Gestión y Operación de la Ciberseguridad

Dr. Víctor A. Villagrá
Profesor Titular de Universidad
Dpto. Ingeniería Telemática – ETSIT- UPM
villagra@dit.upm.es

dit
UPM

Gestión de Ciberseguridad

- Gestión de Redes, Servicios, Sistemas y Aplicaciones:
  - Fault Management
  - Configuration Management
  - Accounting Management
  - Performance Management
  - Security Management

Aspectos Funcionales de la Gestión de Red

- No existe funcionalidad común. Depende de:
  - Tipo de Red gestionada
  - Tipo de Equipos gestionados
  - Objetivos específicos de la gestión de red
- A bajo nivel, todos los métodos se basan en:
  - Monitorización de Red:
    - Gestión de Prestaciones
    - Gestión de Fallos
    - Gestión de Contabilidad
    - Gestión de Configuraciones / Seguridad
  - Control de Red
    - Gestión de Configuraciones / Seguridad

Monitorización de Red

- 4 fases para la monitorización de una red:
  - Definición de la información de gestión que se monitoriza
  - Acceso a la información de monitorización
  - Diseño de mecanismos de monitorización
  - Procesado de la información de monitorización
- Control de Red: fases de definición y acceso.

Definición de la información de monitorización

- De acuerdo a su naturaleza, existen los siguientes tipos:
  - Información estática: no cambia con la actividad de la red.
  - Información dinámica: evoluciona con la propia actividad de la red.
  - Información estadística: postprocesado de la información dinámica que proporciona un mayor significado de gestión.

Definición de la información de monitorización

- ¿ Qué información monitorizar ? Depende de la aplicación:
  - Para gestión de prestaciones: información estadística, generada a partir de información dinámica (tráfico, retardo, etc...)
  - Para gestión de fallos: información dinámica (cambios de estados)
  - Para gestión de configuraciones: información estática (inventario de la red)

Acceso a la Información de Gestión

- Objetivo: monitorización remota de los recursos desde el centro de gestión
- Necesita una cooperación entre los gestores y los equipos gestionados
  - Los equipos deben “querer ser gestionados”: instalación del software de gestión adecuado
- Método común de acceso a la información de gestión, independientemente de la tecnología o fabricante del equipo monitorizado

Modelos de gestión de red integrada: proporcionan la interoperabilidad

Mecanismos de monitorización

- Sondeo o polling: acceso periódico a la información de gestión.
  - Ventaja: Los objetos solo deben estar preparados para responder: simplicidad.
- Event Reporting o notificaciones: los propios recursos envían notificaciones bajo ciertas condiciones.
  - Ventaja: se minimiza el tráfico de gestión por la red.

Dos filosofías de gestión:

➔*Descargar la complejidad hacia los gestores*

➔*Balancear complejidad entre gestores y equipos gestionados*

Procesado de la Información

- Monitorización de una red:
  - Definición de la información de gestión que se monitoriza
  - Acceso a la información de monitorización
  - Diseño de mecanismos de monitorización
  - Procesado de la información de monitorización: Aplicaciones de Gestión asociadas
    - Gestión de Configuraciones
    - Gestión de Fallos
    - Gestión de Prestaciones
    - Gestión de Contabilidad
    - Gestión de Seguridad

Gestión de Configuración

- Gestión de Inventario:
  - Herramientas de autodescubrimiento
  - Combinación con herramientas CAD de gestión de cableado
  - Base de Datos utilizable por el resto de funciones.
- Gestión de Topología
  - Herramientas de autotopología
  - Necesidad de distintas vistas topológicas
- Gestión de Servicios de Directorio
  - Integración con el resto de aplicaciones

Gestión de Configuración

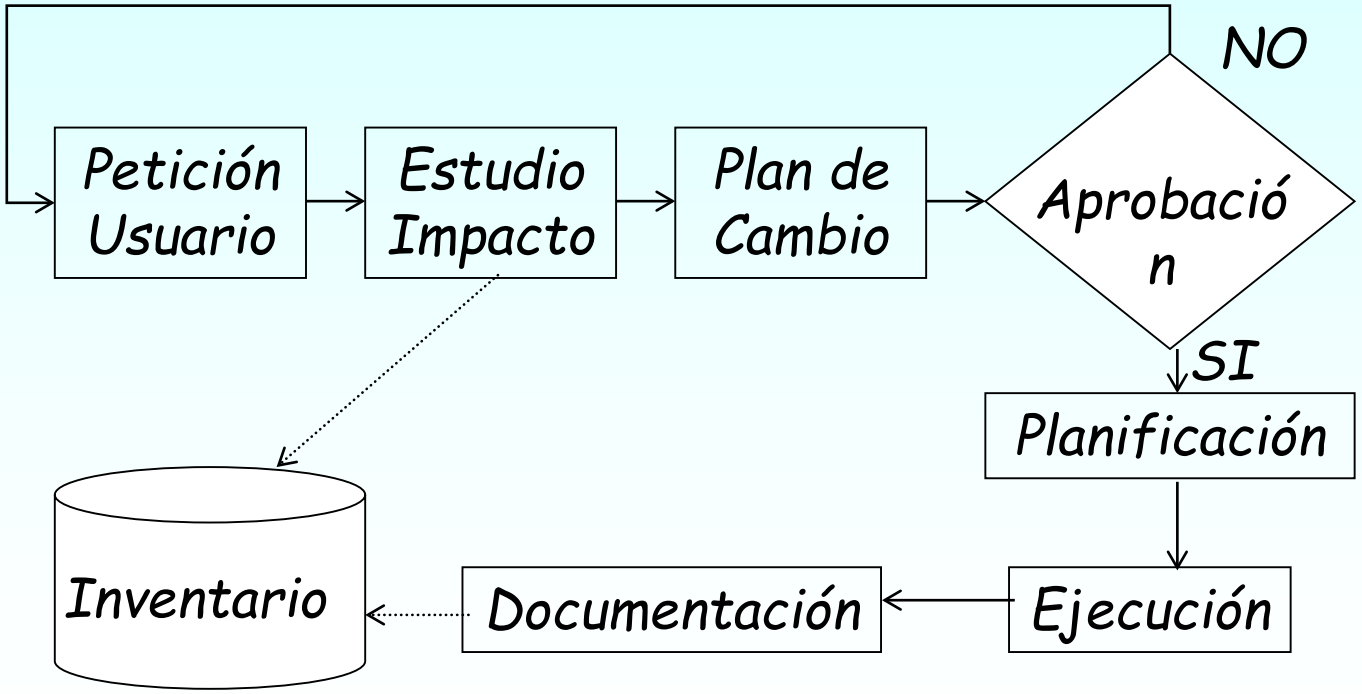
- Gestión de SLAs (Service Level Agreements): Contrato entre cliente/proveedor o entre proveedores sobre servicios a proporcionar y calidades asociadas
  - Identificación de las partes contractuales
  - Identificación del trabajo a realizar
  - Objetivos de niveles de servicio
  - Niveles de servicio proporcionados
  - Multas por incumplimiento
  - Fecha de caducidad
  - Cláusulas de renegociación
  - Prestaciones actuales proporcionadas

Gestión de Configuración

- Gestión de Incidencias: TTS (Trouble Ticket Systems).
  - Fecha/Hora de:
    - Informe de Incidencia
    - Resolución de Incidencia
  - Usuario/Localización
  - Equipo afectado
  - Descripción problema
  - ESTADO
  - Operador(es)
  - Grado de Severidad
  - Historial de Incidencia
  - Comentarios.

Gestión de Configuración

- Gestión de Proveedores Externos (ordenes de procesamiento/aprovisionamiento)
- Gestión de Cambios (reconfiguraciones):



Gestión de Fallos

- Objetivo: mantener dinámicamente el nivel de servicio
- Funciones:
  - Evitar el fallo antes de que suceda
    - Gestión Proactiva
    - Gestión de Pruebas Preventivas
  - Ha sucedido: Gestión del ciclo de vida de incidencias
    - Detección del Fallo (o mejor evitarlo)
    - Aislamiento del Fallo
    - Diagnosis del Fallo
    - Resolución del Fallo

Gestión Proactiva

- Gestión Proactiva: detectar un fallo antes que suceda.
- Evitar fallos detectando “tendencias” hacia fallos
  - Caracterización de tendencias: determinación de umbrales de ciertos parámetros
  - Objetivo: monitorizar estos umbrales o programar notificaciones automáticas

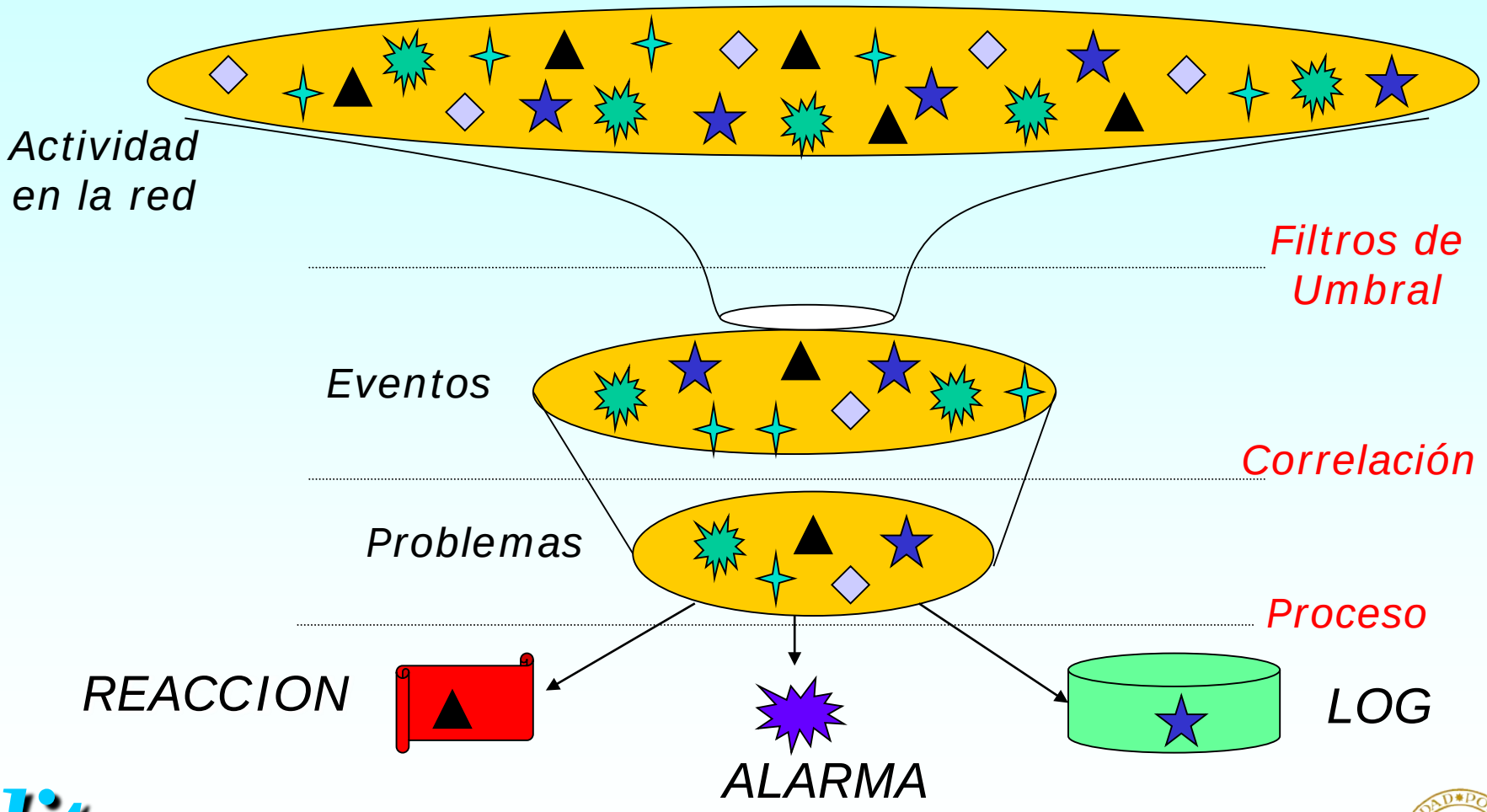
Gestión de Pruebas Preventivas

- Detectan fallos ocultos que no podrían detectarse normalmente
- Suelen ser intrusivas: necesitan desactivación del servicio
  - Pruebas de Conectividad
  - Pruebas de Integridad de Datos
  - Pruebas de Integridad de Protocolos
  - Pruebas de saturación de datos
  - Pruebas de saturación de conexiones
  - Pruebas de tiempo de respuesta
  - Pruebas de bucle
  - Pruebas de diagnóstico

Gestión del Ciclo de Vida de Incidencia

- Detección de Problemas:
  - Alarma de Usuarios
  - Alarma de Herramientas: Gestión Reactiva.
    - Asumir que existen fallos inevitables
    - Detectar lo antes posible el fallo
    - Monitorización periódica (no es posible notificación)
- Aislamiento del fallo
  - La información sobre el fallo puede no ser fiable en cuanto a la fuente del fallo
  - Herramientas de Correlación de Eventos

Correlación de Eventos



Gestión del Ciclo de Vida de Incidencia

- Diagnosis del problema: procedimentado.
- Resolución del problema.
  - Por operadores de help-desk (80-85%)
  - Por operadores técnicos (5-10%)
  - Por especialistas en comunicaciones (2-5%)
  - Por especialistas en aplicaciones (1-3%)
  - Por fabricantes (1-2%)

Gestión de Prestaciones

- Definición de Indicadores de Prestaciones:
  - Orientados a servicio
    - Fiabilidad
    - Disponibilidad
    - Tiempo de Respuesta
  - Orientados a eficiencia
    - Throughput
    - Utilización
- Monitorización de Indicadores de Prestaciones
- Análisis y Refinamiento

Indicadores de Prestaciones: Fiabilidad

- Fiabilidad de un Sistema: Probabilidad de que el sistema falle.
  - Es necesario minimizarlo: los fallos solo deberían darse por fallos de fabricación
  - Gestión proactiva para monitorización de síntomas de fallos.
- Es necesario calcular la fiabilidad global a partir de la fiabilidad individual de los componentes.
  - Fiabilidad de un componente: función probabilidad dependiente del tiempo.
  - Fiabilidad global: composición de fiabilidades individuales.

Indicadores de Prestaciones: Disponibilidad

- Parámetro necesario: disponibilidad de los servicios
- Es necesario traducirlo a disponibilidad de componentes individuales
- Objetivo: maximizar (cumplir) la disponibilidad de los equipos.

$$D = \frac{MTBF}{MTBF + MTTR}$$

MTBF: Mean Time Between Failures
MTTR: Mean Time To Repair

MTBF: Indicador de calidad del equipo
MTTR: Influye:
Tiempo de detección del fallo
Política de mantenimiento utilizada

Indicadores de Prestaciones: Tiempo de Respuesta

- Tiempo de Respuesta: rangos.
  - > 15 sg: Inaceptable para servicios interactivos
  - > 4 sg: Dificultan servicios interactivos encadenados (con memoria del usuario)
  - 2 a 4 sg: Dificultan servicios interactivos que requieran concentración del usuario
  - 2 sg: Limite aceptable normalmente
  - Decimas de segundo: para aplicaciones de tipo gráfico
  - < 0,1 sg: servicios de eco.
- Componentes:
  - Tiempo de transmisión (ida y vuelta)
  - Tiempo de proceso de servicio

Indicadores de Prestaciones

- Throughput:
  - Capacidad real utilizada de un recurso.
- Utilización:
  - Porcentaje de uso de un recurso durante un periodo de tiempo
  - Capacidad real / Capacidad teórica máxima
  - Ej: Utilización de una línea serie, utilización de una Ethernet, etc.

Gestión de Prestaciones

- Monitorización de Indicadores de Prestaciones
  - Disponibilidad: sondeos de estado
  - Tiempo de Respuesta:
    - Tiempo de transmisión: utilización de ecos remotos
    - Tiempo de procesamiento: trazado por aplicaciones
  - Fiabilidad: umbrales de porcentajes de error
  - Utilización: sondas de tráfico
- Análisis y Refinamiento

Gestión de Contabilidad

- Identificación de Componentes de Coste
- Establecimiento de Políticas de Tarificación
- Definición de procedimientos para tarificación
- Gestión de Facturas
- Integración con la Contabilidad Empresarial

El problema de la heterogeneidad

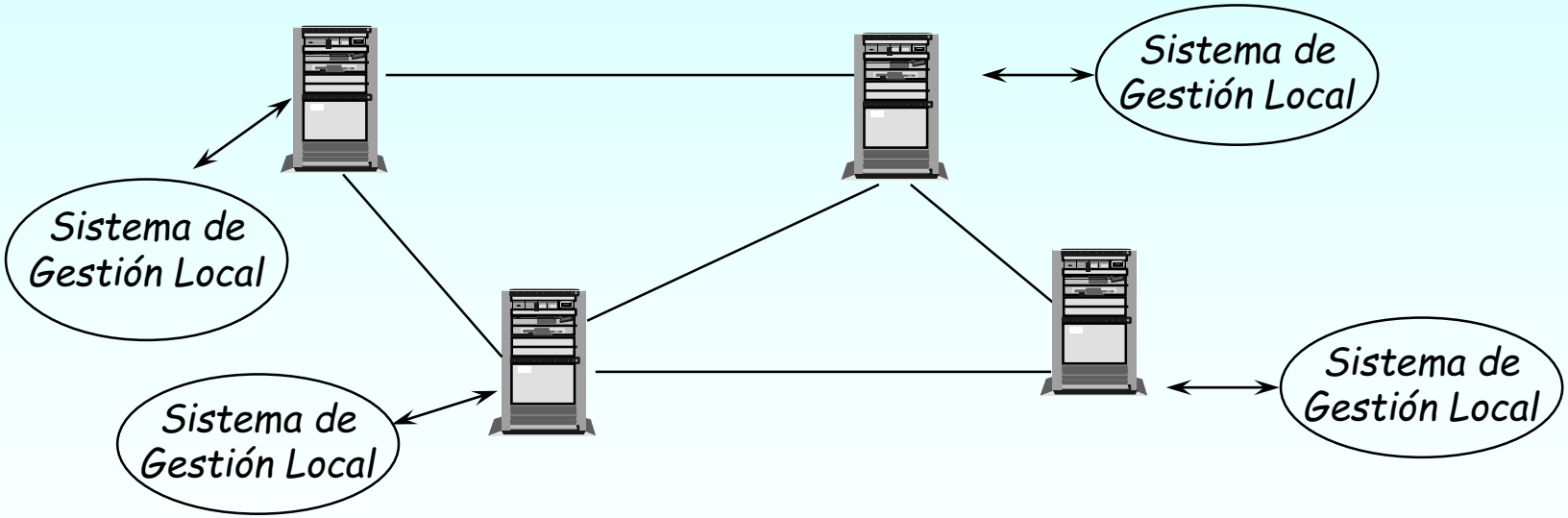
- Interconexión entre equipos: resuelto por arquitecturas de comunicaciones estándares (TCP/IP, X.25, etc.)

- Interconexión Gestor-Equipo:
  - Fabricantes: Intento de establecer carácter propietario (se aseguran la venta del equipo y de su gestor)
  - Usuarios: entornos heterogéneos, de múltiples fabricantes

¿Aumento imparable del número de gestores?

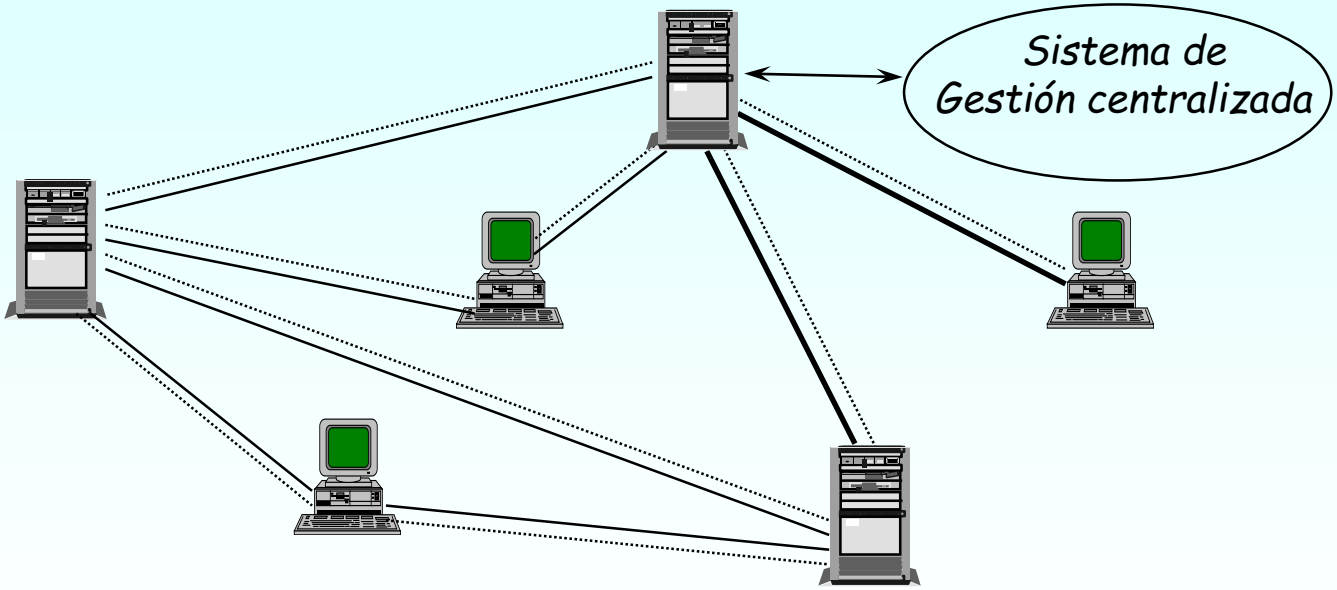
Evolución

- Un primer paso: Gestión Autónoma. Redes con gestión local en cada nodo.



Evolución (II)

- Siguiente paso: Gestión homogénea. Redes homogéneas con un único nodo de gestión centralizado.



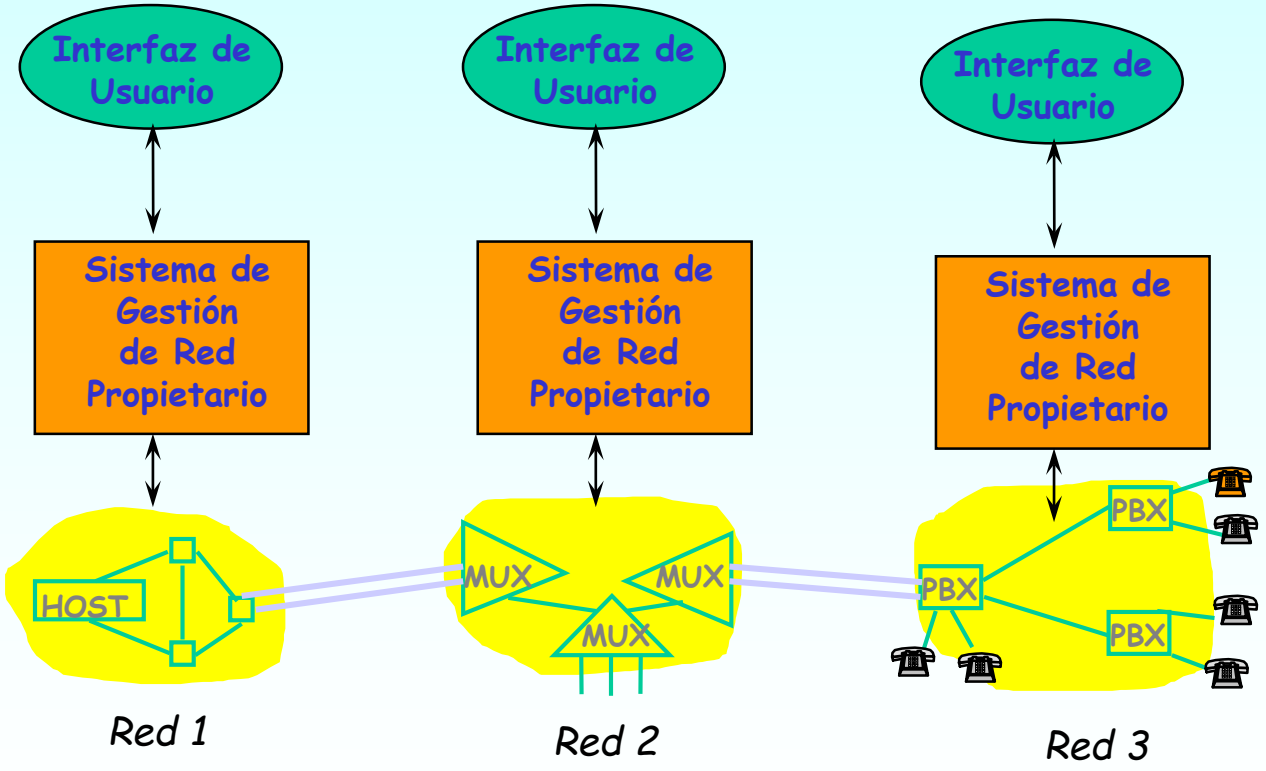
Evolución (III)

- Situación actual: Gestión heterogénea. Ampliación de las redes con la interconexión de productos heterogéneos.

- Ejemplo:
  - Organización que satisface los requisitos de comunicaciones de sus sistemas de información mediante:
    - Red de datos
    - Red de telefonía
    - Transmisión (multiplexores, módem, etc...)

Ejemplo

- Supuesto que los elementos de cada una de las redes son del mismo fabricante, existirían tres centros de gestión de red.

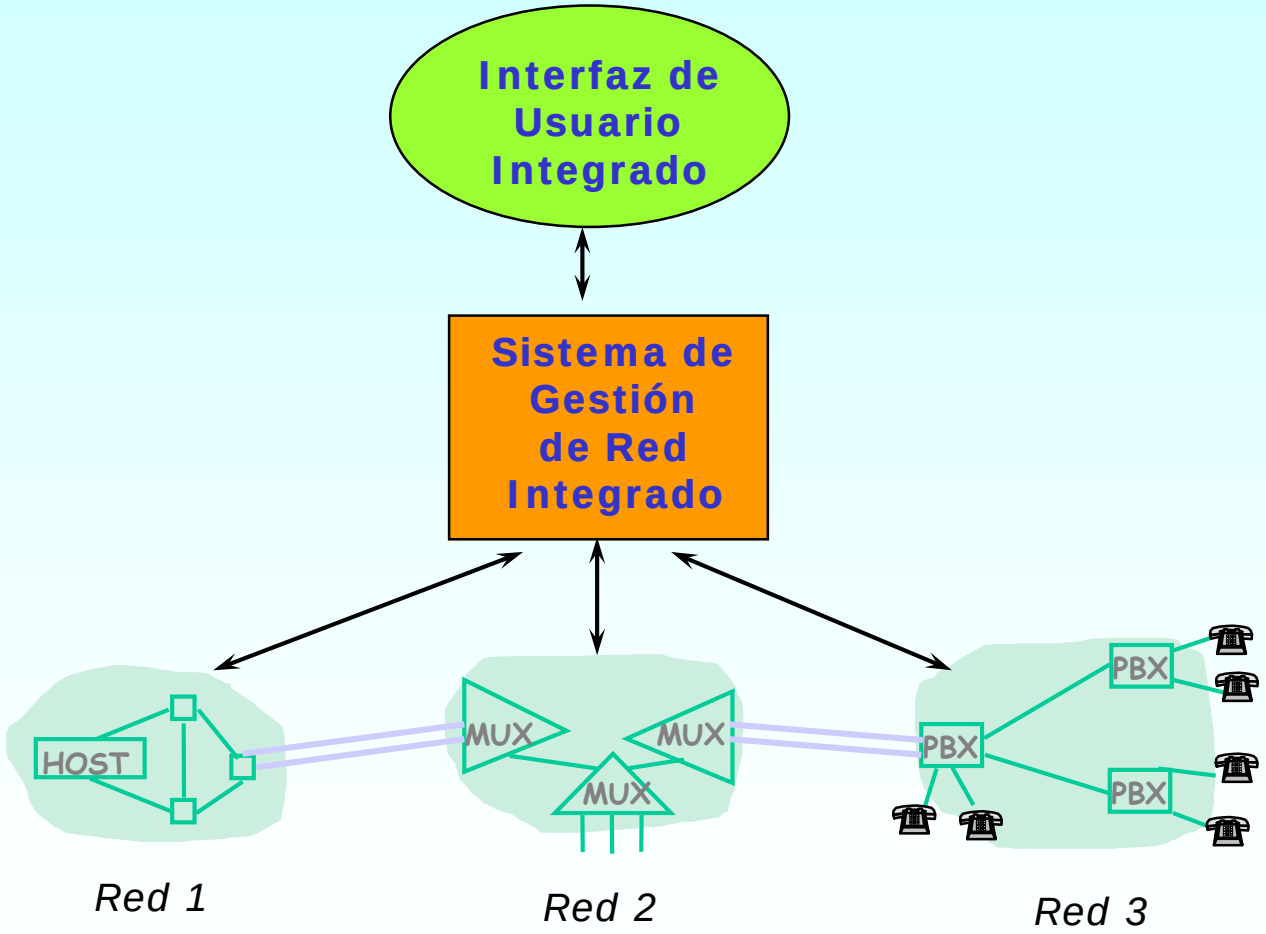


Consecuencias

- Plano de usuario (operador de red): Multiplicidad de interfaces de usuario.
- Plano de aplicación (de gestión): distintos programas de aplicación con funcionalidad similar.
- Plano de información (de gestión): duplicidad y posible inconsistencia de la información almacenada en las bases de datos.

Dificulta el cumplimiento de que la gestión de red sea efectiva en coste.

Gestión integrada



Requisitos de la gestión integrada

- Normalización de las comunicaciones.
  - Es necesario especificar un protocolo entre elemento de red y centro de gestión.
- Normalización de la información.
  - El centro de gestión debe conocer las propiedades de gestión de los elementos de red:
    - Su nombre
    - Formato de las respuestas
  - Definición sintácticamente uniforme de los elementos de red.

Modelos de gestión normalizados

- El objetivo es posibilitar el acceso uniforme a los recursos gestionados
- Se normaliza:
  - Protocolo de comunicaciones
  - Modelo de información de gestión
  - Definiciones de información de gestión
- Base de la gestión integrada

Modelos de gestión de red

ITU - T	Arquitectura *TMN*
ISO	Modelo de *Gestión OSI*
Internet	Modelo de *Gestión Internet*
Web	Modelo de *Gestión WBEM*

Orígenes:

- TMN: Gestión de las redes de telecomunicación
- Gestión OSI: Gestión de la torre de protocolos OSI.
- Gestión Internet: Gestión de routers.
- Gestión WBEM: Gestión basada en Web