

# Explotación de sistemas informáticos

Antoni Carmona i Damians

P03/75037/00697



# Índice


<b>Introducción</b> .....	5
<b>Objetivos</b> .....	6
<b>1. Escenarios de los entornos informáticos en producción</b> .....	7
1.1. Los sistemas de información actuales .....	7
1.2. Los sistemas distribuidos .....	10
<b>2. Diseño, implementación y explotación de un sistema de información para un entorno real</b> .....	13
2.1. Diseño y planificación de un entorno real .....	13
2.2. Implementación de un entorno real .....	14
2.3. La etapa de explotación: la gestión del sistema informático .....	16
2.4. Dimensiones vinculadas a la gestión de los sistemas de información distribuidos .....	18
2.5. El modelo OSI para la gestión de sistemas distribuidos .....	20
<b>3. Gestión de la configuración</b> .....	24
3.1. Introducción .....	24
3.2. Gestión de inventarios .....	28
3.3. Servicios de soporte a la topología del sistema distribuido .....	32
3.4. Gestión de los contratos de nivel de servicio .....	35
3.5. Gestión de partes de incidencias y problemas .....	42
3.6. Control de pedidos y aprovisionamiento .....	47
3.7. Gestión de cambios .....	50
3.8. Servicios de nomenclatura unificada .....	55
3.9. Control de la distribución de <i>software</i> .....	57
3.10. Otras subáreas incluidas en la gestión de la configuración .....	60
<b>4. Gestión de fallos</b> .....	62
4.1. Introducción .....	62
4.2. Problemas específicos de la gestión de fallos en los sistemas distribuidos .....	64
4.3. El esquema de los tres pasos de la gestión de fallos .....	67
4.4. Funciones y esquema general de la gestión de fallos .....	69
4.4.1. Supervisión del sistema distribuido y gestión de alarmas ....	69
4.4.2. Seguimiento y administración dinámica de incidencias .....	74
4.4.3. Medidas de contención inmediata y diferida .....	77
4.4.4. Diagnóstico definitivo, corrección y cierre del fallo .....	79
<b>5. Gestión de prestaciones</b> .....	82
5.1. Introducción .....	82


5.2. Problemas específicos con el rendimiento y prestaciones .....	83
5.3. Esquema general de la gestión de prestaciones .....	85
5.3.1. Definición de los indicadores de prestaciones .....	87
5.3.2. Características de los elementos de monitorización .....	92
5.3.3. Análisis y ajuste .....	93
<b>6. Gestión de seguridad .....</b>	<b>95</b>
6.1. Introducción .....	95
6.2. Conceptos referidos a la seguridad en entornos informáticos .....	96
6.3. Subáreas funcionales en la gestión de seguridad .....	99
6.3.1. Análisis de los riesgos .....	100
6.3.2. Análisis y diseño de los servicios de seguridad .....	102
6.3.3. Implementaciones y soluciones para los servicios de seguridad .....	103
6.3.4. Detección y actuación ante acontecimientos de seguridad .....	105
<b>7. Gestión de contabilidad .....</b>	<b>106</b>
7.1. Introducción .....	106
7.2. Esquema general de la gestión de contabilizaciones .....	108
7.2.1. Diseño y establecimiento de políticas de contabilización .....	109
7.2.2. Recaudación de información de utilización de recursos ....	110
7.2.3. Tarifación e imputación de costes .....	111
<b>8. Gestión de la planificación .....</b>	<b>113</b>
8.1. Introducción .....	113
8.2. Principales dificultades en la gestión de planificación .....	114
8.3. Esquema general y etapas de la gestión de planificación .....	116
8.3.1. Caracterización de la carga y análisis de tendencias .....	117
8.3.2. Análisis del mercado y estudio de alternativas .....	117
8.3.3. Diseño y configuración del plan de evolución .....	118
8.3.4. Realimentación del plan .....	119
<b>9. Tendencias futuras .....</b>	<b>120</b>
9.1. Nuevos requerimientos a los sistemas informáticos .....	120
9.2. Nuevas soluciones para la gestión de sistemas y telecomunicaciones .....	122
<b>Resumen .....</b>	<b>124</b>
<b>Bibliografía .....</b>	<b>125</b>

## Introducción

Este módulo didáctico trata de proporcionar los principales hechos que determinan la utilización de los sistemas informáticos, con toda su complejidad: la puesta en producción de estos sistemas para resolver diferentes problemáticas de gestión y tratamiento de información.

Se verá una introducción a las particularidades de los escenarios en los que se aplica, hoy en día, el proceso informático, y que comenta las características que los singularizan y las implicaciones que tienen en su explotación, siempre encaminadas a un criterio claro: mantener el nivel de servicio deseado.

Por otra parte, los aspectos de gestión de los sistemas informáticos actuales se han visto profundamente afectados por la inmersión de las tecnologías adelantadas de telecomunicación, que casi consolida de forma hegemónica los sistemas distribuidos, sistemas informáticos soportados con recursos y arquitecturas de redes, para cualquier escenario de aplicación. El modelo de gestión OSI, de cinco áreas funcionales principales, será la herramienta más importante de la metodología de explotación de sistemas informáticos, que permitirá introducir aspectos tan básicos como la gestión de seguridad, fallos o prestaciones en un sistema real en producción. 

Finalmente se verá una pincelada de la evolución de la gestión para los sistemas informáticos actuales y futuros, y las herramientas y procedimientos que tienen que gestionarlos. La complejidad aumenta con las fuertes implicaciones de la introducción de las tecnologías y formas propias de Internet en las organizaciones, los nuevos entornos de comercio electrónico y la multiplicidad de los equipamientos terminales de acceso a los sistemas de información. 

## Objetivos

Con los materiales didácticos de este módulo, el estudiante podrá alcanzar los objetivos siguientes:

- 1.** Tener una visión genérica de los escenarios en los que se aplican los sistemas informáticos.
- 2.** Conocer el modelo funcional del OSI para la gestión y administración de sistemas distribuidos.
- 3.** Aprender las diferentes tareas que se desarrollan dentro de la gestión de la configuración, fallos, prestaciones, seguridad y contabilizaciones en un entorno real.
- 4.** Estudiar los procedimientos utilizados a la hora de planificar y diseñar la evolución de un sistema informático.
- 5.** Conocer las tendencias futuras que se prevén en los sistemas informáticos y en las herramientas que los gestionan.

# 1. Escenarios de los entornos informáticos en producción

*“Los sistemas informáticos nos permiten hacer tareas que, hace simplemente unos años, sólo estaban en la imaginación o en los sueños de unos pocos. No imaginamos la pesadilla de no disponer de éstos. ¿O sí?”*

## 1.1. Los sistemas de información actuales

Que los sistemas informáticos se han convertido en un elemento cotidiano de nuestro día a día no sorprende a nadie. De hecho, ésta era la frase de moda a principios de los noventa. Y hace muchos años que trabajamos en la oficina frente a la pantalla de un ordenador, vamos al cajero automático para sacar dinero o para reservar una entrada de teatro y, más recientemente, nos conectamos desde casa a los servidores web de la Bolsa de Nueva York, mientras recibimos en el teléfono móvil el mensaje con las últimas cotizaciones.

Los escenarios en los que hoy se desarrollan los sistemas de información casi son infinitos: desde los simples ordenadores personales que tenemos en casa o las redes locales de unas decenas de usuarios que soportan las pequeñas y medianas empresas, hasta los grandes sistemas corporativos de entidades financieras, de multinacionales o de la Administración Pública, pasando por miles de tipologías en el sector industrial, el comercio y la distribución, la sanidad, el bienestar social o el ocio, los transportes y las comunicaciones, la investigación del medio ambiente o la carrera espacial, la seguridad o la defensa, entre tantos otros.

La diversidad es enorme. La comparación, a según qué orden, es inútil. Incluso no es extraño encontrar escenarios únicos con problemáticas específicas. Pero siempre, en cualquier caso, en la actualidad hay dos factores comunes entre todos éstos: la **complejidad** y la **dependencia**.

**a) Factor de complejidad:** la complejidad de los sistemas de información actuales es muy alta. Bien, es cierto que no son comparables las facilidades y ergonomía de trabajo que tiene, por ejemplo, un usuario cuando utiliza un entorno gráfico multiventana con capacidad multitarea de una increíble potencia y prestaciones y con ayuda concreta sensible al contexto, con respecto a las que disponía hace sólo unos años, con entornos texto, de proceso remoto, pesados y con poca o nula interactividad con sí mismo. Pero el precio, no sólo el coste, es alto.

La complejidad de los elementos físicos se ha incrementado de forma notable, especialmente, como veremos, los relacionados con las telecomunicaciones. Existen centenares de nuevas tecnologías aplicadas a los dispositivos informáticos que les ha permitido disponer de unas prestaciones que se duplican cada dos años o menos, y el coste de estas soluciones baja notablemente día a día

### La década de la sociedad de la información

Los desarrollos de las tecnologías de la información, TI, y la facilidad de las telecomunicaciones actuales son los factores que permiten hablar de **globalización**.

Si la década de los ochenta fue la del desarrollo de los ordenadores y la de los noventa la de las telecomunicaciones, ésta es la de la información ubicua, la de la sociedad de la información.

por los grandes volúmenes de fabricación. La fiabilidad de las tecnologías utilizadas también es creciente, pero también muchos más elementos dependen unos de otros para desarrollar su función, con lo que aumenta en consecuencia la criticidad global.

Sin embargo, es el *software* el elemento que ha experimentado un mayor aumento de la complejidad. La paralelización de infinidad de tareas, la potencia y versatilidad de los entornos gráficos o, simplemente, la búsqueda de la singularidad para distinguirse de la competencia han hecho que, en determinados casos, una herramienta ofimática o un sistema operativo de una estación hayan multiplicado por muchos cientos de veces el código necesario.

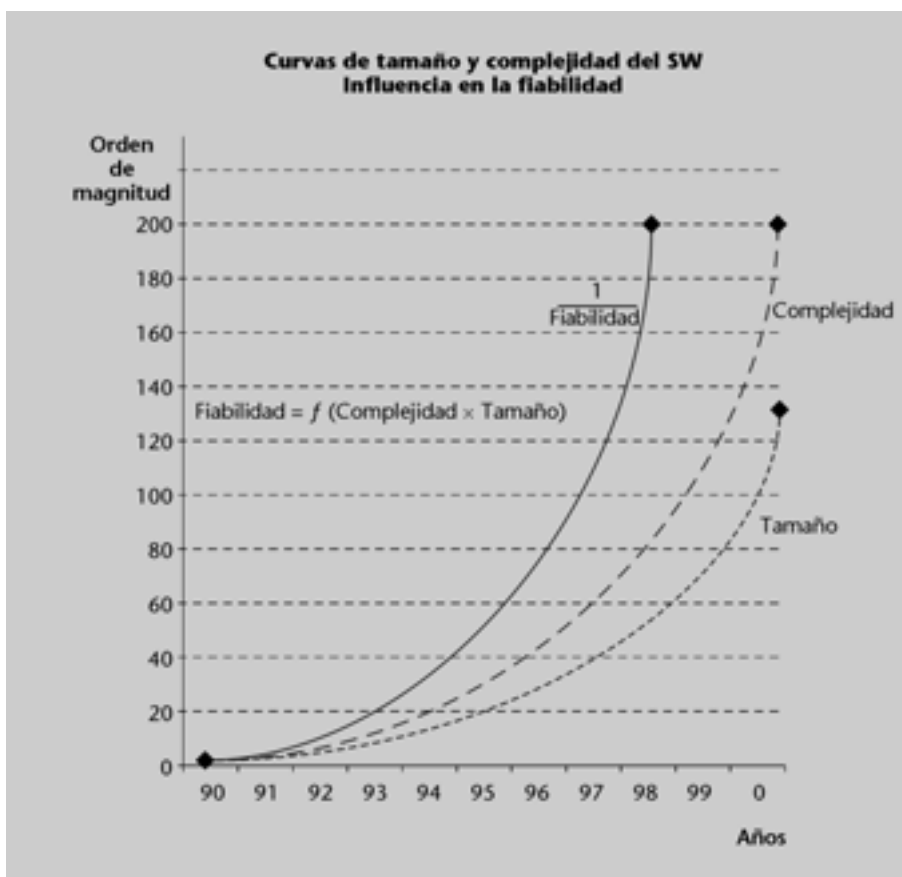
### Un caso de ejemplo de evolución del *software*

La siguiente gráfica muestra los resultados de un análisis que denota la evolución del *software* en los últimos diez años. Por una parte, el aumento cuantitativo, en líneas de código, ha comportado un incremento de entre cien y ciento cincuenta veces con respecto a lo que se necesitaba, lógicamente con una funcionalidad menor (pasar de un sistema operativo que cabía en un disquete a tener que disponer ahora de 200 o 300 MB para soportarlo).

Por otra parte, el grado de magnitud de la complejidad y la tecnología del mismo *software* también se ha multiplicado por cien con respecto a la que tenía hace diez años (cientos de productos conectados o relacionados, mecanismos de intercambio entre aplicaciones, complejos lenguajes de programación, ergonomía del usuario, tecnologías de objetos, comunicaciones y servicios distribuidos en línea, entre muchos otros).

El aumento de tamaño y complejidad hace que las posibilidades de errores se incrementen de forma espectacular, especialmente si se considera que la presión comercial del mercado y la competencia son muy altas y hacen que los productos salgan muy poco probados y verificados para la gran diversidad de escenarios que encontrarán.

Figura 1



Como resultado de todo ello, la función de criticidad aumentaría en un factor de 10.000 (?) en sólo diez años. Aunque en la realidad no existe una linealidad tan estricta, estas cifras proporcionan el grado de magnitud de lo vulnerable que puede ser la fiabilidad de los sistemas actuales.

**b) Factor de dependencia:** estamos acostumbrados a pulsar el botón de puesta en marcha de nuestro ordenador personal, esperar que se cargue el sistema gráfico comúnmente utilizado y disponer de nuestro “escritorio virtual” para que, cuando hagamos clic con el ratón, podamos desarrollar todas las tareas necesarias. No nos planteamos que vayamos al aeropuerto y los sistemas de despacho de billetes y facturación no funcionen y que los vuelos se suspendan uno tras otro. ¿Y a quién le pasa por la cabeza que puede estar un día sin teléfono en su empresa a causa de un “error informático” en el operador?

La dependencia de los sistemas informáticos hoy en día es total. Los sistemas de gestión de todas las organizaciones, grandes y pequeñas, los servicios y suministros básicos, las telecomunicaciones y los medios de transporte o la gestión económico-financiera mundial, como ejemplo, dependen por completo del hecho de que sus recursos informáticos sean totalmente operativos. Simplemente, no hay ninguna alternativa: si no hay sistemas, no hay actividad. En este supuesto no sólo entran en juego las pérdidas, mil millonarias en ocasiones, sino que también nos planteamos el hecho de si simplemente podemos permitirnos que estas cosas ocurran.

#### Un caso de ejemplo: el efecto 2000

El despliegue de acciones preventivas y correctivas y la implantación de mecanismos y procedimientos de contención, impulsados a causa del fatídico **efecto 2000**, no han tenido (como casi todo, también se tiene que decir, en el mundo informático) precedente en la historia, y se espera que no vuelva a suceder un hecho de efectos y consecuencias similar. Aunque había incertidumbre sobre los efectos en los sistemas “empotrados”, la gran preocupación se centraba en confirmar si se habían detectado y corregido de forma conveniente todos los puntos de error en los grandes sistemas de información.

El riesgo de que se produjeran situaciones de emergencia, incluso algunas a escala mundial, justificó los más de cincuenta billones de dólares invertidos en todo el mundo para corregir el efecto (muchas organizaciones que planificaron con una serie de años los trabajos aprovecharon para rediseñar, modernizar y mejorar sus sistemas básicos). Y la presencia, ya en el año 2000, sólo de centenares y centenares de anécdotas, y ninguna catástrofe, los justifica completamente.

Los costes de no disponer de los sistemas no son despreciables, sobre todo en áreas que están intrínsecamente relacionadas con el tema, como algunas basadas en la globalidad de la información. El 8 de febrero de 2000, los servidores corporativos de Yahoo, uno de los principales portales de búsqueda de contenidos en Internet, sufrieron un ataque muy bien planificado que los dejó no operativos durante tres horas y quince minutos. Las pérdidas acumuladas durante este tiempo anunciadas por la compañía ascendieron a ochenta y cinco mil millones de dólares (?).

Las conclusiones a las que se llega no tienen que ser, en absoluto, catastrofistas. Sin embargo, ilustran la importancia que tendrán la gestión y la administración adecuada de los sistemas informáticos en producción, que engloban todas las medidas y acciones dirigidas a mantener la actividad que se espera de éstos.

#### Inicios fáciles, vida complicada

Hace años las principales dificultades para disfrutar de una estructura informática adecuada estaban en las etapas de adquisición e implantación, que concentraban gran parte del coste y las dificultades principales.

Sin embargo, hoy en día el problema no es implantarla, sino mantenerla perfectamente operativa, y es donde se concentra la mayor parte del coste y las dificultades.

#### Filosofía práctica “en tiempo real”

Un director de informática de una gran instalación comentaba a su personal, en los momentos en que concurrían muchas circunstancias problemáticas, seguramente en los más críticos, lo siguiente:

“Yo no invento el escenario, me toca vivir en él igual que a vosotros y, ya que no puedo cambiarlo, nos adaptaremos al mismo tanto como se pueda”.

Mientras tanto diseñaba con sus expertos los mejores métodos de contención y resolución.

Éste es el objetivo común a todos y cada uno de los escenarios en los que utilizamos, y utilizaremos, los sistemas informáticos.

## 1.2. Los sistemas distribuidos

La generalización de las telecomunicaciones informáticas ya se ha consolidado. Los sistemas informáticos, los ordenadores, los sistemas personales, ya no tienen sentido si no están “conectados”.

### La generalización de las telecomunicaciones

En una oficina, la estación de trabajo de un usuario contiene pocos datos y aplicaciones o ninguno, porque está conectada a una red local que permite acceder a una infinidad de servidores de aplicación, servidores de datos, recursos periféricos como impresoras o escáneres, o sistemas de información remotos en otras sedes de la corporación. Los terminales de unos grandes almacenes se conectan con complejos sistemas de control de *stocks*, y los terminales bancarios permiten la validación y proceso de crédito simplemente pasando la tarjeta. La agencia de viajes accede a pesados sistemas en línea para las reservas en infinidad de compañías aéreas, hoteles, alquiler de coches y otros servicios. E, incluso, desde casa nos conectamos a Internet para acceder a una biblioteca virtual y adquirimos el último libro de moda, que recibiremos pasado mañana.

La relación de las telecomunicaciones en los sistemas de información es tan grande que ya no se puede hablar de desatar sus objetivos respectivos. De hecho, la relación es mutua y en las dos direcciones, y así se puede ver en los dos focos siguientes:

**a) Inmersión de las telecomunicaciones en los sistemas informáticos:** es el ámbito más conocido, por lo que, hoy en día, ya hablamos siempre de “informática ubicua”. Algunos de los hechos más representativos son los siguientes:

- La utilización y el avance en las tecnologías de transmisión, cada vez de mayor capacidad y fiabilidad frente a errores\*.
- El abaratamiento de los costes de telecomunicación, gracias al desarrollo tecnológico y el aumento de la oferta del mercado.
- Las ventajas de compartir recursos entre usuarios, departamentos o unidades de las organizaciones, tanto desde el punto de vista de rentabilidad económica como de poder disponer de recursos redundantes o alternativos (ya no depende del mismo puesto de trabajo concreto, si tiene una avería, y se pueden utilizar elementos alternativos en el mismo lugar o en otros).
- Las comunicaciones sobre LAN, MAN o WAN permiten distribuir servicios y aplicaciones a servidores y sistemas especializados, pero también concentrar servicios comunes en pocas grandes unidades (la distribución especializada y la concentración de servidores son dos técnicas opuestas, pero que

### ¿Estamos poco “conectados” todavía?

Los expertos dicen que todavía estamos poco conectados. Si los sistemas corporativos de gestión de las compañías están basados totalmente en las comunicaciones y la filosofía distribuida, la explosión de Internet anuncia que habrá cientos de miles de nuevos terminales, *set-top boxes* para televisión, teléfonos móviles o dispositivos domésticos, que disfrutarán de los servicios de comercio electrónico (*e-commerce*) y de las relaciones negocio a negocio (*business to business*) o B2B.

\* La utilización de la fibra óptica es un paradigma de este hecho.

### Incremento de los operadores de telecomunicaciones

En España se ha pasado de un solo operador a disponer de casi una docena de tipo global o general, además de muchos otros para servicios concretos.

se conjugan y equilibran de forma adecuada en los nuevos entornos para rentabilizar y simplificar la gestión).

- Las telecomunicaciones informáticas, como base de desarrollo y relación comercial, están entrando radicalmente en las organizaciones, que potencian este nuevo “frontal” de negocio o actividad que se les abre con un enorme potencial (no es preciso reiterar lo que es y significa Internet).

#### Informática e ingeniería de telecomunicaciones

Todavía hay personas reticentes, pero los ingenieros de informática y de telecomunicaciones están destinados a trabajar juntos.

**b) Inmersión de la informática en las telecomunicaciones:** hace unos cuantos años, nadie se confundía al distinguir un objeto del mundo de las telecomunicaciones (la tecnología necesaria para transportar electrónicamente información de un lugar a otro) y uno de la informática (procesar sistemáticamente datos con medios electrónicos mediante algoritmos previos, para obtener unos resultados determinados). Y la razón de ello era simple: las telecomunicaciones utilizaban técnicas “analógicas” para desarrollar su cometido, mientras que la informática era la reina del “mundo digital”, de los unos y los ceros, de los bits y los bytes. Pero los hechos son los siguientes:

- Las telecomunicaciones descubrieron las ventajas de la transmisión digital, especialmente cuando apareció una tecnología eficaz y barata para digitalizar todo lo que teníamos del mundo analógico, como la voz, las imágenes, el vídeo en tiempo real o la señal de televisión. Y, cuando la transmisión es digital, realmente son los ordenadores los que hablan entre sí. ¿Dónde acaban y empiezan, pues, unos y otros?
- La utilización de las técnicas digitales ha permitido multiplicar la cantidad de información que se puede transportar por un medio de manera analógica y aumentar de forma considerable el ancho de banda efectivo del que se dispone. Un enlace digital de televisión puede transportar el equivalente a cinco canales analógicos, y una sola línea de enlace digital de telefonía puede transportar de treinta a cien llamadas de voz, cuando antes sólo era posible transportar una.
- La transmisión digital de contenidos concurrentes de datos, voz, imagen y otros servicios hace que se reduzcan los picos y los valles de utilización que tanto afectan a la eficiencia y, por lo tanto, a la rentabilidad de un enlace.
- Los elementos terminales en la transmisión digital son verdaderos sistemas informáticos especializados y disfrutan de las facilidades de éstos por ser flexibles de configurar y actualizar mediante el *software* de sistema que los controla. Además, es fácil disfrutar de las facilidades de redundancia y tolerancia a fallos que caracterizan los entornos informáticos críticos.

Por todo lo expuesto, especialmente al tratar de los sistemas informáticos actuales, se habla cada vez con más frecuencia de sistemas informáticos distribuidos o, simplemente, de **sistemas distribuidos**, para denotar todos los

escenarios en los que tenemos informática o telecomunicaciones. Éste será un término muy utilizado a lo largo de los próximos capítulos y debemos habituarnos a utilizarlo.

### ¿Acabaremos “digitalizados”?

La **digitalización**, proceso mediante el cual una información o medio de tipo analógico es capaz de convertirse en ceros y unos y almacenarse dentro de la memoria de un ordenador o dispositivo similar, ha sido uno de los hechos de moda a finales de la década de los noventa.

Ya quedan lejos los primeros CD musicales, que decían que “se leían con láser”.

Hoy, la telefonía, fija y móvil, el mundo del audio, la imagen o la televisión disfrutan totalmente de ello. Ya veremos hasta dónde estamos digitalizados.

#### Un precursor

Scott MacNealy, presidente ejecutivo y CEO de SUN Microsystems, previó en 1989 que avanzábamos hacia la sinergia de las redes y los ordenadores. Su frase “The network is the computer” se ha convertido en uno de los paradigmas de la época actual.

## 2. Diseño, implementación y explotación de un sistema de información para un entorno real

Como hemos visto, la potencialidad de un sistema informático actual, que sin lugar a dudas será un sistema distribuido, es muy alta. También lo es, no lo olvidemos, su complejidad.

Consultad el tema de la potencialidad de los sistemas informáticos en el apartado 1 de este módulo didáctico.

No debemos perder nunca de vista que un sistema informático, sea cual sea su alcance, extensión o complejidad, se diseña, implanta y opera para un fin concreto, para un uso determinado. Y entre otras razones, este hecho se debe sobre todo a que no es gratuito. En el mundo real no existen los sistemas informáticos *per se*, las “simples implantaciones de prueba” o las configuraciones idílicas que no prevean siempre el equilibrio entre las prestaciones y el coste, adecuado a unos requerimientos determinados.

### Un axioma para recordar

Muchos administradores de sistemas de información cuelgan, en un lugar visible, un axioma que no tienen que olvidar: “En informática siempre hay algo más rápido, más potente, más moderno, y también más caro, que lo que compras. Uno mismo tiene que saber hasta dónde es suficiente”.

### 2.1. Diseño y planificación de un entorno real

La implantación de recursos informáticos en una organización responde a una especificación de necesidades y requerimientos por parte de los usuarios que tienen que disfrutar de éstos y que aportan como resultado la capacidad para utilizar o mejorar procesos determinados.

A partir de estos requerimientos de usuario, los ingenieros de sistemas, o los administradores si se da el caso, diseñarán el **plan del sistema** y procurarán satisfacer al máximo las necesidades, normalmente desde un marco corporativo, no como un conjunto de soluciones aisladas. Es importante la participación activa de los usuarios en esta etapa, así como modelar y adaptar los métodos y soluciones más adecuados, pero sin caer en problemas de “personalización” de soluciones, frecuentes con usuarios sin capacidad de visión corporativa y diseñadores inexpertos.

El **diseño de un sistema** puede prever diferentes grados de alcances, desde el necesario para un entorno no mecanizado, en el que se implantan por primera vez herramientas informáticas (este escenario es ya poco probable hoy en día), a los de actualización y ampliación de entornos complejos ya existentes. Es posible que los cambios que hay que hacer no estén impulsados directamente por los usuarios, sino por los mismos administradores, por razón de actualizaciones, mantenimientos o modificaciones para obtener más prestaciones o fiabilidad.

### Las tareas de planificación

La planificación de nuevos sistemas, o las adaptaciones de los ya existentes, es una tarea que se contrata, en ocasiones, a externos, especialmente si implican elevada complejidad y especialización, que no puede ser adecuadamente cubierta por recursos internos. En estos casos la coordinación con la dirección corporativa debe ser exhaustiva.

En cualquier caso, la **planificación** deberá contener todas las especificaciones de requerimientos y necesidades, y cómo se soportarán con el nuevo sistema con todos los detalles referidos al tipo de elementos, infraestructuras y configuraciones necesarias, redes y otros elementos de telecomunicación, usuarios y recursos implicados. También contará con un estudio de impacto de la implantación en la misma organización y un detallado calendario de hitos y objetivos.

A partir del cierre del plan, las tareas de los ingenieros y administradores se centran en tres ejes objetivos concretos: la **instalación de elementos**, el mantenimiento de los sistemas en producción (tradicionalmente conocido como **explotación**) y la **solución de los problemas** que puedan aparecer.

#### Lenguaje coloquial

Instalar, mantener y resolver se conocen, coloquialmente hablando, como los “deberes de los administradores informáticos”.

## 2.2. Implementación de un entorno real

Como se ha comentado, la planificación adecuada para el despliegue o modificación de un sistema informático será esencial para conseguir el correcto apoyo mecanizado a los requerimientos, así como la no superación de los hitos adecuados, principalmente el tiempo y, sobre todo, el coste.

Los ejes objetivos básicos de instalación, explotación y reparación se articulan sobre cinco tareas, conocidas como las **tareas del ciclo de vida de un sistema** y que son los siguientes:

1) **Construcción/instalación**: a partir de la planificación del sistema informático se determinarán los elementos concretos, infraestructuras, *hardware* y *software*, que tienen que dar apoyo a los servicios requeridos. Es muy habitual que en esta etapa haya gran cantidad de “terceros” involucrados, contratados o subcontratados, especialmente con tareas de instalaciones, cableados o enlaces, entre otros. Su dirección y coordinación son esenciales para conseguir los objetivos deseados.

2) **Mantenimiento**: las tareas de mantenimiento engloban todas las operaciones que se tienen que hacer en el sistema informático para garantizar el nivel de servicio y el nivel operacional. El mantenimiento tiene un único objetivo preventivo, no correctivo.

En cualquier entorno informático, especialmente en los sistemas distribuidos, siempre se realizan tareas de mantenimiento. Pueden ser cambios de componentes *software* por razón de actualizaciones forzadas (*software* que se descataloga, etc.) o actualizaciones de mejora funcional (nuevas versiones con más prestaciones, etc.). También se incluyen las actualizaciones *hardware* para mejorar prestaciones (cambio de CPU, placas y/o, etc.) o por mantenimiento físico preventivo (cambio de unidades de discos, después de un periodo largo en

La contratación de servicios externos se amplía de forma conveniente en el apartado 3 de este módulo didáctico.

#### Mantener ≠ corregir

Con frecuencia, por la misma extensión del lenguaje, se agrupan dentro de las tareas de mantenimiento las operaciones de corrección y resolución de fallos o problemas y otras tareas de apoyo. Pero es un error.

El mantenimiento, en los sistemas informáticos, siempre es una medida preventiva en estado *non defecto* (sin fallo).

servicio y antes de que tengan problemas, cambio de ventiladores, limpieza de filtros, etc.).

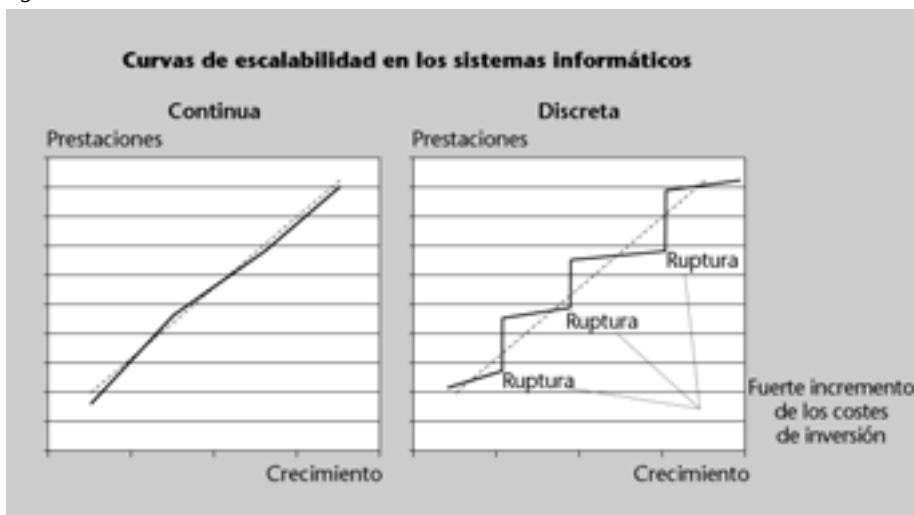
3) **Expansión/crecimiento:** en general, todos los sistemas informáticos se expanden, aunque sólo sea por crecimiento vegetativo, que es el de la misma actividad de los aplicativos del sistema, como el incremento de documentos, el aumento de los apuntes contables o las relaciones de nóminas, entre muchos otros.

Si las tareas asociadas a la expansión y crecimiento están bien planificadas, el sistema contará con una **escalabilidad** adecuada. La escalabilidad es una medida que determina si un sistema informático es capaz de crecer de manera no traumática (imposibilidad, rediseño o cambio total). Una instalación puede disfrutar de una escalabilidad continua si los cocientes entre crecimiento de prestaciones y coste tienen una continuidad más o menos lineal. Estas curvas coinciden normalmente con una instalación basada en sistemas distribuidos abiertos, poco vinculados a soluciones propietarias.

#### Una buena planificación

Los expertos coloquialmente dicen que “un sistema bien planificado se queda pequeño cuando sea necesario”.

Figura 2



Por el contrario, las instalaciones típicas basadas en entornos centralizados, más o menos propietarios, suelen tener curvas de escalabilidad discretas, con notables incrementos de coste cuando se tienen que hacer ampliaciones.

4) **Optimización/mejora/adequación:** las tareas de optimización permiten mantener una curva ascendente de prestaciones a medida que la carga del entorno varía o crece. En los sistemas centralizados son tareas necesarias que permiten mantener una determinada ventana de escalabilidad.

Sin embargo, en los sistemas distribuidos las tareas son imprescindibles para detectar y prever a tiempo los cuellos de botella\*, que pueden aparecer a causa de la gran cantidad de elementos involucrados. Disponer de información actualizada mediante los elementos de monitorización será esencial.

Consultad una ampliación sobre la optimización, mejora y adecuación de los sistemas en el apartado 5 de este módulo didáctico.

\* En inglés, *bottlenecks*.

5) **Resolución de problemas:** los sistemas de información están basados en tecnología y, obviamente, no están exentos de problemas. Aunque el *hardware* es cada día más fiable, se pueden producir averías; algunas tecnologías e infraestructuras de redes y enlaces son especialmente sensibles a ello. Pero la principal causa de problemas en los sistemas informáticos actuales se debe al *software*, tanto por errores de código como por interacción entre diferentes aplicativos, y siempre son muy difíciles de prever.


Consultad una ampliación del tema de la resolución de problemas en el apartado 4 de este módulo didáctico.

La condición esencial será la implantación de una buena política de prevención, basada en un adecuado análisis de riesgos, y de las medidas correctas para minimizar los efectos cuando hay problemas.

Aunque estas tareas se ordenan de forma más o menos secuencial en el caso de una nueva implantación, la casuística real de la evolución del entorno hace que se paralelicen a lo largo del ciclo operacional en producción.

### 2.3. La etapa de explotación: la gestión del sistema informático

La etapa de explotación de un sistema informático corresponde a la del funcionamiento estable del sistema, totalmente implantado y configurado y con una carga igual a la real, es decir, si cumplimos los requerimientos funcionales y las ventanas de servicio para las que se ha diseñado.

Una organización genérica puede disponer, como suele ser habitual, de dos entornos en explotación o más. Este hecho implica sistemas más o menos equivalentes desde el punto de vista funcional, en el que sólo uno de éstos es el real y recibe el nombre de **entorno de producción**. 

#### Explotación ≠ producción

Es corriente, incluso para profesionales experimentados, significar *a priori* la igualdad de los dos términos, que sólo se cumple si precisamente hay un único sistema.

Los responsables de explotación en organizaciones grandes, como una entidad financiera, tienen muy clara la diferencia: el personal de sistemas o de desarrollo puede hacer lo que quiera con los sistemas secundarios, si así es oportuno, pero, en condiciones estables, no les dejarán ni "acercarse" al entorno de producción.

Los casos más frecuentes son aquellas instalaciones en las que se dispone de un segundo sistema, con datos totalmente copiados de los reales y, en ocasiones, sincronizados con el primer sistema de forma unidireccional, sobre el que se hacen las tareas de desarrollo y pruebas.

Al ser este entorno una copia del primero, a efectos prácticos, los perfiles de carga son los reales, pero no hay ningún peligro de afectar al nivel de servicio del entorno principal, el de producción, si se produce un fallo de programación o un caso no previsto que degrade, por ejemplo, una base de datos.

También son frecuentes las instalaciones de misión crítica que disponen de un segundo sistema en explotación que puede asumir las tareas de producción si el sistema principal cae o tiene un problema. Este mecanismo de

contención se compagina, en ocasiones, con el escenario anterior, de entorno de test.


La **gestión de un sistema informático** incluye todas las medidas necesarias para asegurar la efectiva y eficiente operación del sistema informático en producción, sus recursos y sus servicios, de acuerdo con los objetivos corporativos marcados en la organización.

En los casos actuales, la intención de la gestión de los sistemas distribuidos es la de proporcionar un conjunto de herramientas, mecanismos y procedimientos que permitan el apoyo de los servicios y aplicaciones que se ejecutan sobre el sistema distribuido, con el grado de calidad y prestaciones deseado, que denominaremos, genéricamente, el **nivel de servicio** requerido o **QoS\***.

En los apartados 4 y 5 de este módulo didáctico se profundizan los conceptos asociados al nivel de servicio.

\* QoS es el acrónimo de la expresión inglesa *Quality of Service*.

Así pues, en términos generales la gestión incluirá la coordinación de personal, procedimientos y aplicaciones, así como los mecanismos, herramientas, elementos, servicios y recursos que están involucrados en la cadena de producción.

Según las prioridades y el foco de cada conjunto de tareas incluidas, la **gestión de sistemas distribuidos** se subdivide, en ocasiones, en los grupos siguientes: 

- 1) **Gestión de la red:** cuando el foco es la gestión de los servicios de comunicación, así como de todos los recursos, infraestructuras, enlaces, electrónica de red y elementos *hardware* y *software* relacionados.
- 2) **Gestión de sistemas:** cuando el foco es la gestión de los elementos de proceso y elementos finales de usuario, físicos y lógicos, que están soportados sobre las redes. Se incluirán las tareas de gestión de los servidores, la CPU, el *software* de base, los periféricos, los equipos terminales, los procesos y los usuarios, entre muchos otros.
- 3) **Gestión de servicios:** cuando la focalización está orientada a requisitos comunes de establecimiento y mantenimiento de la operación. Algunos ejemplos son el almacenamiento de datos, la distribución del *software* remoto, el control de licencias y el control de incidencias, alarmas y estados del sistema, entre otros.
- 4) **Gestión de aplicaciones:** responsable de las aplicaciones de producción de la organización, que asegura que se cumplen las condiciones de “usabilidad” marcadas en los objetivos.

5) **Gestión de información:** aquellas tareas orientadas al diseño y mantenimiento de la información corporativa a lo largo del sistema, que marcan las pautas de distribución, disponibilidad y accesibilidad adecuadas.

El tipo de escenario, los requerimientos y objetivos o las características tecnológicas marcarán cómo se priorizan estas funciones de la gestión. Pero, más o menos desarrolladas, siempre estarán todas incluidas.

## 2.4. Dimensiones vinculadas a la gestión de los sistemas de información distribuidos

Como se ha visto, la multitud de escenarios diferenciados sobre los que se desarrollan hoy los sistemas distribuidos son muy numerosos. Los diferentes aspectos que tienen un papel determinante también lo son. Y los objetivos del servicio mecanizado y de su calidad, la topología y distribución física y geográfica de los diferentes sitios, las tecnologías utilizadas por la organización, la utilización de servicios de telecomunicación de terceros o la organización del personal informático de apoyo del que se dispone son sólo una pincelada de criterios y factores tecnológicos involucrados, además de su complejidad intrínseca.

Sin embargo, en la vertiente no propiamente tecnológica, cada vez más los objetivos empresariales o corporativos que justifican la existencia de los sistemas, las implicaciones con la gestión corporativa que incluyen las tareas económicas y financieras, la gestión de los recursos humanos, la simple gestión de producción con respecto a las líneas y procesos de negocio o, simplemente, la moda o la imagen que se quiere dar, entre muchos otros, influyen sobre cómo se diseñan, implantan y gestionan aquellos sistemas de información.

Así pues, la complejidad de la gestión de los entornos distribuidos hace obvio pensar que no hay una, y sólo una, solución de gestión que se adapte a todas las situaciones, por lo que éstas se tendrán que adaptar y configurar para cada escenario en particular.

De hecho, la definición de los criterios decisorios sobre los que se basa un modelo de gestión no puede ser única. La especificidad que cada escenario impone sólo se puede modelar y prever con diferentes **planes**, cada uno con un foco multidimensional, que especifica sobre los ejes criterios relevantes que pueden variar a lo largo del tiempo.

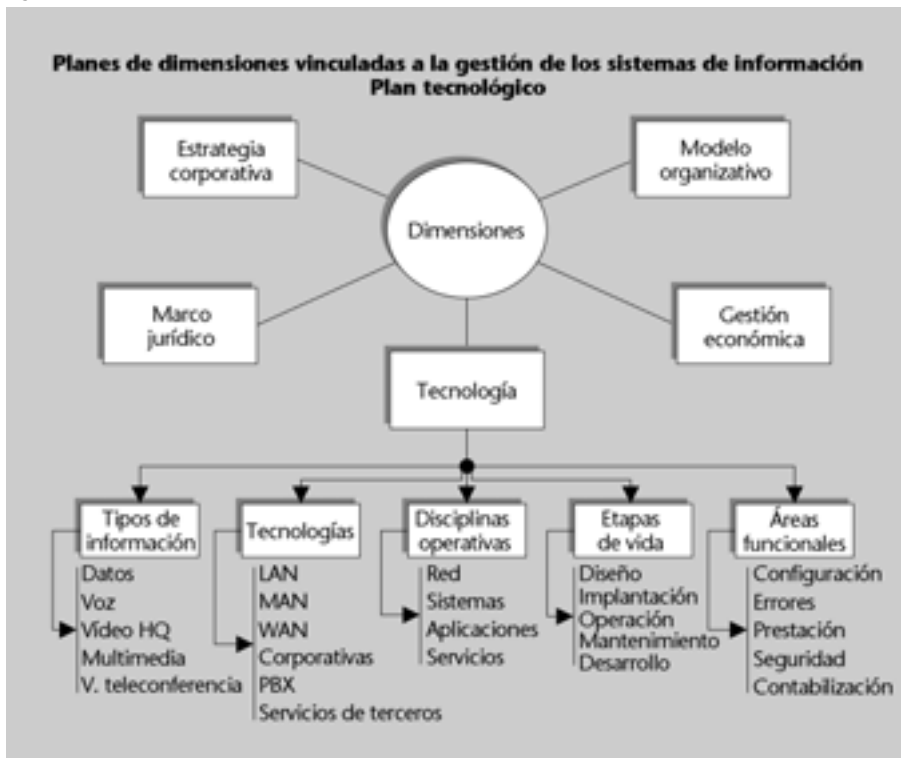
Consultad los conceptos de QoS en el subapartado 2.3 de este módulo didáctico.

### ¡No sólo tecnología!

Los tecnólogos caen con frecuencia en el error de pensar que las problemáticas de gestión de los sistemas distribuidos en una organización son una cuestión tecnológica, que implica los recursos tecnológicos y que sólo se resuelve con tecnología. Los fracasos estrepitosos en la implantación o en la idoneidad de sistemas distribuidos tienen aquí una de sus causas principales.

Así, habrá un plan con dimensiones que reflejen en sus ejes aspectos de la estrategia corporativa de la organización, otro referido al modelo organizativo que despliega la corporación o también los referidos a aspectos de gestión económica o marco jurídico, entre otros. Evidentemente, habrá un plan de dimensiones tecnológicas en el que los criterios de relevancia de los ejes incluyen los criterios familiares en la implantación de tecnologías de la información.

Figura 3



Algunas de las dimensiones que se consideran en el plan tecnológico incluyen, entre otros, aspectos como los siguientes:


- Naturaleza del tipo de información: datos, voz, vídeo de teleconferencia, vídeo de alta calidad, multimedia, etc.
- Las tecnologías utilizadas, como los tipos de redes: LAN, MAN, WAN, redes corporativas, PBX, servicios de terceros, etc.
- Las disciplinas operativas de gestión en entornos informáticos: gestión de elementos de red, gestión de sistemas, gestión de aplicaciones, gestión de servicios, etc.
- El estado en las etapas de vida: diseño, desarrollo, implantación, operación, mantenimiento, etc.
- Las áreas funcionales: configuración, prestaciones, fallos, seguridad, contabilización.

## 2.5. El modelo OSI para la gestión de sistemas distribuidos

A finales de los ochenta, la ISO (International Standards Organization) continuaba con los trabajos englobados dentro de las tareas de normalización que definía y establecía el estándar OSI (Open Systems Interconnection), con la intención de poner orden en el mundo de las tecnologías de la telecomunicación y la información, cada vez más caótico.

En aquellos momentos, los esfuerzos se centraron en definir una propuesta de clasificación de las tareas asociadas a la gestión de sistemas distribuidos. El objetivo era garantizar un elevado grado de interoperatividad al desarrollar e implantar tareas de gestión en los incipientes sistemas abiertos multivendedor.

Después de diferentes propuestas, el modelo de referencia OSI para la gestión de sistemas distribuidos fue definido en torno a una clasificación funcional en cinco áreas. Mediante esta división se conseguía agrupar una serie de subfunciones y tareas muy definidas en cada área funcional, que, a la vez, eran soportadas por un conjunto de procesos y procedimientos, normalmente mecanizados, en cada implementación real.

Las cinco áreas funcionales, también conocidas como **subsistemas de gestión**, son las siguientes: 

1) **Gestión de la configuración:** agrupa un conjunto de actividades de ámbito general en la organización sobre sus sistemas distribuidos, orientados al control de todos los elementos involucrados. Se gestionan los inventarios físicos, los inventarios eléctricos y recursos de comunicación y los inventarios lógicos, tanto los de *software* de base como los de aplicación y utilidades. Se incluyen las tareas de identificación, recopilación de datos, suministro de información de elementos y el apoyo que asegura la operación continua de los servicios de conexión. Asimismo, está dentro de su alcance el control de aprovisionamientos, pedidos, proveedores, contratos, mantenimientos y apoyos, la gestión de los “informes de problemas”\* y la gestión de cambios y distribución de *software*.

La información proporcionada por el área de configuración es esencial para todas las demás áreas funcionales.

2) **Gestión de fallos:** incluye el conjunto de actividades encargadas de mantener dinámicamente, en fase de producción, el nivel de servicio, **QoS**, requerido. Estas actividades incluyen inicialmente todas las tareas que aseguren una alta disponibilidad de los recursos y proporcionen herramientas que permitan la rápida creación de la alarma, la detección y la diagnosis de cualquier acontecimiento o *event* que afecte al nivel de servicio mencionado.


### El modelo OSI

El modelo de referencia OSI, o modelo OSI, estableció un esquema multinivel, las siete capas (*layers*), en el que definía para cada una de éstas las funciones que se tenían que desarrollar en los equipos que establecían la comunicación, así como las estructuras de datos que se intercambian ambas capas homónimas. (Encontraréis más información del modelo OSI en la asignatura *Redes de computadores*.)

### OSI Management Framework

El OSI Management Framework es una parte del OSI Basic Reference Model, regulado en ISO/IEC 7498-4, ISO/IEC 10040 e ISO/IEC 10164-1.

\* En inglés, *trouble tickets*.

 Consultad los conceptos asociados al nivel de servicio en el subapartado 2.3 de este módulo didáctico.

Además, se soportan el diseño y la activación de las medidas de contención del fallo, que permitirán continuar dentro de una determinada ventana de QoS, mediante una estructura de recursos redundantes, aislamientos, copias de seguridad, etc. Finalmente, también forman parte de esta gestión todas las tareas de recuperación que permitirán volver al estado inicial, previo al fallo, con los cambios correspondientes, así como el control de los *logs* y la gestión y actualización de los manuales de actuación.

Una correcta gestión de fallos en un sistema distribuido reduce la posibilidad de que suceda un fallo, y si ocurre, disminuye sus efectos y reduce los tiempos de resolución.

3) **Gestión de prestaciones\***: incluye las facilidades que permiten controlar el comportamiento de los elementos de un sistema informático distribuido en producción, verificar que los niveles de servicio requeridos se cumplan y proporcionar dinámicamente toda la información sobre cómo está trabajando, la efectividad de los recursos que están involucrados y su capacidad utilizada. La información es muy valiosa para detectar o prevenir situaciones de sobrecarga o saturación, que podrían ocasionar un fallo que afectara al QoS. Además, los datos de los parámetros de prestaciones permiten evaluar comportamientos, planificar cambios y ampliaciones, ayudar en la toma de decisiones mediante monitorizaciones y comparaciones y detectar *cuellos de botella* y situaciones de riesgo. Se gestionan también todos los medios de automatización de las monitorizaciones y ajuste\*\*, así como los manuales de procedimientos de evaluación y análisis.

\* En inglés, *performance*.

\*\* En inglés, *tuning*.

La adecuada gestión de las prestaciones de una instalación permite acotar las dificultades de previsión de la carga en un entorno real, adaptar y adecuar los recursos mecanizados a su mejor funcionamiento y, por lo tanto, rentabilizar la inversión financiera en recursos, maximizar su utilización y rendimiento y alargar su periodo de vida operativa.

4) **Gestión de seguridad**: define el conjunto de funciones que aseguran la protección del sistema distribuido en los aspectos de la seguridad informática, basada en los tres criterios de disponibilidad, integridad y confidencialidad. La gestión de la seguridad física y lógica, de las medidas de seguridad activas y pasivas, el análisis de riesgos y su impacto, su minimización, la elaboración e implantación del plan de seguridad en la organización, las tareas administrativas de partición, autorización y vigilancia o la monitorización de violaciones con el levantamiento de alarmas y el seguimiento del éxito de las políticas de seguridad son tareas incluidas en esta área.

La aplicación de las funciones de la gestión de seguridad permite disponer de un entorno en producción “seguro”, ante causas fortuitas y perjuicios y circunstancias intencionadas: muy pocas organizaciones no necesitan y exigen esta garantía.

5) **Gestión de contabilizaciones\***: reúne el conjunto de procesos encargados de la recopilación, anotación, interpretación, procesamiento y facturación, si procede, en la utilización colectiva de recursos de un sistema distribuido. Los nuevos entornos, con una gran orientación a la utilización de recursos comunes, necesitan sistemas de contabilización que cuantifiquen de forma adecuada quién utiliza cada recurso, para poder justificar las respectivas inversiones. Por otra parte, gran cantidad de la información recogida es útil en las áreas de gestión de prestaciones, seguridad y fallos, así como para la planificación de la evolución del entorno distribuido.

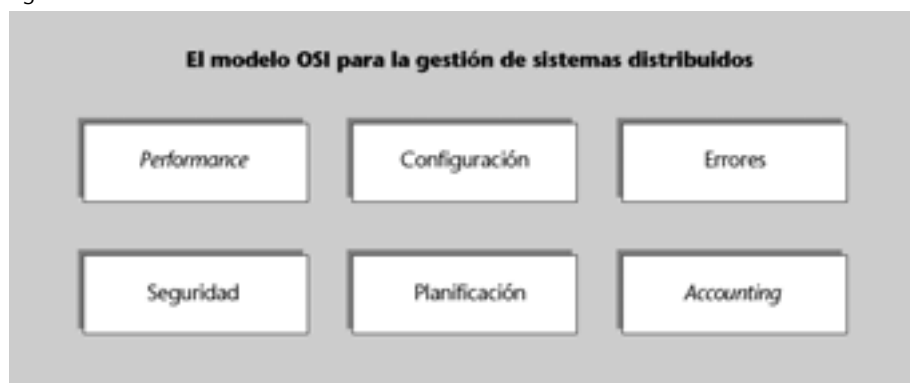
\* En inglés, *accounting*.

La gestión de contabilizaciones toma especial importancia con la creciente evolución hacia la utilización de recursos externos, especialmente en el ámbito de los servicios de telecomunicaciones.

Las cinco áreas definidas reúnen prácticamente todas las tareas, procesos y procedimientos de administración y gestión que se hacen dentro de un entorno de sistemas de información distribuidos. Sin embargo, resulta muy habitual que se hable con frecuencia de un área funcional más: la referida a las **tareas de planificación**. Esta sexta área agrupa todos los procesos que ayudan a optimizar la evolución de una red y todos sus componentes, establecer dinámicamente una aproximación fiable de las tendencias a corto, medio y largo plazo y determinar la utilización y capacidad residual de los recursos y su ciclo de vida operativo.

Se engloban dentro de este subsistema todas las tareas de análisis de información, normalmente proporcionada por el resto de las áreas funcionales, y los procedimientos de optimización respectivos. El impacto del mismo crecimiento vegetativo, el estudio de las medidas de rendimiento de los elementos de la red y de los elementos de proceso, los flujos de tráfico, los requerimientos de carga en condiciones cambiantes, las reglas de dimensionado o las tendencias y obsolescencias tecnológicas son algunas de éstas.

Figura 4




#### Informática de gestión de la informática

Una de las ventajas más importantes que los expertos destacan del modelo OSI es que su estructuración ayuda a organizar, definir y establecer las herramientas informáticas y telemáticas utilizadas para gestionar y administrar sistemas distribuidos.

El concepto *informática de gestión de la informática* es práctico, pero no debemos obviar las profundas ventajas organizativas.

Esta arquitectura funcional, conocida habitualmente como el **modelo OSI de las cinco áreas más una**, forma un conjunto homogéneo, aplicable a cualquier escenario, en el que las áreas no se tienen que considerar en ab-

soluta como compartimentos estancos, sino que la interrelación entre éstas es completa.

Los apartados siguientes definen con mayor detalle cada uno de los subsistemas funcionales del modelo. 

### 3. Gestión de la configuración

La gestión de la configuración es la primera área funcional en la que el modelo OSI clasifica el conjunto de tareas y procesos que hay que desarrollar en cualquier entorno informático en producción basado en redes, prácticamente la totalidad de los existentes hoy en día.

#### 3.1. Introducción

El área de gestión de la configuración agrupa el conjunto de actividades con frecuencia consideradas generales para toda la extensión de los sistemas automatizados de una organización, y administra la información de todos los elementos y recursos que forman el sistema distribuido o se relacionan con el mismo, tanto si son de tipo físicos como lógicos o, incluso, humano.

#### Terminología

El área de gestión de la configuración es conocida normalmente en los textos como *configuration management*, abreviado **CM**.

El horizonte general de las actividades de configuración está especialmente orientado a medio y largo plazo, escenarios en los que es muy necesario disponer de una compleja y eficaz herramienta de información consolidada de un determinado entorno. La información proporcionada por el área es esencial, además de por sí misma, para todo el resto de las áreas funcionales, a las que informa y de las que recoge toda la información que se tenga que almacenar.

Las diferentes tareas que se hacen en su marco son tan variadas como las siguientes:

- Control de los inventarios en todos los ámbitos: físico, “eléctrico”, topológico, lógico o humano, entre otros.
- Información de los proveedores involucrados y su relación con la instalación.
- Gestión de los informes de problemas (*trouble tickets*), control y seguimiento de las resoluciones, de mucha importancia en escenarios de contratación externa (*outsourcing*).
- Control de aprovisionamientos: equipamiento, consumibles, recambios, actualizaciones. Algunos ejemplos son la gestión de los pedidos, validaciones o el control de *stocks*.

- Control y gestión de los cambios en todos los ámbitos: físico, lógico, funcional.
- Control de la distribución del *software* a lo largo del equipamiento de la red: ¿cuál se distribuye?, ¿cómo?, ¿cuánto?
- Directivas generales del nivel de servicio, QoS, en todos los ámbitos y con todos los actores involucrados: contratos de soporte externos, tipo y calidad del servicio contratado a terceros o tipo y calidad del servicio que se nos exigirá internamente, entre otros.
- Control y herramientas para soportar el acceso a los objetos y cómo se distinguen los elementos: nomenclatura, direccionamiento, etc.
- Recopilación, almacenamiento y suministro de información de los elementos de la red y a éstos.

### Ejemplo de gestión de la configuración

La versión X.xx del *software* que corre sobre un conmutador de puertos *Fast ethernet* de nuestra red está causando una serie de problemas de saturación, en condiciones de puntas de carga, ya que a veces queda en un estado de degradación de las prestaciones de conmutación, incluso cuando la punta de tráfico problemática ha cesado.

Consultada la unidad de soporte del fabricante, nos recomienda la actualización del *firmware* del conmutador por la versión Y, pero recomienda que se haga a todos los elementos similares en la instalación. Es necesaria la revisión previa de la versión de cada elemento, y la existencia de más de un centenar de unidades, en diferentes localizaciones geográficas, hace que la operación resulte muy problemática.

Si disponemos de una herramienta adecuada de gestión de configuración, los administradores dispondrían de un informe con la relación de cada versión del *software* en cada equipo o, incluso, podrían generar el mismo dinámicamente, en tiempo real, y planificar sin errores los desplazamientos en las dependencias concretas.

Informe de configuración (versiones de <i>software</i> por equipo)			
Identificación dependencia / Identificador equipo / Núm. serie			Versión
Servicios Centrales. Planta 4. <sup>a</sup>	FH-00123-01	125673402	X.01.2
Servicios Centrales. Planta 4. <sup>a</sup>	FH-00123-02	125673813	Y.11.0
Oficina Blanquerna, 49	FH-00198-01	124431222	X.21.1
Oficina Aragón, 125	FH-00233-01	125673815	Y.11.0

Por su misma complejidad y extensión, con frecuencia se considera que el núcleo central del modelo funcional OSI está representado por el área de configuración, ya que el resto de las áreas necesitan información soportada por ésta para su funcionamiento.

Una de las razones más importantes es el hecho de que esta área es la que proporciona los servicios de nomenclatura, direccionamiento y acceso a los obje-

tos y almacena, a la vez, toda la información de las características. Además, la gestión de los *trouble tickets* y de los cambios hace que administre los datos, sobre todo las críticas, proporcionados por las otras áreas, y constituye un verdadero *repository* común de detalles de la historia de acontecimientos, características, implantaciones, modificaciones o cambios.

Figura 5



En la figura anterior se representan algunos de los flujos principales de información entre áreas. En la práctica, en los entornos en producción, el área de configuración hace prácticamente de enlace entre todas éstas.

Las dificultades comunes al conjunto del área de gestión de configuración están referidas tanto al tipo de actividades que hay que desarrollar, como a la complicación de llevarlas eficazmente a cabo. Estas complicaciones están caracterizadas principalmente por las circunstancias siguientes:

**a) Fragmentación de estructuras de BD:** es muy común, sobre todo en organizaciones medianas y grandes, que la información esté repartida en decenas de bases de datos, con sus correspondientes soportes\*. De esta manera, la información de pedidos, proveedores, garantías, contratos o extensa documentación técnica diversa presenta serios problemas de localización, integridad, fragmentación y actualización.

**b) Redundancia de información:** la sincronización de la información que dispone el centro de proceso de datos o la unidad informática, y otros departamentos de la organización, como el área financiera, almacenes, personal o

#### El concepto de *repository*

Inicialmente utilizado por IBM, con fines más comerciales, para reflejar el lugar único de almacenamiento de información relacionada, es hoy de utilización habitual en el mundo de la gestión de sistemas distribuidos.

#### La importancia del CM

La extensión de las responsabilidades de CM denota, desde el primer momento, una importancia que se trivializa con frecuencia de manera errónea.


\* Sistemas informáticos horizontales, sistemas específicos o, simplemente, documentación en papel.

compras, entre otros, puede ser muy complicada, si no imposible, con los consiguientes problemas operacionales.

c) **Nomenclatura dispersa de los elementos:** es frecuente que las reglas de nomenclatura de los componentes y recursos de la red, cuando existen, no sean homogéneas, por razón de actualizaciones, cambios de arquitectura, precipitaciones o, simplemente, obiedad de su importancia. Si es difícil con recursos tecnológicos similares, la complicación se dispara ante el conjunto de elementos, físicos y lógicos, que forman el sistema distribuido y actúan sobre éste.

d) **Dispersión de productos, soluciones y fabricantes:** las ventajas que tienen los sistemas abiertos contrastan ante las dificultades de equilibrio entre las soluciones de gestión de propósito general y las de aplicación concreta. La interconexión entre éstas, necesaria para mantener una estrategia de integridad, puede ser muy complicada.

e) **Sistemas y redes de telecomunicación no integradas:** muchas organizaciones no disponen de redes de datos totalmente integradas y pocas disponen de estructuras y medios comunes para todos los servicios que necesitan arquitecturas distribuidas, como los de datos, voz, imagen, seguridad o vigilancia. El desarrollo tecnológico y la consecuente reducción de los costes hacen que se produzcan cada vez más avances en esta línea, con un nuevo ámbito corporativo y único de todos aquellos servicios.

Desde el punto de vista operacional del conjunto de actividades que la gestión de la configuración integra, con toda la información y sus procesos asociados, se definen tres ejes básicos de enfoque: 

1) **Descriptivo:** descripción de la organización y distribución de recursos, tanto física como geográfica o espacial\*, de cómo están interconectados los recursos y de las relaciones lógicas entre éstos\*\*.

2) **Procedimental:** inventario de los procesos de explotación, manipulación y operación de la estructura de los recursos del sistema distribuido, establecimiento de los parámetros que controlan la operación normal y cumplimiento de los niveles de servicio preestablecidos.

3) **Generacional:** apoyo a la generación de nuevos procedimientos y valores de las parametrizaciones, a partir de un cambio en determinados elementos de la estructura del sistema distribuido, o su papel, relaciones o relevancia, adaptando y manteniendo las condiciones de operación normal predefinidas. Todas las tareas de adaptación de nuevos elementos a las condiciones del entorno se encuentran aquí contenidas\*.

#### Sistemas abiertos y sistemas propietarios

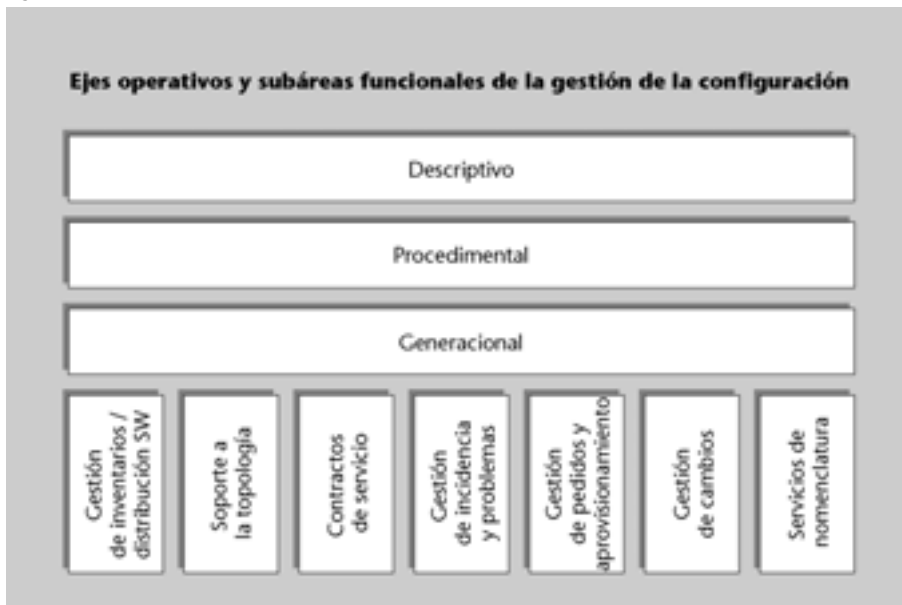
En general, se conocen como **sistemas abiertos** (*open systems*) los sistemas fabricados, soportados o implantados por múltiples fabricantes, en contraste con los **sistemas propietarios** o **arquitecturas propietarias** (*legacy systems*) ligadas a una empresa o marca concreta. El UNIX o la arquitectura AS/400 de IBM son ejemplos, respectivamente, de sistemas abiertos y propietarios. Pero hay mucha polémica, de origen claramente comercial, sobre dónde acaba un sistema abierto y dónde empieza un sistema propietario.

\* Enlaces, electrónica de red, equipamiento terminal de usuario, servidores, *hosts*, *software* de base y de aplicación, usuarios, etc.

\*\* Relaciones cliente-servidor, prioridades, perfiles de seguridad, relaciones datos-aplicaciones, etc.

\* Configurar elementos, instalar un nuevo *software*, cambios topológicos, cambios del perfil de carga, etc.

Figura 6




Dentro de la extensa variedad de escenarios basados en sistemas distribuidos, cada uno de los ejes –que siempre están presentes– asumirá la entidad y relevancia que le corresponda. En todos los casos cruzan horizontalmente el conjunto estructurado de actividades del área, conocidas como **subáreas de la gestión de la configuración**. Todas éstas se implantan sobre las herramientas informáticas correspondientes.

Las subáreas que tradicionalmente se consideran dentro de la CM son la gestión del inventario global, los servicios de soporte a la topología del sistema distribuido, la gestión de las contrataciones de servicio, la gestión de incidencias y problemas, el control de pedidos y aprovisionamiento, la gestión de cambios, los servicios de nomenclatura unificada y el control de la distribución del *software*. Los siguientes subpartados expondrán las características de cada una de estas subáreas.

### 3.2. Gestión de inventarios

El objetivo del subsistema de gestión de inventarios es proporcionar una herramienta eficaz de recuperación de información en línea, referida a los componentes instalados en el sistema distribuido, con todas sus características, relaciones y funciones, integrando todos los aspectos involucrados.

El concepto de **inventario global integrado** se prevé, en ocasiones de manera errónea, con respecto a cuáles son sus focos de actuación. Aunque el conjunto del equipamiento físico y en general el equipamiento lógico no presentan confusiones, los inventarios deben prever todas las posibles relaciones estableci-

das con la base de recursos tecnológicos instalados, conocidos en ocasiones como **inventarios funcionales** o **inventarios operacionales**. 

Bajo estos tres focos de actuación, las **categorías de elementos de inventario** que se utilizan con frecuencia son las seis siguientes, y citamos algunos de los atributos representativos:

a) **Equipamiento:** incluye todos los equipos electrónicos de proceso de datos, tanto unidades servidoras como elementos terminales, electrónica y equipos de telecomunicación, periféricos, equipamiento de control y gestión, así como los enlaces de red conectados al usuario final. Normalmente se establecen subdivisiones jerárquicas de los componentes de los elementos y se especifican las relaciones entre sí (*host*, placas de CPU, controladores I/O, procesadores). Algunos atributos son los códigos de identificación, el tipo de equipo, la jerarquía de componentes, la localización física, la identificación del fabricante y del proveedor y sus servicios asociados, fechas de instalación y tiempo en servicio, etc.

b) **Enlaces físicos:** incluye las conexiones físicas, con medios de cobre, fibra o electromagnéticos, con dos equipos de telecomunicación. Su función es la de soportar el transporte de los circuitos lógicos. Atributos de esta categoría son los identificadores, la localización e identificación de los extremos, los fabricantes, los instaladores, los propietarios si son terceros, el soporte y mantenimiento, las fechas de instalación, etc.

c) **Circuitos lógicos:** son todas las conexiones lógicas entre dos nodos del sistema distribuido, que soportan una aplicación o un servicio, utilizan un enlace físico o más y pueden tener anchos de banda diferentes. Algunos atributos son los códigos de identificación, la identificación de los nodos terminales, los anchos de banda disponibles, los enlaces utilizados, etc.

d) **Software de base y software de aplicación:** se incluyen todos los recursos *software* utilizados en la organización, tanto los referidos a *software* de base, sistemas operacionales, *firmware* de electrónica, frontales transaccionales, motores de base de datos, herramientas de administración y gestión, etc., como los referidos al *software* de aplicación, de ámbito corporativo, departamental o personal. Los atributos utilizados en esta categoría son el tipo del *software*, la versión y el nivel, las opciones y parámetros, los pedazos para resolver *bugs*, la identificación de proveedores, mantenedores, cuadernos de carga, fechas, etc.

e) **Servicios:** son todos los contratos y compromisos que se establecen entre terceros, externos a la organización, para proporcionar una determinada función en torno al sistema distribuido (tareas de mantenimiento y reparación, instalación de infraestructuras, programación, apoyo con centros de atención telefónica, etc.). También incluye los compromisos que asume el departamento de informática con sus usuarios sobre los niveles de servicio que se presta-

#### Los bugs

Los *bugs*, o errores de programación en una aplicación, son la causa principal de problemas en los sistemas modernos. El equipamiento *hardware* es cada día más seguro, pero el aumento de tamaño y complejidad del *software* hace que para muchas compañías productoras no sea rentable sacar *bug free software*.

blezcan (ventanas de disponibilidad, tiempo de respuesta, funcionalidad de las aplicaciones, etc.). Algunos atributos que se incluyen en esta categoría son los códigos de identificación, proveedores, clientes o usuarios, unidades, hitos y medidas del servicio proporcionado, contactos, marco legal, etc.

f) **Proveedores:** hace referencia a todo el detalle de información de los proveedores de servicio externo, a unas funciones específicas y a unas áreas de actuación concretas sobre determinados componentes del sistema distribuido. En organizaciones grandes, este inventario refleja también los mismos recursos humanos internos del departamento de TI\* (tecnologías de la información). Son atributos de esta categoría los identificadores, las referencias de contacto, identificación de personas y perfiles de conocimientos, direcciones, historia contractual, servicios en curso, etc.

\* TI es la sigla de tecnologías de la información.

g) **Localización:** se refiere a la información de localización física, geográfica y espacial de cada objeto y recurso del sistema distribuido. Se incluyen los elementos de proceso, centrales y terminales, la electrónica de red, la topología de las redes y su camino físico, o la localización de una estructura de base de datos o una aplicación en los servidores, entre muchas. Los identificadores y todos los calificadores de identificación de localización, información gráfica incluida, son algunos de los atributos utilizados.

Cualquier herramienta para la gestión de la configuración utiliza los procesos, identificadores e información general que le proporciona el subsistema de inventarios. Como consecuencia de ello este subsistema no sólo podrá contener información estática o simplemente almacenada fuera de línea de la actividad real del sistema distribuido. El objetivo es que la herramienta de gestión contenga en sus bases de datos integrados los repositorios, el estado instantáneo del sistema distribuido, una “fotografía” en un momento determinado en unos perfiles de trabajo, carga o problemáticas concretas, o al menos que sea capaz de tenerlos.

Para la herramienta de configuración será imprescindible identificar qué elementos y recursos están en juego, cómo actúan, en qué condición se encuentran o de quién dependen. Además, esta información es necesaria para el resto de las áreas de gestión.

Generalmente, la caracterización de los objetos en fase de producción se hace mediante cuatro grupos de indicadores:

a) **Indicadores de existencia:** el objeto o recurso “existe” si es accesible e identificable en tiempo real para las herramientas de gestión de la configuración. Normalmente habrá sido dado de alta, con sus características, de manera manual o con medios automáticos.

**b) Atributos:** se describen todas las propiedades del objeto, datos operacionales y de configuración e instalación, opciones, parámetros por defecto. En operación real no se pueden añadir propiedades, sólo pueden cambiar su valor.

**c) Indicadores de estado:** representan las condiciones instantáneas de un objeto o recurso o de algunos de sus componentes con respecto a su disponibilidad y viabilidad operativa.

**d) Indicadores de relación:** son indicadores que definen interdependencias entre recursos, tanto físicas como lógicas y funcionales. Los elementos de red o protocolos utilizados en un enlace y los recursos redundantes alternativos o elementos involucrados que soportan una determinada aplicación son algunos ejemplos.

El conjunto de información de los repositorios de gestión de la configuración, o BD de configuración, se conoce tradicionalmente con el nombre de **MIB**, *Management Information Base*, que soporta todas las estructuras para la información de la gestión del entorno y de la misma.

Todos los subsistemas de soporte de inventarios contienen instrumentos eficaces para las tres funciones básicas de adquisición de datos, almacenamiento y recuperación de información.

La **adquisición de datos** está soportada genéricamente por mecanismos manuales y automáticos. La recaudación manual, aquella que es físicamente introducida por los mismos administradores de la red, puede llegar a ser muy tediosa y normalmente se restringe a las creaciones de alta (primera vez) o a aquellos objetos y situaciones que no se pueden registrar por medios automáticos.

La adquisición automática utiliza mecanismos que son capaces de obtener información de los mismos objetos y recursos mediante protocolos de interrogación y herramientas que se ejecutan en los elementos remotos para conformar sus características. La **adquisición automática** puede ser de dos tipos:

- **guiada**, o **periódica**, si está invocada por el administrador;
- **transparente**, o **permanente**, si es arrancada por el mismo entorno, por cambios de estado o acontecimientos en los objetos, como un *login* de usuario o un fallo.

Finalmente, las herramientas de descubrimiento automático (*discovering*) permiten a los administradores conocer e identificar nuevos elementos en el sistema distribuido y hacer mapas e informes correspondientes. Son muy útiles en entornos grandes, con una carencia de cambios muy elevada.

#### Ejemplos de indicadores de estado

Las operaciones normal (*running*), en espera (*stand-by*) o detención por fallo (*fault halt*), o las operaciones de arranque (*coldboot*, *warm reset*), son algunos ejemplos de indicadores de estado.

#### La MIB

La MIB es un concepto activamente utilizado en el mundo de la gestión, que se ha heredado de la arquitectura de **SNMP** (*Single Network Management Protocol*), pero que no está soportado ni estandarizado por OSI. El estándar OSI para la organización de estructuras de BD de gestión es el **SMI** (*Structure of Managed Information*).

#### Los entornos grandes

Los entornos grandes son muy variables y evolucionables. Tradicionalmente se conocen como *ever-changing*.

Los medios de almacenamiento de información de configuración son variados. Genéricamente, un punto crítico de decisión es la definición de qué información se guardará, garantizando siempre su consistencia y disponibilidad. Normalmente se utilizan las recomendaciones de los estándares, que separan los atributos en los que son obligatorios\*, los opcionales y las operaciones básicas con los mismos objetos, pero puede haber diferencias notables de profundidad según el escenario del entorno.

\* En inglés, *mandatory*.

Para acabar, la recuperación de datos se ha visto favorecida por las potentes herramientas de BD relacionales y la ergonomía de las herramientas gráficas. Es habitual contar con la existencia de motores de recuperación, con búsquedas predefinidas y capacidad de interrogación, por ejemplo con SQL, herramientas de visualización *top-down* y vistas homogéneas o procedimientos de cruce, jerarquización y correlación de elementos dispersos.

Figura 7

Product/Model	Serial Number	User Contact	Dept Code
Monitor COMPAQ/Monocrom	03425222A...	Provisional	Baja
Monitor COMPAQ/Monocrom	03425222A209	Provisional	Baja
Monitor COMPAQ/Monocrom	02425222A...	Provisional	Baja
Monitor COMPAQ/Monocrom	02425222A407	Provisional	Contabil.
Impresora EPSON/LX-800	0HX7046647	Fuera de servicio	Baja
Impresora EPSON/LX-800	0HX7046639	Fuera de servicio	Baja
Impresora EPSON/LX-800	0HX7046654	Fuera de servicio	Baja
Impresora EPSON/LX-800	0HX7046645	Fuera de servicio	Baja
cpu IBM/PS/2	5500DFWP2	Averiado	Baja
Monitor NETSET/Monocrom	T0205242	Averiado	Baja
cpu COMPAQ Deskpro/486 N	8044HAQ31161	Maria Perelló	Biblioteca
Disc dur 420Mb/type 22		Maria Perelló	Biblioteca
Monitor COMPAQ/Monocrom	03425222A633	Maria Perelló	Biblioteca
Filtro monitor		Maria Perelló	Biblioteca
Impresora EPSON/LX-800	0HX7046659	Maria Perelló	Biblioteca

#### Ejemplo de herramienta de gestión de configuración

La siguiente base de datos es un ejemplo de pantalla que han proporcionado los servicios de inventario de herramientas de gestión de configuración.

### 3.3. Servicios de soporte a la topología del sistema distribuido

El objetivo del subsistema de soporte a la topología es proporcionar una visualización y representación gráfica de los aspectos físicos, lógicos y funcionales de los elementos y recursos, considerándolos de manera individual o de manera integrada.

La complejidad de los sistemas distribuidos actuales hace que la gestión y control de sus componentes, objetos, recursos, relaciones, jerarquías y dependencias, entre otros, no sean "fácilmente" tratables por los administradores sin herramientas diseñadas con conceptos de ergonomía que hace unos años se trivializaban.

#### Complejidad de los sistemas distribuidos

Con este ejemplo queremos poner de manifiesto la complejidad de los sistemas distribuidos. Imaginemos el caso de una instalación que dispone de los inventarios de sus recursos

de las casi cien oficinas en la ciudad, enlazadas por medios de comunicación contratados a operadores externos. Toda la información se encuentra en un conjunto de listados de configuración muy exhaustivos, con todos los datos que definen las características de cada oficina, y de una extensión superior a las quinientas hojas.

Si en una de las jornadas con más carga de trabajo el operador de comunicaciones tiene una avería importante en la mitad de su red, pero el operador externo le propone resolver la situación y enlazar sucursales directamente, ¿hasta qué punto le puede resultar útil a un administrador tomar una decisión de qué sucursales reconecta, cuáles detiene o, simplemente, a cuáles avisa? Toda la información de localizaciones, prioridades, tamaño de las sedes u otros datos relevantes está en los listados, pero éstos resultan inmanejables, sobre todo por la presión de estar en producción sin dar servicio.

Las herramientas gráficas de la topología de las sucursales en la ciudad, la red de enlaces o la priorización visual de la importancia de una sucursal podían haber sido definitivas para contener la situación de forma adecuada y en un tiempo mínimo de afectación al servicio. Como éstos, hay centenares de ejemplos en la operación real de sistemas distribuidos medios y grandes.

Las herramientas de soporte a la topología se enfocan hacia los **datos de configuración estáticos**, con respecto a la configuración en curso, o hacia estados de momentos anteriores, guardados como históricos. Sin embargo, también es importante la vertiente del conjunto de **información dinámica**, en gran parte conseguida en tiempo real en el momento en que se produce un determinado acontecimiento, un cambio o una circunstancia concreta.

El manejo de información estática se utiliza sobre todo en la localización física y eléctrica de los componentes terminales, periféricos o electrónica de red. Los cableados, la canalización y la ubicación de fibras o radioenlaces, las vías capaces de enlazar dos localizaciones, especialmente en WAN y MAN malladas e, incluso, la ubicación del equipamiento dentro de los bastidores\* son algunos ejemplos. Los informes de consolidación y todos los estudios estadísticos y de planificación también utilizan estos servicios.

La información recogida de manera dinámica con frecuencia resulta esencial para el resto de las áreas de gestión. El soporte gráfico a la gestión de fallos permite correlacionar filtros de acontecimientos, activar o desconectar alarmas, proporcionar facilidades de aislamiento de objetos, circuitos, servicios o aplicaciones afectados y permite el acceso a las herramientas de *trouble ticket* y los asistentes de resolución de problemas. La visualización de recursos de comunicación saturados o las gráficas de tendencia de carga son ejemplos de utilidades en el área de prestaciones.

Para conseguir el soporte de todas estas funciones, incluidas las de la misma gestión de la configuración, como el control de inventarios o la gestión de cambios, los servicios de soporte a la topología tienen que proporcionar la **capacidad de presentación multinivel\***, que permitirá visualizar diferentes vistas del sistema distribuido, e integrar aspectos físicos y lógicos. Los niveles mínimos recomendados por OSI son los siguientes:

- **Red:** referida a la visualización de todo el sistema distribuido, con la identificación de los nodos desde un punto de vista funcional\*, o a la topología física en la jerarquía más alta\*\*. Alguna condición de que suceda algún nodo puede ser rápidamente identificada\*\*\*.

#### En los últimos años...

... se ha superado completamente la idea de los efectos "cosméticos" de las herramientas con importante soporte gráfico. Las ventajas sobre otras herramientas son evidentes y es frecuente la utilización de equipamiento específico, *workstations* gráficas especializadas, para la visualización.

\* En inglés, *racks*.

\* En inglés, *multi layer*.

\* Sedes centrales, delegaciones regionales, etc.

\*\* Países o ciudades, si es el caso, o todo un campus, etc.

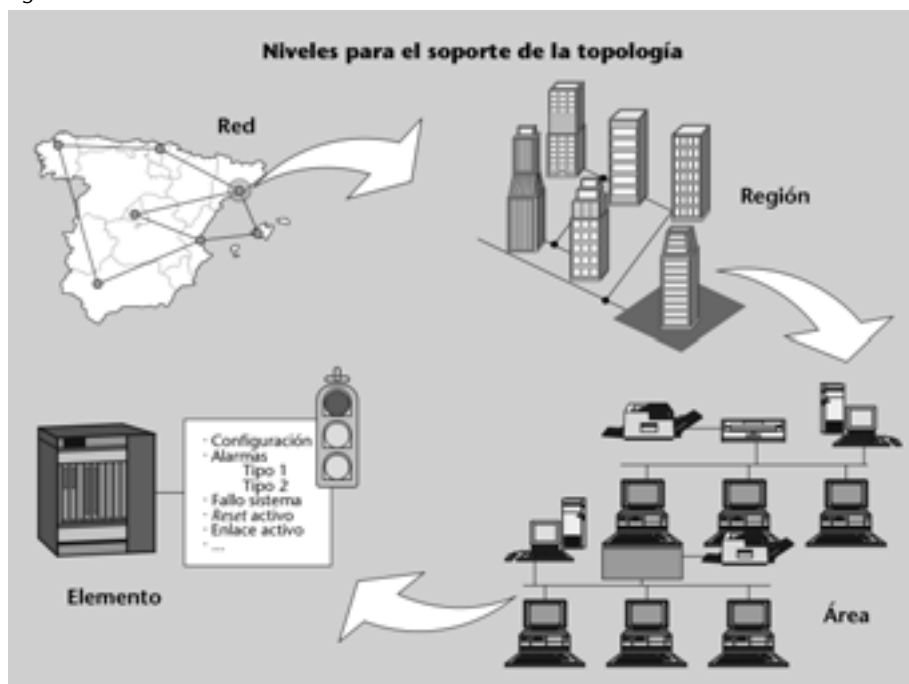
\*\*\* Cambio de colores, ventanas de acontecimientos, etc.


- **Región:** asociada a la visualización de un nodo concreto. Puede ser una ciudad, una delegación o un edificio en el campus. Permite identificar los principales componentes topológicos y funcionales en el nodo y los elementos que lo comunican con los demás nodos\* y enseñar, si procede, características del área o áreas afectadas.
- **Área:** en este nivel, el administrador tiene acceso a la topología física del área e identifica todos los componentes del sistema distribuido en función específica. La estructura de las LAN, los equipos terminales y periféricos, la electrónica de red, los servidores locales y departamentales, las aplicaciones instaladas en éstos o los usuarios declarados son ejemplos del nivel de detalle del que se dispone. En el caso de problemas por fallos, prestaciones o ataques de seguridad, se ven claramente los elementos afectados.
- **Elemento:** muestra un elemento en detalle, con todas sus características, tanto las recogidas de manera estática como el estado y valores en un momento determinado, obtenidos dinámicamente. En el nivel del elemento se puede acceder a herramientas de actuación sobre el objeto para hacer cambios u otras operaciones.

\* Troncales, redes públicas, etc.

Las facilidades de soporte de la topología permiten establecer análisis *top-down*, que contribuyen a responder de forma eficaz a situaciones críticas, especialmente bajo condiciones de fallo. Los recursos gráficos, como los colores, los cambios de figuras y formas, el marcaje de flujos, ventanas y capacidades de *zooming*, ayudan a facilitar la ergonomía en la utilización de las herramientas.

Figura 8



Ahora bien, la capacidad multinivel no queda simplemente restringida a la capacidad de segmentación jerárquica en planes homogéneos. Una de las capacidades más importantes consiste en la posibilidad de establecer un nivel, que se suele denominar **vista**, con componentes vinculados por criterios físicos, lógicos o funcionales: 

a) Una **vista de ámbito físico** concreta puede mostrar todos los elementos de un determinado tipo, como por ejemplo conmutadores ATM o servidores NT, pero en el ámbito de red, es decir, en el ámbito de todo el sistema distribuido. Con una vista de ámbito físico, el administrador, en una sola pantalla, puede saber los nodos de alto nivel en los que se encuentra este equipamiento, su estado y sus características.

b) Una **vista de ámbito lógico** puede mostrar los diferentes medios de enlace entre nodos o sedes, cuáles son las aplicaciones que los utilizan, la utilización media o máxima de los enlaces para cada una de éstas, cómo se restablecerán y balancearán los flujos en caso de que se produzca la caída de alguno de éstos y qué aplicaciones se mantendrán levantadas en el ámbito de servicio restringido.

c) En último término, una **vista de ámbito funcional** nos ofrece la posibilidad de relacionar a los usuarios y perfiles de uso con una o varias aplicaciones relacionadas, así como establecer en qué nodos o en qué sedes hay perfiles de responsabilidad análoga y planificar cambios o formación de los recursos humanos implicados.

### 3.4. Gestión de los contratos de nivel de servicio

El objetivo del subsistema de gestión de los contratos de nivel de servicio es asegurar una metodología estándar que asegure una efectividad en los compromisos y contratos de servicio, en el ámbito de las TI, externos con nuestra organización, tanto si éstos son los que hacen el servicio como si lo hace nuestra organización, y así evitar llegar a las “**crisis contractuales**”.

Los **contratos de nivel de servicio**, conocidos normalmente por el acrónimo **SLA\***, responden a una tendencia cada vez más importante a la hora de llevar a cabo muchas tareas típicas de un entorno con sistemas distribuidos. De esta manera, cada vez es más frecuente contratar externamente servicios relacionados con el conjunto del área de tecnologías de la información.

\* SLA es el acrónimo de *Service Level Agreement*.

Los servicios contratados pueden ser muy variados. La tendencia es eliminar de la organización aquellas tareas y funciones que no aportan valor añadido a sus líneas de negocio. En esta línea, las empresas contratan muchas tareas de la vertiente de sistemas, como mantenimiento de equipamiento, instalación

de infraestructuras de comunicación, soporte a los usuarios finales mediante servicios de *help desk* y centros de atención telefónica, o mantenimiento y tareas microinformáticas, entre otras.

En la vertiente del desarrollo, también cada vez se utiliza más la contratación a terceros, y se restringen los recursos de desarrollo interno, si existen y según su calificación, a la dirección de proyectos o al mantenimiento vegetativo de las aplicaciones. El aumento de la utilización de soluciones paquetizadas también ha tenido un fuerte impacto en el perfil de los recursos del área de *software*, tanto internos como contratados.

**Las soluciones paquetizadas: los ERP**

Las plataformas tecnológicas de gestión empresarial, conocidas como ERP (Enterprise Resource Planning), son mucho más que “paquetes” más o menos generales. Cada vez más se piden especialistas en SAP R/3, ORACLE Financials, Baan, PeopleSoft y muchas otras.

Al implantarlas, se intenta reducir al máximo el desarrollo de código mediante la utilización de las soluciones estándares, profundamente parametrizadas.

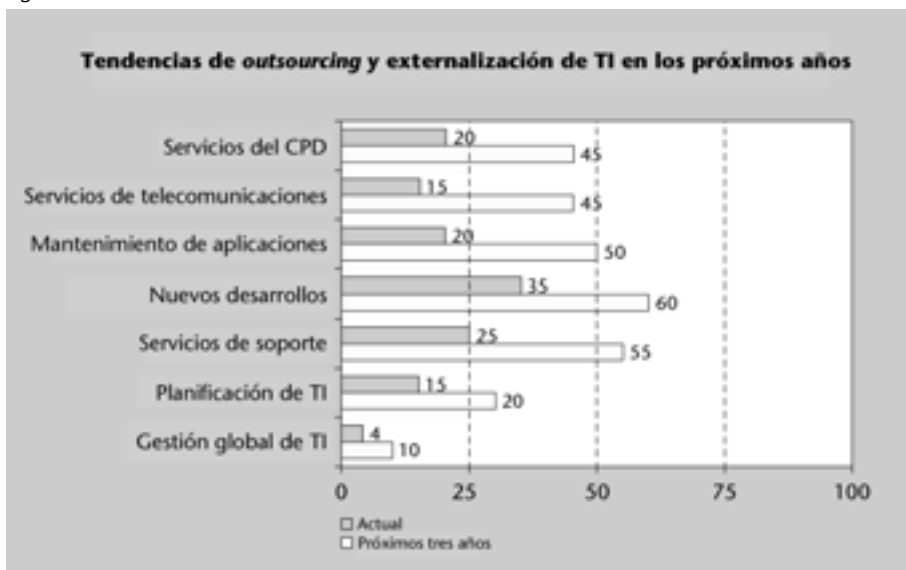
Además del impacto organizativo, las repercusiones sobre el área tecnológica, tanto en los medios técnicos (redes, unidades de proceso, etc.) como en los recursos humanos, no son triviales.


Sin embargo, la contratación externa puede tener un mayor alcance. Al principio de los noventa, había muchas organizaciones que contrataban, parcial o totalmente, el soporte informático y telemático a terceros. Se daban esquemas de departamentos de TI con centenares de personas que en ocasiones sólo disponían de una unidad de coordinación con unos pocos gestores. Esta política, conocida como *outsourcing*, continúa vigente hoy en día, aunque predomina la contratación de tareas y funciones más concretas, el *outtasking*, que mantiene dentro de la organización los recursos hasta el nivel de la dirección de proyectos, mientras que los especialistas concretos son externos.

**Los centros de atención de usuarios**

Los centros de atención de usuarios, CAU o unidades de *help desk*, rentabilizan el soporte de los usuarios finales, sobre todo en el ámbito microinformático, pero también para grandes aplicaciones corporativas, que utilizan normalmente centros de atención telefónica (*call-centers*), con las correspondientes ACD (*automatic call distribution*), que dan control y fluidez a los llamamientos entrantes.

Figura 9



Las principales razones de estas **tendencias de contratación externa** son las siguientes: 


1) **Aumento exponencial de la complejidad:** asociada a cualquier proyecto informático hoy en día, incluso los de tamaño reducido. Este hecho implica una alta calificación de los directores y una cantidad elevada de especialistas, que pueden tardar incluso un año en formarse de modo adecuado. Es imposible para la mayoría de las organizaciones disponer de estos recursos internos.

2) **Proliferación y dispersión de las soluciones tecnológicas:** la riqueza de un mercado con muchos fabricantes, proveedores y soluciones y la consiguiente competencia entre sí aportan un desarrollo técnico extraordinario, difícilmente comparable al de otros sectores. Pero muchas de estas tecnologías pueden tener una vigencia muy corta y ser discontinuas o no soportadas en prácticamente el tiempo de adquisición, formación, pruebas y primeros desarrollos e instalaciones.

3) **Movilidad de los recursos:** los recursos humanos cualificados, tanto en el ámbito de dirección estratégica o dirección de proyectos como en el de especialistas, no son sencillos de retener por las compañías, y se establece una notable movilidad en el sector. El consiguiente aumento de salarios y otras prestaciones sólo se puede ver compensado por una alta rentabilidad, que normalmente sólo consiguen empresas consultoras que son contratadas por clientes finales para hacer los proyectos.

4) **Aumento de los costes:** en el mundo empresarial actual todas las actuaciones están sujetas, como es lógico, a un balance positivo entre inversiones y costes, y a los beneficios de las líneas de negocio. Los proyectos informáticos, incluso los mismos departamentos de informática, se tienen que desarrollar, en general, con políticas de contención de costes que *per se* vienen impuestas por los puntos anteriores. La contratación de servicios, siempre con plenas garantías de éxito, es una de las herramientas que hay que utilizar.

Desde el punto de vista más simple, un **contrato de nivel de servicio (SLA)** es un contrato formal escrito, con la vigencia de derecho y factible de ser sometido a juicio si se incumple.

Estos casos o los más complejos deben contener los apartados siguientes: 

a) **Identificación de las partes:** en un contrato de servicio, las partes que intervienen tienen que estar bien definidas en todos los aspectos. Se especifica, por parte del cliente o contratante, los representantes y cargos de dirección y coordinación en todos los niveles, estratégicos, tácticos y operacionales, así como el departamento o unidad al que representan. La definición previa del escenario de la organización y del sistema distribuido suele ser una carencia frecuen-

te y no es accesorio que todos los detalles generalistas se especifiquen de forma conveniente. Resulta obvio que aquellos detalles que afecten directamente al contrato se tienen que plasmar con toda minuciosidad, ya que la garantía de la estabilidad del escenario es siempre responsabilidad del cliente.

Con respecto al realizador del servicio, contratado o proveedor, además de la información general, jurídica y administrativa, es recomendable el detalle de particularidades débiles como la especificación de los recursos humanos, y su perfil, que harán los servicios, los criterios de sustitución, los seguros ante determinadas responsabilidades subsidiarias, la estructura y organización del comité de conflictos o la posibilidad y características, si procede, de subcontratación.

En el caso nada extraño de que entren en juego más de un proveedor, para hacer todas las tareas, algunas o parte de éstas, se tienen que enfatizar los papeles y compromisos de cada uno de éstos, porque es muy fácil que se produzcan efectos en cadena (la quiebra de uno afecta al otro y, por lo tanto, finalmente, al cliente) o circulares (cada proveedor está pendiente de otro mientras el cliente no tiene el servicio).

**b) Descripción de las tareas que hay que realizar:** la especificación de tareas dentro del SLA debería cumplir el doble objetivo de que dichas tareas sean claras y explícitas para personas no expertas y que los detalles más concretos queden muy determinados. La documentación estructurada jerárquicamente, con anexos técnicos, suele ser una buena herramienta.

Los volúmenes referidos a los pedidos de servicio se diseñan normalmente bajo condiciones medias de carga, según magnitudes como el número de usuarios, transacciones por minuto, tasas de fallo, ventas planificadas o *hits web* esperados, entre muchos otros, pero se tienen que prever medidas para alcanzar las puntas\* o los valles\*\*. Si se han estimado los indicadores de volumen, hay que prever los mecanismos y algoritmos de recálculo y renegociación internos del contrato, o añadir sus componentes variables.

\* Posibilidad de no cumplir el nivel de servicio contratado.  
\*\* Aumento de los costes fijos.

Los servicios considerados esenciales, como los de transmisión de voz y datos o los de aplicación corporativos, tienen una mención especial con respecto a la definición estricta de los objetivos, magnitudes y prioridades, ya que de estos servicios suele depender todo el sistema distribuido e, implícitamente, toda la organización que soporta.

**c) Tarifación de los servicios:** los costes que comporta para un cliente un contrato de servicio suelen estar dimensionados entre los valores reales que comportaría hacer internamente las tareas y los costes de oportunidad, es decir, lo que comporta a la organización el hecho de no hacer ni contratar el servicio.

Básicamente, los contratos pueden ser cerrados o abiertos, según, respectivamente, si establecen un importe global y fijo para un conjunto de tareas que

hay que realizar dentro de un periodo, o si tarifican de forma individual un catálogo de tareas y miden las tareas hechas en un determinado periodo y facturan el importe correspondiente.

Los contratos cerrados son más simples, pero tienen que estar bien calculados, porque si el proveedor tiene pérdidas, justificadas por mal dimensionado del cliente\*, forzará la renegociación o renunciará. Por otra parte, la principal desventaja de los contratos abiertos es que en pocas ocasiones se establecen límites en el número de tareas individuales solicitadas, y se atomizan los servicios y se disparan los costes. En cualquier caso, el contrato especificará todos los importes, los procedimientos de certificaciones, los procedimientos administrativos de facturación o las cláusulas y costes de rescisión, entre otros datos.

\* Contratos a la baja.

**d) Descripción de los niveles de servicio:** los niveles de servicio que medirá el cliente con un contrato de servicio se determinan siempre según los criterios de disponibilidad, rendimiento a las respuestas y su exactitud.

Muchos de los parámetros utilizados en la medida del nivel de servicio de un SLA se incluyen dentro del área funcional de prestaciones y se verán con más detalle en el subapartado 5.3.1 de este módulo didáctico.

La **disponibilidad** es el primer factor que constata un usuario o cliente y está referida a la especificación del tiempo máximo –y en qué momento– en el que el servicio no es operacional, por fallos u otras causas. No basta con determinar *a priori* en qué momentos no puede haber caídas o “0” de servicio, sino con qué frecuencia y distribución se pueden producir.

Ya no son las clásicas grandes organizaciones críticas, como hospitales, aeropuertos, centrales eléctricas, instalaciones militares o centros de seguridad, entre otros, las que necesitan ventanas de disponibilidad 7 × 24\* en muchos servicios, sino que cada vez más aparecen servicios a pequeñas y medianas estructuras con estos requerimientos: la disponibilidad de los servicios web puede llegar a ser crítica para organizaciones que dependan de éstos, que hasta hace poco eran considerados de baja prioridad.

\* Es decir, “veinticuatro horas al día, siete días a la semana”.

Los **parámetros de rendimiento de respuesta** de un servicio deben cumplir las ventanas de calidad operativa, dentro de las cuales se puede llevar a cabo la actividad normal para la que están diseñados.

#### La calidad operativa

La calidad operativa es una de las medidas básicas del nivel de servicio. De hecho, el acrónimo QoS se utiliza por lo común para indicar el nivel de servicio requerido.

#### Ejemplos de parámetros de rendimiento de respuesta

Cuando un sistema continúa disponible con un fallo abierto, pero los tiempos de respuesta que proporciona son inaceptables, se tienen que establecer cuáles son los mínimos de la disponibilidad operativa del servicio. El tiempo que se tarda en hacer un trabajo, repetitivo o no, los tiempos de respuesta, los de intervención y resolución en el caso de averías, plazo de entrega de componentes y reposición, tanto máximos como mínimos, entre otros, son criterios de medida del rendimiento en los SLA.

Finalmente, las **medidas de exactitud** en el servicio proporcionado se asocian normalmente a los controles de calidad que el proveedor establece al hacer las tareas.

### Ejemplos de medidas de exactitud

Si un servicio de soporte y mantenimiento está disponible las veinticuatro horas y los rendimientos de respuesta siempre están por debajo de los máximos, pero las incidencias o consultas no quedan muy resueltas y se repiten las incidencias de forma continua, seguramente no se están cumpliendo las condiciones del contrato, en caso de que se hayan especificado de manera correcta.

Las problemáticas de exactitud, importantes pero fácilmente detectables en el marco de los servicios de soporte y servicios de *hardware* diferentes, en la vertiente de la contratación de desarrollos y servicios de *software* en general, pueden esconder graves efectos a medio y largo plazo.

El seguimiento adecuado de estos parámetros detectará rápidamente desviaciones en el cumplimiento de los contratos, a la vez que aporta una herramienta básica, junto con las áreas de gestión de fallos y de prestaciones, para detectar cambios en las condiciones preestablecidas del escenario y cumplir en el área de gestión de planificación.

e) **Penalizaciones por incumplimiento:** las penalizaciones\* por incumplimiento de contrato son imprescindibles para evitar o, al menos minimizar, los fallos de servicio en el SLA. En los esquemas más simples, las penalizaciones se ejecutan normalmente mediante restricciones o disminuciones a la facturación del proveedor del servicio (contrapago o abono), aunque si el pago es de antemano o la contraprestación no es económica, el procedimiento puede ser más complejo.

\* En inglés, *penalties*.

En cualquier caso, las penalizaciones siempre implicarán, por parte del cliente, una valoración de los riesgos de quiebra del servicio, el coste que repercute en la organización a causa de la reducción parcial o total de la actividad, y los efectos de “correctivo” que comporten para el proveedor en el futuro, así como las ventanas de aplicación y los criterios de actuación, absolutos o de tendencias.

Figura 10



La penalización de más alto nivel es, sin duda, la denuncia del contrato con las actuaciones judiciales correspondientes, si tienen lugar.

**f) Previsiones de modificación y adaptación de los contratos:** las condiciones de renegociación de un contrato deberían aparecer claramente especificadas por ambas partes, con la definición de las causas principales que pueden llevar a exigirla. Los motivos principales son, por una parte, las modificaciones en el escenario base sobre el que se han definido las características del servicio y sus tarifas y costes correspondientes y, por otra, la denuncia o agotamiento por incumplimiento de los niveles de servicio establecidos.

Es conveniente especificar las condiciones de renovación automática o renovación revisada, los incrementos vegetativos de tarifas mediante, por ejemplo, el IPC, la consideración de cambios de inventario y los algoritmos de recálculo, la revisión de las unidades de medida o los mecanismos de denuncia para ambas partes, entre otros.

Finalmente, la previsión para poder hacer bajo el marco del contrato principal contratos reducidos o anexos es una buena herramienta para tareas urgentes o no planificadas, así como para “proyectos piloto” con evaluación de nuevos servicios mediante contratos de ensayo\*.

\* En inglés, *trial agreements*.

**g) Fechas y periodos de vigencia y expiración:** los contratos de servicio se tienen que fijar a un periodo de tiempo determinado, que puede ir desde unos pocos días a varios años. Independientemente de si disponen de renovación automática, es necesario que no se los considere “eternos”, sobre todo para mantener “activo” el interés del proveedor.

Se debe tener en cuenta que los contratos de más de una serie de años presentan con frecuencia muchos problemas de adaptación, por razón del continuo cambio que se produce en el mundo de las tecnologías de la información y que hace variar, en ocasiones por completo, las condiciones del escenario tecnológico de la organización.

Hasta ahora se han visto las características de los contratos de servicio establecidos por clientes propietarios de los sistemas distribuidos. Pero el actual escenario tecnológico y empresarial favorece la existencia de organizaciones que, gracias a sistemas y redes complejas, ofrecen al mercado sus servicios, y establece los correspondientes SLA que los compromete con los respectivos clientes. Los servicios ofrecidos pertenecen a dos categorías:

- los **servicios básicos**, caracterizados por el hecho de que están directamente implementados mediante los recursos del sistema distribuido en producción,

#### Ejemplos de servicios básicos y suplementarios

Como ejemplos de servicios básicos y servicios suplementarios podemos mencionar, respectivamente, los siguientes:

Los servicios de transmisión y telecomunicación, que permiten a los clientes transmitir información, con unas condiciones de prestaciones y calidad establecidas, y los entornos pesados de sistemas y servicios de aplicación.

Los operadores de telecomunicaciones y los grandes CPD alquilados en *outsourcing*.

- y los **servicios suplementarios**, que proporcionan a los clientes la capacidad adecuada para utilizar los servicios básicos.

En la parte de los servicios suplementarios se incluyen los referidos a servicios de formación, de información general y de ayuda en línea, los de consultoría y planificación y, finalmente, los de instalación, mantenimiento y soporte del entorno.

### 3.5. Gestión de partes de incidencias y problemas

El objetivo del subsistema de gestión de partes o registros de incidencias y problemas, conocido tradicionalmente como **sistemas de trouble tickets** o TTS, es proporcionar una herramienta adecuada que reúna todos los datos referidos a incidencias, problemas y, en general, fallos desde el momento en que se detectan; las etapas de diagnóstico y contención y, finalmente, la correspondiente corrección. Todo esto proporciona una valiosa información para incidencias futuras.

Abreviaremos *sistema de trouble tickets* con el acrónimo TTS.

Las herramientas utilizadas deben permitir un seguimiento efectivo posterior de todas las etapas de la incidencia o fallo; están enfocadas en gran medida a procesos y guías de identificación, contención y resolución rápida de problemas, procedimientos siempre críticos cuando los sistemas están en producción a causa de la tensión implícita del personal administrador de la red. Cualquier información que ayude a resolver o a minimizar los efectos se utiliza también en otras tareas de gestión del sistema distribuido, como por ejemplo las siguientes:

1) **Rendimientos y cumplimientos de tareas y servicios contratados a proveedores externos (SLA)**: son especialmente importantes si los externos están relacionados con los procedimientos de detección, contención o corrección de los fallos. La externalización de los servicios de *help desk* o los centros de atención telefónica, especialistas de segundo nivel o tareas *in situ* de mantenimiento y soporte, como la reparación física de equipamiento de usuario (PC, terminales o periféricos) y enlaces de comunicación, son ejemplos comunes.

2) **Bases de datos de conocimientos**: los sistemas de ayuda a la resolución de problemas se pueden alimentar de sistemas anexos, como el de gestión de cambios o herramientas remotas de configuración y cambio de parámetros, a los que devuelve la información correspondiente, normalmente cuando el registro de incidencia es cerrado, con el fin de evitar repeticiones o extensiones del problema.

3) **Repositorio de información de históricos**: la información recogida en los *trouble tickets* contiene datos referidos a los elementos de la red que concen-

#### Incidencias

Como se ve más adelante en la gestión de fallos, una **incidencia** es cualquier éxito no deseado que aparece en un sistema distribuido en producción y que podría degenerar y afectar al nivel de servicio.

En la gestión de redes, un **fallo** es una incidencia que afecta, parcial o totalmente, al nivel de servicio deseado, tanto si es la de un componente o recurso determinado como si es la que afecta a todo el sistema distribuido.

tran más incidencias, las frecuencias, escenarios y perfiles de carga de los puntos y elementos que han resultado más críticos, así como a la efectividad de actuación de los procesos de diagnóstico y resolución, sobre todo ante emergencias. El análisis cuantitativo y cualitativo de la información será muy valioso para la gestión de planificación en cuanto al diseño de perfiles de disponibilidad y cambios evolutivos y correctivos de la instalación.

### **Ejemplo de gestión de incidencias y problemas**

En un escenario con herramientas integradas de gestión de incidencias, supongamos una red de tamaño mediano/grande distribuida en diferentes sedes relativamente dispersas. Un usuario remoto quiere acceder a uno de los sistemas corporativos de la organización, pero su PC es incapaz de establecer una conexión con el servidor correspondiente, aunque esporádicamente ha hecho anteriores accesos al servicio, hace sólo unos meses. Después de insistir, llama al único número de la unidad de *help desk* y lo notifica al operador que lo atiende. Esta etapa de soporte se conoce como **primer nivel**.

El operador, con los detalles del usuario que extrae de la herramienta de inventarios y los que le proporciona directamente, comprueba que el problema no se haya producido antes, abre un parte de incidencia y le asigna un código identificador, que proporciona al usuario. Mediante el código el usuario podrá consultar en cualquier momento el sistema de registros abiertos y conocer en qué estado se encuentra la resolución de su problema y de qué o de quién está pendiente.

Desde la sede de la unidad, el operador hace comprobaciones básicas de conectividad y disponibilidad de los elementos implicados, PC, enlace, servidores, etc., sin detectar ninguna anomalía, y consulta al sistema de TTS si hay precedentes o similitudes del problema para determinar antecedentes que orienten una posible solución inmediata. Todas las operaciones están registradas y, si la búsqueda es negativa, el operador transfiere el informe al nivel de especialistas relacionados con la materia concreta, conocidos como **segundo nivel**.

El primer especialista del área de conocimientos disponible recibirá por el sistema en línea de registros abiertos toda la información referida a este sistema, con todos los pasos, detalles o informaciones relevantes que el primer nivel haya hecho. La búsqueda en sistemas complejos de resolución de fallos, referida a efectos similares, informa de que la causa más probable es la de un defecto de configuración en un elemento de red. La consulta al sistema de gestión de cambios, referidos a los recursos comunes entre el usuario y el servidor, detalla la realización de operaciones de restauraciones de configuración hace unas semanas en los encaminadores de entrada. Un acceso a éstos mediante la herramienta de configuración remota revela que uno de ellos, el activo, tiene activado de forma incorrecta un filtro para la dirección concreta. La configuración es cambiada y reiniciada.

Todo el proceso se documenta de forma exhaustiva, incluso las acciones tomadas, los detalles de configuración o detalles útiles para la detección rápida, si se reproduce una situación similar. El sistema avisa al usuario de que ya puede iniciar el servicio requerido. El informe se cierra.

Los procedimientos asociados a la gestión de incidencias y problemas comprenden un conjunto de tareas de diseño, desarrollo, implantación y explotación de herramientas, muchas de éstas sobre sistemas informáticos complejos, que soportarán los diferentes flujos de los procedimientos y los integrarán de forma conveniente.

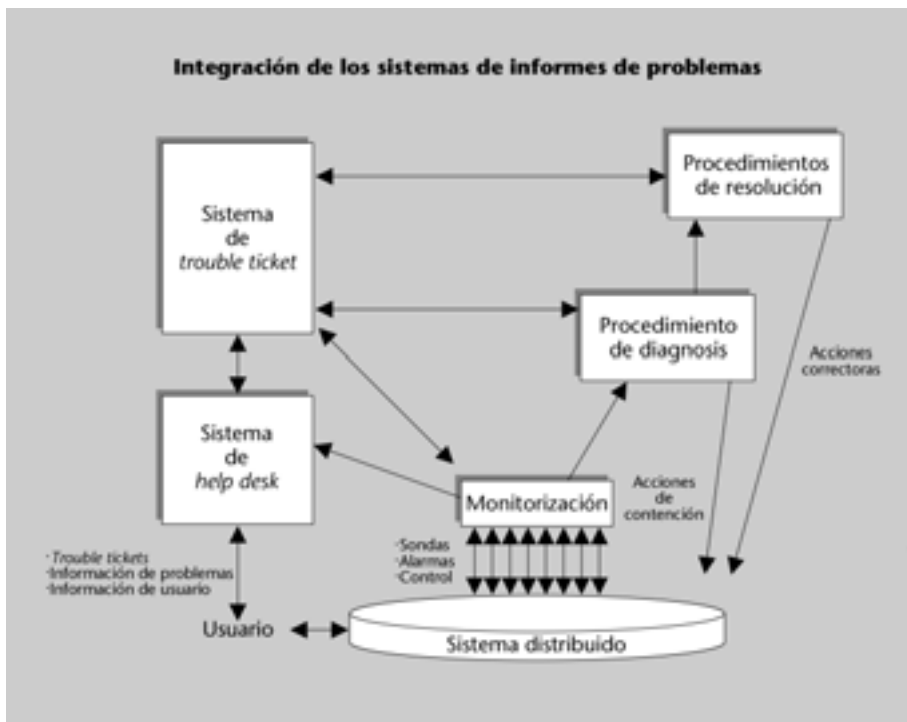
### **Normalización y estandarización de las herramientas TTS**

Hay una serie de normalizaciones y estandarizaciones con respecto a las herramientas de TTS que aseguran una interoperatividad a medida que se implantan estas plataformas. Una de las utilizadas es la **recomendación X.790 de la ITU**, que propone una estanda-

rización para las estructuras de información y la funcionalidad de las acciones y los procedimientos, de acuerdo con la definición de áreas funcionales de gestión OSI.

La recomendación define una serie de clases de objetos de gestión de los TT (MOC), que incluyen informes de problemas, informes de proveedores, los registros de *logs*, y las actividades de reparación o informaciones de contacto, entre otros.

Figura 11



Gracias al impacto positivo que tiene en las organizaciones la utilización de estas herramientas o servicios, se ha producido una proliferación de plataformas que las soportan. En un nivel general, todas estas herramientas y servicios tienen en cuenta los procedimientos básicos implicados, que son los siguientes:

a) **Diseño de la información del registro de incidencias:** la información que debe estar registrada en el TT contendrá detalles específicos de cada entorno, pero la mayor parte de los datos son de carácter genérico. Con respecto a la identificación del registro, aparecerán las fechas y horas de ocurrencia del problema y de comunicación en el *help desk*, sitios y elementos afectados, infraestructura de red utilizada, codificación inicial del problema, operador, etc., e información referida al contacto que lo comunica, tipo de entrada\*, usuario con datos de localización o datos del proveedor o tercero, si lo es.

\* Telefónica, alta remota de partes, correo electrónico, procedimientos automáticos.

La descripción del problema incluirá el estado de los componentes y del problema, prioridades, responsabilidades, descripciones detalladas, áreas afectadas, tipo de escalamiento, identificación, contacto y seguimiento de acciones de terceros. Finalmente, se especificarán las relaciones *a priori* con otros partes de incidencia, abiertos o cerrados, de la misma manera que si hay tareas de mantenimiento preventivo incluidas.

**b) Procedimientos de apertura, flujo y cierre de registros:** los procedimientos establecidos en un escenario concreto dependerán del diseño y de la organización de las unidades implicadas. Según si el centro de atención telefónica\* es interno o externo, las características del primer nivel pueden variar, sobre todo con respecto a la interoperatividad entre el usuario y el operador y el mismo sistema que tiene la incidencia.

\* En inglés, *call center*.

La asignación de partes abiertos a recursos especialistas de segundo nivel dependerá de si la organización dispone de dichos partes o de si los tiene disponibles en un momento determinado, y puede utilizar recursos externos, normalmente incluidos en un contrato de servicio (SLA\*). Los recursos de tercer nivel son siempre organizaciones externas especializadas que se encargan de tareas concretas, involucradas en la resolución de problemas de forma permanente, como por ejemplo el mantenimiento del *hardware* del fabricante, la corrección de *bugs* del *software* de base o, de forma ocasional, la reparación de una fibra rota por las brigadas de nuestra empresa cableadora.

\* SLA es el acrónimo inglés del término *contrato de servicio*.

Todos los flujos de asignación de tareas de diagnosis y resolución, y los procedimientos asociados a éstas, se gestionan mediante la herramienta de TT, que considerará la ordenación por criterios temporales, disponibilidad de recursos, prioridades de las tareas y gravedad o criticidad del problema. En general, el flujo normal de la resolución de problemas se puede ver afectado por circunstancias como las siguientes:

- De tipo cronológico, en las que a partir de un determinado periodo de tiempo puede ser más urgente solucionar la incidencia o en las que, a medida que pasa el tiempo –horas o días–, se hace más innecesaria la resolución.
- Para la localización física y geográfica, que aprovecha para resolver todos los informes abiertos, independientemente de su prioridad, en una determinada delegación remota a la que se envían recursos de mantenimiento pertinentes, o simplemente cuando se actualizan equipos en un *rack* concreto, o el *software* de un equipamiento.
- Por la naturaleza del problema y sus afectados con respecto a circunstancias de encadenamiento, funcionales o incluso de imagen externa, así como cuáles son los recursos y los actores implicados: una simple cuestión de ofimática se puede considerar grave si es la cuarta reincidencia o si el afectado “es el director general”.

**c) Asociación de registros:** el cruce de la información de incidencias y problemas es uno de los recursos de más frutos para la contención y rápida corrección en situaciones críticas. El objetivo es convertir toda la información almacenada en los TT en una base de datos de conocimientos y experiencia que se pueda tratar con herramientas sistemáticas.

Son muchos los aspectos que se pueden cruzar para determinar comportamientos relacionados. Todos estos aspectos están basados en general en las vías siguientes:

- Protagonistas comunes, como los equipamientos iguales, similares o equivalentes, las mismas localizaciones u otras próximas, o los usuarios, administradores comunes o terceros.
- Síntomas *a priori* comunes, como las observaciones de los usuarios y administradores, los efectos sobre otros componentes de la red o las alarmas recibidas.
- Medidas de solución similares o relacionadas, tanto tecnológicas como funcionales y operacionales.
- Medidas recomendadas de actuación preventivas o correctivas similares, que detectan riesgos comunes, escenarios desfavorables o estrategias poco fiables.

Cuanto más extensa sea la base de datos de conocimientos, más relaciones, cruces y, por lo tanto, conclusiones se podrán extraer. Por este motivo, las plataformas de TT aumentan gradualmente su eficacia a medida que pasa el tiempo y hay más casos registrados. Para complementar este hecho, varios proveedores ofrecen a sus plataformas conocimientos “precargados”, basados en la experiencia de otras instalaciones previas.

#### **Los productos de gestión TT**

Los productos de gestión de TT que ya se adquieren con una profunda base de conocimientos fundamentada en experiencias de otras instalaciones que se actualizan cada dos meses y que, evidentemente, se puede completar con todos los casos propios, han entrado con mucha fuerza en los grandes entornos de sistemas distribuidos, incluso con el inconveniente de su elevado coste.

Las ventajas son claras: un sistema de este tipo puede proporcionar “desde el primer día” los mismos conocimientos que un numeroso grupo de especialistas, que requieren una inversión en tiempo y coste muy alta y a veces inalcanzable.

Finalmente, la eficacia de los sistemas que cruzan la información aumenta con la utilización de técnicas de tratamiento masivo de información, como las utilizadas en las arquitecturas de “almacén” y “minería de datos”\*, y la implementación de sistemas expertos y técnicas de inteligencia artificial.

\* En inglés, *data warehouse*,  
*data mining*.

**d) Procedimientos de proceso conjunto para tareas de evaluación:** los administradores del sistema distribuido utilizan la información de los registros de incidencia, una vez que están convenientemente cerrados, como herramienta de análisis y evaluación de comportamientos, con la finalidad de disminuir su frecuencia o mejorar la eficacia de las actuaciones. El estudio puede considerar algunos de los aspectos siguientes:

- La incidencia sobre el área afectada y si la responsabilidad es suya o no (uso inadecuado de los recursos, poca formación o desinterés de aprendizaje, etc.).

- Los proveedores y fabricantes implicados (elevada frecuencia de problemas con las tareas hechas, trabajos de baja calidad, etc.).
- Los elementos afectados (familias de productos iguales o similares, etc.).
- La eficiencia de la respuesta de terceros (reiteración de problemas ya resueltos, planificaciones y trabajos preventivos, etc.).
- El análisis de periodos (tiempo medio entre fallos, tiempo medio de actuación, tiempo medio de reparación, ratios entre los tiempos planificados y los reales, etc.).

e) **Procedimientos de seguimiento y tratamiento de registros pendientes:** generalmente, la herramienta de control del flujo de los partes de incidencia detecta los que superan unas determinadas duraciones e hitos de tiempo. Esta funcionalidad es especialmente útil cuando se encadenan segundos y terceros niveles de soporte, en muchas ocasiones responsabilizados a terceros, que se pueden ver afectados por momentos de elevada incidencia o, simplemente, por tener asignada una prioridad baja.

#### **Cierre de registros pendientes no resueltos**

Un caso especial, y común, del tratamiento de registros pendientes es el del cierre de registros pendientes no resueltos. Siempre se fija un máximo de tiempo en el que un informe de incidencia puede estar abierto. En este momento, o a veces antes, se especifican y registran de forma conveniente causas de agotamiento como las siguientes:

- La no determinación del problema.
- La no reiteración en el caso de un problema intermitente.
- El cambio del escenario (cambio de los elementos afectados, actualización, obsolescencia).
- Los cambios operacionales (no se utiliza el elemento o recurso que tiene la incidencia).
- La incapacidad de solucionar el problema (*bugs* del *software* discontinuo que no se corregirán, *hardware* no mantenido o sin recambios).

Los sistemas de soporte integrado de *trouble tickets* representan una herramienta valiosa para el área de gestión de fallos, como se verá más adelante.

Ved con más detalle los sistemas de soporte integrado de *trouble tickets* en el apartado 4 de este módulo didáctico.



### **3.6. Control de pedidos y aprovisionamiento**

Aunque la relación entre nuestra instalación y los proveedores externos sigue, en general, los mecanismos tradicionales, cuando el número de órdenes de suministro a éstos es muy elevado, la organización se puede dotar de mecanismos más o menos automáticos de comunicación. Hay entornos en los que la utilización del intercambio electrónico de documentos, EDI, está convenientemente implantada. Hoy en día también se utilizan técnicas basadas en web y el comercio electrónico, para el acceso a catálogos y ofertas, pedidos en línea o seguimiento de su estado.

Los sistemas utilizados deben permitir la gestión de todos los pasos incluidos dentro de la cadena de procesos de aprovisionamiento, tanto si se refieren a nuevo equipamiento o componentes inventariables como si se trata de consumibles de cualquier naturaleza. En el momento de la petición se analiza si se disponen en *stock* o si deben ser provistos por terceros, según las prestaciones de los proveedores, acuerdos firmados o tarifas y ofertas de las que se disponga.

Las herramientas tienen que soportar el conjunto de procesos de logística, como el control y verificación de recepciones, la distribución a los lugares de instalación o almacenamiento, la gestión de los recursos humanos internos y externos necesarios para la implantación y la comprobación de su correcto funcionamiento y suministro al usuario, unidad o departamento destinatario.

Además, también se gestiona el resto de las tareas administrativas, que pueden ir desde la gestión y comprobación de los elementos y servicios facturados por los proveedores hasta el control y confirmación de pagos, según la interrelación con el área económico-financiera de nuestra organización.

Finalmente, se incluyen las tareas de gestión y control de los periodos y condiciones de garantía de nuevos elementos e instalaciones, y de los periodos de prueba y evaluación, así como el control de los momentos en los que se tienen que suscribir los correspondientes contratos de mantenimiento si proceden, los periodos de vigencia y las fechas de expiración de la cobertura.

### **Ejemplo de control de pedidos y aprovisionamiento**

En la organización que nos sirve de ejemplo, de tamaño mediano, los pedidos de cualquier recurso tecnológico relacionado con el sistema distribuido se gestionan por la unidad de pedidos del departamento de TI, que dispone de un sistema integrado de gestión de aprovisionamientos.

La manera de acceder a dicha organización es mediante el único número de atención, un centro de atención telefónica que también es el acceso a los servicios de soporte y *help desk*. El usuario es transferido al operador de pedidos, que lo identifica convenientemente, y explica de forma genérica lo que quiere: el encargo de unos nuevos catálogos de producto por parte de su supervisor hace que necesite unos dispositivos de impresión en color de determinada calidad y un periférico para escanear algunos originales. También solicita una licencia del *software* de retoque fotográfico utilizado corporativamente y el acceso urgente a un curso rápido recordatorio. Para extraer la información solicita un alta de acceso al servidor de históricos de catálogos. Finalmente, no da detalles de la conveniencia o no de cambiar las características de su puesto de trabajo, pero indica la necesidad de utilizar los requerimientos en un plazo no superior a siete días. Todas las autorizaciones serán certificadas por su supervisor.

El operador de pedidos abrirá el registro correspondiente, comprobará las autorizaciones y lanzará las sub tareas adecuadas. La primera de éstas es una orden de adquisición de los nuevos elementos periféricos, incluso el cambio de equipo, una vez consultada en el inventario la insuficiencia de la configuración de la que dispone. Si los elementos no se tienen en *stock*, se generarán los pedidos a los proveedores adecuados, según las últimas condiciones ofrecidas.

La solicitud de plaza en el curso de formación, la reserva de los técnicos de instalación, la instalación de una licencia del *software* o la autorización al nuevo servidor siguen procesos similares. La evolución de los pedidos de aprovisionamiento y servicio se puede seguir con el sistema, incluso por parte del mismo usuario. Un día antes del plazo, el equipamiento está instalado y es operativo. El usuario valida el pedido: acaba el curso al día siguiente. Los inventarios y la información del sistema de gestión de cambios son convenientemente actualizados. La facturación de los costes es imputada para contabi-

#### **Mecanismos automáticos de comunicación**

El objetivo del subsistema de gestión de pedidos y aprovisionamientos, en la gestión de la configuración de un sistema distribuido, es el de soportar los aplicativos, datos y procedimientos orientados a la adquisición de nuevos elementos y servicios, el procesamiento de los pedidos respectivos y la gestión de los proveedores y, finalmente, la actualización de los inventarios correspondientes. En ocasiones, los pedidos se hacen extensivos a todas las peticiones de servicio.

lidad interna en el departamento correspondiente y el informe de aprovisionamiento queda cerrado.

Muchas organizaciones que disponen de herramientas de gestión integradas de pedidos y aprovisionamientos utilizan también la plataforma para la gestión de todos los pedidos de servicio que llegan al departamento de TI, y no se limitan a los elementos físicos concretos. De esta manera se canalizan todas las solicitudes típicas de servicios de usuario final, como las de formación; cambios de configuración o de ubicación; actualizaciones y autorizaciones de acceso; pequeños y medianos desarrollos; operaciones de volcado, transformación o migración de datos, o soporte ofimático, entre otras.

#### El subsistema de aprovisionamiento...

... está muy vinculado a la gestión de inventarios, a la de los contratos de servicio y a la de cambios, con los que intercambia información de forma constante.

Gracias a los controles de flujos, recursos y tareas y a los instrumentos que permiten un seguimiento efectivo de todas las etapas para su posterior evaluación, el entorno de gestión de pedidos de recursos toma el papel de **entorno de gestión de aprovisionamiento de servicios** y se convierte en el núcleo de coordinación de la actividad diaria del departamento de tecnologías de la información.

Con relación a los aspectos más administrativos, la gestión de aprovisionamientos guarda mucha similitud con las plataformas utilizadas en medianas y grandes organizaciones, para el control de *stocks* y la gestión de almacenes, con las logísticas necesarias. Pero en el marco de los sistemas distribuidos se tienen que controlar aspectos más particulares, como los siguientes:

- a) Las incidencias de productos y servicios, que pueden afectar al nivel operacional de manera no proporcional a su importancia o complejidad.
- b) La criticidad de determinados elementos o servicios, que puede recomendar la adquisición de recursos con menores prestaciones, pero más probados o con una base instalada mayor.
- c) Los condicionantes de obsolescencia tecnológica, que pueden imponer la asunción de costes más importantes a la hora de la adquisición de equipamiento, sobre todo en el área de infraestructuras.
- d) La manera y condiciones en las que los recursos serán soportados por el fabricante o proveedor durante toda su vida operativa, y los compromisos que adquiere con nuestra instalación.
- e) La asociación de los costes de adquisición e implantación en los diferentes ámbitos de la organización, tanto el corporativo como el departamental y el de usuario final. Haya imputación o no, es imprescindible que los actores im-


plicados tomen conciencia del equilibrio entre costes o inversiones, y los beneficios y mejoras obtenidas.

### 3.7. Gestión de cambios

El objetivo del subsistema de gestión de cambios es planificar y coordinar la implementación de cambios en un sistema distribuido, originados por unas necesidades determinadas, que modifican el escenario tecnológico que tenía, con la intención de que los niveles de servicio preestablecidos para el resto del sistema no se vean afectados por la intervención.

La gestión de cambios incluye todas las operaciones, intervenciones, tareas, instalaciones o desarrollos que transforman un sistema distribuido, en menor o mayor medida, en un nuevo estado tecnológico, que satisface los requerimientos de la organización o de los usuarios. El incumplimiento, la adaptación o la mejora de los contratos de nivel de servicio pueden ser causas de ello.

Por otra parte, la gestión de cambios se aplica en toda intervención que requiere ser planificada, según sus consecuencias, eventualidades o condiciones, y que puede coordinar diferentes actores en diferentes procesos implicados. En instalaciones con cientos o miles de elementos y recursos sobre la red, la problemática no es sólo la realización del cambio, sino cómo se administra y gestiona éste y que mantenga siempre el control sobre cualquier efecto no previsto o deseado.

Las razones que provocan un cambio en un sistema distribuido se engloban dentro de las categorías siguientes: 

**a) Vanguardia tecnológica:** con la finalidad de continuar teniendo un papel competitivo, las organizaciones actualizan sus sistemas, aplicaciones e infraestructuras y coinciden con intervalos prefijados, crecimiento activo y vegetativo, grado de desarrollo de la competencia, disponibilidad presupuestaria, estudios y reingeniería de procedimientos o, simplemente, criterios de moda o imagen. Todos los motivos están orientados hacia una mejora del rendimiento global de la organización.

**b) Requerimientos de la gestión de incidencias y problemas:** en un sistema distribuido es muy posible que se impongan cambios a causa de incidencias que, administradas de forma conveniente para la gestión de problemas, requieren modificaciones de más alto nivel, coste o impacto y se salen del alcance de responsabilidad para su corrección.

Estas solicitudes se pueden generar antes de la aparición del problema (a la hora de disminuir los riesgos de una determinada incidencia o fallo), mientras está abierto (en las etapas de la diagnosis o, con más frecuencia, en las de resolución) o con posterioridad (recomiendan nuevas configuraciones más seguras o resoluciones más adecuadas o de menor impacto). Todos los motivos están orientados a mantener el rendimiento global de la organización.

c) **Requerimientos de producción y explotación:** a menudo los requerimientos concretos de los usuarios, en un determinado momento, no se pueden cumplir con el estado en curso del sistema distribuido. La necesidad de desarrollar un nuevo módulo de aplicación, añadir prestaciones a un componente o recurso, acceder a un nuevo servicio o simplemente cambiar de ubicación, entre muchos otros, pueden imponer cambios que acomoden los nuevos requerimientos.

La gestión de cambios tiene la responsabilidad de coordinar la planificación, la aprobación, la ejecución y la documentación y el registro adecuado.


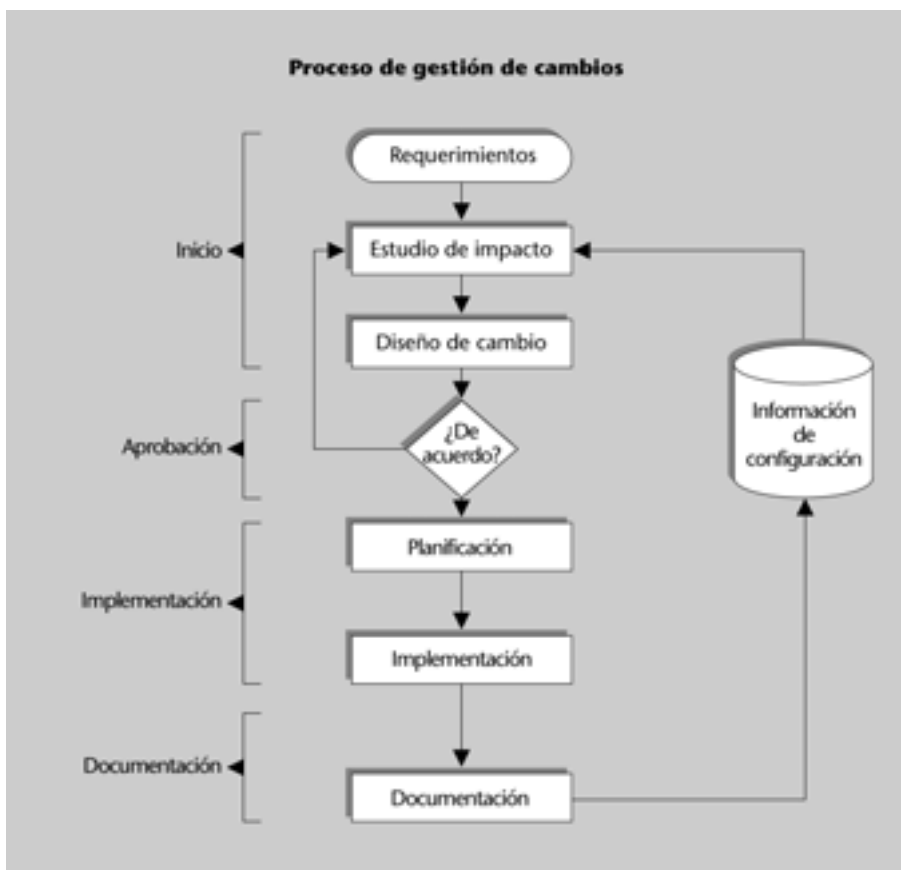
Según estas responsabilidades, el proceso de administración de cambios se divide en las cuatro etapas siguientes, secuenciadas de forma cronológica: 

Figura 12



## 1) Petición e iniciación del proceso de cambio

La petición e iniciación del proceso de cambio es la primera etapa de dicho proceso. La apertura del procedimiento puede ser a requerimiento de los usuarios o de alguna unidad de la organización, o de carácter interno del departamento de TI, por razón de la involucración con problemas abiertos o cerrados. Se tienen que especificar todos los requerimientos que aconsejan el cambio, así como todos los detalles de elementos o recursos involucrados.

### **¿Por qué no los cableados en los racks?**

Los **sistemas de cableado**, especialmente los de tipo estructurado, que tantas ventajas han aportado a las instalaciones en los últimos años, con frecuencia no se prevén en la gestión de cambios, a pesar de su importancia, hasta que se llega a situaciones críticas.

Es frecuente ver *racks*, con las terminaciones del cableado y la electrónica de red, totalmente ocultos “bajo una manta de estolones”, o *patch cords*, impenetrable e indefinida. La modificación de un enlace o su simple identificación puede ser una tarea imposible, ya que las conexiones no suelen estar registradas ni los cambios documentados, y aquí se concentran muchos de los fallos en operación real.

La **configuración de los patches** es un recurso más que hay que inventariar, y todas las modificaciones deben seguir el flujo habitual de cualquier cambio.

En el formulario de petición de cambio, que se puede iniciar mediante el acceso telefónico al centro único de atención y soporte, y mediante el diálogo con el operador correspondiente por correo electrónico o fax, o por el mismo usuario sobre el sistema de alta remota, figurarán estructuradas todas las informaciones que en aquellos momentos se conocen.

El **formulario de petición de cambio** formará parte de la documentación final y contendrá datos como la cabecera de identificación; la fecha de solicitud; los datos del solicitante, usuario individual o responsable de la unidad o departamento; localización del solicitante / localización del cambio; descripción del cambio con suficiente detalle; razones y justificaciones del cambio, elementos y recursos involucrados e identificación de inventario; componentes de la red afectados por el cambio y tipo de impacto previsto en éstos; fecha máxima de cumplimiento; personal interno o externo afectado por el cambio; personal interno o externo involucrado en el desarrollo y ejecución del cambio; personal supervisor y autorizador; cambios anteriores relacionados; prioridad y posibilidades de restaurar la situación inicial y procedimiento propuesto en caso de fallo en el cambio.

Algunos de los datos del formulario se pueden completar con las correspondientes anotaciones a lo largo del proceso del cambio.

Por otra parte, es frecuente, sobre todo en grandes organizaciones, que los detalles de esfuerzo, así como la referencia de elementos y recursos afectados, respondan a una visión acotada o limitada del sistema distribuido y minimicen el impacto real. Será necesario un estudio detallado más generalista, o **estudio de impacto**, consolidado con los datos de configuración e información de in-

ventarios. Los datos procedentes de la gestión de *trouble tickets* o de la gestión de aprovisionamientos pueden ser muy útiles, referidos, respectivamente, a la relación con informes de incidencia abiertos o cerrados y a la información de proveedores, suministradores y productos.

Toda la información referida a las características para el desarrollo del cambio debe quedar perfectamente definida en el **documento de planificación del cambio**. En general se tienen que considerar los precedentes –incluidas referencias a cambios anteriores–, la urgencia de la petición, los efectos de no hacer el cambio, la documentación de todos los procesos técnicos involucrados, los procedimientos de recursos internos y de terceros, los esfuerzos y plazos esperados, los riesgos involucrados, los costes directos e indirectos, las logísticas necesarias y el impacto sobre el nivel de servicio en la etapa de ejecución (en ciertos casos podría ser necesario el hecho de suspender el servicio parcial o totalmente sobre el sistema distribuido).

Es posible que el equipo que analiza la petición, y que lleva a cabo el estudio de impacto y el plan de cambio, llegue a la conclusión de que no es factible o recomendable su ejecución, pero deberá hacer todos los esfuerzos pertinentes para documentar y proporcionar los estudios a la comisión o unidad de aprobación.

## 2) Aprobación

La implementación de la propuesta de cambio está totalmente condicionada al hecho de que la unidad de decisión la apruebe de forma conveniente. Excepto en los casos en los que se tratan decisiones totalmente internas al departamento de TI, sin ninguna repercusión en el usuario o en la organización, los responsables de decisión tienen una naturaleza multidisciplinaria en la organización, lo que normalmente les permite tener una visión amplia de los objetivos corporativos y evaluar costes, beneficios y riesgos.

### **El serio problema de ser “juez y parte”**

Un error clásico en organizaciones pequeñas y medianas es el problema de ser “juez y parte”, es decir, que la decisión con respecto a la propuesta de cambio esté a cargo exclusivamente de la dirección informática. Es un error porque es fácil alterar la objetividad con la que se debe tratar la decisión de un cambio. Las unidades de TI pequeñas o mal dimensionadas van siempre “sobradas” de trabajo pendiente y pueden minimizar los beneficios o magnificar los costes o riesgos si el cambio les provoca un excesivo impacto en su día a día.

Así pues, la funcionalidad del sistema distribuido es como la quiere la unidad del TI, no como la quiere la organización.


A la vista del estudio de impacto y del plan de cambio, la decisión se puede clasificar como **urgente**, **ejecutable** o **no ejecutable**. Los primeros casos suelen estar referidos a cambios relacionados con problemas abiertos, pendientes de resolución inmediata. En el último caso, se puede especificar, si procede, otro análisis a partir de ciertas modificaciones en los requerimientos de usuario, un nuevo estudio de impacto con nuevas perspectivas de actuación, una

modificación de aspectos del plan de implantación o una combinación de todos éstos. En caso contrario, el registro de cambio se cierra definitivamente.

### 3) Implementación del cambio

Los cambios solicitados o aprobados se procesan para ser llevados a cabo durante esta etapa. Se tienen en consideración los respectivos requerimientos tecnológicos y funcionales implicados, que aparecen en la documentación del plan de cambio.

A partir del plan de cambio, y según los criterios de prioridad y de urgencia que aparezcan determinados en éste, o que haya modificado la unidad de decisión, se hará la planificación de ejecución. En esta planificación deben aparecer todas las subtareas implicadas en el cambio, con el detalle de las operaciones y procedimientos que hay que realizar, por qué actores y en qué momentos, los instantes de sincronización entre las tareas y los puntos de evaluación intermedia, entre otros. Es tradicional la utilización de técnicas y herramientas gráficas, con diagramas de Gantt o diagramas de Pert, a la hora de diseñar la ejecución. Si las herramientas permiten la realimentación, se facilita el seguimiento de las etapas y tareas de la ejecución y se detecta rápidamente si hay retardos u otros efectos.

Excepto en casos muy acotados y sencillos, la **ejecución de las tareas** se hace normalmente en dos etapas: 

- La primera es la **ejecución en modo de test**, que reproduce los procesos que hay que hacer sobre un entorno paralelo de pruebas, similar al real.
- La segunda, o definitiva, es la implementación sobre el entorno de producción, o **entorno real**.

El objetivo es evaluar los efectos no previstos en la planificación y es deseable que la prueba sea muy similar en el entorno de producción. Puesto que no siempre se puede disponer de entornos de ensayo paralelos totalmente equivalentes, en ocasiones se descompone la prueba en componentes que se puedan evaluar en el entorno de test por separado o, si no hay otra vía, en el entorno real pero en condiciones certificadas, que no pueden afectar a los niveles de servicio.

Si las pruebas de entorno de test son satisfactorias, se inicia la planificación para la ejecución en real. Los procedimientos de restauración a la situación previa\* tienen que estar probados y preparados para cualquier circunstancia adversa. Los resultados previstos son evaluados según las previsiones del plan, y hay que tomar nota de los tiempos de afectación en los niveles de servicio, especialmente los que implican disponibilidad de los recursos\*\*.

\* En inglés, *rollback*.  
\*\* En inglés, *downtime*.

#### 4) Documentación

La etapa final del proceso, una vez que se ha consolidado la ejecución del cambio, es la de documentación. Cuando se utilizan técnicas y herramientas adecuadas en las etapas anteriores, el registro del sistema de gestión de cambios contiene prácticamente toda la información necesaria, que se puede complementar con análisis a corto, medio o largo plazo si se cumplen de forma adecuada las expectativas.

El cierre del registro de cambio finaliza con la consolidación de todas las modificaciones en el subsistema de gestión de inventarios, y en los de gestión de incidencias y de aprovisionamiento, si se da el caso.

Desde este momento, las búsquedas en el sistema de gestión de cambios proporcionarán toda la información que desee el administrador, como el estado de los cambios en curso; informes según el usuario o departamento; componentes, recursos, fechas y periodos; prioridades o responsabilidades; informes de componentes afectados o alterados por cambios, o informes cronológicos de acciones.

La conclusión final que se puede extraer referida al subsistema de gestión de cambios es que la eficacia de sus procedimientos depende en gran parte del grado de automatización del que dispone, y aumenta a medida que se incrementa el soporte informático y se integran tareas y datos del resto de los subsistemas.

### 3.8. Servicios de nomenclatura unificada

El objetivo de la subárea de servicios de nomenclatura y direccionamiento unificado, conocidos frecuentemente como *servicios de directorio*, es el de proporcionar unos mecanismos eficientes y ágiles de acceso, manipulación y actualización de la información referida a la gestión de configuración y sus subsistemas, así como el del resto de las áreas de gestión, que puede estar repartido en numerosos y diferentes sistemas, bases de datos, ficheros o elementos distribuidos.

Los servicios de directorio representan una solución para facilitar el acceso a información de gestión del sistema distribuido que con frecuencia está contenida en una gran variedad de sistemas informáticos con diferentes arquitecturas y sistemas operativos, bases de datos implantadas sobre plataformas diferentes, aplicaciones corporativas de ámbito general y aplicaciones de gestión específica, o elementos concretos de la red.

Esta capacidad de acceso permitirá al administrador disponer de **vistas lógicas unificadas\***, independientemente del hecho de que los datos residan en muchos lugares y con formatos diferentes.

#### Nomenclatura

Para indicar los servicios de directorio también se suele utilizar la expresión *servicio de nombres (Name Services)*.

\* En inglés, *views*.

Con este mecanismo las solicitudes de información se hacen al servicio de directorio con un formato estándar, y es éste mismo el que se encarga de solicitar la petición de lectura o actualización de datos en el motor correspondiente, con su lenguaje nativo y esquema de base de datos. Si, además, los tiempos de respuesta, incrementados por el esfuerzo de traducción, se mueven dentro de los normales, la herramienta de directorios resulta totalmente funcional.


Cada aplicación vertical trabaja con sus formatos particulares, pero la transparencia del mecanismo provoca, con vistas a las aplicaciones de integración que cruzan, relacionan y presentan los datos al administrador, el efecto de estar trabajando con un motor y un repositorio único. Las funciones de importación y exportación de datos a aplicaciones paralelas fuera del entorno de gestión, como las de gestión financiera, de facturación o de recursos humanos, por ejemplo, se soportan sin más dificultad.

#### Ventajas de las vistas lógicas unificadas

Una de las primeras ventajas de vistas es que permiten disfrutar de una relativa independencia de los motores de base de datos relacionales (DBRMS) y, por lo tanto, permiten que unos sistemas convivan con los demás, implantados sobre ORACLE, Informix, DB/2, Sybase, Adabas o SQL Server, entre otros.

Figura 13



Otra de las ventajas inmediatas de los servicios de directorio es la de proporcionar la incorporación de un esquema de seguridad único y homogéneo y adaptar el acceso de los usuarios a diferentes tipos de recursos físicos (terminales, servidores, enlaces, etc.), lógicos (aplicaciones, servicios, etc.) o funcionales (autorizaciones, funciones en las aplicaciones, etc.), según su perfil único para todo el sistema distribuido. 

La solución adecuada sería disponer de un sistema único, estandarizado, de nomenclatura para todos los elementos y estructuras de información relacionados con la gestión del entorno. Los **servicios de directorio**, que en resumen se encargan de la traducción de direcciones lógicas de los recursos, se relegarían a un procedimiento más o menos provisional, limitado según el tiempo de implantación del estándar.

Sin embargo, la realidad es que durante los últimos años no sólo se ha consolidado la utilización de un estándar, sino que han proliferado nuevas propuestas de servicios de directorios, algunas de carácter general y otras totalmente vinculadas a productos y compañías concretas.

#### **Ejemplo de proliferación de propuestas de servicios de directorios**

El servicio X.500 es la propuesta de OSI para los servicios de directorio y se espera que poco a poco se convierta en el elemento común en todas las arquitecturas, aunque el proceso es más lento que lo deseado.

LDAP (*Lightweight Directory Acces Protocol*) es otra de las propuestas más extendidas. Hay muchas otras, entre las que destacan DNS, NIS y NIS+, DNA y NDS.

Para aumentar la complejidad, muchas marcas han desarrollado o adoptado servicios de directorio específicos de su plataforma o producto, como por ejemplo Lotus Notes o Microsoft Exchange.

Si el hecho en nuestra instalación es la existencia de diferentes soluciones de directorio, es preciso que haya un mecanismo que permita el acceso simultáneo y la modificación consistente e íntegra de datos en diferentes directorios. Algunos productos ya incorporan pasarelas con X.500 o LDAP, que permiten interconectar los servicios, esperando que éstos se consoliden en un plazo relativamente corto de tiempo.

### **3.9. Control de la distribución de *software***

El objetivo del control de la distribución de *software* es proporcionar un instrumento eficaz que permita conocer las características del *software* en los elementos remotos, almacenar la información de forma adecuada y, finalmente, actualizar el *software* de los elementos remotos en nuevas versiones, de la manera más automática posible.

En muchas instalaciones de tamaño mediano y grande, el conjunto de tareas relacionadas con el control y la distribución del *software* en los elementos remotos puede llegar a ocupar la mayor parte del tiempo de los equipos humanos disponibles, si las organizaciones no se dotan de las herramientas adecuadas. Hay que tener en cuenta que intervienen prácticamente todos los elementos distribuidos, tanto si son elementos de usuario (terminales, PC, periféricos, etc.) o de proceso (servidores, *mainframes*, etc.), como si es la electrónica de red (concentradores, conmutadores, *routers*, etc.).

#### **La gestión y control de la distribución del *software*...**

... se considera en ocasiones incluida en la gestión de inventarios por la fuerte interrelación que mantienen, junto con la de aprovisionamientos, entre otras.

#### **Ejemplo de control y distribución del *software* en elementos remotos**

El proceso de actualización del terminal de usuario más clásico, un PC, con los sistemas operativos más utilizados, Windows 95, 98 o NT, puede llevar a un operador una hora de trabajo por lugar, si se requiere reinstalación. Si además se tienen que instalar aplicaciones en local (ofimática, herramientas de trabajo compartido *-groupware-*, herramientas de programación, navegador web, etc.), el tiempo por lugar puede ser de tres horas.

En el peor de los casos, si la instalación tiene simplemente unos cien usuarios, distribuidos en media docena de edificios, y consideramos desplazamientos y fallos, pueden ser necesarias cuatrocientas horas, cerca de dos meses, del trabajo continuo de una persona para hacerlo. El tiempo se reducirá si se incrementa el personal (no el coste), si tenemos en cuenta que hay actualizaciones que se tienen que hacer en todo el sistema al mismo tiempo o en grandes áreas a la vez. Si éste fuera el caso, con un tiempo máximo de tres días sin ningún tipo de servicio informático, necesitamos diecisiete técnicos para llevar a cabo dicha instalación.

Si la red tiene una magnitud de centenares o de miles de usuarios, las cifras son, cuando menos, absurdas.

La complejidad de este subsistema no sólo se deriva del problema de la sustitución o actualización del *software* en elementos remotos, sino también del control y la verificación de la configuración *software* existente, con todas las opciones, versiones y parámetros en los que se configura. El conocimiento de las características existentes y necesarias en cada nodo en el que se ejecuta, instala o actualiza un *software* será esencial. Muchos de los detalles de configuración serán proporcionados por la gestión de inventarios, de aquí la importante interconexión entre los subsistemas.

La administración de licencias de determinado *software* merece una mención especial. Hay productos *software* que permiten, en una instalación distribuida, disponer de un número de licencias global, que se pueden instalar en todos los lugares que sea necesario mientras que no se supere, lógicamente, el número de licencias adquiridas. Incluso hay fabricantes que permiten la instalación del *software* sin limitación de número mientras la organización se responsabilice, *de jure* o *de facto*, de que no se ejecuten de forma concurrente más licencias que las adquiridas.

Sin embargo, en el otro extremo se sitúan productos que están serializados e identificados para cada instalación o actualización, normalmente con la finalidad de evitar fraudes de copia o utilización ilegal (sin la licencia adecuada). Muchas de las facilidades de clonación o copia masiva no se pueden utilizar, hecho que requiere una intervención particularizada del operador.

### **La “piratería informática”**

A pesar del concepto “popular” de que los productos de *software* se pueden copiar sin problema (¿por qué hay que pagar por una cosa que ya tenemos y gratis?), la política de control de licencias se va extendiendo, por fin, a las medianas y pequeñas organizaciones. La lucha contra la “piratería informática”, el fraude informático del uso no licenciado de programas es cada vez más contundente, y se le destinan cantidades muy grandes de dinero (siempre mucho menos del que se pierde por miedo al fraude). No vale la pena arriesgarse a escándalos y sanciones, en ocasiones cien veces superiores al coste de la licencia.

A grandes rasgos, las fases de actuación de este subsistema en un entorno genérico comprenden las tareas siguientes:

- Conocimiento de la configuración actual en cada nodo.
- Selección (si es factible) del producto que hay que utilizar, distribuir o actualizar.

- Planificación de la distribución y selección de los nodos involucrados.
- Distribución del *software* en los nodos mediante técnicas de imposición desde el administrador\* o por solicitud de cada nodo al nodo administrador\*\*.
- Instalación, actualización y reconfiguración.
- Control de licencias.
- Actualizaciones de inventario.
- Monitorizaciones remotas.

\* Herramientas *push*.  
\*\* Técnicas *pull*.

Según el tipo de procedimiento utilizado para la distribución remota, las herramientas se clasifican en manuales y automáticas:

1) Las **herramientas manuales** efectúan el análisis remoto a partir de requerimientos del operador de una manera mayoritariamente interactiva y lanzan diferentes sondas o mecanismos *software* o establecen sesiones en remoto\* para conocer las configuraciones y versiones de cada elemento. Según los resultados se tomarán las acciones oportunas.

\* En inglés, *rlogins*.

2) Por otra parte, las **herramientas automáticas** permiten hacer todas o, al menos, gran parte de las tareas y fases de actuación mediante procedimientos de *software* preconfigurado. El análisis remoto y la distribución e instalación se pueden hacer con periodicidad y ejecutar sin la intervención del operador (en *background*). Incluso ya hay herramientas que permiten la realización de estas operaciones en tiempo de producción, es decir, mientras se lleva a cabo la actividad cotidiana de los usuarios.

#### Actualización en tiempo de producción

Gran parte del *software* ofimático y determinadas funciones de los sistemas operativos del puesto de trabajo permiten actualizar componentes *software* periódicamente o al producirse un determinado acontecimiento (a la hora de hacer el *login*, al lanzar las aplicaciones, etc.), si aseguramos que la instalación siempre está en un estado actualizado y uniforme.

En estos momentos, la opinión de la industria está dividida en dos enfoques que se relacionan en gran medida con la problemática de la distribución del *software*:

1) Por una parte están los que alimentan la idea de que los sistemas de usuario final, equipos de sobremesa\*, mayoritariamente PC, deben continuar creciendo en prestaciones, velocidades, espacio en disco, memoria, para poder contener y ejecutar el *software* de terminal cada vez mayor y más pesado.

\* En inglés, *desktops*.

2) La posición contraria viene de los que creen que el *software* del terminal debe ser lo más ligero posible, la potencia debe residir en los sistemas y servidores centrales y la capacidad tiene que darla la red, que transportará lo que sea necesario.

#### Hechos sobre la problemática de la distribución del *software*

Es cierto que la potencia de un PC actual permite cosas inimaginables hace diez años para un ordenador de su precio y tamaño. Sin embargo, también es cierto que la voz de alarma

suenan cada vez más fuerte en contra de los crecientes costes asociados de mantener y actualizar el *software* y reemplazar los equipos (obsolescencia forzosa a los dos o tres años), especialmente en las grandes organizaciones con miles de usuarios, que no pueden o quieren mantener la curva de inversión.

Hay cálculos hechos por prestigiosas consultoras que estiman que el coste de mantener operativo un sitio de tipo PC, incluso el importe de adquisición, las cuotas de mantenimiento, las licencias del *software*, las averías y problemas, y la pérdida que éstas provocan, entre otros, oscila entre los cuatro mil y los seis mil dólares/año. Muchas compañías grandes lo corroboran. Los defensores y fabricantes del “cliente pesado” (*thick o fat client*) lo consideran una total exageración.

Por este motivo, las arquitecturas basadas en la simplificación de los clientes, arquitecturas de “cliente fino” (*thin clients*), están adquiriendo más adeptos, sobre todo en estas grandes organizaciones. Se calcula que ya hay más de un millón de sitios inspirados en esta filosofía (PC en modo terminal, terminales gráficos Windows, Network Computers, etc.), y son pocos comparados con el número total de PC con configuración clásica.

Sin ninguna duda, el impacto en los próximos años de una vía u otra tendrá consecuencias positivas y negativas, por las tareas de actualización y mantenimiento cada vez más complicadas. El éxito está asegurado *a priori* por los nuevos entornos que minimicen el esfuerzo de gestión y administración.

### 3.10. Otras subáreas incluidas en la gestión de la configuración

Hay una serie de funciones y tareas complementarias que también suelen estar agrupadas como subsistemas de la gestión de configuración, generalmente por la fuerte interrelación que tienen con la gestión de inventarios o la de aprovisionamientos, entre otras.

Una de las funciones que con frecuencia es más asumida por el área de tecnologías de la información en una organización es la **gestión de activos fijos**. Se conoce así la extensión que se incorpora en la gestión de inventarios referida a los aspectos económicos relacionados con los elementos.

#### Terminología

La gestión de activos fijos se conoce por lo común como *asset management*.

De esta manera la organización puede planificar, analizar y desarrollar políticas de inversión sobre la base de criterios adicionales a los puramente tecnológicos, como el coste de adquisición, el coste de producción, las amortizaciones soportadas, la reevaluación de infraestructuras, la rentabilidad de los elementos adquiridos y alquilados o las reevaluaciones del potencial humano, entre otros. Así pues, los cálculos relacionados con el “coste de propiedad” de los medios e infraestructuras de la organización se pueden calcular con la certeza de que los elementos son los que hay realmente en cada momento.

Otra función, en ocasiones generalizada dentro de la gestión de la configuración, es la **gestión de operaciones**. Se incluyen todas las tareas que desarrollan los administradores y operadores del sistema distribuido, de manera más o menos cotidiana, en el proceso de mantener la instalación en producción.

Prácticamente todas las tareas de operación de un sistema en producción se tratan e incluyen en diferentes subsistemas de las áreas del modelo OSI, tanto de configuración como de fallos, prestaciones, contabilizaciones o seguridad.

Pero es cierto que en instalaciones complejas la información referida a las tareas cotidianas se almacena y trata de manera agrupada, facilita el seguimiento y disminuye errores de operación.

### **Ejemplo de agrupación del tiempo de operación**

Si las tareas que tienen que hacer los operadores de un gran centro de cálculo, referidas a numerosos aspectos de la administración cotidiana del sistema, están recogidas y gestionadas por una única herramienta, que interacciona la información con los correspondientes subsistemas de seguridad, fallos, configuración, etc., conocer en cada momento qué tiene que hacer cada persona es más fácil.

Si la instalación requiere trabajos distribuidos en turnos, o si cambian procedimientos clásicos y antiguos, repetidos hasta la fecha cientos de veces, es posible que los administradores ejecuten procesos erróneos o varíen el orden correcto de lanzamiento de los procesos, simplemente por cotidianidad (siempre lo hacen, o lo hacían, de otra manera), con la consiguiente afectación al nivel de servicio. Una herramienta integrada que organice, informe y controle la actividad de operación en cada momento será muy útil.

## 4. Gestión de fallos

La gestión de fallos es una de las áreas más importantes dentro del modelo OSI por la responsabilidad que tiene con respecto a mantener el nivel de servicio, QoS requerido, ante incidencias en el sistema distribuido. Muchas organizaciones inician la racionalización de la administración de sus sistemas por el área de fallos, que suele ser, pues, la más dotada de medios.

### 4.1. Introducción

El primer objetivo de la gestión de fallos en un nivel más operacional es el de incrementar y asegurar un adecuado grado de confianza con el sistema distribuido, y proporciona a los administradores herramientas que detecten y localicen problemas lo antes posible, ayuden a aislar elementos conflictivos y proporcionen mecanismos de recuperación y resolución rápidos y eficaces.

#### Terminología

El área de gestión de fallos se conoce normalmente en los textos como *fault management*, FM.

Dado que un fallo se considera genéricamente como una desviación de los requerimientos predefinidos con respecto al nivel de disponibilidad y operación de un elemento, servicio o función del sistema, la gestión de fallos engloba todo el conjunto de procedimientos y tareas, previos y posteriores a los que suceda, encargados de mantener el nivel de servicio, o QoS exigido, y que aseguran unos mínimos bajo cualquier circunstancia. Éste es su objetivo estratégico.


El horizonte general de las actividades de gestión y administración de fallos está esencialmente orientado a corto y medio plazo, ya que en este momento se tiene que asegurar el servicio. La eficacia de las medidas de contención, que nos permitirán contener el nivel de servicio dentro de unos márgenes, será esencial. Pero hay otras tareas que no se tienen que hacer bajo la presión del sistema bajo mínimos, que están orientadas a la prevención, a la mejora de los mecanismos de contención y al diseño de la eficacia de las soluciones, que tienen horizontes a más largo plazo y que se adaptan a los cambios a los que el sistema esté sometido.

En un ámbito general, las diferentes tareas que se hacen dentro de su marco incluyen las siguientes:

- Monitorización del estado del sistema distribuido.
- Normalización, establecimiento, recepción y reacción en las alarmas.
- Diagnóstico de las causas de fallos.

- Jerarquía de causas y efectos.
- Mecanismos de aislamiento de elementos con fallos.
- Implementación de mecanismos y barreras de propagación de errores.
- Diseño y pruebas de mecanismos de contención y de medidas de recuperación.
- Interactuación con el subsistema de problemas e incidencias\*.
- Recepción de notificaciones de incidencias y problemas desde las otras áreas, especialmente la de prestaciones y seguridad.
- Soporte e información a los usuarios en condiciones de fallo.

\* En inglés, *trouble tickets*.

La interpretación de los términos que intervienen en la nomenclatura de los acontecimientos relacionados con la gestión de fallos puede llevar a ambigüedad. Ésta es la interpretación más habitual: 

#### Nomenclatura de sistemas tolerantes a fallos

Hay metodologías diseñadas para definir sistemas tolerantes a fallos que denominan **fallo** a un defecto en el sistema, **error** a una alteración de las condiciones de servicio y **fallida** al hecho de que el sistema esté fuera de servicio.

- Un fallo (*fault*) es un estado, provocado por cualquier problema o combinación de problemas que afecta al nivel de servicio, parcial o totalmente, de manera localizada o extendida.
- Un problema es un estado no deseado en el sistema, provocado por una incidencia que no afecta al nivel de servicio pero que puede originar un fallo si degenera.
- Una incidencia es cualquier acontecimiento que podría estar relacionado o no con una degeneración posterior a un problema o fallo, y que hay que analizar.

#### Ejemplo de las tareas efectuadas por la gestión de fallos

En el centro de atención a usuarios de nuestra organización han entrado dos nuevas incidencias, una referida a los problemas que tienen una serie de usuarios de una misma unidad con su impresora departamental, y la otra a unas cuantas desconexiones del servidor sufridas a lo largo de la mañana en algunos puestos de trabajo de una delegación concreta.

El operador del *help desk* extrae información para la incidencia de impresión sin poder determinar *a priori* cuál es la causa. El fallo se traspasa a los especialistas de segundo nivel mientras que el operador redirecciona las correspondientes colas de impresión a una impresora análoga próxima. Los usuarios pueden imprimir y el fallo está contenido.

En el momento de iniciar el análisis de las desconexiones, recibe en la pantalla la notificación de emergencia desde el sistema de gestión de fallos porque el enlace *frame relay* con la delegación ha caído completamente. La información es muy útil, porque éste se encarga de notificarlo a los supervisores corporativos correspondientes y de atender a las decenas de llamadas de usuarios que se empiezan a producir y que notifican que no pueden trabajar.


El equipo de administradores no puede recobrar el control del enlace desde el centro de gestión, pero a los quince minutos hay personal técnico externo desplazado, notificado automáticamente por el sistema. La reinicialización rápida del enlace no responde (parece ser causa del operador) y se piden instrucciones al centro de gestión. Los administradores consultan las posibilidades de que disponen y deciden hacer una serie de líneas RDSI multiplexadas para restablecer un enlace alternativo. La operación ya se ha hecho con anterioridad, se buscan los informes de incidencia que la detallaban y se inician los cambios de reconfiguración en los servicios centrales respectivos. El correcto seguimiento de los pasos especificados permite levantar el enlace en sólo quince minutos, y el servicio queda operativo con la restricción del 33% de usuarios (para restringir la carga, no conviene que trabaje uno de cada tres) y la desconexión de los servicios web.

Al mismo tiempo, los técnicos del operador, orientados por los perfiles de rendimiento, acontecimientos de reinicialización y microcortes registrados durante las últimas semanas, comunican la naturaleza física del problema y dan una ventana máxima de resolución de seis horas, después de las cuales el enlace se podrá restablecer. Los administradores planifican la restauración del servicio en las condiciones iniciales y abren las tareas de diseño oportunas para que las medidas de contención con el enlace alternativo se habiliten automáticamente o justo con intervención en remoto.

Mientras tanto, ya se ha desplazado un técnico a la impresora en cuestión. Todas las pruebas de prediagnóstico son correctas, pero es cierto que en ocasiones los trabajos quedan degradados. Si la comparamos con la otra que funciona correctamente, no hay diferencias, y el técnico procede a cambiar los componentes diferentes. El procedimiento de “prueba y error” empieza por la casuística más sencilla: el cambio del cable de conexión por uno nuevo. Las pruebas son satisfactorias. La diagnosis no ha sido inmediata, pero la resolución está confirmada.

## 4.2. Problemas específicos de la gestión de fallos en los sistemas distribuidos

La gestión de fallos ha sido bien definida por los sistemas de información tradicionales hace muchos años. Sin embargo, aunque no es extraño encontrar metodologías utilizadas en los grandes entornos centralizados de los años setenta, con toda la coherencia y aplicabilidad genérica para hoy en día, la dificultad de los entornos distribuidos actuales, totalmente basados en redes, hace muy complicada la gestión de fallos si, como veremos, ésta no está bien dotada de las herramientas adecuadas.

Las problemáticas específicas de esta área asociadas a los sistemas distribuidos son las siguientes: 

### a) Imposibilidad de operación plena si en determinados elementos de la red hay problemas o fallos.

En la época en la que los sistemas de información sólo se basaban en grandes *mainframes* centralizados, la facilidad para hacer seguro y fiable todo el entorno estaba circunscrita a los recursos que los administradores tenían a su lado o a unos pocos metros.

La interrelación que tienen los recursos en los sistemas distribuidos actuales es un factor que maximiza la rentabilidad de su utilización, basada en una compartición de muchos de estos recursos. Sin embargo, por otra parte, es factible que el fallo en un determinado elemento afecte al servicio de muchos otros recursos, o a un servicio o elemento al que no habíamos previsto que estaría correlacionado. Estas circunstancias aseveran los hechos reales de que en una red un componente de sólo unos miles de pesetas puede derribar sistemas de cientos de millones y provocar las pérdidas pertinentes.

Los componentes tecnológicos de un sistema distribuido no pueden asegurar nunca al 100% que no tendrán ningún fallo. Hoy en día, la electrónica, los enlaces de comunicación o el mismo *software* pueden tener niveles de fiabilidad muy altos, pero en absoluto esta fiabilidad es total. Dado que no se pueden evitar los efectos comentados de degradación encadenada del servicio, si hay un fallo en determinados componentes, la primera medida que se utiliza es la redundancia.

La **redundancia** implica la existencia de más de un recurso para hacer una determinada función. En caso de fallo en uno de éstos, la función puede continuar siendo desarrollada por otro u otros. El servicio así mantenido no cae, y se puede resolver el fallo con la reparación, modificación o cambio del recurso dañado. Es, pues, una medida de contención (asegura un determinado nivel de servicio), no de corrección (restaura la condición prefallo).

No debemos caer en una confusión común:

**redundancia ≠ gestión de fallos.**

La redundancia es una herramienta imprescindible para la gestión de fallos, pero no es, en absoluto, el fin mismo del área.

Los **sistemas redundantes**, o **sistemas de vías alternativas**, implementan diferentes mecanismos de funcionamiento que se pueden combinar entre sí como los siguientes:

- **Elementos redundantes estáticos:** los elementos redundantes están ociosos mientras el elemento principal hace las tareas. Si hay un fallo en el principal, éste o éstos asumen las tareas. La rentabilidad de los elementos redundantes es nula mientras no haya fallos (lo más deseable).
- **Elementos redundantes dinámicos:** todos los elementos se reparten las tareas o carga, y todos disponen de bastante capacidad residual para que, en caso de fallo de uno, éstas sean soportadas por aquel o aquellos que continúan el servicio.
- **Redundancia pasiva:** la conmutación de la asignación de tareas o carga entre un elemento que ha fallado y el elemento redundante siempre implica una afectación importante, total o parcial, del servicio. En ocasiones es necesaria la intervención manual de los operadores.
- **Redundancia activa:** el procedimiento de conmutación entre el sistema principal, con un fallo, y el sistema o sistemas secundarios (redundantes) es totalmente automático y transparente y no afecta al servicio, como en el proceso de restauración, una vez resuelto.

### Los sistemas RAID

Aunque toda la redundancia es cara, hay elementos que por su extensión de uso han conseguido mecanismos redundantes eficaces y perfectamente asumibles en términos de coste.

Uno de los mejores ejemplos es el de las técnicas **RAID** (*Redundant Array of Inexpensive Devices*), que consiste en la utilización de muchas unidades de disco baratas, en lugar de las muy caras y fiables (?), combinadas entre sí con elementos *software* y *hardware* y mecanismos de redundancia de datos, que permiten tolerar que uno de los discos deje de funcionar, sin perder un solo byte. La unidad averiada puede ser retirada, con frecuencia en caliente (*hot swap*), y lanzada mientras insertamos otra nueva. Las configuraciones RAID 1 (discos en espejo o *mirroring*) y RAID 5 son las más utilizadas.

La redundancia es la única técnica que asegura procedimientos de contención eficaces, pero no es barata. Además del coste duplicado, como mínimo, de la adquisición de los elementos, aparecen costes importantes asociados a la capacidad y medios de conmutación entre los recursos. A los instrumentos de detección del fallo se tienen que añadir nuevos enlaces, electrónica de red, *hardware* especializado y, sobre todo, *software* de control. La simple redundancia de un servidor de base de datos puede representar incluso entre tres y cinco veces el coste del sistema único, si la configuración es activa y dinámica, por ejemplo.

#### **b) Detección, identificación y diagnóstico lentos y poco eficientes.**

Los procesos iniciales de la gestión de fallos permiten conocer que se ha producido un fallo, saber cuál es e, incluso, aventurar o determinar sus causas.

Sin embargo, con frecuencia, en muchas organizaciones estos procedimientos son lentos y poco eficientes y se mueven por impulsos y reacciones “nerviosas”. En estas circunstancias los tiempos de caída\* pueden ser muy elevados y sin ningún perfil determinista para sucesivas reincidencias.

\* En inglés, *downtime*.

La causa de que los tiempos de caída sean demasiados altos suele ser la incorrecta o insuficiente instrumentación y la inadecuada correlación entre las diferentes alarmas. Las herramientas de gestión que permiten ayudar a los administradores a tomar las observaciones y decisiones correctas mejoran de forma sustancial los procesos de diagnóstico y evitan que la asignación de recursos humanos expertos en la determinación del fallo aumente exponencialmente. Los subsistemas de *trouble ticket*, en ocasiones asistidos por sistemas expertos y técnicas de inteligencia artificial, tendrán un papel esencial.

#### **c) Integración insuficiente de la gestión de fallos dentro de todo el marco de gestión del sistema distribuido.**

Si la integración de la gestión de fallos con el resto de las áreas de administración del entorno no tiene unos niveles mínimos, difícilmente se podrá conseguir una respuesta eficiente en toda la cadena de procesos asociada a un fallo.

Es bastante común que los centros de administración de la red se encuentren llenos de consolas que monitorizan algunos sistemas concretos, otras referidas a determinados aspectos de administración y, finalmente, las de algún producto de integración de información de gestión. Si el entorno es grande, habrá un considerable número de operadores y administradores que pueden, por cuestiones obvias del día a día, no comentarse acontecimientos u observaciones que pueden ser vinculantes para otro.

Por otra parte, el cruce con la información del resto de las áreas OSI resulta esencial: ¿qué elementos y con qué configuración? (configuración); ¿qué niveles de rendimiento había antes/después? (prestaciones); ¿quién o qué la ha utilizado? (seguridad); ¿cómo/cuándo se utiliza? (contabilización). Éstos son ejemplos genéricos. Este intercambio de información es básico para mantener una “vista única” del fallo sobre el sistema distribuido, facilita la integración y permite el análisis de dependencias y correlaciones.

Desde el punto de vista de los administradores, el principal beneficio que se obtiene de la adecuada gestión de fallos es romper el “ciclo de apagafuegos” (o de bomberos), escenario muy grave y muy frecuente en determinadas organizaciones a causa de una mentalización de administración sólo correctiva.

### ¿Informáticos o bomberos?

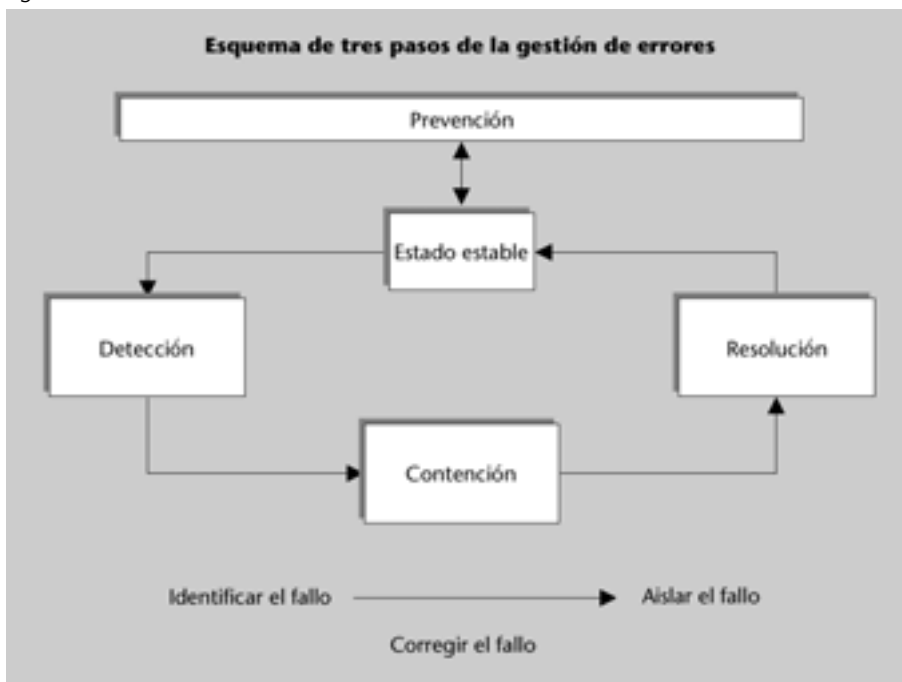
En los ciclos de apagafuegos (*fire fighting*) no queda tiempo para planificar, analizar los riesgos, variar la instalación y adoptar otras medidas preventivas.

La permanencia de los administradores en un estado de emergencia continua, haciendo de bomberos en cada momento y empalmando una incidencia o desastre tras otro, sólo lleva a la ineficacia y desmoralización personal, por las continuas quejas de los superiores y de los usuarios.

### 4.3. El esquema de los tres pasos de la gestión de fallos

Desde un punto de vista simplificado, pero muy ilustrativo, el flujo de la gestión de fallos se representa con frecuencia mediante el denominado **esquema de los tres pasos**, que consta de las etapas siguientes:

Figura 14



1) **Identificar el fallo**: detectar e identificar correctamente los efectos y pre-diagnosticar un fallo.

2) **Aislar el fallo**: tareas que permiten la no propagación del fallo y sus efectos, y procesos y mecanismos de contención, que mantienen un determinado nivel de servicio. El fallo continúa abierto.

3) **Corregir el fallo:** procedimientos que posibilitan la restauración de la situación prefallo, con todas las garantías *a priori* de que las causas concretas son eliminadas, y que reemplazan componentes dañados, cambian las configuraciones o características o sustituyen elementos, topologías, equipamiento o *software*, entre otros.

Uno de los aspectos más significativos del esquema de los tres pasos es que las etapas no son estrictamente secuenciales. Sólo lo son en el momento de inicio y finalización de cada una de éstas, y normalmente son procesos discontinuos.

#### Ejemplo de detección, contención y corrección de fallos

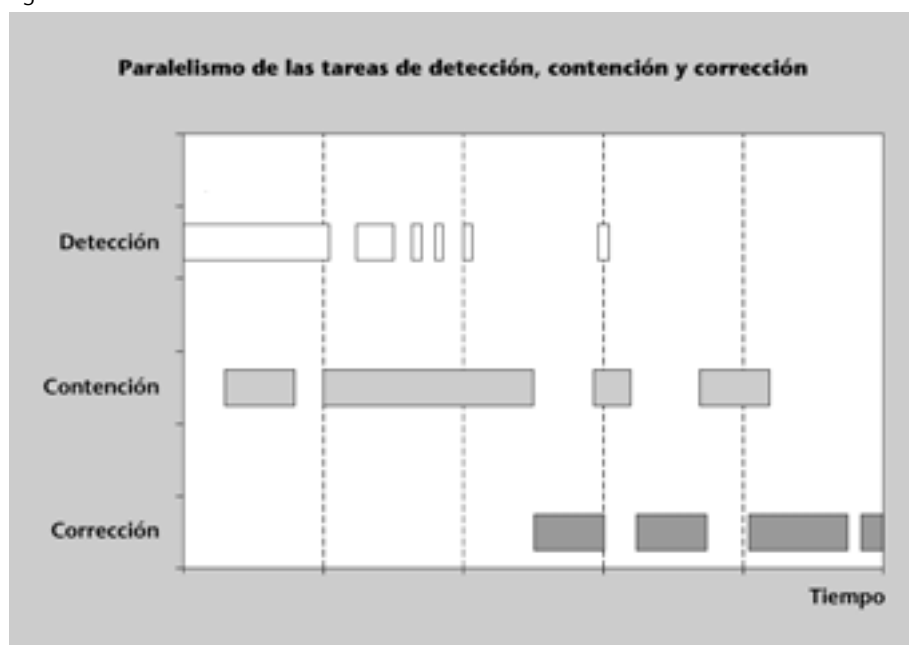
En un servidor de base de datos, dotado de sistemas de disco redundantes, se produce un error de lectura en uno de los discos. Los agentes y sondas correspondientes detectan el fallo, desconectan el disco del error y mantienen el servicio mediante los mecanismos RAID incorporados. En la consola del administrador una alarma muestra el fallo, los elementos afectados y el estado actual. En este momento ya se han producido procesos asociados a la detección y contención del fallo.

Aunque la primera diagnosis es el fallo físico del dispositivo, el administrador consulta la herramienta de incidencias y problemas buscando referencias similares. Hace dos meses se produjo un fallo similar en la delegación de Canarias y después del cambio del disco, aparentemente dañado, el fallo se repitió al cabo de unas horas. Hicieron falta diferentes jornadas para determinar la posible inestabilidad en un módulo del *software* de RAID en el servidor, que se reemplazó por una versión corregida, y así se resolvió el fallo.


A causa de que el proceso requiere reinstalar el *software* de control de los discos, el administrador traspasa la base de datos del primer servidor al servidor de base de datos secundario. La operación se hace de noche, y aprovecha las detenciones para hacer las copias de seguridad. A continuación se actualiza el *software* conflictivo en el primer servidor y se hacen pruebas exhaustivas durante la jornada de la mañana. La producción se mantiene con el segundo servidor.

Las pruebas son satisfactorias. La misma noche se hace el proceso inverso hacia el servidor primario. Después de las pruebas adecuadas se restaura la situación prefallo. Ésta se cierra con una secuencia de tareas discontinuas de detección, contención y corrección.

Figura 15



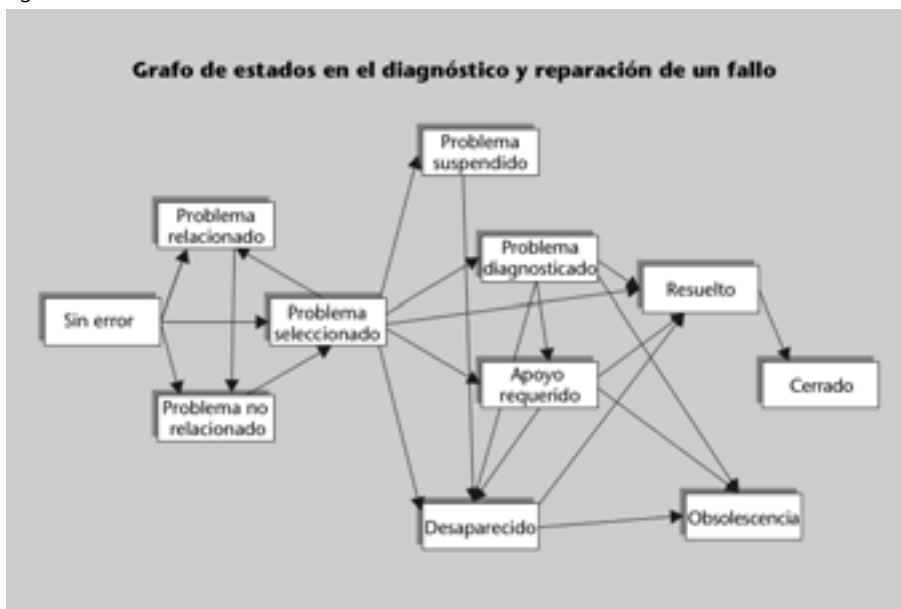
#### 4.4. Funciones y esquema general de la gestión de fallos

Las funciones y flujos de información concretos que son desarrollados por los procesos y herramientas de soporte de la gestión de fallos extienden, con criterios más operativos, las etapas del esquema de los tres pasos. Son las siguientes: 

- 1) Supervisión del sistema distribuido y gestión de alarmas.
- 2) Apertura y actualización de la gestión de incidencias.
- 3) Medidas de contención inmediata y diferida.
- 4) Análisis y determinación de causas del fallo.
- 5) Corrección del fallo y las circunstancias de éste.
- 6) "Test", restauración y cierre.

En la figura 16 se representa el flujo de la diagnosis y resolución de un fallo, englobadas en las funciones mencionadas. Algunas de éstas se desarrollan a continuación.

Figura 16



##### 4.4.1. Supervisión del sistema distribuido y gestión de alarmas

La primera de las etapas para el procesamiento de fallos se encarga de las tareas asociadas al diseño, activación, remisión, filtrado y proceso o resolución de alarmas.

Una **alarma** en un sistema distribuido es la notificación, establecida y programada *a priori*, que hace un objeto en el sistema de gestión para indicar que se ha producido un determinado hecho en su contexto, referido normalmente a una incidencia o problema, y que podría originar o, incluso, haber originado un fallo.

Todas estas tareas se agrupan en cuatro bloques de subfunciones.

### 1) Extracción de información basada en los monitores

En el sistema distribuido todas las alarmas son generadas por unos elementos *hardware* y *software*, añadidos y ligados al mismo objeto, denominados **agentes de monitorización** (*agents* o MoAg). Estos agentes contienen, entre otros elementos, las sondas que permiten detectar los acontecimientos, el *software* de control, activación y codificación, y el soporte del protocolo de información de gestión utilizado para comunicar con el sistema de gestión, lógicamente mediante la misma red.

El **acontecimiento** es un cambio del estado de un parámetro o condición, que dispone de la sonda correspondiente para ser registrado cuando ocurre y que tiene significado para la gestión del sistema.

De los millones de cambios que suceden en un elemento (desde el punto de vista informático, millones de operaciones y cambios internos, bus, registros, memoria, etc.) sólo son acontecimientos los que se pueden detectar de forma inequívoca en todas las condiciones.

Las alarmas generadas por los objetos del sistema obedecen a una condición preprogramada, y previamente activada, de observación de determinados acontecimientos. Pueden ser un cambio de tipo booleano (haya portadora, desbordamiento, componente no preparado, proceso corriente, etc., o no) o el valor de un parámetro que supera un máximo o un mínimo en una escala (tiempo de espera superior a cinco segundos, 80% del CPU, menos del 5% de ocupación del canal, etc.).

Es muy frecuente que un acontecimiento determinado producido en el sistema, adecuadamente detectado por el agente de monitorización, ya represente, *per se*, una condición de fallo. Es posible que no represente todavía un fallo, pero que el administrador quiera conocer que se ha producido tal hecho, que puede ayudar a prevenir un fallo posterior. En los dos casos hay que generar la alarma correspondiente. Hay dos mecanismos para dar a conocer al sistema de gestión, y por consiguiente al administrador, la alarma producida. Son los siguientes:

a) La **transmisión de acontecimientos de alarma\***: es el sistema más utilizado y, para determinados tipos de alarmas, las críticas o las que requieren actuación inmediata, es imprescindible. Consiste en el envío hacia el sistema de gestión de la PDU\*\* correspondiente, con los códigos de identificación de la alarma, el acontecimiento y, lógicamente, el objeto, de la manera más compacta posible. Es muy eficiente, pero cabe la posibilidad de que la información

#### SNMP y CMIS/CMIP

SNMP (*Single Network Management Protocol*) es uno de los más populares protocolos de gestión utilizados en las redes actuales, sobre todo LAN y MAN. CMIS/CMIP es la propuesta de la OSI, muy potente pero pesada, muy utilizada en los entornos de operador de telecomunicaciones. Hay muchas más pilas de protocolos utilizadas, tanto propietarias como de uso estandarizado.

\* En inglés, *traps*.

\*\* PDU es la sigla de *Protocol Data Unit*.

no llegue al destinatario, porque nunca utiliza una comunicación orientada a la conexión.

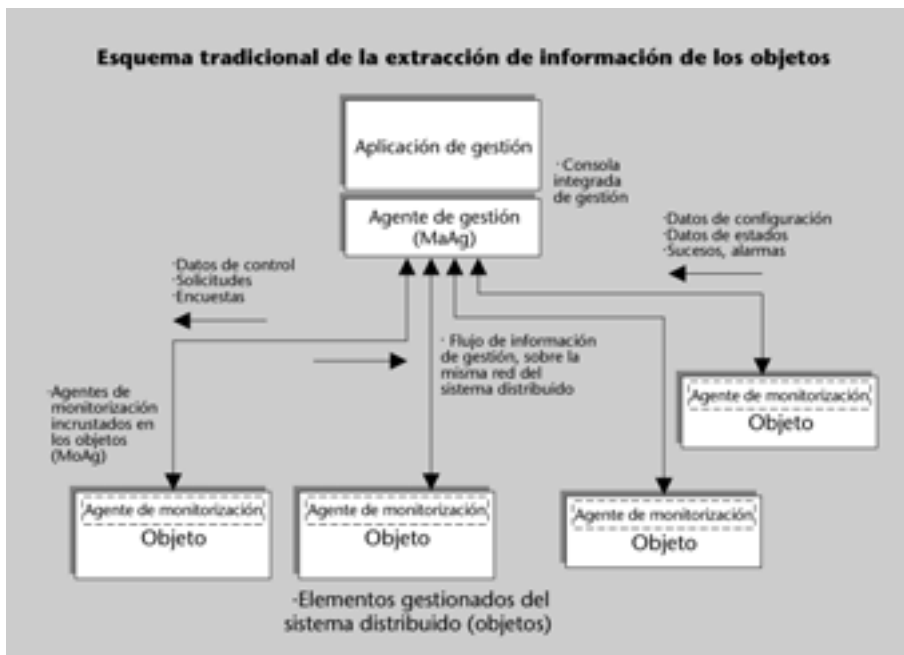
b) Los **mecanismos de interrogación\***: es un mecanismo poco o nada eficiente para fallos críticos, pero es útil para condiciones no severas, con poca frecuencia de actualización. Este mecanismo consiste en la interrogación por parte del sistema de gestión al agente del objeto, del estado y condiciones y de las alarmas registradas, si las hay. Es bueno en aquellas condiciones en las que se pueden haber perdido los *traps* de alarma o en las que simplemente no se han generado. El análisis de elementos para actualizar inventarios, o los mecanismos de comprobación de la existencia de objetos, son algunos ejemplos.

\* En inglés, *polling*.

#### Los *watchdogs*

Los mecanismos de comprobación de existencia o "supervivencia" de los objetos también reciben el nombre de *protocolos de eco* y, de forma más coloquial, *watchdogs*.

Figura 17



## 2) Filtrado de los acontecimientos producidos

Las alarmas que se producen en todo el alcance de un sistema distribuido son tratadas por unos mecanismos de filtrado inicial, denominado **filtrado jerárquico por capas\***. Este filtrado se desarrolla en dos ámbitos:

\* En inglés, *layered filtering*.

a) **Ámbito global**: selecciona las alarmas y, por lo tanto, los acontecimientos que tienen que ser gestionados por el siguiente nivel de procesamiento. Puede estar establecido para todo el sistema, para unas áreas concretas o para determinados elementos.

b) **Ámbito interno**: se encarga de identificar y determinar relaciones entre las alarmas. A partir de toda la información proporcionada por éstas, como el tipo, los elementos, los instantes de generación o la criticidad, entre otros, el ámbito interno puede establecer comparaciones y agruparlas por causas y/o

efectos similares, con lo que permitiría determinar secuencias de encadenamiento, prioridad y correlación. De esta forma la correlación permite, a partir del análisis de un conjunto de alarmas, filtrar algunas de las mismas o todas y generar una nueva alarma para su proceso posterior, que es realmente la que indica al administrador el problema o fallo real.

Figura 18



### Un caso de ejemplo de filtrado de fallos

Un enlace de una delegación de la empresa está soportado por un primario RDSI (2 Mb) con dos *routers* (encaminadores) de última generación. Transportan servicios de voz (telefonía) y datos. Implementan unos agentes de monitorización de alto nivel, que permiten controlar centenares de estados, condiciones y excepciones relacionados con todos los protocolos, incluidos los de capas superiores, que se soportan sobre el enlace. Todos los acontecimientos se dejan activados.

Ante una ruptura física del medio, se generarían decenas y decenas de alarmas referidas a las rupturas de comunicación para cada protocolo. Si el sistema de gestión no fuera capaz de filtrar de forma conveniente la situación, el administrador difícilmente podría saber qué está pasando realmente en medio de tanta información.

La correlación conveniente de las alarmas permite generar única y específicamente la alarma correcta que engloba, desde el punto de vista operacional, todas las otras: la ruptura física del medio.

### 3) Procesamiento de las alarmas

El **calificador de alarmas** analiza aquellas que se han filtrado de forma conveniente. Las alarmas se asignan a los procesadores de alarmas según las características de identificación, las prioridades o la información de correlación. Estos procesadores, implementaciones complejas de *software*, se clasifican por los criterios de comportamiento y por la función que realizan.

#### Los sistemas de filtrado y correlación de alarmas...

... más potentes implementan complejos algoritmos *software* y disponen, en ocasiones, de capacidad de almacenar alarmas producidas mucho tiempo atrás, por si es preciso establecer relaciones y agrupaciones.

#### Terminología

A menudo los procesadores de alarmas se conocen como *event processors*, pero dichas alarmas se refieren a alarmas generadas por acontecimientos.

Los calificadores de alarmas se clasifican según el comportamiento operacional:

a) **Pasivos:** no desencadenan acciones específicas, sino que se orientan hacia la preparación y estructuración de la información para etapas o procesos posteriores. Los principales son los siguientes:

- **Anotadores\***, para almacenamiento global, destinados a análisis exhaustivos.
- **De muestreo\***, para almacenamiento parcial, sólo de determinados acontecimientos y útiles para el análisis de tendencias y comportamiento.
- **De estado\***, que permiten guardar una “fotografía” del estado instantáneo de un elemento y reflejar todos los cambios que se produzcan.

\* En inglés, *loggers*.

\* En inglés, *samplers*.

\* En inglés, *status*.

b) **Activos:** activan y hacen funciones a partir de la información o tipo del acontecimiento o alarma. Los principales son los siguientes:

- **De contención**, habilitan funciones, normalmente automáticas, de contención del fallo.
- **De resolución**, implementan procedimientos de corrección del fallo.

Con respecto a la función que implementan, se clasifican de la manera siguiente:

- Por el área o áreas OSI implicadas: clasificación funcional clásica, asociada a los diferentes subsistemas de cada área.
- Por el efecto de la alarma o fallo: en función de una clasificación de importancia, criticidad o prioridad. Una de las clasificaciones utilizadas es la siguiente:
  - Permanente, si el fallo no se corrige solo; requiere intervención.
  - Temporal, si el fallo se corrige por sí sólo después de un periodo de tiempo.
  - Estimado, si el fallo no se ha producido pero los precedentes indican que es inminente.
  - Obsoleto, si el acontecimiento o fallo no se considera a causa de que el periodo de tiempo (minutos, horas, meses, etc.) que ha pasado lo ha vuelto obsoleto.
  - Afectación, si hay efectos o daños que afectan al objeto y obligan a un nivel de servicio reducido.

- Inhibición, cuando el elemento afectado por el fallo está totalmente fuera de servicio, sin ninguna capacidad de producción.
- Por la información particular de la alarma: según los datos específicos de la alarma. Algunos de los más comunes son los siguientes:
  - Marcas de tiempo\*, de los momentos de creación, recepción, correlación, etc.
  - Importancia, según cómo está catalogado el fallo (crítico, principal, menor, aviso o indeterminado).
- Por la información particular del objeto: según las características concretas del elemento o componentes afectados, su estado o su papel dentro del sistema distribuido.

\* En inglés, *time stamping*.

### Actividades paralelas de manipulación y proceso de alarmas

Junto con las funciones descritas, la gestión de alarmas es la encargada de tareas complementarias que se hacen paralelamente a las mencionadas o con posterioridad en condiciones estables sin fallo, para diseñar, analizar y evaluar las medidas y los procedimientos. Algunas de las tareas son las siguientes:

- Control de alarmas activas.
- Control del histórico de alarmas.
- Mecanismos de inhibición.
- Rehabilitación y restauración de estados.
- Simulación de agrupamientos, priorizaciones y correlaciones.

#### 4.4.2. Seguimiento y administración dinámica de incidencias

La segunda de las etapas de la cadena de proceso de fallos se encarga de la coordinación de todas las tareas que hay que desarrollar, una vez que el fallo ha sido confirmado por la gestión de alarmas anterior.

Las acciones de prediagnos, cruce con información anterior y determinación concreta de las causas reciben una atención especial. Como es habitual, la eficacia aumenta cuanto más automatizado sea el proceso, enlazando dinámicamente con el resto de las etapas del área o subsistemas de las demás.

La interrelación con el subsistema de gestión de incidencias del área de configuración resulta obvio y esencial. Las principales tareas conectan con muchos de sus procesos, y proporcionan y recogen información respectiva.

Algunas de las tareas más significativas dentro del marco de la dinámica de incidencias son las que mencionamos a continuación:

- Apertura de los partes de incidencia.
- Asignación de recursos humanos a las tareas de diagnóstico, contención y resolución: control de perfiles y responsabilidades, aplicadas al personal interno especialista y generalista, y a los recursos y organizaciones internas.
- Control y seguimiento de los estados y flujos: pruebas de diagnóstico.
- Control de la información histórica: información de los históricos puros, contenida en los partes de problemas cerrados, y de las fuentes de información que pueden completar los sistemas de ayuda a la diagnosis.

Uno de los principales objetivos de la gestión de fallos es reducir el tiempo de resolución y restauración de las condiciones estables. Un factor importante será el de decidir qué recursos y qué perfiles se asignan a los problemas, según la complejidad, criticidad o disponibilidad de medios.

Como norma general, se han establecido cinco niveles de clasificación de los problemas, según los recursos que se asignan para su resolución, la proporción que representan, el área o componentes en los que generalmente se originan y el esfuerzo de detección y resolución.

Los niveles de problemas mencionados cumplen unas características determinadas, que mencionamos a continuación:

### 1) Características del primer nivel

- Gestionado por las herramientas de *help desk* de usuario final y sus operadores.
- Los problemas normalmente no son de origen técnico, sino que están relacionados con tratamientos y manipulaciones de usuario.
- En una organización bien soportada representan entre el 80% y el 85% de las incidencias que se producen.
- Diagnóstico rápida. En la mayoría la resolución puede ser remota, y buena parte de éstas se abren, analizan, diagnostican y resuelven durante una sola llamada.

### 2) Características del segundo nivel

- Gestionado por los operadores de red y de sistemas específicos.
- El problema tiene un carácter técnico sencillo, pero no puede ser resuelto por la unidad de *help desk*.

#### Ejemplos de problemas de primer nivel

La pérdida de configuración de una impresora o el fallo en un *login* en un servidor son casos de problemas de primer nivel.

#### Ejemplos de problemas de segundo nivel

Algunos casos de problemas de segundo nivel pueden ser, por ejemplo, la desconfiguración y bloqueo de un encaminador (*router*) o la inestabilidad de un enlace.

- Representan entre un 5% y un 10% de las incidencias que se producen.
- Diagnósis considerable, que implica algún análisis más profundo en remoto o la consulta de información histórica.

### 3) Características del tercer nivel

- Gestionado por especialistas de redes, telecomunicaciones, sistemas o aplicaciones relacionadas.
- Problemas críticos y complejos, pero que se detectan sin dificultad.
- Representan entre un 2% y un 5% de las incidencias que se producen y que con frecuencia se relacionan con la complejidad tecnológica y las soluciones multivendedor.
- Diagnósis muy considerable, que implica siempre la utilización de recursos humanos de altos conocimientos y herramientas de análisis complejas.

#### Ejemplos de problemas de tercer nivel

La caída de la red troncal de voz y datos por problemas de sincronización y configuración de los conmutadores ATM, o la inestabilidad de un servidor al asumir muchos procesos son casos de problemas de tercer nivel.

### 4) Características del cuarto nivel

- Gestionado por especialistas de aplicación.
- Son problemas muy variados, localizados o extensos, normalmente imputables al diseño, desarrollo o mantenimiento de aplicaciones.
- Representan entre un 1% y un 5% de las incidencias producidas.
- No son fácilmente identificables y, en ocasiones, la detección puede pasar mucho tiempo después de que hayan sucedido. El seguimiento y la reproducción controlada del fallo puede no ser posible.

#### Ejemplos de problemas de cuarto nivel

La degradación de la integridad de tablas de la base de datos de gestión financiera, o la pérdida de saldos consolidados en diferentes cuentas y procedimientos de un banco representan casos de problemas de cuarto nivel.

### 5) Características del quinto nivel

- Gestionados únicamente por los constructores y desarrolladores de sistemas, *software* de base y grandes aplicaciones.
- De entrada los problemas son muy concretos, porque si no serían intratables.
- Representan entre un 1% y un 2% de las incidencias totales que se producen.
- Diagnósis muy pesada, basada normalmente en la comparación de efectos similares en muchas instalaciones con características comunes. Según la gravedad se pueden resolver a un corto plazo, pero a veces se retrasan a nuevas actualizaciones o cambio de versiones. Son las más involucradas en procesos de rediseño.

#### Ejemplos de problemas de quinto nivel

Algunos casos de problemas de quinto nivel son, por ejemplo, *bugs* en módulos del sistema operativo de los servidores cuando se utilizan en escenarios como el nuestro o incompatibilidad de coexistencia de dos entornos de aplicación corporativos.

### 4.4.3. Medidas de contención inmediata y diferida

Las medidas de contención con un fallo abierto permiten evitar una afectación total a causa del fallo y aseguran un determinado umbral mínimo de servicio, que se preestablece antes.

De esta manera, el servicio continúa dentro de una determinada ventana de calidad, contenta a los usuarios y permite a los administradores concentrar toda su actividad en la diagnosis correcta y la resolución adecuada.

#### Ejemplo de medidas de contención


Si un enlace dedicado, al que está conectado una delegación con la central, cae, está previsto un mecanismo de contención automático que permite encaminar todo el tráfico para una serie de líneas RDSI alternativas.

En caso de fallo, las prestaciones de transporte a disposición de los usuarios son sensiblemente inferiores, pero permiten mantener unos tiempos de respuesta que no son nunca superiores al 50% de los tiempos normales, hito que marca el límite máximo de la ventana de servicio.

La situación contenida así es estable y permite a los administradores concentrarse en la resolución del enlace caído.

Los mecanismos de contención pueden actuar inmediatamente, como en el caso de los sistemas tolerantes a fallos, que disponen de fuerte redundancia activa y automática para poder alcanzar la caída o detención de algún elemento interno\*. También se pueden activar con posterioridad, de manera diferida, a requerimiento normalmente del administrador y para diferentes aspectos de contención.

En todos los casos, los procedimientos de actuación siempre están basados en una correcta prediagnosis del problema, según los precedentes o los efectos observados, que permitan activar los mecanismos de contención establecidos antes. Si por aquel fallo no se ha establecido un mecanismo previo de contención, el administrador deberá tomar las mejores decisiones de restablecimiento y restricción del servicio sobre la base de toda la información de que disponga sobre el tema.

Según la naturaleza del mecanismo de actuación, las medidas de contención se clasifican en las siguientes, con sus principales características: 

#### 1) Medidas de contención manuales

Éstas son sus características:

- a) Requieren completamente la intervención de personas, por lo general los administradores y operadores, para activar procesos de contención, que pueden implicar reconfiguraciones del objeto o de los elementos relacionados.
- b) Tienen un coste menor, porque normalmente están basadas en los recursos de administración y operación existentes.

#### Terminología

En ocasiones, los mecanismos de contención de fallos son conocidos también como *mecanismos de reconfiguración* o *backup* (copias de seguridad). Debemos tener precaución porque estos términos pueden inducir a confusión si no se conoce el contexto concreto al que se refieren.

\* Como discos, memoria, CPU, buses de I/O, etc.

#### Las medidas manuales, ¿contraproducentes?

Se ha demostrado que, incluso para administradores experimentados, con fallos abiertos y sistemas de contención totalmente manuales, la presión del entorno puede hacer que, de cinco decisiones tomadas, una de éstas sea totalmente contraproducente y que agrave el fallo en el peor de los casos.

c) En general, son poco eficientes y la respuesta que dan ante caídas del nivel de servicio es de poca agilidad. En situaciones críticas, con una fuerte presión del entorno y de los usuarios, o ante situaciones infrecuentes con medidas de contención poco probadas, la prudencia y eficacia de los procesos manuales pueden representar un peligro en ocasiones mayor que el mismo fallo.

## 2) Medidas de contención automáticas

Estas medidas presentan las características siguientes:

a) El proceso de identificación del problema, diagnosis y selección de las medidas de contención y su activación y ejecución es totalmente automático y desasistido de la intervención de los administradores.

b) Tienen un coste elevado debido a la complejidad de las herramientas que los implementan.

c) Son muy eficaces, siempre que estén correctamente configuradas para la instalación concreta, y perfectamente al día. Son las únicas que se pueden implantar dentro de los mismos elementos con garantías o en entornos en los que no es posible ninguna intervención humana.

d) Las pruebas hechas en condiciones de prefallo deben ser muy exhaustivas, con el fin de prever todos los casos y, sobre todo, de asegurar que la activación y la ejecución de las medidas de contención no son fortuitas ni erróneas.

e) Se tienen que revisar y actualizar de forma permanente. Los cambios mínimos en las premisas pueden ser totalmente determinantes para el fracaso del sistema.

### Los riesgos de las medidas de contención automáticas

El gran riesgo de los sistemas automáticos de contención es que se activen cuando no se trata del fallo que corresponde, no determinen correctamente su causa o, simplemente, se ejecuten incluso sin fallo. Hay precedentes importantes, incluso algunos relacionados con sistemas tolerantes a fallos.

Uno de éstos es el de una arquitectura de base de datos replicada, preparada para un soporte completo para el sistema secundario en caso de fallo del primario y que en determinadas circunstancias de estrés para carga daba el control a la segunda imagen cuando en paralelo la primera estaba activa. El sistema empezaba con un “ping-pong” entre los dos sistemas, hasta que ambas bases de datos quedaban totalmente degradadas e inservibles. Eran los datos reales de producción, y el sistema de contención creía que había hecho lo correcto.

## 3) Medidas de contención semiautomáticas o híbridas

Las características de estas medidas de contención son las que mencionamos a continuación:

a) El proceso está totalmente asistido de manera automática, pero las decisiones finales, órdenes de activación o tareas críticas son tomadas por el adminis-

### Las medidas semiautomáticas...

... representan la solución elegida en las organizaciones medianas y grandes, con un grado mayor o menor o de complejidad en los sistemas de ayuda a la decisión.

trador. Toda la automatización se convierte en una orientación de sistema de ayuda a la toma de decisiones.

b) Tienen un coste elevado a causa de la complejidad de las herramientas de soporte, similares a las de proceso automático. Los recursos son normalmente los de administración interna.

c) Combinan las ventajas de eficacia de los procedimientos automáticos con el control, análisis y seguimiento de los manuales, pero disminuyen la posibilidad de error humano, por desconocimiento, exceso de información o precedentes desconocidos.

La selección de un mecanismo de actuación u otro en nuestro entorno tiene que considerar aspectos de disponibilidad de recursos humanos, inversiones necesarias, criticidad del servicio y criterios tecnológicos y funcionales, entre otros.

Algunos de los aspectos más importantes a la hora de hacer la selección de estos mecanismos son los siguientes:


a) **Tiempo de conmutación:** determinación del máximo tiempo que el servicio puede estar desempleado sin causar efectos críticos o, incluso, catastróficos. Se lo conoce como el tiempo máximo de caída\* y puede ir desde cero o nulo, para determinadas instalaciones de misión crítica, hasta unas horas o días. Lógicamente, aquellos escenarios que requieran tiempo de caída nulo dispondrán de redundancia completa de dos sistemas o más totalmente en línea. Cuando las tareas de conmutación implican reconfiguración y restauración de copias de seguridad, los tiempos se pueden convertir fácilmente en días.

\* También llamado *maxim downtime*.

b) **Frecuencia del fallo:** cuanto más frecuente sea el fallo, o la posibilidad de que éste suceda, más recomendable será que las medidas de contención utilicen medios automáticos.

c) **Independencia de la intervención humana:** cuando no se puede o no se desea la intervención de recursos humanos, es preciso que el sistema esté asistido de forma automática. Pueden ser necesarias para operaciones nocturnas y de fin de semana, o en sedes remotas o insalubres.

#### 4.4.4. Diagnóstico definitivo, corrección y cierre del fallo

Las tareas de diagnóstico definitivo del fallo y de sus causas normalmente son posteriores a la activación de medidas de contención. En general se basarán en la información que se ha obtenido en la prediagnóstico y en la que contienen las bases de datos de *trouble tickets*, las de soporte de los proveedores y otros boletines similares. 

## Los boletines de problemas

Los problemas etiquetados o catalogados representan un mecanismo, en ocasiones muy eficaz, para la diagnosis rápida de fallos. Además de las herramientas propias de los *trouble tickets*, es muy usual la utilización de sistemas expertos que son alimentados periódicamente por su fabricante con nuevos problemas y medidas de resolución. También son frecuentes los boletines basados en soporte web que los fabricantes y proveedores ofrecen y con una información sobre fallos de ámbito mundial que se actualiza “en caliente” con la información de todas las organizaciones usuarias.

Generalmente, si el problema es identificado y reconocido, se implementa el procedimiento de resolución especificado, con las convenientes adaptaciones, si procede, en nuestro escenario. Si no hay ninguna referencia al problema en los boletines de información mencionados, se inicia un proceso de análisis detallado a partir de los elementos afectados, con unos esquemas que generalmente son “de arriba abajo”\* y “de igual a igual”\*\*. La capacidad para aislar los elementos a medida que avanzan las tareas es fundamental, especialmente si dichos elementos no están ya aislados con los mecanismos de contención activados.

\* En inglés, *top-down*.  
\*\* En inglés, *peer elements*.

Al segmentar el problema, es posible que algún punto de conflicto sí aparezca identificado en las bases de datos, porque no se le conocían los efectos concretos que observaban en un nivel superior. Si no es el caso, en los correspondientes niveles se inicia una iteración de procedimientos de prueba y error (*trial and error*), hasta que se llega, a ser posible, a conclusiones.

### “Prueba y error”, sí; cambios sin arbitrio, no

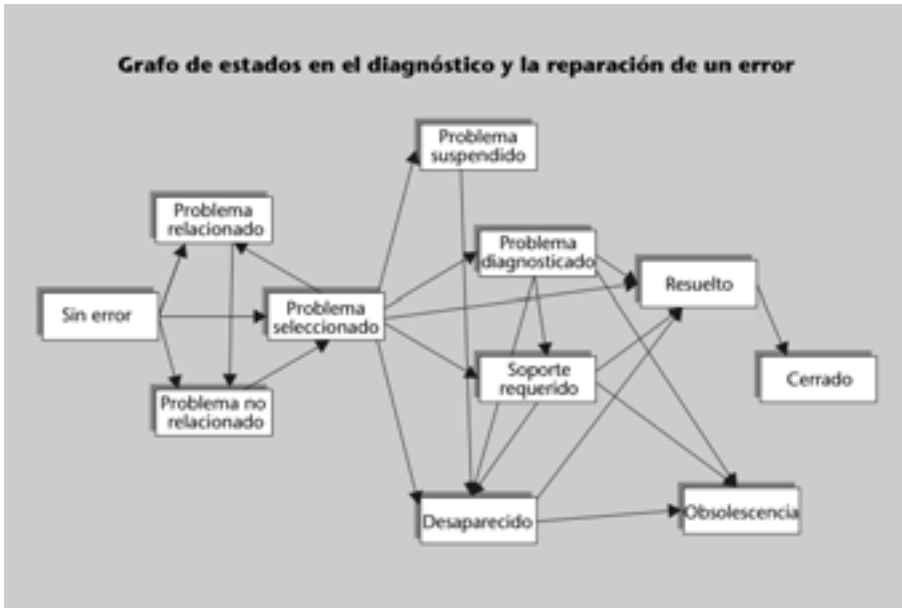
Los procedimientos de prueba y error son, en muchas ocasiones, la única fórmula para la diagnosis real de un fallo. En contra de la impresión popular, la metodología que hay que seguir no es, en absoluto, un cambio de un elemento por otro sucesivamente hasta que el fallo desaparece. Los cambios o modificaciones se tienen que planificar de manera que conformen unidades independientes desde el punto de vista del fallo y ejecutando siempre una sola al mismo tiempo para poder asociar los efectos. En momentos de estrés suele ser común efectuar una serie de pruebas al mismo tiempo para contener o resolver el fallo, que no lo determinan en concreción y lo reproducen con mayor severidad posteriormente.

Si el fallo queda bien diagnosticado, tanto para estar en los boletines como para el éxito del proceso de prueba y error, se desarrollan las medidas de solución y se prueban los elementos afectados de forma exhaustiva, en entorno de test. En general sólo en el caso de una confirmación plena se desarrollan las medidas en el entorno real, se restauran los elementos correspondientes y se recupera el estado prefallo.

Los **sistemas y herramientas de ayuda a la diagnosis** estructuran los estados en los que se puede encontrar el proceso y los flujos entre éstos.

En un nivel general los estados principales que se definen son los del grafo de transición que aparece en la figura.

Figura 19



En un caso de fallo el estado deseado es siempre el de salida por cierre. Sin embargo, para determinar el estado de fallos no resueltos que, por diferentes circunstancias, ya no afectan al nivel de servicio, es necesario el concepto de **obsolescencia**.

El otro caso es la **expiración**, referida a los fallos no resueltos pero que han superado un tiempo razonable\*, después del cual se establecen como definitivas las medidas de contención o se procede a la reconfiguración del entorno afectado.

\* Días, semanas, meses.

Las últimas tareas son las de documentación y actualización de los informes de incidencia y del resto de las bases de datos y boletines, con el fin de ayudar y mejorar la eficiencia en casos posteriores.

## 5. Gestión de prestaciones

La gestión de prestaciones dentro del modelo OSI se podía considerar como una complementación operativa de la gestión de fallos, ya que, aunque esta última es la responsable de que el sistema distribuido funcione, la gestión de prestaciones se encarga de que funcione correctamente y mide los parámetros pertinentes que aseguran los niveles de servicio y rendimientos necesarios. Junto con los fallos, esta área es una de las que se implementan primero en las organizaciones, aunque sea de manera poco integrada.

Consultad los niveles de servicio, QoS, en el apartado 4 de este módulo didáctico.

### 5.1. Introducción

El objetivo de la gestión de prestaciones es soportar y coordinar todo el conjunto de actividades que se requieren para evaluar continuamente los principales indicadores de prestaciones y rendimiento del sistema distribuido.

#### Terminología

El área de gestión de prestaciones es conocida normalmente en los textos como *performance management*, PM.


El área permitirá, por una parte, determinar, monitorizar y mantener los niveles de servicio y, por la otra, identificar los “cuellos de botella” actuales y potenciales en el futuro. Finalmente, el área genera una información esencial para la toma de decisiones de planificación, modificación y crecimiento del entorno, así como para analizar las tendencias de consumos y necesidades a corto, medio y largo plazo.

#### Los “cuellos de botella”

Los **cuellos de botella**, o *bottle-necks*, son los efectos de no crecimiento e, incluso, los de degradación que experimenta un sistema cuando uno de los recursos ha llegado a los límites de su capacidad. Si un sistema va sobrado de CPU, pero los buses del I/O están ya al 100%, no admitirá que se incorporen nuevos procesos concurrentes, aunque la CPU u otros recursos estén muy por debajo de su capacidad máxima. Los buses del I/O son en este momento el cuello de botella del sistema.

Desde el punto de vista del administrador del sistema, el principal beneficio que se obtiene de la gestión de prestaciones es la reducción de los casos de degradación e inaccesibilidad por sobreutilización de determinados recursos, que redundan en la provisión a los usuarios de unas condiciones de servicio adecuadas, sino óptimas. Este hecho es muy importante sobre todo en entornos en los que la carga puede oscilar en gran medida a lo largo del tiempo de producción, por ejemplo durante el día.

Finalmente, el área alcanza el hecho de proporcionar un sustrato que asocie una adecuada combinación de herramientas e instrumentos de monitorización, medida y análisis, para llevar a cabo una eficiente administración de la capacidad y utilización del sistema global en general y de todos sus elementos en particular, en tiempo real o casi real, minimizando la pérdida de instantaneidad.

Dentro de un marco general las diferentes tareas que lleva a cabo la gestión de prestaciones incluyen las siguientes: 

- Establecimiento de los parámetros relevantes de medida de los niveles de servicio y las correspondientes métricas.

- Selección, diseño e implementación de los mecanismos y procedimientos de monitorización.
- Monitorización de los acontecimientos que indiquen la superación de márgenes y ventanas y la posibilidad de un cuello de botella.
- Evaluación de resultados y análisis de tendencias que permitan la predicción de fallos antes de que sucedan.
- Evaluación de históricos para determinados comportamientos en situaciones de error o estrés del sistema.
- Procedimientos reactivos ante cambios positivos o degradativos de los parámetros de QoS y herramientas de autoajuste\*.
- Soporte a la planificación de prestaciones y capacidad\*.
- Predicción analítica o por simulación del comportamiento para una evolución del escenario (nuevas infraestructuras, nuevas aplicaciones, cambios de configuración, etc.).

\* En inglés, *auto tuning*.

\* En inglés, *capacity planning*.

## 5.2. Problemas específicos con el rendimiento y prestaciones

De la misma manera que sucede con la gestión de fallos, los mecanismos y la funcionalidad de la gestión de prestaciones están muy arraigados a los sistemas de información desde prácticamente su creación. En este sentido, muchas técnicas utilizadas en los *mainframes* de los setenta, en los que no se podía dejar perder ningún tanto por ciento de capacidad de los escasísimos y costosos recursos, son válidas hoy en día para los servidores más actuales.

Sin embargo, la complejidad y dispersión de los sistemas distribuidos actuales añaden tantas dificultades o más que a la misma gestión de fallos para conocer cuál es el comportamiento de un recurso en una sede remota o si el tiempo de respuesta que obtiene es similar al que determinamos localmente, por ejemplo.

### El problema del *fatware*

Al principio de los años noventa, los complejos cálculos del análisis de las prestaciones de un sistema, los cálculos de dimensionado o las estimaciones de carga cayeron en desuso. La justificación residía en el hecho de que el precio del *hardware*, en comparación con muchas de sus prestaciones, era cada día más económico, y era más rentable "comprar grande" que perder el tiempo en cálculos. Pocas veces, y en todos los entornos, han tenido tan poca importancia específica la cantidad de memoria necesaria, la potencia mínima y máxima de la CPU o la capacidad de concurrencia de procesos y usuarios.

Ya más a mediados y a finales de los noventa, el crecimiento casi exponencial de necesidades del *software* y su ineficacia desde el punto de vista de rendimiento, efectos conocidos coloquialmente como *fatware*, han replanteado de nuevo la necesidad de planificar y estimar de forma conveniente los recursos.

Las **problemáticas de la evaluación del rendimiento y las prestaciones**, en un sistema distribuido en producción, se engloban en tres conjuntos genéricos, en los que se aprecian los problemas de coherencia que los administradores tienen delante.

A continuación haremos una descripción de los tipos de problemáticas que acabamos de mencionar: 

**a) Problemas de coherencia “vertical” de los niveles de prestaciones:** las redes y enlaces que soportan las comunicaciones y las pilas de procesos del *software* de base y de aplicación que corren en los sistemas informáticos tienen dificultades para establecer unos criterios de coherencia de prestaciones en sentido vertical, es decir, con respecto a las capas, funciones o procesos inferiores que utilizan y a las capas superiores a las que dan servicio.

Con las excepciones correspondientes, es frecuente que servicios de alto nivel y con fuertes implicaciones sobre el QoS necesario, como el transporte de voz sobre la red, no establezcan de forma conveniente una jerarquía sobre los servicios inferiores que utiliza que asegure el nivel de prestaciones “cliente” que requiere. Si añadimos que los servicios que necesiten y esperen el correspondiente nivel pueden ser numerosos, la degradación de sus prestaciones, e incluso la no operación, está asegurada.

Los sistemas de proceso\* tienen un comportamiento más determinista con respecto a la asignación de cuotas de prestaciones y utilización competitiva de los recursos del sistema porque el mismo sistema operativo controla tales asignaciones. Pero en el caso de sistemas pesados (por ejemplo, motores de base de datos, sistemas transaccionales, servidores de ERP y CRM, etc.) con una fuerte variación del perfil de carga, las tareas de balanceo, redistribución y afinamiento pueden ser muy complejas o contraproducentes si no se prevén las herramientas adecuadas (por ejemplo, la cuota que tienen que reservar para asegurar las prestaciones a cada nivel superior).

\* Como servidores, *mainframes*, etc.

**b) Problemas de coherencia horizontal de los niveles de prestaciones:** las dificultades para establecer unos criterios de coherencia de prestaciones en sentido horizontal, es decir, prestaciones de un servicio “extremo a extremo”\* en la red son importantes y nada simples de observar.

\* En inglés, *end to end*.

Un servicio extremo a extremo está constituido para una concatenación de diferentes servicios, cada uno con diferentes prestaciones, que difícilmente pueden negociar entre sí las reservas de utilización y rendimiento necesarias. El control de los puntos de la cadena en los que el nivel de QoS para un determinado servicio sale de las ventanas válidas puede ser costoso o imposible.

### Ejemplos de servicios extremo a extremo

Existen centenares de ejemplos de servicios extremo a extremo en los sistemas distribuidos actuales. Por ejemplo, la conexión de un PC de una LAN remota al conjunto de servidores corporativos, en los que las prestaciones globales se pueden ver influidas por infinidad de criterios, como la potencia del PC, las prestaciones de la LAN, la contención del *router*, la velocidad y utilización de las líneas externas, el frontal de comunicaciones, las prestaciones de la LAN o troncales de los servidores, o el perfil de carga que éstos asumen en aquel momento.

c) **Problemas de coherencia con las métricas y métodos de medida de los niveles de prestaciones:** el procedimiento óptimo para asegurar el nivel de servicio requerido de un conjunto de recursos pasaría por la capacidad de poderlo medir con las mismas métricas en cada recurso involucrado. Con frecuencia este tema no es posible (no podemos medir las prestaciones de un enlace *frame relay* en términos de tiempo de respuesta máximo, que es nuestro indicador real del servicio), e incluso las mismas métricas utilizadas para diferentes fabricantes no son coherentes entre sí (velocidades de reloj con tecnologías de CPU diferentes, capacidad de conmutación con diferentes políticas de contención, etc.).

En resumen, los problemas de coherencia, muchos por falta de la pertinente estandarización y de visión global, así como la dificultad o incapacidad para el análisis “instantáneo” en tiempo de producción, son los principales obstáculos que encuentra la gestión de prestaciones.

### 5.3. Esquema general de la gestión de prestaciones

La gestión de prestaciones está constituida, de manera muy ilustrativa, por tres conjuntos de tareas, que mencionamos a continuación:

1) **Tareas de planificación de objetivos:** se encargan inicialmente de determinar cuáles son los servicios que se evaluarán y en qué nivel, y la política de objetivos que se desea\*.

\* Puede ser estático, determinado dentro de una ventana, el mejor posible, el menor, etc.

Según los servicios elegidos, se tienen que seleccionar los parámetros y las métricas con las que se medirán (tiempo de respuesta máximo, transacciones por segundo, número de usuarios concurrentes, etc.).

Finalmente, hay que establecer los puntos genéricos de medida de los parámetros y se tiene muy en cuenta la dispersión en el sistema distribuido (la medida del tiempo de servicio en el mismo servidor puede ser una ínfima parte del real en un lugar y momento determinado).

2) **Tareas de monitorización y control de ventanas de valores:** las tareas de monitorización incluyen todas las operaciones referidas al diseño, implantación y habilitación de las sondas en respuesta a determinados acontecimientos.

tos. Los acontecimientos pueden ser de tipo booleano o numérico, continuo\* o discreto\*\*.

\* Por ejemplo, un contador.  
\*\* Como una escala de valores.

El control de las ventanas de valor permite habilitar que se nos informe de manera conveniente cuando un parámetro sobrepasa un determinado valor o decrece por debajo de otro y activa el correspondiente acontecimiento. Las condiciones de las ventanas pueden ser variadas en tiempo de producción.

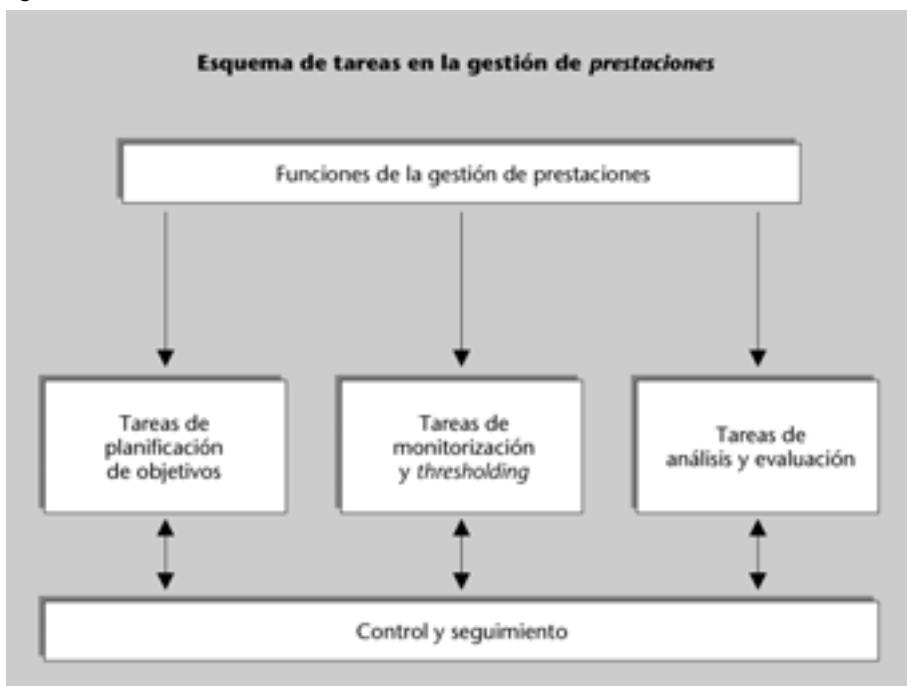
**Terminología**  
La gestión de las ventanas de valores es conocida con frecuencia como *thresholding*.

Con frecuencia los agentes de monitorización de los objetos elegidos como puntos de medida correlacionan acontecimientos según el histórico inmediato. En todos los casos intercambian información con el sistema de gestión central.

3) **Tareas de análisis y evaluación:** se dividen en dos grupos, según si trabajan con un horizonte de tiempo real o casi real o si, por el contrario, se encargan del análisis exhaustivo de datos recopilados del sistema con anterioridad, de manera masiva o selectiva.

Las primeras son necesarias para los mecanismos de ajuste en tiempo real y, lógicamente, para todo el control de los niveles de servicio, tanto en condiciones normales como previas y posteriores a un fallo. Las segundas se utilizan mayoritariamente para los estudios de capacidad y análisis de tendencias y, en determinados casos, para el análisis de causas o efectos de determinados fallos.

Figura 20



A continuación se desarrollan algunos aspectos destacados de las tareas mencionadas.

### 5.3.1. Definición de los indicadores de prestaciones

Los indicadores de prestaciones\* se encargan de definir los tipos y las métricas de medida de los parámetros de indicación de las prestaciones al sistema.

\* En inglés, *performance*.

Los indicadores definidos tienen que ser suficientes para controlar nuestro escenario, especialmente bajo condiciones cambiantes.

Hay pocas estandarizaciones referidas a los indicadores de prestaciones, pero generalmente se clasifican en dos categorías:

1) **Indicadores de prestaciones orientados al servicio:** son aquellos que están orientados a los requerimientos e intereses del usuario final concreto. Desde la perspectiva de los usuarios, son los únicos parámetros significativos referentes a los niveles de QoS que necesitan. Los más importantes y utilizados son los tres siguientes:

a) **Disponibilidad\*:** es el primero y más importante indicador que percibe un usuario final cuando trabaja sobre un sistema informático cualquiera. Controla el cociente entre el tiempo que un usuario ha dispuesto de acceso a un servicio o recurso con respecto al tiempo total que debería haber estado disponible.

\* En inglés, *availability*.

$$\text{Disponibilidad} = \frac{\text{Tiempo el recurso ha estado disponible para el usuario}}{\text{Tiempo total}}$$

En un entorno informático cualquiera, el 100% del tiempo está compuesto por el tanto por ciento de disponibilidad más el de detención (*downtime*). El porcentaje de detención incluye las detenciones provocadas por fallos, pero también las de tareas de mantenimiento y operación (copias y copias de seguridad, rearranques, actualizaciones, etc.). La distribución de los porcentajes depende totalmente de cómo se diseñe la organización.

Por otra parte, se deben tener muy en cuenta los condicionantes de disponibilidad, que son propios del escenario. Los principales son los siguientes:

- **Ventana operacional o de servicio**, que representa el periodo en el que el sistema tiene que estar disponible. Pueden ser unas cuantas horas al día o las veinticuatro horas al día los siete días de la semana en sistemas de alta disponibilidad.
- **Tiempo máximo de caída**, que es el periodo máximo que un servicio puede estar sin servicio, bajo cualquier circunstancia. Puede ir desde unas cuantas horas a pocos minutos o menos.

#### ¿Una fiabilidad del 100%?

El 100% de disponibilidad, o disponibilidad absoluta, no se puede asegurar nunca en un entorno informático y, especialmente, en un entorno distribuido. La utilización de tecnología, aunque sea muy segura, no es infalible; además, la multitud de componentes y servicios que tienen comportamientos no deterministas, especialmente en las redes, añaden más incertidumbre a la garantía absoluta de no detención.

- **Frecuencia de caídas**, que determina cómo se distribuyen de forma temporal las detenciones a lo largo del tiempo. Una instalación puede asumir unas detenciones del servicio estipuladas en una media de seis horas en seis meses. Es posible que soporte quince minutos de detención media máxima a la semana (distribución uniforme de las seis horas), pero seguramente será catastrófica una única detención de seis horas dentro de los mismos seis meses.

A pesar de las dificultades de los entornos en red, es habitual ver indicadores de disponibilidad muy altos y es frecuente disponer de valores próximos o superiores al 99% para determinados elementos. El hecho de ver porcentajes del 99,97% o 99,98% podrían proporcionar una falsa sensación de casi fiabilidad absoluta.

### Ejemplo de disponibilidad

La tabla siguiente muestra un ejemplo que cruza diferentes condicionantes de disponibilidad. Apreciad cuáles son las medias obtenidas en el 99,5% (que parece alta) en tres escenarios y cuál tiene que ser para mantener un entorno de misión crítica (paradas inferiores al minuto, con muy poca frecuencia).

	Disponibilidad	Ventana operacional	Frecuencia media de caídas		
<b>Tiempo máximo de caída aceptable</b>			<b>1 hora</b> Sistemas de disponibilidad media	<b>5 minutos</b> Sistemas de alta disponibilidad	<b>1 minuto (o menos)</b> Sistemas de misión crítica
<b>Caso A1</b>	<b>99,5%</b>	<b>8 horas al día, los 5 días</b>	<b>Cada 5 semanas</b>	<b>Cada 2 días</b>	<b>Cada 9 horas</b>
<b>Caso A2</b>	<b>99,5%</b>	<b>24 horas al día, los 7 días (7 × 24)</b>	<b>Cada 8 días</b>	<b>Cada 16 horas</b>	<b>Cada 3 horas</b>
<b>Caso B</b>	<b>99,995%</b>	<b>24 horas al día, los 7 días (7 × 24)</b>			<b>Cada 6 días</b>

La disponibilidad de elementos individuales, especialmente la del *hardware*, se calcula a partir del intervalo medio entre fallos y los otros, que se relacionan por la expresión que tenemos a continuación:

MTBF es la sigla de la expresión inglesa *Mean Time Between Failures*.

$$\text{Disponibilidad} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTD} + \text{MTTR} + \text{MTOR}}$$

donde están representados los valores siguientes:

- **MTBF** es el intervalo medio entre fallos.
- **MTTD** es el intervalo medio de diagnóstico.
- **MTTR** es el intervalo medio para el inicio de la resolución.
- **MTOR** es el intervalo medio de resolución.

Evidentemente, el objetivo de maximizar la disponibilidad sucede porque el MTBF es sensiblemente mucho mayor que los otros intervalos.

Para finalizar, debemos valorar que la disponibilidad de un servicio disminuye a medida que intervienen más elementos necesarios (a causa del producto de las disponibilidades). Sólo en el caso de redundancia la disponibilidad aumenta.

**b) Tiempo de respuesta:** después del indicador de disponibilidad, es el que más rápidamente analiza y mide el usuario cuando trabaja. Mide el periodo de tiempo de contestación de un sistema, es decir, el intervalo que va desde que un usuario pulsa la tecla o hace clic en el botón correspondiente hasta que recibe la respuesta del sistema.

En un sistema distribuido el tiempo de respuesta estará constituido por la suma de un conjunto de intervalos de transferencia hacia el servidor, los intervalos de procesamiento y los de transferencia hacia el usuario y presentación. En la figura se observa el desglose de los diferentes intervalos que intervienen en tiempo de respuesta.

Normalmente, en un entorno informático distribuido, el tiempo de respuesta se ve más afectado por el comportamiento no determinista de las redes y medios de comunicación que por las latencias producidas en las unidades de proceso, que son más modelables.

**¿Cuál es el tiempo mínimo de respuesta?**

En ocasiones, los esfuerzos por aumentar el rendimiento de un sistema obtienen unos frutos que no se pueden aprovechar.

Si se aumentan las prestaciones en un sistema y se consiguen bajar los tiempos de respuesta a la mitad, se tendrá que considerar el valor absoluto de lo que se mejora: si son ocho segundos, cuatro, y si es uno, medio.

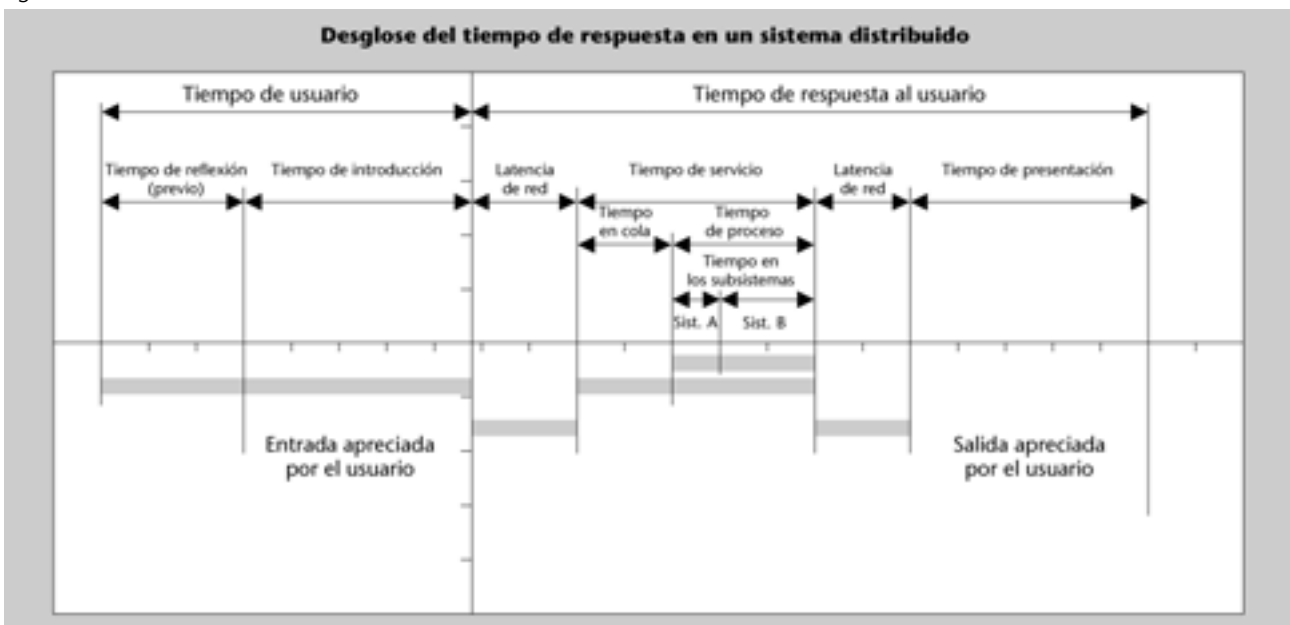
Normalmente, en un sistema distribuido las respuestas inferiores a los dos segundos en entornos conversacionales son inútiles y representan un despliegue innecesario de medios, con los costes consiguientes.

Cuando se supera un tiempo determinado, el **tiempo de respuesta máximo**, el sistema deja de ser funcional. En ocasiones, sin embargo, el criterio es demasiado subjetivo. Por este motivo se establece normalmente un **tiempo de respuesta deseable**, además del tiempo máximo.

**Subjetividad del tiempo de respuesta**

Todo el mundo está de acuerdo en que un cajero automático debería responder en menos de cinco o seis segundos y que si tarda más de dos minutos en contestar seguramente cancelaremos la operación o nos marcharemos. Pero el periodo entre los dos extremos puede ser demasiado grande.

Figura 21




c) **Exactitud\***: la exactitud es un indicador de prestaciones que, por desgracia, el usuario sólo considera en los casos más evidentes. En general su sentido es el de determinar el grado de fiabilidad de las respuestas de un sistema y ayudar, si es preciso, a incrementarlo.

\* En inglés, *accuracy*.

En los sistemas distribuidos actuales, la exactitud no se centra en los típicos errores de transmisión de las líneas de hace diez o quince años\*, ya que los sistemas de comunicación son extremadamente seguros en este aspecto, sino en unos conceptos más funcionales.

\* Caracteres perdidos, suciedad, etc.

Se observa el posible comportamiento errático de un sistema (inestabilidad, oscilaciones de prestaciones, etc.) o de una aplicación (comportamiento no homogéneo o equilibrado, pérdida de integridad de las respuestas, reordenamientos de operaciones no deseadas, etc.).

2) **Indicadores de prestaciones orientados a la eficiencia**: son aquellos que están orientados a los requerimientos e intereses de la organización y ofrecen el servicio a toda la comunidad de usuarios. Desde la perspectiva de los administradores, estos parámetros permiten conocer cómo se está utilizando el conjunto de recursos del sistema distribuido, especialmente los fuertemente compartidos. Los más importantes y utilizados son los tres siguientes: 

a) **Caudal de servicio\***: es una medida instantánea del número de elementos, operaciones o éxitos individuales por unidad de tiempo que soporta un recurso determinado. Se expresa siempre como un cociente y es una medida muy orientada a los servicios de aplicación.

\* En inglés, *throughput*.

Existen centenares de medidas de *throughput* utilizadas en un sistema informático. Los MIPS, o millones de instrucciones por segundo, los Kbits por segundo de un enlace, el número de transacciones o sesiones por minuto, el número de páginas impresas por hora o el número de llamamientos diarios al *help desk* son sólo unos ejemplos.

b) **Capacidad\***: la capacidad de un recurso, elemento o servicio es el caudal o *throughput* máximo que puede soportar en unas condiciones determinadas. La capacidad se establece en ocasiones referida a unas hipotéticas condiciones ideales y estables de utilización del recurso, mientras que en otras se simulan o reproducen las condiciones reales a la hora de medirlo.

\* En inglés, *capacity*.

Es importante determinar si la medida de capacidad del recurso se refiere al primer o al segundo escenario, porque las diferencias pueden ser muy lejanas.

#### Un ejemplo de medida de capacidad

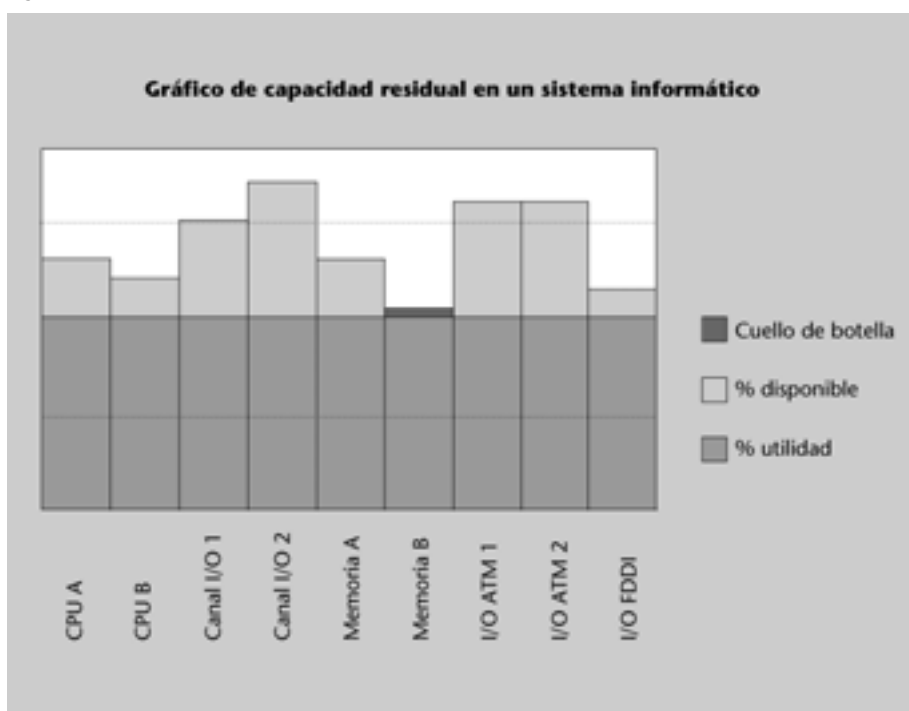
Algunas arquitecturas de CPU actuales, basadas en modelos superescalares y *pipes* de proceso paralelo, permiten establecer unas medidas de capacidad, en condiciones ideales,

muy altas, expresadas en millones de instrucciones por segundo. Pero la realidad reduce las espectaculares medidas cinco, diez o hasta treinta veces en el peor de los casos, porque el *software* de producción no sólo contiene las instrucciones concretas más eficientes y con el orden más adecuado.

Finalmente, uno de los usos más adecuados de las medidas es el **análisis de la capacidad residual\***, que se encarga de conocer qué margen queda en un recurso desde el caudal utilizado hasta la capacidad. Si homogeneizamos la capacidad de los recursos, se pueden detectar fácilmente cuáles serán los cuellos de botella si la carga aumenta. La figura 22 muestra un gráfico de capacidad residual para una serie de recursos.

\* En inglés, *capacity planning*.

Figura 22



c) **Utilización:** es la medida dinámica de cómo se utilizan los recursos. Esta medida controla en cada momento qué recursos están disponibles o en cuáles tendremos que esperar para acceder a ellos o disponer de los mismos.

Los **diagramas de utilización** son una de las herramientas más utilizadas para conocer los criterios de utilización de un conjunto de recursos concurrentes y relacionados, que permiten obtener las condiciones de encabalgamiento y de secuenciación que mejor equilibren un sistema en producción. Los **diagramas de Gantt** y los **diagramas de Kiviat** son los más utilizados.

Si, además, se dispone de un seguimiento en tiempo real de la utilización, se pueden obtener los datos referidos al comportamiento y equilibrio del sistema en los correspondientes diagramas y en condiciones dinámicas de carga.

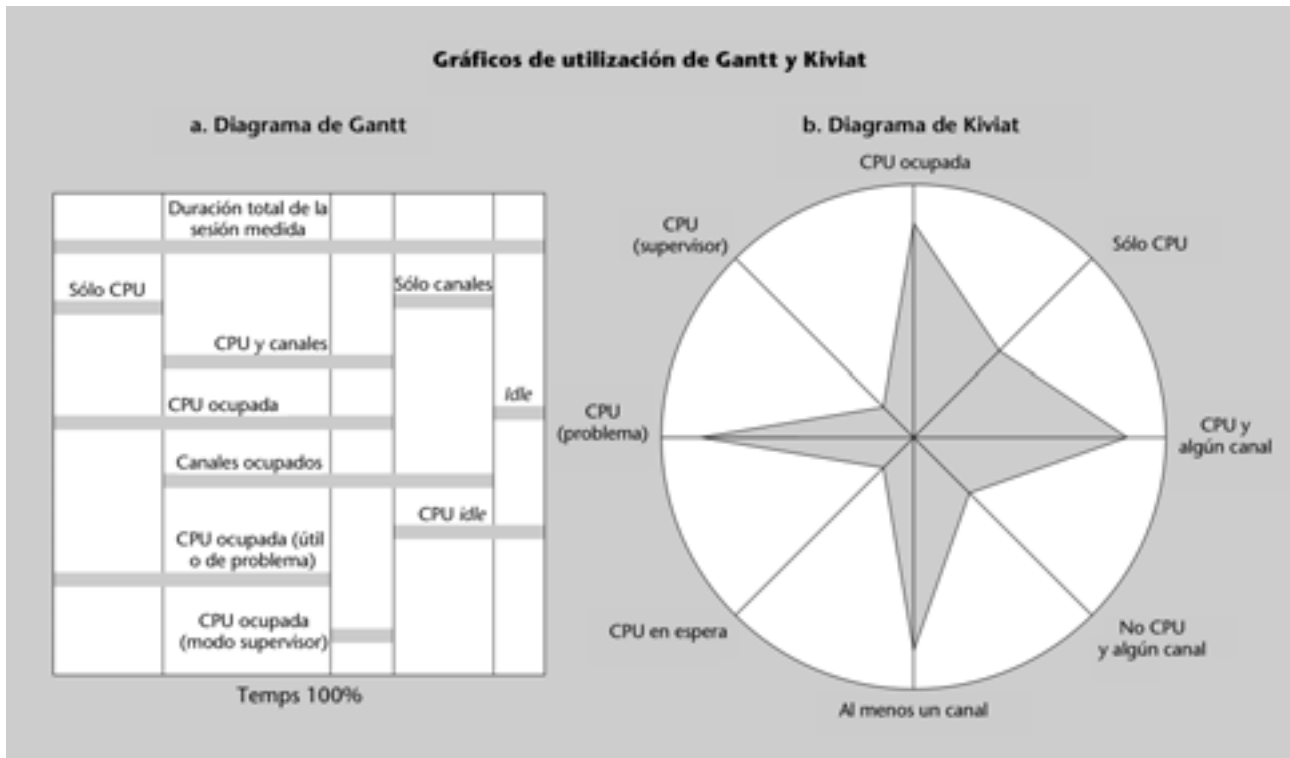
#### Ejemplos de medidas de la utilización

Algunos ejemplos de este tipo de medidas son el tanto por ciento de utilización de CPU, el uso de un canal de transmisión, el espacio disponible en un volumen o los terminales de acceso al sistema.

#### Seguimiento en tiempo real

En un sistema distribuido en producción se utilizan muchas medidas de la utilización.

Figura 23



### 5.3.2. Características de los elementos de monitorización

Los elementos de monitorización utilizados en los sistemas distribuidos actuales han experimentado un cambio extraordinario sobre todo en los últimos años. La popularización de la utilización de microprocesadores a un coste irrisorio, la bajada de los costes del *hardware* general y la inclusión cada vez más frecuente de sondas en el *software* de base hacen que los elementos pongan al alcance de los administradores un enorme conjunto de información, referida a los parámetros de prestaciones, en ocasiones incluso desmesurado por la saturación de la capacidad de análisis de los mismos técnicos.

Consultad las características de los elementos de monitorización en el apartado 1 del módulo "Técnicas de medida y de presentación de los resultados" de esta asignatura.

Las facilidades en las tecnologías de monitorización y las prestaciones crecientes de las redes marcan un aumento constante de las políticas de **monitorización continua o en línea** en los sistemas distribuidos.

A grandes rasgos, las ventajas e inconvenientes que hay que tener en cuenta de los elementos de monitorización son los siguientes:

#### 1) Ventajas

- Capacidad para captar, conocer y analizar la información cuando se produce (por ejemplo, en el momento de cambios en los indicadores).
- Histórico inmediato, o a más periodo, que permite los estudios de predicción de condiciones.

- Información obtenida en tiempo real, necesaria para las tareas de afinamiento y adaptación\* a la carga instantánea o casi instantánea.

\* En inglés, *tunning*.

## 2) Inconvenientes

- Volumen muy elevado de información que se debe almacenar y mantener.

Recursos especializados para el correcto análisis.

- Sobrecarga\* que tienen los elementos, los medios de comunicación, el *software* de base y de aplicación o las mismas consolas de gestión.
- En ocasiones, falta de integridad con las medidas de diferentes instrumentos para diferentes arquitecturas, proveedores o servicios.

\* En inglés, *overhead*.

### 5.3.3. Análisis y ajuste

Las medidas y mecanismos de control de comportamiento y prestaciones, efectuadas sobre un sistema distribuido, serían bastante inútiles si, sobre la base de su análisis, no se pudieran tomar las oportunas actuaciones de ajuste al mismo sistema. Las acciones efectuadas en esta línea permitirán adaptarse mejor a las características cambiantes de la carga, mejorarán los resultados de servicio y rentabilizarán las inversiones. 🎯

Una **regla de oro del ajuste de los sistemas de información** dice lo siguiente: cuanto mejor ajustado está un sistema informático, más alta es su utilización. Pero al utilizarse más, necesita más ajuste.

Puede parecer que lo expuesto hace referencia a la canción de nunca acabar, pero la realidad de los entornos en producción es, mayoritariamente, ésta.

Finalmente, hay una serie de “normas de conducta” que es recomendable que sigáis en los procesos de análisis y ajuste de prestaciones. Citamos algunas a continuación:

- a) Definir claramente los objetivos. Es importante saber adónde se destina la línea principal, que tiene que coincidir con los criterios corporativos\*.
- b) Definir los intervalos y ventanas de tiempo, determinar cuáles se utilizan, las condiciones razonables de partida, cuándo se tienen que reajustar y las razones para hacerlo.

\* Por ejemplo, favorecer a los usuarios, bajar los costes, potenciar el uso, etc.

- c) Los análisis y afinamientos del sistema tienen que estar orientados a conseguir “los niveles requeridos de prestaciones y servicio”, no hacen falta “los mejores posibles”.
- d) Estimar siempre la balanza de costes y beneficios\*.
- e) Observar la regla del 80-20: en general, el 20% de la carga es la responsable del 80% de la demanda de utilización de recursos. Centrarse en esta regla maximizará los resultados.
- f) Fijar como objetivos los recursos más críticos y centrar esfuerzos.
- g) Considerar, actualizar y mantener los estudios de capacidad residual, porque son los que determinan *a priori* los posibles cuellos de botella y, por lo tanto, los cambios más urgentes.

\* Más prestaciones siempre son deseables, pero ¿a qué precio?

## 6. Gestión de seguridad

Dentro del modelo funcional OSI, la gestión de seguridad es el complemento necesario a las funciones de las áreas de fallos y prestaciones para conseguir que un sistema informático pueda ser considerado “fiable” y proporcione la confianza necesaria a la dirección, a los usuarios y a los mismos administradores. Sólo estos entornos pueden alcanzar con éxito el cúmulo de problemáticas que tiene cualquier escenario en producción real.

### 6.1. Introducción

El **objetivo de la gestión de seguridad** es proporcionar la adecuada protección del sistema informático ante amenazas, riesgos y, en general, cualquier tipo de éxito no deseado, tanto si es intencionado y malicioso como si se debe a causas accidentales y no intencionadas.

#### Terminología

El área de gestión de seguridad es conocida normalmente en los textos como *Security Management, SM*.

Desde el punto de vista de la dirección de la organización, una correcta aplicación de los criterios de seguridad permite que ésta sea poco o nada **vulnerable**, es decir, que reduzca la posibilidad de que sucedan incidentes desagradables, en absoluto deseados, que pueden tener incluso consecuencias catastróficas.

#### La vulnerabilidad de los sistemas de información

La **vulnerabilidad**, desde un punto de vista genérico, puede afectar a muchos niveles de la organización: ¿qué pasa si la sede central sufre un incendio, roban en una delegación o un empleado vende información a la competencia? Sin embargo, cuando una organización es fuertemente dependiente de sus recursos informáticos (la mayoría de las organizaciones actuales), la vulnerabilidad, en todos los aspectos, se maximiza y el impacto se puede convertir en fatal.

¿Qué sucedería si un sistema de control de vuelo tuviera un error de programación e hiciera que un avión se estrellase, un banco perdiera toda la información de cuentas de los clientes a causa del sabotaje de un empleado descontento o el operador de un sistema de apoyo a la supervivencia de enfermos coronarios se equivocara en una orden de operación y lo desconectara sin darse cuenta? Todos, por desgracia, son **ejemplos reales**.

Por otro lado, desde el foco más operacional de los administradores del sistema, las **funciones de seguridad** les proporcionan las herramientas de protección de los recursos del entorno.

Finalmente, los usuarios esperan que el sistema informático los “ayude”, les permita, realmente, desarrollar sus funciones dentro de la organización, y son cada día más exigentes en hacer que se cumpla. Alguien que haya perdido archivos “misteriosamente”, que no pueda acceder con frecuencia al sistema por diferentes circunstancias o que luche desesperadamente día a día contra un

#### Ejemplos de funciones de seguridad

El acceso y entrada al sistema distribuido, el control del acceso y la utilización de las aplicaciones teniendo en cuenta los perfiles de cada usuario concreto, la protección del secreto de determinados datos e informaciones, la detección de virus y *software* extraño o la evaluación de riesgos concretos y la toma de medidas para minimizarlos son algunos ejemplos de funciones de seguridad.

bajo nivel de prestaciones y unas dificultades de utilización enormes no se le puede pedir “confianza en el sistema”.

Dentro de un marco general las diferentes tareas que gestiona el área de seguridad se agrupan en dos categorías: las de reducción de la posibilidad de sufrir un riesgo o amenaza y las de provisión de mecanismos de contención y minimización de los efectos.

Algunas actividades incluidas en el área de gestión de la seguridad son las siguientes:

- Análisis y evaluación de los riesgos y amenazas.
- Definición, implantación y seguimiento de las políticas de seguridad.
- Provisión de medios de identificación, certificación y autorización de usuarios o procesos.
- Minimización de la posibilidad de intrusión con diferentes niveles de control.
- Monitorización en tiempo real de los estados de seguridad y de las violaciones o intentos, mal intencionados o por error o accidente.
- Provisión de medios que garanticen la integridad de la información.
- Dotación de herramientas y mecanismos que garanticen la confidencialidad de datos y procesos restringidos.
- Seguimiento de todos los acontecimientos y éxitos relacionados para análisis exhaustivos *a posteriori*.

#### **La importancia de la gestión de la seguridad**

Podemos poner no uno, sino cientos y cientos de ejemplos de errores en la seguridad, por desgracia reales, ¡y muchos con consecuencias catastróficas!

Hay gran cantidad de libros y documentos que los comentan, especialmente aquellos incidentes que han sido sometidos a investigación oficial o judicial. Son muy útiles a la hora de conocer “qué nos puede pasar” si no adoptamos las medidas oportunas, tanto para los mismos administradores como para las consultoras especializadas en seguridad informática.

¡Tened presente que se estima que sólo son reportados por las organizaciones (sobre todo por cuestiones de imagen) menos de un quince por ciento de los casos!

## **6.2. Conceptos referidos a la seguridad en entornos informáticos**

Desde el punto de vista funcional, la **seguridad informática** se soporta siempre sobre tres ejes conocidos como *criterios de seguridad informática*.


Los tres criterios de seguridad informática mencionados se explican a continuación:

1) **Disponibilidad:** referente a la capacidad de utilización de un sistema informático cuando así sea requerido. Desde el punto de vista de la vulnerabilidad,

la disponibilidad redonda elementos y proporciona vías alternativas y herramientas de no negación del servicio.

2) **Integridad:** referente a la necesidad de que los datos de un sistema y éste mismo mantengan una coherencia, consistencia y uniformidad temporal. Se dará la pérdida de la integridad, por ejemplo, si diferentes estructuras de datos interrelacionados pierden las claves entre sí, si éstas están pero son erróneas o si las diferentes bases de datos no pertenecen al mismo momento temporal.

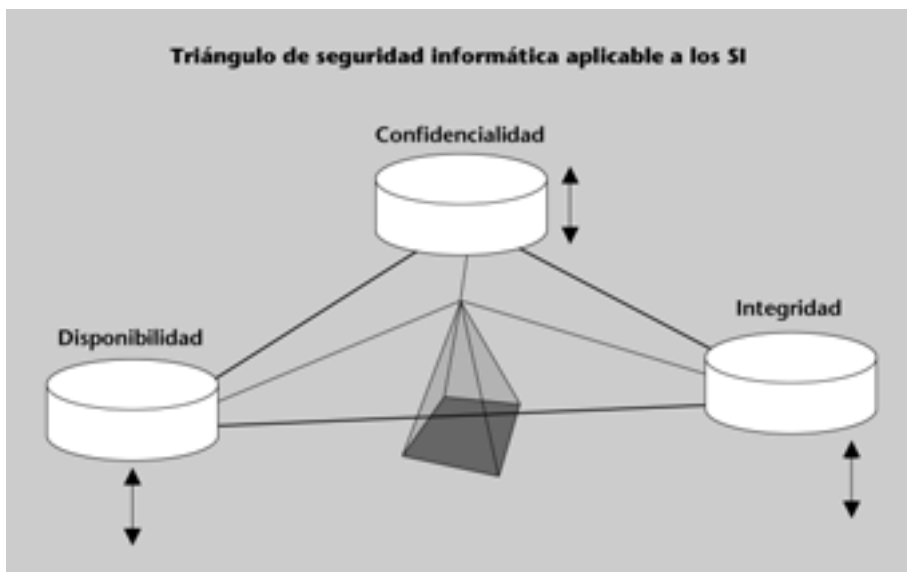
3) **Confidencialidad:** relativa a la protección de información frente a accesos, manipulaciones o simples observaciones por parte de personas, internas o externas, no autorizadas.

Los tres criterios mantienen una relación simbiótica entre sí, ya que el aumento de las medidas y actuaciones en un criterio afecta de forma negativa a uno o a los dos restantes. La plasmación gráfica de este hecho recibe el nombre de **triángulo de seguridad informática**. 

#### Seguridad ≠ confidencialidad

A menudo muchas personas de las organizaciones caen en el error de considerar que la **seguridad informática** sólo se refiere a los conceptos de garantizar la confidencialidad de la información. Es una equivocación grave que puede obviar riesgos importantes o amenazas al entorno.

Figura 24




#### El triángulo de seguridad informática

Desde un punto de vista bastante plástico, el triángulo de seguridad informática se comporta como si estuviera encima de un puntero, justo en su centro. Si sube un vértice, es decir, si se incrementa el peso de un criterio, un vértice o los otros dos bajan, o sea, disminuyen su eficacia.

Si una organización quiere reforzar los criterios de confidencialidad, se pueden incrementar las medidas y barreras de acceso, por ejemplo, si se implantan dos niveles de contraseñas y se utiliza la tarjeta inteligente. Pero si el director, para autorizar una operación comercial urgente, no puede entrar porque ha olvidado alguna de las contraseñas o porque la tarjeta no le funciona, habrá una crisis de disponibilidad, que se verá gravemente afectada.

El aumento de la disponibilidad de un sistema de base de datos se consigue mediante la implantación de redundancia, es decir, la duplicación y sincronización de las mismas BD. Sin embargo, una estructura de datos múltiple contribuye totalmente a la posibilidad de pérdida de la integridad y facilita los ataques contra la confidencialidad de los datos al haber más sitios para controlar.

Los condicionantes de los costes tienen un peso fundamental a la hora de definir las políticas de seguridad y, sobre todo, el alcance de las medidas que hay que tomar. Será necesaria una correcta evaluación y valoración de los riesgos y sus perjuicios a la organización para determinar el punto de equilibrio.

Hay tres segmentos sobre los que se puede situar este punto, en la curva de la función entre riesgos y amenazas y las inversiones que hay que asumir: 

a) **Inversión alta, baja o vulnerabilidad muy baja:** no hay restricciones con respecto a la minimización de la vulnerabilidad y el impacto. Justificada en organizaciones gubernamentales, defiende empresas con información muy estratégica, entre otras.

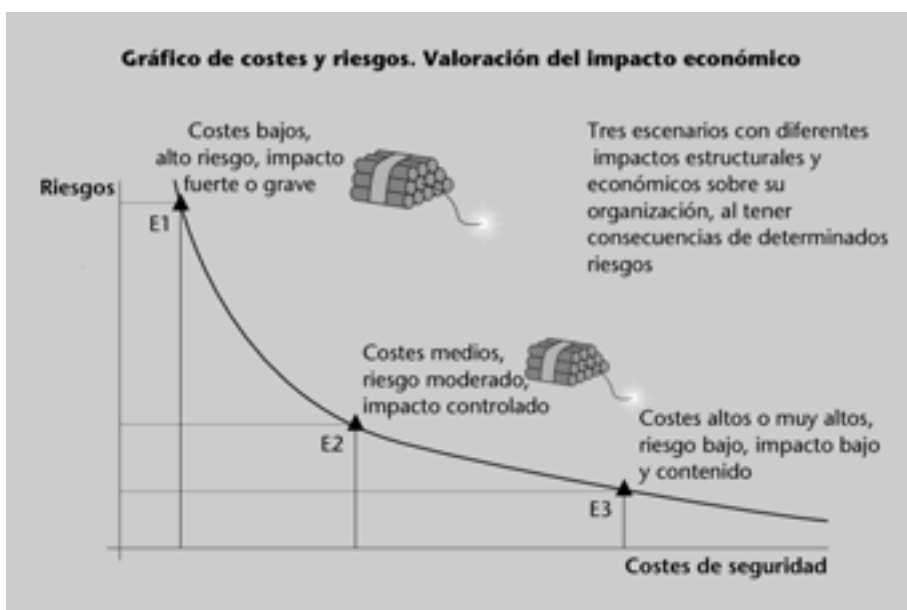
b) **Inversión moderada, vulnerabilidad disminuida:** se establecen unos niveles de seguridad adecuados para la mayoría de los riesgos y amenazas conocidas, pero los sucesos muy extraordinarios, de mayor o menor impacto, no se prevén. La mayoría de las organizaciones de tamaño mediano y grande se sitúa en este segmento.

c) **Inversión baja o nula, vulnerabilidad alta o total:** la inversión en medidas de seguridad sólo cubre algunos aspectos operacionales. La vulnerabilidad es muy alta y puede implicar un impacto muy importante, pero también están los casos de impacto de poco coste en organizaciones poco dependientes de los sistemas de información. Excepto en estos últimos casos, las organizaciones suelen estar en este segmento hasta que tienen un incidente más o menos grave.


#### La adecuación de...

... inversiones a las necesidades: una organización puede invertir fortunas en la implementación de medidas de confidencialidad, medios criptográficos o, incluso, medios biométricos de autenticación de acceso a los datos. Pero si la fuga de información prácticamente no tiene impacto para la organización y se da como caso extremo, las excepcionales –y muy caras– medidas son **una mera anécdota** para impresionar.

Figura 25




Sin duda, las dificultades de implantación de una política de seguridad correcta en un entorno de sistemas distribuidos dependen totalmente de las características del escenario, de los riesgos generales y particulares y de su impacto correspondiente.

A pesar de todo, generalmente se establecen dos grandes categorías que engloban las problemáticas, que son las siguientes: 

1) **Pérdida de definición de los objetivos de seguridad:** para muchas organizaciones, el concepto de seguridad es disperso, tanto en el ámbito de la dirección como en el de todo el personal involucrado, usuarios y administradores. Conocer los riesgos, determinar qué hay que proteger del sistema distribuido o asignar responsabilidades a los actores es básico para asignar presupuesto a áreas, elementos o servicios concretos. Hay que tener en cuenta que a menudo, si no existe una adecuada concienciación, la gestión de seguridad se considera simplemente una **sobrecarga** (*overhead*) de trabajo o de consumo de recursos informáticos.

2) **Falta de la instrumentación adecuada:** las políticas de seguridad que hay que adoptar en la organización tienen que estar acompañadas de la implantación de herramientas, instrumentos, procedimientos y dispositivos adecuados. La información de éxitos o violaciones, el cubrimiento de los agujeros técnicos de seguridad, los ataques pasivos o activos, el funcionamiento incorrecto o errático de un recurso o la incorrecta o ambigua utilización de un servicio por parte de los usuarios se tienen que detectar de forma conveniente, a ser posible en tiempo real, y registrar para el análisis posterior.

### 6.3. Subáreas funcionales en la gestión de seguridad


Desde un punto de vista operacional y general, la gestión de seguridad informática sigue un esquema simple de cuatro etapas, que son las siguientes: 

1) **Identificar la información o los servicios sensibles:** el análisis puede tener diferentes grados de profundidad, si se considera el modelo organizativo y funcional de cada actor.

2) **Determinar los puntos de entrada de amenazas o puntos de impacto de los riesgos:** especialmente en los sistemas distribuidos, que pueden mantener muchos frentes inseguros.

3) **Asegurar los puntos de entrada o de impacto:** aplicación pasiva o activa de herramientas de protección, ocultación y barrera.

4) **Mantener, monitorizar y controlar el nivel de seguro de los puntos:** aplicación de herramientas y procedimientos de seguimiento y grabación de estados y éxitos.

Al aplicar este esquema operativo simple sobre las herramientas, procedimientos y tareas de administración y gestión de la seguridad, éstos se agrupan en cuatro subáreas funcionales, que se ven a continuación con algunas características. 

#### Conciencia de seguridad

¡El tópicos de escribir la contraseña en un *post-it* pegado bajo el teclado es real!

Se precisa una política de formación y concienciación del personal en materia de seguridad para que las medidas adoptadas, de cualquier nivel, tengan éxito. No servirá de nada la política exhaustiva de contraseñas si después dichas contraseñas no se guardan de forma conveniente o se dejan las sesiones y terminales desatendidos.

Recordad que el personal interno provoca, intencionadamente o no, tres de cada cuatro incidentes de seguridad.

#### Conciencia de seguridad de los administradores

Los primeros que deben tomar conciencia de seguridad son los administradores, especialmente en instalaciones pequeñas. ¿Cuántas veces descuidan el hecho de "perder el tiempo" con las copias de seguridad, si tienen otras cosas más urgentes que hacer?

### 6.3.1. Análisis de los riesgos

El análisis de los riesgos y amenazas es un proceso que suele tener una etapa inicial larga y compleja de descubrimiento y evaluación, pero que debe ser continuado y actualizado a lo largo del tiempo para que resulte adecuado a las condiciones reales de evolución del escenario.

Es frecuente que, por error, muchos de los riesgos reales no se consideren en los primeros análisis. Puede ser a causa del desconocimiento, infravaloración de su impacto o, simplemente, por considerar obvio que determinados riesgos no nos pasarán. Si no se tiene suficiente experiencia, es muy recomendable que una consultora especializada nos ayude en las tareas de análisis.

#### Ejemplos de errores en la evaluación de los riesgos

A la hora de diseñar una sala de máquinas de un CPD siempre se consideran las medidas contra incendio, muchas de éstas difíciles y caras de implantar. Sin embargo, ¿cuántas veces, por desgracia, se considera el caso de estar afectado por una simple pero grave gotera causada por infraestructuras defectuosas del edificio o por lluvias extremas típicas en la cuenca mediterránea (la tristemente famosa gota fría)?

De hecho, los daños por agua, junto con las sobretensiones y los efectos de los rayos, son las principales causas de desastre físico en nuestro entorno. Algunos de éstos se pueden evitar y para los demás hay que dotarse de mecanismos que minimicen sus efectos.

En el gráfico de la figura 26, basado en el estudio de miles de organizaciones, se observa que las sobrecargas y transitorios de alimentación son la causa más frecuente de desastre, mientras que el mayor coste de impacto de una amenaza es el del fuego. Pero fijaos en que el robo de datos, *software* o equipamiento o problemas ocasionados por intrusiones son los que, con una notable diferencia, originan más pérdidas a la organización.

Figura 26



#### La explosión de Internet

Hoy en día, ninguna organización puede prescindir del acceso a Internet y la utilización de los servidores web. Por otro lado, la explosión del comercio electrónico, el *e-commerce*, que multiplicará exponencialmente estos tipos de servicios, ya ha empezado.

Todavía es pronto para evaluar el impacto sobre la vulnerabilidad de las organizaciones en este nuevo escenario, pero se prevé muy elevado y grave. Se impone una utilización de todas las medidas disponibles, antes de que sea tarde.

Finalmente, observad que la vulnerabilidad de los entornos distribuidos multiplica varias veces la que tradicionalmente se asociaba a los sistemas centralizados. Además de la dispersión de elementos, la complejidad de las redes de área local y los mecanismos de intrusión maliciosa (virus, bombas lógicas, caballos de Troya, *hackers*, etc.), añaden gran número de nuevas amenazas. 🚫

La siguiente tabla muestra algunas de las más conocidas y el criterio de seguridad que, en general, afectan principalmente:

Denominación	Riesgos y amenazas Descripción	Requerimientos			
		Disponibilidad	Integridad	Confidencialidad	Jurídicos/morales
Analizadores de tráfico	Obtención de datos pinchando las líneas de comunicación y analizando el tráfico.			✓	
Bombas lógicas	Modificación de un <i>software</i> para que ejecute algo en determinadas circunstancias.	✓	✓	✓	
Caballos de Troya	Programa que se presenta con una función pero que realmente hace otra.	✓	✓	✓	
Colarse	Aprovechamiento de que alguien autorizado está entrando en un servicio para entrar también sin identificación.	✓	✓	✓	
Datos obsoletos	Información desactualizada o inexacta que puede inducir a errores.		✓		✓
Daños intencionados en datos	Destrucción maliciosa de información por diferentes causas.		✓		
Denegación de servicio	Medidas para dificultar o impedir la utilización de un determinado servicio.	✓			
Desastres físicos	Daños por fuego, agua o desastres naturales.	✓	✓		
Desfalcos	Cambio o falseamiento de datos y estados.		✓		
Descuidos ( <i>bumbling</i> )	Errores humanos producidos por accidentes o baja formación.	✓	✓	✓	
Herramientas de edición de sistemas	Uso de herramientas externas muy potentes y sofisticadas para modificar accesos, datos, derechos, etc.	✓	✓	✓	
Errores de programación	Errores no intencionados en el <i>software</i> de base o de aplicación.	✓	✓	✓	
Falsedad de destino	Cambio del mecanismo de destino de una información hacia alguien no deseado.			✓	
Falsificación	Creación ilegal de documentos o autorizaciones.		✓		
Fraude	Explotación de recursos para obtener beneficio personal.		✓		

Denominación	Riesgos y amenazas Descripción	Requerimientos			
		Disponibilidad	Integridad	Confidencialidad	Jurídicos/morales
<b>Piratería de software</b>	Copia ilegal de <i>software</i> y documentación.				✓
<b>Puertas de atrás (back doors)</b>	Medio alternativo y secreto de entrada en el sistema.	✓	✓	✓	
<b>Propagaciones electromagnéticas</b>	Aquellas que pueden perturbar el funcionamiento de elementos o difundir datos confidenciales.	✓		✓	
<b>Búsqueda en la basura</b>	Búsqueda de información de listados en la papelera, archivos borrados de cintas y discos, etc.			✓	
<b>Robo</b>	Robo de elementos, información, servicios, etc.	✓	✓	✓	
<b>Sabotaje</b>	Destrucción y manipulación maliciosa de elementos físicos o lógicos.	✓	✓		
<b>Sobrecarga</b>	Sobrecarga de los recursos del sistema para conseguir su caída o fallo.	✓			
<b>Suplantación</b>	Hacerse pasar por alguien que no se es.	✓	✓	✓	
<b>Tergiversación</b>	Engaño diciendo que un resultado o efecto es del sistema, cuando es un efecto humano provocado.			✓	✓
<b>Virus</b>	Programa que tiene la capacidad de pegarse a otros para su reproducción.	✓	✓		

### 6.3.2. Análisis y diseño de los servicios de seguridad

El número y características de las medidas y servicios de seguridad que se pueden aplicar a una organización para evitar riesgos dependerán de múltiples factores, como por ejemplo el nivel de sofisticación y complejidad, los costes, los esfuerzos de implementación y los de mantenimiento o la demanda de recursos humanos internos o externos.

Sin embargo, normalmente un solo servicio o medida no puede proteger el sistema informático de las violaciones de seguridad que puede sufrir, por lo que a menudo se utiliza una combinación de éstos. Además de conseguir una mejor adecuación de las medidas a las amenazas, también se cuenta con la ventaja, por ejemplo con el control de la confidencialidad, de que si se viola o se salta un servicio habrá una barrera siguiente, otro servicio de seguridad, que lo detectará o contendrá.

Algunos de los servicios que tradicionalmente se exigen incluyen los siguientes:

- **Múltiples niveles de autenticación:** la autenticación (asegurar que es realmente lo que dice que es) se basa inicialmente en contraseñas que pueden es-

tar jerarquizadas y que acotan niveles más críticos de seguridad. A menudo la autenticación está reforzada mediante la utilización de otros elementos, como claves físicas, tarjetas inteligentes o, incluso, parámetros biomédicos.

### ¡Autenticación de película!

Los **parámetros biomédicos**, como la lectura de la huella del dedo o de la mano, el reconocimiento de la voz, la identificación de caracteres faciales o la lectura del fondo de retina, han salido de las películas de ciencia ficción para ser utilizados hoy en día en el mundo real. El aumento de la fiabilidad de los dispositivos y la bajada de precios lo permiten.

Sin embargo, debemos tener en cuenta los perjuicios de disponibilidad si la persona que es realmente no es autenticada y autorizada simplemente porque un escáner está sucio o porque el usuario tiene la voz asfixiada.

- **Autenticación simétrica:** se utiliza para certificar que, a partir de un momento determinado, ambas partes son las que dicen ser y no hay suplantaciones.
- **Acuse de recepción y certificaciones para terceros:** son necesarias diferentes técnicas de autenticación basadas en la emisión de certificados, dos a dos y para terceros, que registren la identificación de los actores, el tipo de relación que establecen y el periodo temporal de validez del certificado.
- **Impedimentos de los procesos de escucha y captura de tráfico:** algunos analizadores de tráfico\* se pueden utilizar simplemente desde un PC portátil conectado a un punto LAN libre y obtener, mediante escucha pasiva, información crítica que pasa por la red (contraseñas, identificación de usuarios, certificados, datos confidenciales, etc.). Es precisa la utilización de técnicas criptográficas y marcas de tiempo\*\* para evitarlos.
- **Control de la integridad:** servicios que proporcionen garantías de protección ante eliminaciones, modificaciones, inserciones y repeticiones de segmentos de datos que circulan por la red.

\* En inglés, *sniffers*.  
\*\* En inglés, *time stamping*.

### 6.3.3. Implementaciones y soluciones para los servicios de seguridad

Ciertas medidas utilizadas para implementar los servicios de seguridad anteriores ya se han mencionado. Éstas son algunas, con determinados detalles:

- **Codificación de la información:** las técnicas criptográficas se encargan de transformar de forma adecuada una información para que, si se accede a ésta de manera fraudulenta, sea ilegible. Las dos técnicas básicas son las de clave simétrica y de clave asimétrica:
  - Los sistemas de **clave simétrica**, también denominados de **clave única o privada**, utilizan la misma clave para cifrar y descifrar la información. Quien tiene la clave puede abrir los mensajes, por lo que tiene que estar bien guardada. El algoritmo más conocido y utilizado es el DES.

- Los sistemas de **clave asimétrica**, también conocidos como de **clave pública**, están basados en un par de claves. Una, la pública, se utiliza para cifrar los mensajes y puede ser conocida por todo el mundo. La otra, la privada, es la que descifra la información y sólo la debe conocer el destinatario. El algoritmo más conocido y utilizado es el RSA.

En ocasiones, estos sistemas se ven complementados por la utilización de **técnicas de firma digital**, que consisten en el proceso algorítmico de la información con el fin de obtener su correspondiente firma. Si la información se modifica o altera, el proceso dará una firma diferente y se detectará el error o el fraude.

- **Filtrado:** los mecanismos basados en el filtrado se encargan de un encaminamiento selectivo de los paquetes de diferentes niveles de protocolos que circulan por la red. De esta manera es fácil discriminar el acceso según el punto de origen, el destinatario, el tipo de protocolo o la marca de tiempo, entre otros.
- **Métodos de barrera:** los métodos de barrera se basan en técnicas similares a los procedimientos de filtrado, pero los aspectos selectivos y discriminatorios son más funcionales, normalmente relacionados con el tipo de servicio o aplicación. El objetivo es hacer particiones del sistema distribuido para evitar que, si se produce una violación, ésta quede restringida a un área determinada. Los mecanismos de este tipo más conocidos actualmente son los **cortafuegos\*** de última generación.

Los cortafuegos han nacido de la necesidad de disminuir la vulnerabilidad del protocolo TCP/IP, muy potente pero débil desde del punto de vista de la seguridad, y que se ha impuesto casi como la única tecnología desde la explosión de Internet, y han evolucionado desde unos simples encaminadores hasta complejos sistemas de autorización de bajo, medio y alto nivel, basados en reglas complejas y, en determinados casos, con motores de inferencia utilizados en los sistemas expertos.

- **Certificados emitidos por terceros:** las técnicas de certificación de terceros permiten asignar las tareas de arbitrio de la validez de una relación entre dos actores a un juez o notario informático que identificará, comprobará, autorizará y registrará la relación.

Finalmente, uno de los componentes imprescindibles que se echa de menos en muchas organizaciones a la hora de diseñar e implementar medidas y herramientas de seguridad adecuadas a los objetivos, perfiles y capacidad de la organización es el **plan de seguridad**. Éste es un documento que debe registrar todas las características mencionadas y también los correspondientes subplanes de contingencia, que se tienen que aplicar si se producen violaciones u otras circunstancias no deseadas.

#### La firma electrónica

Es tal el impulso que se está aplicando en la implantación de las nuevas tecnologías en el comercio, la Administración Pública, las relaciones contractuales y decenas de áreas objetivo, que se exige la necesidad de regulación jurídica de todos estos nuevos procedimientos.

La Ley de Firma Electrónica del Estado, aprobada en septiembre de 1999 y basada en técnicas de certificación, es uno de los primeros pasos que permitirán la utilización de las nuevas tecnologías, aunque con muchos detractores, con menos sensación de "vulnerabilidad tecnológica".

\* En inglés, *firewalls*.

#### Los "notarios electrónicos"

Uno de los primeros esquemas que se hicieron en la línea de certificación para terceros fue el **Kerberos**, basado en un servidor local de autenticación.

Hoy en día, todos los mecanismos y procedimientos de relación certificada entre dos, especialmente las referidas al comercio electrónico (SET, SSL) y a las relaciones con la Administración, utilizan técnicas de certificado de terceros.

### 6.3.4. Detección y actuación ante acontecimientos de seguridad

Los mecanismos de detección ante violaciones de la seguridad han avanzado mucho en los últimos años y permiten una notificación del acontecimiento prácticamente en tiempo real. Estas medidas, denominadas **dinámicas**, permiten la notificación a los sistemas de control de seguridad e, incluso, la generación de alarmas de la gestión de fallos si el nivel de servicio preestablecido se puede ver afectado.

Por otro lado, las medidas **estáticas**, basadas en el estudio detallado de las tablas de anotación de movimientos\*, hechos, operaciones o cualquier otro suceso correcto, habitual y cotidiano ayudarán mucho a discriminar fallos de detección de las medidas activas. Su importancia se destaca cuando se tiene en cuenta que las nuevas medidas activas están diseñadas para luchar contra una nueva amenaza, pero siempre es una medida *a posteriori* a la aparición de aquélla.

\* En inglés, *logs*.

#### ¿Es suficiente con los antivirus?

La lucha contra la infección por virus es un buen ejemplo. Una organización (¡tendrían que ser todas!) puede estar perfectamente protegida con los sistemas antivirus de última generación, actualizados mensualmente, que permiten detectar los miles de virus que existen en este momento. Sin embargo, si no se dispone de medidas que impidan o minimicen los riesgos de entrada, puede ser atacada por un nuevo virus que el antivirus no conoce y resultar totalmente indefensa, y lo que es peor, con la falsa seguridad de que se piensa que no corre ningún peligro.

Se calcula que se crean tres nuevos virus malignos al día en todo el mundo. Y los antivirus son siempre medidas *a posteriori* a que éstos hayan atacado y dañado a unas o muchas organizaciones y que se hayan predetectado, aislado, analizado y programado convenientemente los detectores adecuados.

Finalmente, y como sucede en la gestión de fallos, no se puede asegurar nunca al cien por cien que ningún riesgo o amenaza está totalmente controlado y que la resistencia en las violaciones de seguridad es total. Es muy necesaria la implantación de herramientas y medidas de contención, a ser posible bien asediadas, con procedimientos claros de quiénes tienen que actuar en caso necesario y cómo.

Los **planes de contingencia** o emergencia, fundamentales dentro del plan de seguridad, contienen todos estos procedimientos y se tienen que revisar con frecuencia para que no se conviertan en unos manuales olvidados que nunca, por suerte hasta ahora, se habían utilizado.

## 7. Gestión de contabilidad

La última de las cinco áreas definidas en el modelo funcional OSI es la gestión de contabilizaciones, que se encarga de medir cómo, con qué grado y por qué usuarios son utilizados los recursos, dentro de todo el alcance del sistema distribuido. En los entornos actuales, fuertemente orientados a la utilización de recursos compartidos, las medidas son la herramienta que permite establecer compensaciones presupuestarias y justificaciones de nuevas inversiones en recursos, así como el control exhaustivo de los diferentes servicios contratados a externos.

### 7.1. Introducción

El principal objetivo de la **gestión de contabilizaciones** es el de proporcionar un conjunto de herramientas y procedimientos orientados a la medida de las estadísticas de utilización de los elementos y servicios de la red.

#### Terminología

El área gestión de contabilizaciones es conocida normalmente en los textos como *accounting management*, AM.

La información así recogida puede ser analizada y utilizada hacia las dos orientaciones de los procesos de contabilización, que son los siguientes:

1) La **orientación de planificación y control** permite, a partir del análisis de las correspondientes estadísticas de consumo, proporcionar a los administradores una valiosa información a la hora de mantener o reasignar el sitio y el papel de los recursos compartidos. Dicha orientación se basa en unos parámetros y objetivos más técnicos, con el fin de conocer con precisión cómo se utilizan los recursos, en qué medida y en qué momento, y obtener el perfil de utilización que presenta cada usuario o unidad. Entre otros, el administrador puede determinar los valores de uso útil (de producción), de uso accesorio (reintentos, pruebas, etc.) y el consumo por el mismo funcionamiento (*overhead*).

2) La segunda vertiente del área de gestión es la **orientación de imputación de cargas y costes**, que quiere alcanzar unos objetivos más financieros, basados en el equilibrio de inversiones, y su adecuación y rentabilización. La medida de utilización de los recursos y servicios por los usuarios, que proviene de los procesos anteriores, permite establecer políticas de asignación e imputación de costes teniendo en cuenta el uso, que simplemente se pueden anotar en el efecto estadístico y de compensación, o incluso facturar convenientemente de manera periódica.

La proliferación de la contratación externa de servicios, especialmente los relacionados con servicios de telecomunicación, servicios básicos\* o de valor añadido\*\*, ha hecho especialmente crítica esta área y los mecanismos de medida e imputación que utiliza. Para la organización que contrata estos servicios hay que llevar un control sobre los consumos, los niveles de servicio obtenidos, la imputación de las tarifas correctas en cada momento, si procede, o los perfiles de crecimiento para la planificación financiera.

\* Como voz, líneas, enlaces, etc.  
\*\* Como web, correo electrónico, centros de atención telefónica, etc.

### **La utilización no es gratuita**

Las técnicas de imputación de costes están adquiriendo más aceptación en las grandes organizaciones. Sin lugar a dudas, cargar el número de llamadas telefónicas de un departamento, el tiempo y capacidad utilizada de los enlaces con Internet, el espacio en disco utilizado o el número de asistencias solicitadas al *help desk* o a externos ayuda a una utilización racional de los recursos compartidos, sin la falsa copia de seguridad que representa una imputación corporativa de los costes.

Finalmente, la decisión de implantar o no la facturación dineraria de estos servicios en los departamentos o usuarios dependerá de la estrategia financiera de la organización.

Sin embargo, lógicamente, las empresas que proporcionan a otros este tipo de servicios son las que requieren una gestión más precisa y exhaustiva, porque de ello depende su salud y rentabilidad financiera. Además de la complejidad y fiabilidad de los mecanismos de medida de los servicios proporcionados, se incluirán todas las funciones de generación de cargos, facturación, gestión de clientes y contratos o gestión de pagos, entre otros.

### **Depender totalmente del *accounting* (gestión de contabilizaciones)**

No cabe ninguna duda de que los grandes proveedores de servicios públicos de telecomunicación, conocidos como operadores o TELCO, disponen de sistemas de contabilización casi tan importantes como la misma infraestructura y servicios que proporcionan.

Sin embargo, hay demasiados ejemplos de pequeñas y medianas empresas proveedoras de servicios de valor añadido (VAN) que se han hundido en grandes pérdidas (proveedores de acceso a Internet, centros de llamadas, *hosting* de webs, etc.).

La falta de previsión (muchos de sus costes son fijos, independientemente de la cartera de clientes) y en especial **los errores de contabilización y facturación de servicios** han sido las causas.

Algunas de las actividades incluidas en las tareas de la gestión de contabilizaciones son las siguientes:

- Identificación de los componentes y servicios que hay que medir.
- Establecimiento de las métricas de medida de cada utilización.
- Implantación de las sondas de monitorización de uso.
- Captura y almacenamiento de datos de consumo.
- Asignación y control de cuotas de utilización.
- Diseño y establecimiento de las políticas de cargo.
- Mecanismos de imputación de costes en los departamentos o usuarios.
- Facturación y periodificación de los costes.

### **El impacto de Internet en los sistemas distribuidos**

Como ya se ha comentado varias veces, el impacto que Internet comporta en muchos aspectos de la gestión y administración de sistemas distribuidos es con frecuencia mucho más alto que el que se prevé en un primer momento.


En una organización en la que pueden trabajar quinientas personas, los consumos de los servicios ofimáticos solían estar bastante acotados. Los servidores estaban suficientemente dimensionados para alcanzar un gran conjunto de documentos, hojas de cálculo, pequeñas bases de datos personales o departamentales, presentaciones comerciales o correo electrónico. La instalación de cuotas máximas no había sido hasta ahora necesaria, porque el consumo de estos archivos no requería, normalmente nunca, más de unos cincuenta MBytes por usuario y ellos mismos, más o menos, lo controlaban borrando los archivos obsoletos.

Sin embargo, de forma increíble, en los últimos meses los administradores habían detectado un crecimiento extraordinario de las necesidades de espacio en disco, que obligaba a adelantar la adquisición de más dispositivos y creaba verdaderos problemas de operación, especialmente con las copias de seguridad.

Un análisis exhaustivo reveló que decenas de usuarios habían activado servicios y canales de información de Internet, en general relacionada con su actividad dentro de la organización, pero que cargaba día y noche en sus particiones en segundo plano (*background*) centenares de páginas web. No sólo mucha de esta extensa información no podía ser consultada por el tiempo que llevaba, sino que el usuario no podía determinar *a priori* si le entrarían uno, diez o cien megabytes de información cada día. Además, numerosos usuarios se habían suscrito a los mismos canales y había decenas de copias de la misma voluminosa información. Se había estado a punto del colapso en varias ocasiones.

El diseño de la suscripción a los canales de manera corporativa y la designación de personal encargado de su administración resolvieron el problema de forma satisfactoria, sin renunciar a la ventaja de esta nueva fuente de información. Sin duda, los administradores establecieron cuotas máximas de ocupación de las particiones de cada usuario, ¡por si acaso!

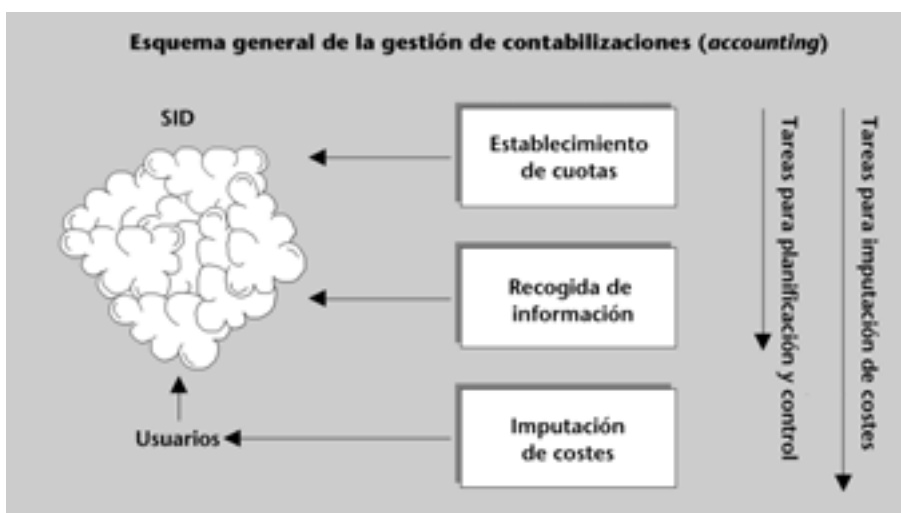
## 7.2. Esquema general de la gestión de contabilizaciones

Las funciones que se desarrollan dentro del área de gestión de contabilizaciones se agrupan en tres etapas principales, que son las siguientes: 

- 1) Establecimiento de políticas, recursos de medida, métricas y cuotas de utilización.
- 2) Recaudación de la información con respecto a la utilización de los recursos.
- 3) Tarifación e imputación de costes de utilización a los usuarios.

El esquema general de la gestión de *accounting* en un sistema informático está representado en la figura siguiente, y algunos detalles destacables de cada una de éstas se comentan a continuación.

Figura 27



### 7.2.1. Diseño y establecimiento de políticas de contabilización

Generalmente se prevén tres áreas previas a la hora de diseñar y establecer las políticas de contabilización, que son respectivamente la selección de elementos, la selección de métricas y la determinación y asignación de cuotas.

#### a) Selección de elementos

La clasificación de los elementos que pueden ser objeto de contabilización de uso puede responder a diferentes criterios de la organización. Con un carácter de propósito general, se puede utilizar la relación de categorías y componentes siguiente:

- **Elementos *hardware*:** todas las medidas directamente relacionadas con magnitudes físicas de los elementos del sistema distribuido, como utilización del CPU, ocupación en los discos y cintas, ocupación de canales y dispositivos de I/O, Kbytes o paquetes transferidos por un enlace, circuitos de terceros contratados o páginas escaneadas o impresas, entre muchos otros.
- **Elementos *software*:** medidas hechas sobre componentes del *software* de base, desde el que pertenece a los sistemas centrales hasta el que corresponde a la electrónica de red, y sobre el de aplicación.
- **Servicios:** incluye todos los servicios que proporciona el sistema distribuido a los usuarios, como la medida de calidad y disponibilidad de los mismos servicios de telecomunicación y de red, la utilización de las unidades y herramientas de ayuda corporativas (*help desk*, boletines, etc.), o los servicios de tipo general, como el número de *logins* en el sistema o las horas de utilización, entre otros.
- **Recursos humanos:** número de consultas, intervenciones, horas u operaciones hechas, tanto por recursos internos como por recursos externos contratados.
- **Servicios auxiliares\*:** se incluyen todas las medidas referidas a la infraestructura y servicios de base no tecnológicos, como los costes inmobiliarios, alquileres, consumos de electricidad, gas y agua, seguros, mantenimientos y reformas, impuestos y los correspondientes cocientes por empleado, hora de trabajo o nivel de facturación, entre otros.

#### Medidas sobre los componentes *software*

Algunas de estas medidas son el número de transacciones por unidad de tiempo hechas contra un motor de base de datos, número de consultas y actualizaciones hechas por un usuario, utilización de los recursos *hardware* de cada componente de aplicación o herramientas de soporte utilizadas en un periodo.

\* En ángulos, *facilities*.

#### b) Selección de métricas

Las métricas utilizadas para contabilizar deben permitir identificar sin duda el uso del recurso y tienen que ser perdurables y consistentes en el tiempo, dentro del entorno del escenario del sistema informático. Existen decenas de métricas válidas, algunas de éstas inspiradas en los parámetros de indicación de

prestaciones\*, en el área de gestión de prestaciones. En la anterior relación de elementos aparecían unas cuantas.

\* En inglés, *performance*.

### La métrica tiene que ser consistente

No puede haber dudas de interpretación de una determinada métrica. Si se contabilizan el número de llamadas atendidas por un centro de soporte, hay que tener en cuenta cómo se prevén las llamadas fallidas, repetidas o reiteradas, por ejemplo.

Además, la métrica tiene que perdurar y ser consistente. Si se cuentan las transacciones por minuto, un nuevo frontal de comunicaciones que, por ejemplo, las agrupe, puede proporcionar unas medidas no coherentes con las anteriores.

## c) Determinación y asignación de cuotas

Las cuotas son ventanas de utilización de los recursos compartidos que permiten establecer limitaciones en determinadas circunstancias. De hecho, son la primera herramienta de ayuda a los administradores para establecer un control sobre el uso que hace cada usuario del sistema, y esta condición resulta esencial para mantener los niveles de servicio globales preestablecidos.

Los impedimentos que imponen las cuotas ayudan al hecho de que no se produzcan, si no se desean (normalmente es así), monopolizaciones provocadas o no intencionadas. De esta manera el servicio global queda protegido contra acaparamientos no deseados, especialmente los fortuitos, por su misma falta de previsión de que sucedan.

### Un caso de ejemplo de establecimiento de cuotas

Cualquier instalación de tamaño mediano o grande establece cuotas, casi por defecto, a la hora de asignar un perfil de uso a un usuario. Las cuotas de espacio en disco son de las más habituales, para el perjuicio global que puede provocar un llenado desmesurado de los discos, reducir las prestaciones e, incluso, bloquear el uso del dispositivo o de todo el sistema. Las cuotas de CPU pueden ser igual de críticas, si un *software* tiene un error o pierde el control, y entra en bucles infinitos que cada vez pueden solicitar más CPU. Es habitual establecer cuotas incluso para la utilización de periféricos, como impresoras o escáneres, a fin de que un usuario no monopolice continuamente y se creen conflictos entre el personal.

### ¿Son infinitas las líneas?

En los últimos años las cuotas de servicios de comunicación tienen un especial interés, sobre todo con la explosión de Internet en las organizaciones. Las líneas, tanto de entrada como de salida, siempre están limitadas, por lo que un acaparamiento en cualquier sentido puede degradar el servicio hasta límites no operativos. Si éste no se produce por razones de producción, por ejemplo, con transferencias simultáneas de ficheros que se podrían hacer por la noche, o utilización accesorias y por diversión, las consecuencias son más graves.

## 7.2.2. Recaudación de información de utilización de recursos

Las medidas de utilización de los recursos son recogidas por las correspondientes sondas de monitorización, establecidas para este efecto. Es habitual que estas sondas estén en los agentes de monitorización de los objetos, porque las medidas son necesarias para el resto de las áreas de gestión del sistema distribuido.

Las herramientas de contabilización almacenan los datos que llegan en diferentes frecuencias. En algunos casos, la comunicación se produce en tiempo real, referente a éxitos o acontecimientos que se acaban de producir. En otros casos es en diferido, cuando la información de los acontecimientos está formada por los objetos, pero corresponden a un determinado periodo anterior y suelen es-

tar marcados en el tiempo. Finalmente, hay informaciones que son recogidas por la misma herramienta de contabilización, periódicamente, mediante procedimientos de *polling* o mecanismos similares.

La información de consumos almacenada suele ser requerida a medio plazo, por lo general con periodicidad semanal o mensual, aunque excepcionalmente puede haber recursos críticos que requieran análisis o proceso de imputación diario.

#### Los servicios de accounting,...

... en entornos de administración y gestión bien integrados, son los que comunican mucha de la información que necesitan el resto de las áreas, especialmente la gestión de configuración y la gestión de prestaciones. Evidentemente, a medio y largo plazo, la información es esencial para la gestión de la planificación.

### 7.2.3. Tarifación e imputación de costes

El beneficio que proporciona el hecho de dar a conocer a cada usuario, departamento o unidad el perfil de consumo de los diferentes recursos ayuda a su planificación y “uso racional”, con visión corporativa, sin lugar a dudas. Según su estrategia financiera, la organización puede decidir, además, la facturación de los mencionados consumos, en criterios dinerarios, tanto si se restan de las cuotas de beneficio de la misma unidad, como del presupuesto anual que la unidad disponga (contabilidad presupuestaria).

En este sentido, las **políticas de cargo de costes** se clasifican en las siguientes:

- **Cargo nulo:** se contabilizan los costes de utilización y se informa a los usuarios, para el efecto informativo, de ayuda a la planificación y el “buen uso”.
- **Cargo parcial:** se factura a la unidad una parte proporcional del coste de un recurso, según diferentes cocientes como el uso, la productividad o la participación en beneficios, entre otros. El resto del coste es asumido como corporativo.
- **Cargo total:** la imputación del coste es total, en ocasiones independiente del uso hecho.


A la vez, los **procedimientos de imputación de costes** pueden aplicar tres mecanismos básicos:

- **Coste proporcional:** todos los costes se dividen linealmente entre todos los usuarios. Es el procedimiento más simple de gestionar.
- **Coste por responsabilidad:** se aplican “pesos” que ponderan la utilización de los recursos por la unidad. Es el esquema utilizado con mayor frecuencia.
- **Coste estandarizado:** el coste total del recurso se divide entre los indicadores de producción (facturación, ventas, etc.) de la unidad. Cuanto más utilización, que repercute con más beneficio obtenido, menos coste. El recurso es

fuertemente soportado por los que lo utilizan en poco rendimiento de la producción corporativa.

Para finalizar, los **momentos de imputación de los costes** se agrupan principalmente en dos métodos:

- **Instalación del servicio:** la facturación se lleva a cabo al finalizar el trabajo de instalación de infraestructuras u otros elementos. Si hay tarifas de utilización, mantenimiento o soporte, éstas se pueden cubrir mensualmente.
- **Periódicamente:** se imputan los costes de manera periódica cada mes o trimestre, por ejemplo, y se contabilizan las tarifas fijas y, si procede, la tarificación de consumos.

Sean cuales sean la política de cargo de costes y el procedimiento de imputación elegidos, siempre hay que considerar las ventanas preestablecidas de nivel de servicio, especialmente las referidas a la calidad y la disponibilidad. Estos niveles, que deben estar preestablecidos por contrato, pueden restar unos determinados importes o compensaciones, si no se ha llegado a las cuotas contratadas. De la misma manera que el impago de los costes, la continuidad de los incumplimientos puede llevar a la rescisión del contrato y a la finalización del servicio. 

## 8. Gestión de la planificación

Aunque son cinco las áreas definidas en el modelo funcional OSI para la administración de sistemas distribuidos, a menudo se habla de la sexta área del modelo, la gestión de la planificación. Su cometido engloba todos los procesos relacionados con la planificación de la evolución del sistema y analiza su estado, las tendencias previstas y los objetivos definidos por la organización. La relevancia que representan estas tareas es fundamental en la época actual, en la que los cambios en las organizaciones están fuertemente basados en las sinergias con las tecnologías de la información y comunicaciones que las soportan.

### 8.1. Introducción

El principal objetivo de la gestión de planificación es el de proporcionar las metodologías y procedimientos orientados a determinar una mejor y más correcta evolución del sistema distribuido.

#### Terminología

El área de gestión de la planificación es conocida normalmente en los textos como *planning management*, PM.

La información inicial se desarrolla según las características actuales del sistema y los objetivos corporativos marcados. Los estudios de tendencias de evolución de la carga, su capacidad de absorción y de crecimiento de los elementos y el análisis de los productos y tendencias del mercado son requisitos para la elaboración del plan de evolución correspondiente.

Desde un punto de vista estratégico, las tareas de planificación quieren cumplir los compromisos de nivel de servicio; a medida que evolucionan los requerimientos de carga, optimizan la utilización de los recursos disponibles con un coste establecido dentro de los objetivos financieros.

La gestión de planificación es un proceso continuo que se desarrolla día a día, paralelo a la misma actividad del sistema y durante todo su ciclo de vida. La concreta evolución del sistema interacciona con la planificación, si ésta es adecuada, y permite un proceso sin rupturas, al menos si no se producen cambios del escenario traumáticos.

Algunas de las actividades incluidas en las tareas de la gestión de planificación son las siguientes:

- Definición y diseño de la estrategia corporativa de evolución en los sistemas de información.
- Cuantificación y análisis de las características de la carga actual.

- Análisis de los niveles de servicio y comportamiento general del sistema distribuido en el escenario.
- Identificación de la capacidad residual y cuellos de botella que afecten al crecimiento.
- Análisis de tendencias de comportamiento y diseño de tendencias previstas.
- Estudios de previsión de carga futura.
- Observación del mercado tecnológico y las tendencias organizativas.
- Diseño y elaboración de los planes de requerimientos y evolución.
- Implantación del plan de evolución.
- Testeo y realimentación de información en el plan.

### Un caso de ejemplo de la gestión de la planificación

Todos los sistemas informáticos tienen que evolucionar, tanto por cambios en el escenario, modificaciones de las características de la carga o variaciones de los niveles de servicio, como por obsolescencia tecnológica o funcional de los componentes o la misma evolución vegetativa. Y en todos hay que planificar de forma adecuada las acciones que hay que efectuar y las prioridades que se deben tomar.

Un entidad bancaria, por ejemplo, con una etapa de estrategia corporativa de expansión plantea abrir un número importante de sucursales, que en tres años duplicarán las actuales. El objetivo marcado por la dirección puede ser el de minimizar el coste de la red necesaria, pero siempre cumpliendo los requerimientos que garanticen un tiempo de respuesta inferior a dos segundos en el 95% de las transacciones totales y una capacidad de transacciones por segundo mínima determinada.

El plan proporcionará todas las pautas de diseño, infraestructuras que hay que hacer, servicios que se deben contratar, dimensionado de equipos, servicios de instalación, mantenimiento y soporte o formación de administradores y usuarios, entre otros, y para toda la planificación de expansión, en los tres años. Pero deberá prever los cambios que la oferta de operadores de comunicación, los avances tecnológicos e, incluso, la aceleración o freno de la estrategia expansiva puedan dar.

## 8.2. Principales dificultades en la gestión de planificación

Muchas de las dificultades que se presentan en la gestión de la planificación de los sistemas distribuidos actuales son comunes a las del resto de las áreas de gestión, ya comentadas, y que enfatizan, sobre todo, la dispersión y heterogeneidad de los recursos del sistema.

Sin embargo, existe una serie de factores más particulares en las tareas de planificación que representan los puntos de mayor dificultad o más difíciles de precisar a causa del objetivo de futuro que se quiere alcanzar. Algunos de dichos factores son los siguientes:

- **Problemáticas en la definición de la carga tipo:** será difícil determinar la evolución futura de la carga si no es posible determinar con suficiente exactitud las características de la carga actual, y establecer unos comportamientos o ventanas tipo. La información proporcionada por la gestión de prestaciones será fundamental.
- **Determinación clara de los niveles de servicio:** es importante conocer sobre el nuevo escenario cómo se cumplen los niveles de servicio prees-

### Terminología

La descripción y modelización de las características de la carga de un sistema informático se conoce normalmente como *caracterización de la carga*.

tablecidos para prever la evolución, estimación y necesidades de QoS en el futuro. Si hay terceros involucrados, las medidas nos informarán de si es aconsejable mantenerlos, renegociar condiciones o buscar alternativas.

- **Detección y eliminación de los cuellos de botella:** si son problemáticos cuando aparecen en el crecimiento vegetativo del sistema, se convierten en un factor muy crítico si se detectan en momentos de emergencia, bajo condiciones de fallo contenido. En estas ocasiones, es fácil que se produzcan “efectos dominó”, que acaban deteniendo totalmente el servicio.

#### **Los temidos “efectos dominó”**

Los “efectos dominó”, la caída secuencial de muchos de los recursos del sistema hasta llegar a menudo a la caída total, normalmente son provocados por un fallo que ha sido analizado sin apenas considerar el escenario que lo rodea o la ligera evolución que éste experimenta con el paso del tiempo.

Un recurso puede disponer de unos sistemas de contención de fallos muy adecuados, que aisladamente le confieren una gran fiabilidad, pero el fallo debe quedar bastante aislado del resto de los elementos y servicios (extremado tiempo de conmutación, información de caída, reconfiguraciones, etc.) para no provocar efectos colaterales, uno tras otro.

Los efectos dominó son responsables de la mayor parte de las catástrofes producidas en los sistemas informáticos y sobre éstos, y su prevención es un objetivo claro de la gestión de fallos y la gestión de planificación.

- **Problemáticas asociadas a los productos y los elementos:** no todo lo que dicen los proveedores y fabricantes que hacen, sus elementos físicos o los productos *software*, es verdad. El comportamiento real de muchas arquitecturas de proceso y de comunicación, soluciones *software*, herramientas de base y de aplicación y muchos otros componentes se aleja de lo que dicen sus especificaciones. El efecto no corresponde tanto a la extensión y tamaño del sistema distribuido, como a las interacciones o “efectos secundarios” que se producen en entornos complejos.

#### **Los “efectos secundarios”**

Los problemas ocasionados por la interacción de elementos, especialmente del *software*, se pueden convertir en la pesadilla de un administrador a la hora de estabilizar las nuevas configuraciones del escenario, en principio bien planificadas. Pocos fabricantes avisan *a priori* de que su producto puede tener problemas de interacción con otro, porque afectaría a su imagen, por lo que los diseñadores deberán estar muy atentos a boletines de problemas, otras instalaciones o unidades de soporte (suelen ser más francas que las comerciales).

No es, en principio, un problema de magnitud: una pequeña LAN con multitud de protocolos, sistemas operativos y combinaciones de productos de aplicación y ofimáticos puede tener más problemas de interacción que una gran red de miles de puestos de trabajo, pero más homogénea.

- **Estrategias corporativas difundidas, erráticas o poco concretas:** no siempre las estrategias marcadas por la dirección son claras. En ocasiones, todo un proyecto bien calculado y planificado no se lleva a cabo por cambios presupuestarios. O lo que es peor, los criterios cambian una vez que ha empezado a desarrollarse, se multiplican por cinco las magnitudes y se reduce el tiempo a la mitad. La planificación deja paso, pues, a la improvisación, y los resultados pueden ser caóticos.

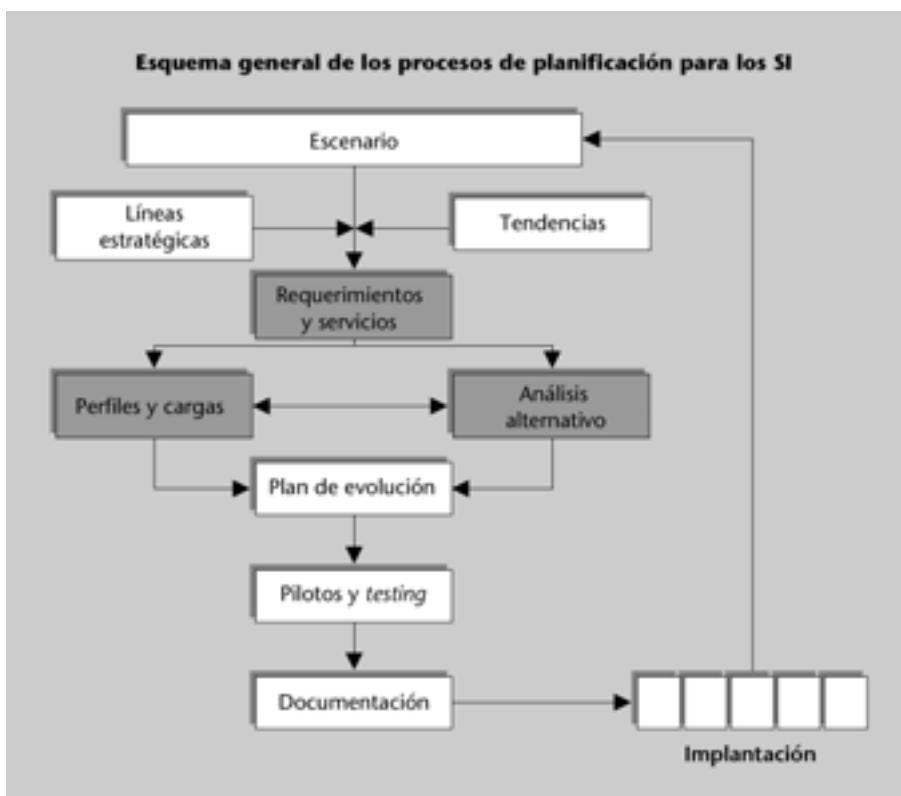
- **Insuficiente cuantificación de las necesidades de los usuarios:** en ocasiones no se prevén correctamente o con detalle las necesidades de los usuarios (o bien éstos no las comunican de una manera lo bastante clara). El resultado es una planificación a la baja que normalmente acaba con un incremento presupuestario innecesario.
- **Debilidad, incorrección o falta de las herramientas adecuadas:** la correlación de factores a la hora de planificar es fundamental. Si las herramientas o procedimientos utilizados no pueden prever, al mismo tiempo, multitud de parámetros y segmentos vinculados\*, se puede perder la visión de rentabilización y optimización del conjunto.
- **Recursos humanos de planificación:** en general, en las organizaciones hay pocas personas con la capacidad de entender los planes estratégicos y los vínculos con las necesidades de los usuarios y los criterios de evolución del sistema. A menudo estos recursos se contratan externamente y su éxito depende de la capacidad que tengan para “extraer” la información real de la organización, para plasmarla en la planificación.


\* Coste, tipo de equipamiento, prestaciones, facilidades de instalación o uso, etc.

### 8.3. Esquema general y etapas de la gestión de planificación


El esquema general de las principales etapas de los procesos de planificación, con sus flujos correspondientes, queda reflejado en la figura que presentamos a continuación:

Figura 28



Las etapas funcionales que aparecen en el esquema son las siguientes: 

- 1) Definición del escenario.
- 2) Definición de la estrategia corporativa.
- 3) Caracterización de la carga y análisis de tendencias.
- 4) Análisis del mercado y estudio de alternativas.
- 5) Diseño y configuración del plan de evolución del sistema.
- 6) Implantación piloto y testeo.
- 7) Documentación.
- 8) Realimentación del plan.

A continuación explicaremos algunos de los más relevantes. 

### 8.3.1. Caracterización de la carga y análisis de tendencias

En esta etapa se analizan las características de la carga actual con todos sus detalles y, generalmente, ésta se descompone en segmentos acotados que representan departamentos, áreas o servicios de la organización.

#### Detalles de la carga

Número de usuarios, número de aplicaciones, capacidades y caudales (*throughput*) de los recursos, indicadores de nivel de servicio, estudios de capacidad residual, entre muchos otros.

Las tareas de caracterización de la carga se tendrían que repetir periódicamente (al menos dos o tres veces al año o más si hace falta) y comparar los datos obtenidos con los reflejados en las medidas y planificaciones anteriores. Éste es el mecanismo básico del **análisis de tendencias**, que es más adecuado cuantas más medidas se lleven a cabo.

#### La segmentación de la carga

Es importante que la segmentación procure particiones que se puedan coordinar con los criterios de la dirección, de manera que creen entidades "más homogéneas". La dirección no puede, ni quiere saber, la capacidad de un enlace con una delegación, pero sí que tiene unos objetivos corporativos de servicio (más usuarios, más capacidad de atención a clientes, etc.). La segmentación ayuda, en criterios tan dispares, estratégicos y tecnológicos, a coordinarse.

### 8.3.2. Análisis del mercado y estudio de alternativas

Como es lógico, la evolución de un sistema informático, y en especial la de los fuertemente distribuidos, está totalmente influenciada por el "estado del arte" de la tecnología en aquel momento. En los últimos años la proliferación de soluciones, fabricantes, proveedores, integradores y otros actores es desorbitada.

Las ventajas que comporta esta competencia con vistas al avance y desarrollo tecnológico no tiene comparación. Pero la otra cara de la moneda está en el hecho de que, en pocos años, y a veces en uno escaso, las soluciones tecnológicas con más futuro pueden estar desfasadas o descatalogadas, e incluso sin mantenimiento o soporte. Tenemos decenas de ejemplos, muchos de éstos relacionados con las primeras marcas más importantes y populares.

Los motivos del cambio en la estrategia de un fabricante pueden venir de la mano de una revolución tecnológica (nuevos chips, abaratamiento de costes, normalizaciones, etc.); de una presión de la competencia, que lo obliga a replantear sus

objetivos y medios o, simplemente, por criterios estrictamente comerciales o incluso de moda. En cualquier caso, el impacto en las organizaciones usuarias de esta tecnología puede ser extremadamente grande y costoso.

### La aceleración del desarrollo tecnológico y sus problemas

Existen ejemplos famosos de fabricantes que han discontinuado herramientas de programación relativamente al poco tiempo de su aparición. Este hecho ha pillado desprevenidas a muchas organizaciones con grandes desarrollos, que ya han invertido muchos miles de horas o que justo acaban de entrar en producción, y hace que peligre todo el soporte y mantenimiento.

Los costes, dinerarios, de imagen y de impacto, al tener que invertir años de trabajo, son muy altos y han llevado a más de una compañía a la quiebra.

Los planificadores deberán considerar las ventajas e inconvenientes de tecnologías innovadoras, incluso de los fabricantes más serios, con respecto a otras más probadas y extendidas, y convertir este factor de extensión (conocido como la “base instalada”) muchas veces en el prioritario.

Lo ideal sería el seguimiento continuo de la información técnica de los proveedores y fabricantes, publicaciones especializadas, acontecimientos relevantes de presentación de nuevas soluciones, el análisis de proyectos prototipo y pilotos y, especialmente, cuando se pueda, el hecho de compartir experiencias con otras instalaciones representativas (los denominados “foros de usuarios”\*).

\* Como dice el dicho popular, “no hay que inventar la rueda dos veces”.

### 8.3.3. Diseño y configuración del plan de evolución

Además de lo que ya se ha comentado sobre el diseño y la configuración del plan de evolución en los subapartados anteriores, hay un aspecto que está variando mucho en los últimos años y que impone fuertes exigencias en la elaboración de los planes de evolución: el **horizonte temporal de los plazos**.

#### El tiempo web

El estrés tecnológico de algunas organizaciones actuales, especialmente las relacionadas con Internet, han puesto de moda el extraño concepto de los *tiempos web*, en los que las horas, los días o los años duran mucho menos de lo habitual.

Algunas compañías han conseguido crecer un 1.000% sus primeros tres meses de actividad (?) y continuar con curvas crecientes. Otras han desaparecido a los pocos meses con pérdidas espectaculares.

Con estos incrementos y decrecimientos, ¿quién planifica?

Lo que se consideraba corto, medio o largo plazo a finales de los ochenta, o en compañías con planificaciones a diez, veinte o treinta años, suena una “eternidad de la noche de los tiempos” en organizaciones de hoy en día en las que su “largo plazo” es a sólo cuatro o seis meses.

#### Interpretaciones y horizontes de plazos para tres modelos de organizaciones

La tabla siguiente muestra un ejemplo de las diferentes interpretaciones y horizontes de los plazos para tres modelos de organización. Las organizaciones de la primera columna

han desplazado gradualmente sus objetivos y planificaciones a horizontes próximos a la segunda columna:

	<b>Grandes organizaciones, como operadores de telecomunicaciones (infraestructuras), seguros, banca, Administración Pública, con planificación a largo plazo (visión tradicional de los ochenta)</b>	<b>Organizaciones de cualquier tamaño, con planificación, más o menos precisa, de los objetivos corporativos y de los sistemas de información (visión de los noventa)</b>	<b>Organizaciones relacionadas con determinados servicios Internet "Tiempo web" (¿visión de 2000?)</b>
<b>Largo plazo</b>	20 años	5 años	6 meses-1 año
<b>Medio plazo</b>	5 años	1 año	1-4 semanas
<b>Corto plazo</b>	1 año	3-6 meses	1-3 días

#### 8.3.4. Realimentación del plan

En todos los casos en los que se diseña, ejecuta e implanta un plan de evolución se tiene que prever su realimentación con los parámetros que permiten que se pueda adaptar a las variaciones del escenario, de la carga o de los objetivos a medida que se implanta.

Algunas organizaciones descritas en el subpartado anterior lo necesitan todavía más.

A grandes rasgos, las tareas operativas que permiten adaptar el plan a los nuevos requerimientos y exigencias sin disparar los costes se basan en los factores siguientes:

- 1) Actualización de algunos componentes del sistema distribuido por parte de otros con más prestaciones o adaptación a los requerimientos.
- 2) Extensión y expansión de los sistemas, infraestructuras o servicios existentes, que se colapsan o llegan a los límites de capacidad, y tareas de afinamiento más precisas.
- 3) Cambio de tecnología de base de los sistemas, medios de comunicación. En ocasiones, la actualización del sistema operativo, la implantación de una nueva pila de protocolos o el simple cambio de chips, entre otros, pueden mejorar las prestaciones del sistema distribuido con un coste muy acotado.
- 4) Utilización de aplicaciones más eficientes desde el punto de vista de consumo de recursos, que puede implicar la reprogramación, la búsqueda de operaciones frecuentes poco eficientes, la recompilación o el cambio de alguna otra tecnología.

## 9. Tendencias futuras

Es obvio que los sistemas de información y la inmersión de las telecomunicaciones se han convertido en el sustrato de prácticamente todas las organizaciones actuales. Para muchas de éstas, la dependencia de los sistemas de información es tan grande que no sólo no podrían operar sin éstos, sino que la simple sospecha por parte de su clientela o del público en general de que eso pasara podría tener un impacto muy negativo en su actividad.

Nos hemos acostumbrado a que los sistemas informáticos siempre tienen que funcionar, pero la creciente complejidad y la presión de dependencia hacen que su gestión y administración deban ser las adecuadas. A continuación se describen las tendencias para la explotación y administración de sistemas de información que se están implantando actualmente y las que se esperan en los próximos años.

### 9.1. Nuevos requerimientos a los sistemas informáticos

A medida que se desarrollan las modernas maneras de gestionar una organización, aparecen nuevos escenarios en los requerimientos de los sistemas de información que la soportan. Especialmente con la explosión de Internet, los modelos ya adelantados de empresas perfectamente integradas en el funcionamiento interno, su *backoffice*, muchas de éstas con plataformas corporativas consolidadas, dan paso a una potenciación del “frontal de negocio”, el *frontoffice*. Este paso les permitirá entrar en el nuevo rol del comercio electrónico y las transacciones comerciales ubicuas, en cualquier lugar y en cualquier momento.

El impacto en los sistemas de información y telecomunicación ya es, y será, muy importante. Éstas son algunas de las características y tendencias que marcan estos cambios:

- **Extensión completa a las intranets y extranets:** la extensión del uso de las tecnologías de Internet sobre las LAN y WAN ha implicado una tendencia a utilizar esta tecnología, especialmente los servicios web, como frontal universal de todos los servicios de la organización, y constituye el embrión de una intranet, o extranet si está orientada al exterior. Muchas organizaciones ya han migrado totalmente sus aplicativos a esta tecnología.
- **Creciente importancia de los contratos de nivel de servicio (SLA):** se prevé una creciente demanda de los servicios externalizados cubiertos por

Soporte para intranets/extranets.

Proliferación SLA.

un SLA, tanto en número como en responsabilidades de las funciones. Algunas funciones de administración también serán externalizadas.

- **Criticidad de servicios considerados de baja prioridad:** algunos servicios considerados hasta ahora de baja prioridad, como el correo electrónico, pasarán a convertirse en elementos esenciales de producción, sobre todo por la interacción con otros servicios de negocio.
- **Incremento de los servicios sensibles a la seguridad:** se incrementarán los servicios más sensibles a los criterios de seguridad desde el punto de vista tanto de la confidencialidad como de los que aseguren su adecuada disponibilidad e integridad. El comercio electrónico, el banco en casa o los pedidos de aprovisionamientos telemáticos son algunos ejemplos de ello.
- **Tendencia a la globalización:** en realidad la era de la globalización de la información ya ha llegado. El hecho de no poder calcular cuántos accederán a nuestros servicios *a priori* (web) obligará a una planificación y seguimiento detallados de los elementos involucrados, especialmente si forman parte de la cadena de producción.
- **Frecuentes cambios en las configuraciones y topologías:** habrá una tendencia cada vez más destacada a reubicar equipos de personal, delegaciones o trabajo en casa del cliente, entre otros. Los frecuentes cambios de configuraciones pueden complicar la gestión del sistema y ya se está evaluando, por ejemplo, la implantación de infraestructuras “virtuales” basadas en estructuras malladas reales.
- **Crecimiento de los servicios móviles y ubicuos:** el comportamiento de los usuarios ha variado los últimos años, en los que muchos de ellos ya están dotados de sus correspondientes ordenadores portátiles para el trabajo cotidiano. Pero el avance en las tecnologías de comunicación móviles (WAP, móviles de banda ancha, etc.) puede hacer aparecer un nuevo tipo de usuario, el “usuario ubicuo”, que ni siquiera dispone de un espacio en la oficina, pero tiene los mismos requerimientos funcionales o más que los “tradicionales”. En cualquier caso, se tendrán que diseñar procedimientos específicos de gestión y administración.
- **Sistemas de procesamiento y almacenamiento en red:** el avance en el ancho de banda, la fiabilidad de las comunicaciones LAN y MAN y el impulso de los sistemas abiertos, que conectan todo con todo, han hecho que se empiecen a implantar soluciones de procesamiento y gran almacenamiento distribuido, basados en comunicaciones de red, y han relegado a la obsolescencia los *clusters* tradicionales o las grandes unidades de almacenamiento específicas de cada sistema.

Más servicios críticos.

Criticidad con la seguridad.

Factores de globalización.

Frecuente movilidad y cambio.

Incremento de los servicios móviles.

Arquitecturas de *network clustering*.

- **Creciente complejidad de los servicios MAN y WAN:** los servicios de comunicación con ventanas de QoS empiezan a ser habituales en los sistemas distribuidos, para soportar aplicaciones de voz, videoconferencia, imagen vídeo HQ o servicios de sincronización para sistemas en tiempo real. Se espera un incremento cada vez mayor de este tipo de servicios, que requieren una gestión muy adecuada y ajustada.
- **Simplificación de los equipos terminales:** ya se está impulsando un retorno a la concentración de complejidad, y disminuye especialmente la de los nodos terminales, a cambio de aumentar la complejidad de la red. Las arquitecturas de terminales gráficos de red, Network Computers y otros similares, intentan quitar de encima de los administradores la multitud de problemas de sitios pesados, como los PC, tanto en términos de coste como con la eficiencia de su administración.

Servicios de alta QoS en MAN/WAN.

Arquitecturas *Thin-Client*.

## 9.2. Nuevas soluciones para la gestión de sistemas y telecomunicaciones

Si hay cambios en las características y objetivos de los nuevos sistemas distribuidos, vendrán lógicamente acompañados de cambios en las estrategias, metodologías y herramientas de gestión y administración.

Los cambios que exponemos a continuación son algunos de éstos:

- **Más automatización de la gestión y administración:** se está trabajando en la línea de dotar de más automatismo el control y la realización de determinadas tareas de gestión, de manera que éstas sólo sean coordinadas y supervisadas por los administradores.
- **Crecimiento de la capacidad de los agentes:** la potencia y complejidad de proceso de los agentes aumentarán considerablemente, gracias a los costes reducidos de los sistemas microprocesados incrustados, y permitirán hacer muchas más funciones *in situ* en el mismo objeto gestionado.
- **Crecimiento de la gestión de servicios finales:** la gestión de los servicios está adquiriendo un notable avance sobre la misma gestión de los recursos y elementos físicos. Muchos de éstos aumentan la funcionalidad “en cliente”, totalmente en tiempo de ejecución, y aparecen nuevos parámetros de gestión orientados al cliente.
- **Crecimiento de las herramientas y soluciones de gestión de aplicaciones:** la gestión orientada a aplicaciones, tanto la incrustada como la que se hace mediante herramientas externas, se está introduciendo en los entornos medianos y grandes. La principal razón para ello es la eficacia del con-

Más automatización.

Agentes más potentes.

Servicios *end to end*.

Gestión de aplicaciones.

trol y la información proporcionada con indicadores orientados a la utilización y a la eficiencia, por ejemplo en sistemas basados en pesados motores de base de datos transaccionales.

- **Utilización de la gestión basada en web:** ha aparecido ya una serie de productos de consola de gestión basados en interfaz web, con todas las facilidades que ofrece este frontal. Sin embargo, la mayor utilidad viene dada por recursos pesados, como servidores o grandes conmutadores, que implementan de forma nativa el acceso a los agentes y a la gestión particular simplemente accediendo a un puerto de éstos, sin tener que utilizar otro *software* más que un navegador. Para pequeñas instalaciones o elementos aislados puede ser una técnica útil de la gestión remota.
- **Gestión y administración de los flujos de trabajo (*workflow*):** están en desarrollo una serie de soluciones que tratarán de completar las herramientas de gestión tecnológica (elementos, redes, servicios, etc.) con herramientas de gestión de la corporación coordinándose con los flujos de trabajo de la organización (cliente-servicio, proveedor-servicio, usuario-servicio interno, etc.).
- **Plataformas de integración corporativa de la gestión (*frameworks*):** se espera que la integración de las herramientas de gestión gane en profundidad y eficacia. La falta de integración puede ser un problema que se agrave con el aumento de complejidad de los sistemas distribuidos y la aparición de nuevas arquitecturas y soluciones de gestión. La tendencia más favorable parece que son los productos basados en plataformas estructurales o *frameworks*, que proporcionan los servicios básicos de gestión y de comunicación entre módulos y permiten añadir componentes (*cartridges*) específicos de los productos o elementos que hay que gestionar.

Gestión mediante web.

Integración del *workflow* corporativo.

*Frameworks* corporativos.

## Resumen

En este módulo didáctico se han desarrollado las características básicas que definen los sistemas informáticos actuales, siempre basados en redes de comunicación, especialmente desde el punto de vista de las tareas y problemáticas que se desprenden de su mantenimiento en producción y explotación.

La aplicación de los métodos analíticos y procedimientos de medida, estudiados en la primera parte de evaluación, sobre los sistemas distribuidos reales implantados en las organizaciones actuales, permiten establecer cuáles son los criterios que hay que tener en cuenta a la hora de diseñar, implantar, desarrollar y operar los entornos en la enorme variedad de escenarios que podemos encontrar.

Un repaso a los principales factores que determinan las características de los diferentes escenarios ha permitido la introducción de los conceptos referentes al **nivel de servicio** deseado en una instalación, su medida y las tareas involucradas en su mantenimiento.

La visión operacional de las funciones que se desarrollan en cualquier entorno en producción se han analizado a partir del **modelo funcional OSI** para la gestión de sistemas informáticos, que representa un adecuado modelo de plataforma metodológica para englobar y relacionar las tareas ordinarias y extraordinarias de un departamento de sistemas de información y comunicaciones.

El modelo de gestión nos ha proporcionado un desglose de las tareas relacionadas con la gestión de la configuración de los sistemas, la gestión de fallos, el control de la seguridad informática, el análisis y gestión de las prestaciones del entorno en producción, las contabilizaciones y medidas asociadas y un marco de las consideraciones en la planificación y adecuación evolutiva del mismo entorno.

Finalmente, se ha considerado necesaria la inclusión de algunas referencias y grandes rasgos asociados a la gestión y explotación de los sistemas informáticos actuales y futuros, en los que predominan unas dinámicas muy aceleradas de cambios y crecimientos, además de la inclusión de nuevas tecnologías y maneras, que a menudo son muy innovadoras y, por lo tanto, poco probadas y analizadas en las problemáticas de producción. La extensión de Internet, la popularización de los servicios en línea o la globalización, que impone fuertes criterios de disponibilidad  $7 \times 24$ , son algunos ejemplos de ello.

## Bibliografía

**Ghetie, I.G.** (1997). *Networks and Systems Management*. Boston/Londres: Kluwer Academic Publishers.

**Gunther, N.J.** (1998). *The Practical Performance Analyst: Performance-by-design for Distributed Systems*. McGraw-Hill (Series on Computer Communications).

**Hegering, H.G.** (1999). *Integrated Management of Networked Systems*. San Francisco: Morgan Kaufmann.

**Higginbottom, G.** (1998). *Performance Evaluation of Communication Networks*. Boston: Artech House.

**Leinwald, A.** (1994). *Network Management, a Practical Perspective*. Addison-Wesley.

**Shuey, R.L.** (1997). *Architecture of Distributed Computer Systems*. Massachusetts: Addison-Wesley.

**Sloman, M.** (1996). *Network and Distributed Systems Management*. Wokingham: Addison-Wesley.

**Stang, D.J.** (1993). *Network Security Secrets*. San Mateo: IDG Books Worldwide.

**Stallings, W.** (1993). *SNMP, SNMPv2 and CMIP, a Practical Guide to Network Management Standards*. Addison-Wesley.

**Storey, N.** (1996). *Safety-critical Computer Systems*. Massachusetts: Addison-Wesley.

**Terplan, K.** (1992). *Communication Networks Management*. Prentice Hall.

