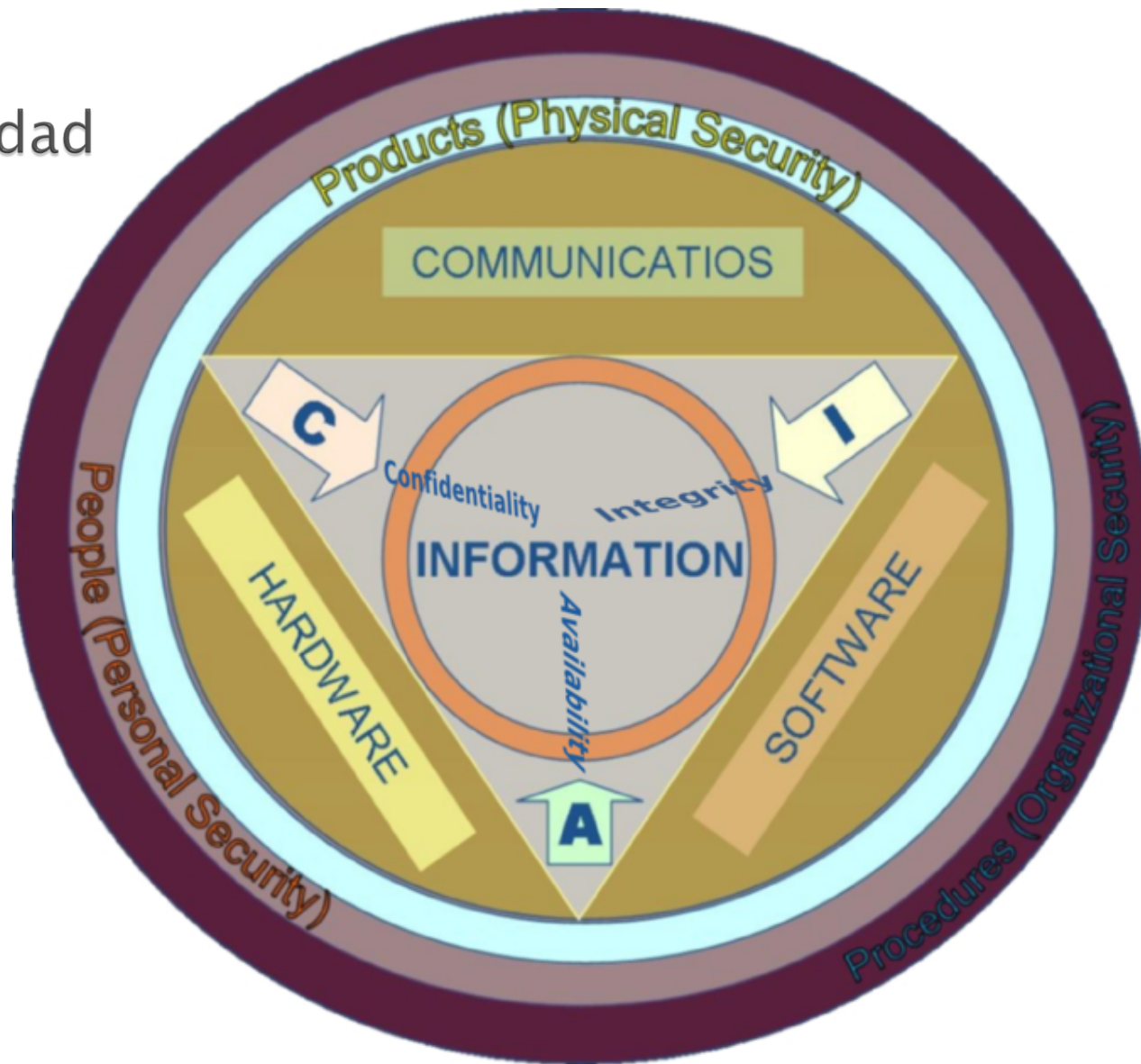


Gestión de Seguridad

- ▶ Controlar acceso a los recursos de la red de acuerdo a regulaciones bien definidas
 - Medidas organizativas y técnicas que combinadas garantizan disponibilidad, confidencialidad, e integridad de la red, como:
 - Quién y como autoriza acceso?
 - Protegerse de posibilidad de acceso no autorizado
 - (palabras claves, generadores de claves aleatorias, certificados de SSL)
 - Uso periódico de herramientas para analizar y controlar el uso legítimo de la red



Gestión de Seguridad



Gestión de Seguridad: Herramientas

▶ Herramientas

- Sondeo de vulnerabilidades
 - Nessus (www.nessus.org)
- Análisis de bitácoras (logs)
 - swatch – reportes via e-mail
- Filtros de Servicios
 - iptables, tcpwrappers, firewalls
- Cifrado
 - SSH – cifrado de sesiones interactivas
 - SSL
- Revisión de Integridad
 - Tripwire – monitorea cambios en sistema de ficheros

▶ Mantenerse actualizado es muy importante

- Listas de información
 - CERT
 - BugTraq
- Mantener software y firmware actualizado



Gestión de Seguridad

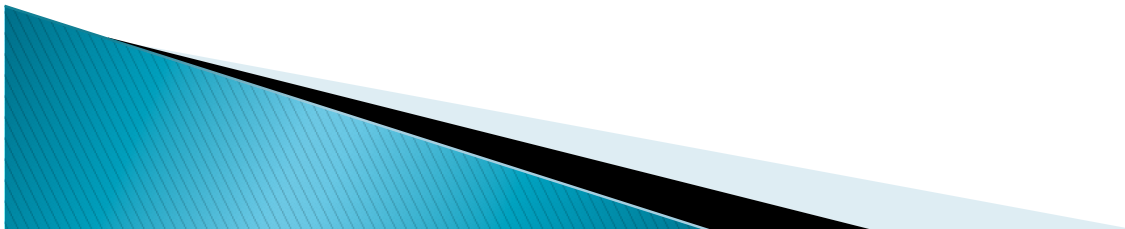
Este es un caso tomado de la vida real....

.....

```
tcp4      0      0 147.28.0.34.80      193.169.4.191.10558  SYN_RCVD
tcp4      0      0 147.28.0.62.80      193.169.4.154.10589  SYN_RCVD
tcp4      0      0 147.28.0.34.80      193.169.4.154.10589  SYN_RCVD
tcp4      0      0 147.28.0.62.80      193.169.4.164.11353  SYN_RCVD
tcp4      0      0 147.28.0.34.80      193.169.4.164.11353  SYN_RCVD
tcp4      0      0 147.28.0.62.25      201.88.17.237.2104   SYN_RCVD
tcp4      0      0 147.28.0.62.80      193.169.4.224.5167    SYN_RCVD
tcp4      0      0 147.28.0.34.80      193.169.4.224.5167    SYN_RCVD
tcp4      0      0 147.28.0.34.80      193.169.4.178.5323    SYN_RCVD
tcp4      0      0 147.28.0.62.80      193.169.4.178.5323    SYN_RCVD
tcp4      0      0 147.28.0.34.80      193.169.4.207.7156    SYN_RCVD
tcp4      0      0 147.28.0.62.80      193.169.4.207.7156    SYN_RCVD
tcp4      0      0 147.28.0.34.80      193.169.4.203.6892    SYN_RCVD
tcp4      0      0 147.28.0.62.80      193.169.4.203.6892    SYN_RCVD
tcp4      0      0 147.28.0.62.80      193.169.4.213.7608    SYN_RCVD
tcp4      0      0 147.28.0.34.80      193.169.4.213.7608    SYN_RCVD
tcp4      0      0 147.28.0.62.80      193.169.4.227.72      SYN_RCVD
tcp4      0      0 147.28.0.34.80      193.169.4.227.72      SYN_RCVD
tcp4      0      0 147.28.0.34.80      193.169.4.131.760     SYN_RCVD
```

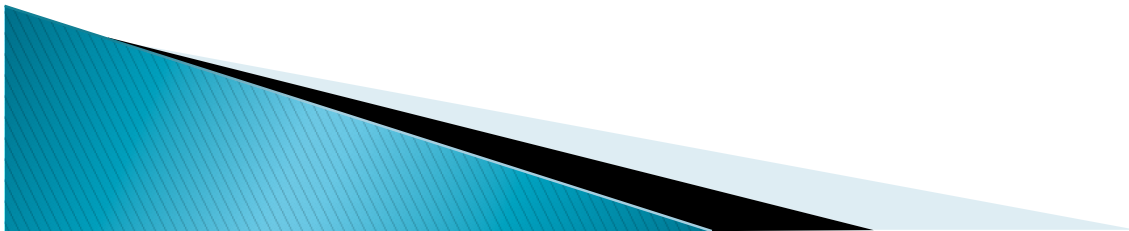
```
$ netstat -na | grep SYN_RCVD | grep 193.169 | wc -l
```

248



¿Cuales herramientas usar?

- Mientras más simple de mantener, mejor
 - Son herramientas, no productos comerciales
- No “reinventar la rueda”
 - Seguro que alguien ya paso’ por esto, y preparó una solución
- Hacer uso de herramientas gratuitas
 - (Muchas!) Nagios, Zabbix, OpenNMS, Cacti, others...
- Automatizar, automatizar!
 - RANCID, Puppet, Nagios, cfengine....



¿Preguntas?

