fs2007

V Foro de Seguridad RedIRIS

Intrusión, detección, desconexión y actuación

Víctor Barahona
Universidad Autónoma de Madrid

Puerto de la Cruz, 12-13 Abril 2007

UAM UNIVERSIDAD AUTONOMA DE MADRID

Red IRIS

Agenda

- Entorno.
- Herramientas técnicas.
- Herramientas administrativas.
- Procedimiento.
- Recursos humanos.
- Problemática.
- Reflexiones.
- Proyectos a corto plazo.

Entorno: usuarios

- 40.000 usuarios.
- 15.000 IPs estáticas.
- Usuarios wifi.
- Disparidad de sistemas operativos.

Herramientas técnicas

- Antivirus. (Trend)
- IDS. (Snort + ACRI)
- Firewall. (FW-1)
- Gestor de Ancho de banda. (Packeteer+Report Center)
- Escaneos Automatizados (Cancerbero)

Intrusión detectada…

- ¿Y ahora que hago?

  Filtrado.

  Notificación.

- Resultado:

  Incidentes eternos.

  Ataques internos.

El usuario y sus circunstancias

- YO administro mi PC
- YO actualizo si quiero.
- YO no meto contraseña.
- YO no valido en domino.
- YO instalo el antivirus que quiero y si quiero.

VALE, PERO A MI RED NO TE CONECTAS

Herramientas administrativas

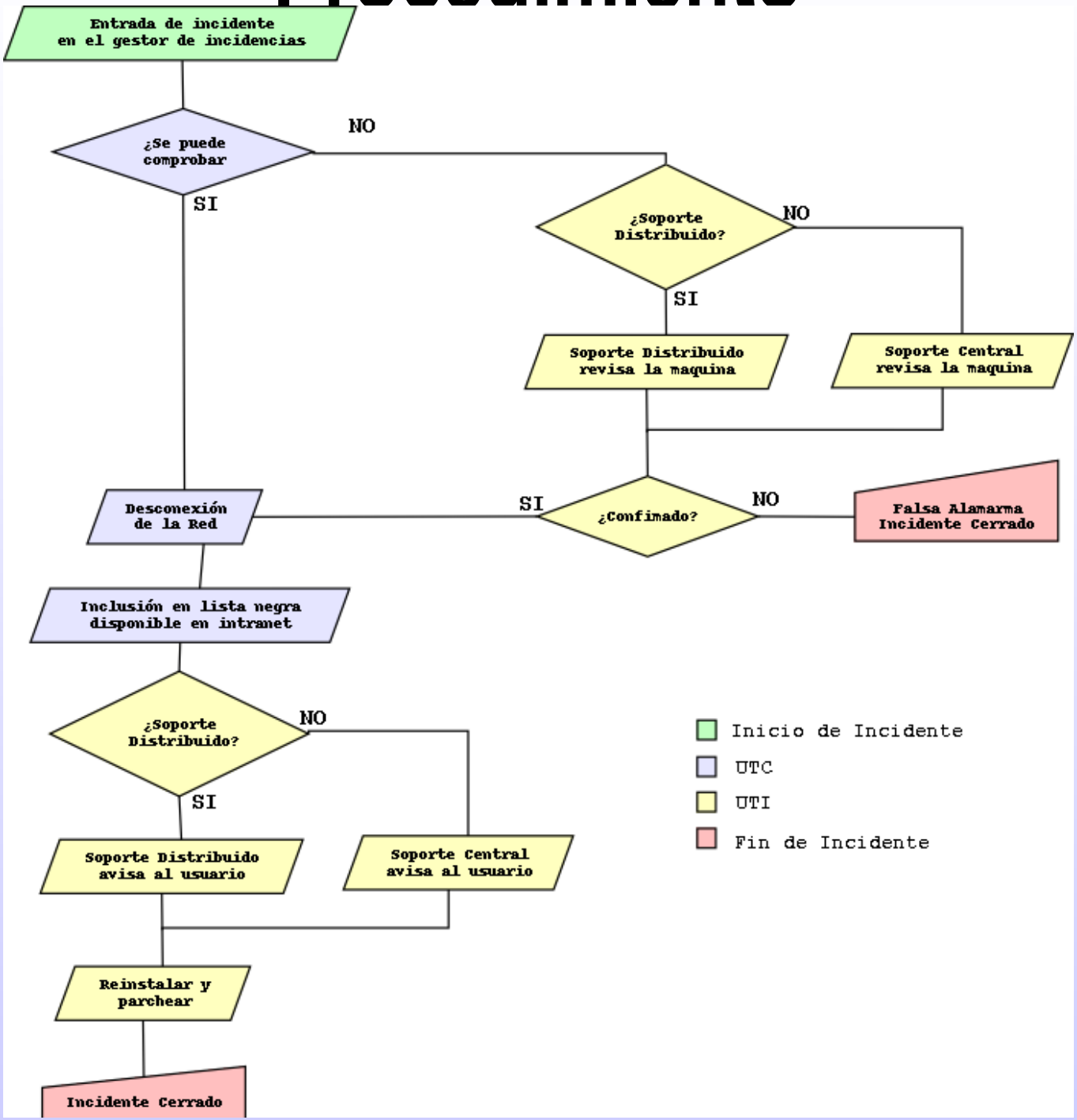
- 2004 Normas de Uso Aceptable y Seguridad (aka NUAS)

  Establece normas mínimas para conectar a la red.

  Establece sanciones para los infractores (desconexión)

- Normas ≠ Politica
- Desconectar ≠ Filtrar
- Con normativa las cosas cambian.

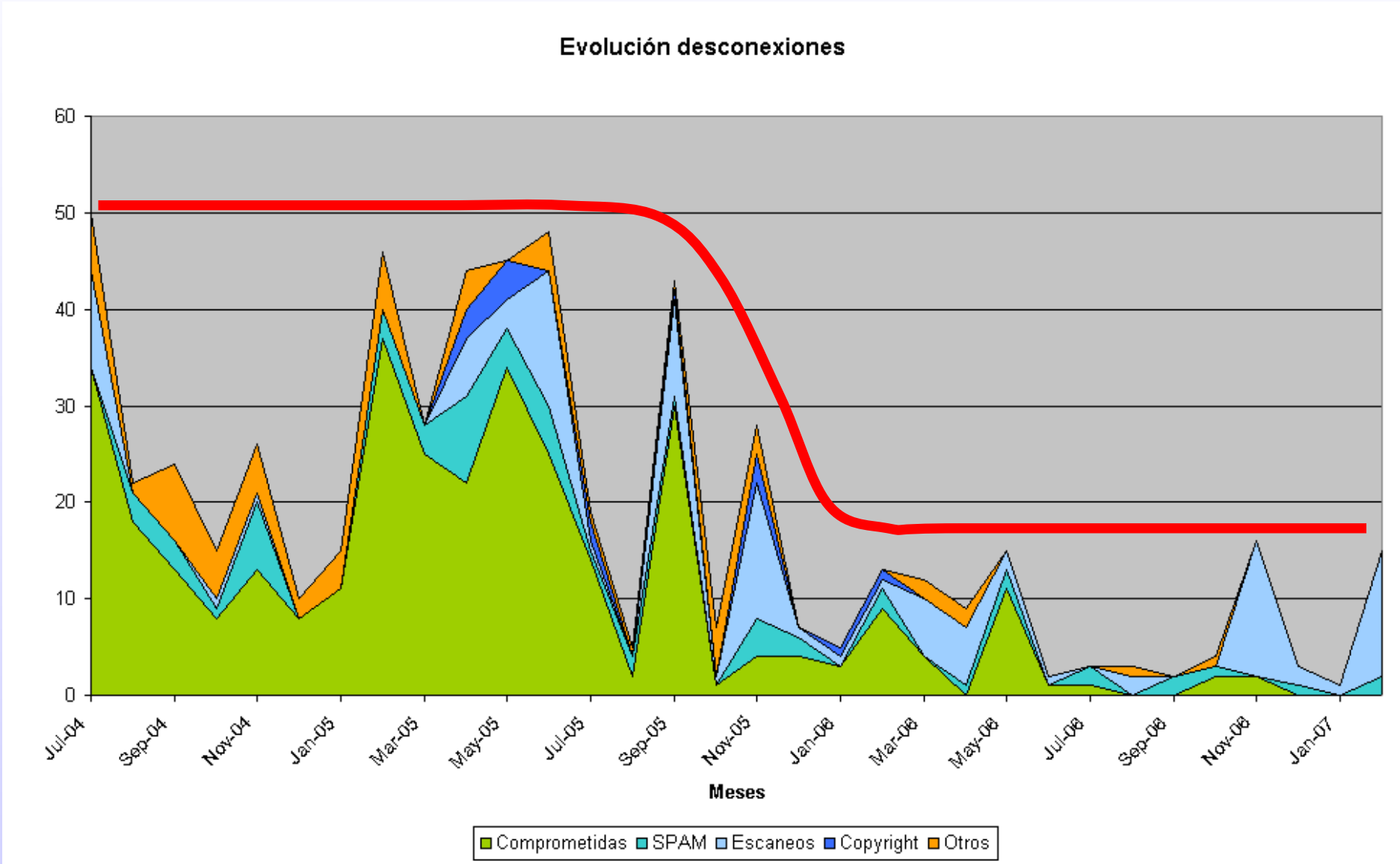
Procedimiento



Recursos Humanos

- Seguridad: 2
- Gestión de red: 1
- CAU: 2 - 4
- Soporte Central: 2 - 4
- Soporte Distribuido: 24 (2 por edificio)

Evolución de incidentes I



Reflexiones

- Teoría de la evolución.
- Mejora en sistemas operativos.
- Cambio en el tipo de ataques.
- ¿Hemos perdido efectividad en la detección?
- Evolucionar o morir.

Proyectos a corto plazo

- Desarrollo de Cancerbero.
- Automatización de desconexiones (DESCONII).
- Análisis de flujos (NFSEN).
- Reactivar ACRI.

Referencias

- NUAS: http://www.uam.es/servicios/ti/cau/doc/NUAS.pdf
- Cancerbero: http://cancerbero.sourceforge.net
- ACRI: http://www.rediris.es/cert/proyectos/acri.es.html