



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

Índice Tema 6

Introducción.

1. Concepto de organización.
2. Tipos de organización.
 - 2.1. Estructura.
 - 2.2. Diseño.
 - 2.3. Sistema de funcionamiento.
3. Organización de un centro de sistemas y tecnologías de la información.
4. Dirección de proyectos.
5. Desarrollo y mantenimiento.
6. Seguridad.
7. Logística.
8. Sistemas y bases de datos.
9. Comunicaciones.
10. Centro de atención a usuarios.
 - 10.1. Ciclo de una incidencia.
 - 10.2. Estructura a tres niveles.
 - 10.3. Relaciones con los centros de la periferia.
11. Vulnerabilidades y riesgos.
 - 11.1. Concepto de vulnerabilidad.
 - 11.2. Riesgos potenciales.
12. Instalaciones.
 - 12.1. Localización del centro de proceso de datos. Aspectos a considerar.

- 12.2. Seguridad contra incendios.
- 12.3. Seguridad de las conducciones.
- 12.4. Control de accesos.
- 12.5. Sensores y alarmas.
- 12.6. Sistemas de cableado.
 - 12.6.1. Cableado estructurado.
- 13. Dimensionamiento del equipamiento físico. Planificación de la capacidad.
 - 13.1. Definición.
 - 13.2. Necesidad de la planificación.
- 14. Factores a considerar.
 - 14.1. Características de la carga de trabajo.
 - 14.2. Utilización de los recursos.
 - 14.3. Evaluación del comportamiento de un sistema.
- 15. Actividades a realizar.
- 16. Metodologías de planificación de la capacidad.
 - 16.1. Reglas basadas en la experiencia.
 - 16.2. Proyección lineal.
 - 16.3. Teoría de colas.
 - 16.4. Simulación.
 - 16.5. Bench-mark.



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

TEMA 6

Estructura y organización de un departamento de sistemas de información. Planificación física de un centro de tratamiento de la información. Vulnerabilidades, riesgo y protección. Instalaciones. Dimensionamiento de equipos. Factores a considerar.

INTRODUCCIÓN.

La primera pregunta que nos debemos hacer es ¿qué es un Centro de Sistemas y Tecnologías de la Información? Podríamos definirlo como el proveedor de servicios basados en tecnologías de la información y de las propias tecnologías dentro de una organización para ayudar a ésta a conseguir sus objetivos de negocio. Los servicios y tecnologías ofrecidos deberán adecuarse a unos niveles de calidad y servicio.

Obsérvese que, de acuerdo con esta definición, la organización de un centro de sistemas y tecnologías de la información no es única, no existe una organización tipo y la nuestra será mejor o peor según nos desviemos más o menos del patrón. La organización del departamento de Tecnologías de la Información deberá ser la más adecuada para conseguir los objetivos marcados en su definición.

La Administración Pública tiene un objetivo principal asignado: servicio a los ciudadanos. En este sentido cada Organismo actúa dentro de su ámbito de competencia, por ejemplo: la Guardia Civil tiene encomendada la seguridad ciudadana, Fomento tiene las obras públicas y civiles, etc. La Organización del Centro TIC deberá ser la idónea (funciones, responsabilidades, capacidad de decisión, etc.) para proveer de servicios de calidad al organismo sin ningún tipo de prerrequisito aparte de los marcados por el régimen jurídico al que se somete la Administración.

A lo largo de este tema se definirán los aspectos más relevantes de una organización y diferentes diseños de organizaciones.

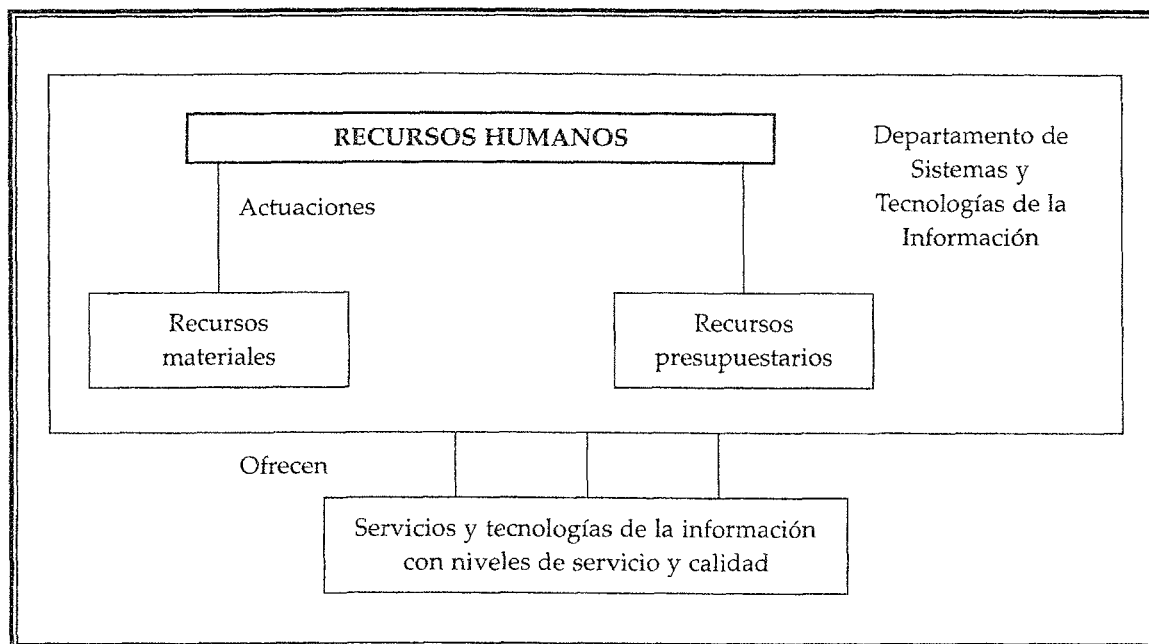
Otro de los aspectos a valorar es la planificación de un centro TIC: tipos de instalaciones, localización, dimensionamiento de equipos, etc.

Se verán algunos métodos de planificación y aspectos a considerar.



1. CONCEPTO DE ORGANIZACIÓN.

Una organización de cualquier tipo se compone de recursos humanos, materiales y presupuestarios. Todos estos recursos están estructurados de una determinada manera. En términos generales podríamos decir que existe una interactuación de los recursos humanos sobre los materiales y presupuestarios con el fin de obtener unos niveles de servicio con unos criterios de calidad. El Centro de Sistemas y Tecnologías de la Información es un caso particular de cualquier organización.



La organización de un conjunto de recursos (humanos, materiales, intelectuales, etc.) supone lo siguiente:

- Establecer una división del trabajo determinando:
 - Los diferentes tipos de trabajo.
 - Las actividades y tareas a desarrollar.
 - La definición de puestos.
- Agrupar los puestos homogéneos en departamentos.
- Establecer la delegación de autoridad mediante la fijación de la cadena jerárquica y la esfera de control; así como la centralización y descentralización de tareas.
- Establecimiento de la línea (las unidades productivas o de gestión directa) y el staff (las unidades de apoyo a las unidades de línea).
- Establecimiento de un plan de inversiones, gastos corrientes y control presupuestario.

2. TIPOS DE ORGANIZACIÓN.

Los tipos de organización vienen determinados por las tres siguientes variables: estructura, diseño y tipo de funcionamiento.

2.1. ESTRUCTURA.

Las estructuras más extendidas en la mayoría de las organizaciones son las siguientes:

• Estructura funcional.

La separación del trabajo se hace de acuerdo a las funciones que se tengan asignadas dentro de la organización.

La estructura funcional tiene como exigencias:

- Una coordinación muy profunda entre las diferentes unidades de la organización.
- La necesidad de documentar todo con precisión.
- La necesidad de la máxima formalización.

La no existencia de una adecuada coordinación puede ocasionar el mal funcionamiento de toda la organización.

Ventajas:

- Se aprovechan mucho mejor los recursos humanos al no estar adjudicados a un único proyecto.
- Se conoce mejor la organización desde arriba, ya que al trabajar en cadena el fallo en cualquiera de las unidades (análisis, programación, sistemas, explotación) se detecta inmediatamente porque las restantes unidades se ven afectadas.
- Se evita el riesgo de la dependencia excesiva de unos pocos expertos, ya que todo el mundo va trabajando en todas las aplicaciones de la organización.

Inconvenientes:

- Se requiere una muy buena coordinación, porque todos los departamentos deben trabajar al unísono al no haber independencia entre ellos.
- Hay una cierta falta de especialización. Como los empleados deben trabajar en diferentes aplicaciones no llegan a profundizar en ninguna de ellas.

• Estructura sectorial.

La estructura sectorial tiene como exigencia fundamental el que estén diferenciadas perfectamente las distintas actividades o líneas de negocio básicas de la organización, evitando el que los diferentes grupos tengan interferencias entre sí.

Ventajas:

- Alta especialización del personal al trabajar siempre en la misma aplicación.
- Autonomía de funcionamiento de cada departamento al ser independiente su trabajo del trabajo del resto de los departamentos. Si el departamento de nómina tiene sus técnicos de sistemas, sus analistas, sus programadores, sus operadores, etc., no depende de ninguna otra unidad para poder trabajar.
- No se necesita una coordinación excesiva a alto nivel ya que cada departamento, es independiente.

Inconvenientes:

- Riesgo de contar con pocos especialistas que conozcan una determinada aplicación. A veces una aplicación es llevada sólo por un analista y un programador; y una eventual decisión suya de abandonar la organización puede provocar graves problemas.
- Desaprovechamiento del personal. Cuando hay poco trabajo en un departamento, su personal no es aprovechado por otro departamento que estuviese desbordado de trabajo.

• Estructura mixta.

En la estructura mixta se pretende coger lo mejor de las estructuras funcional y sectorial y evitar lo peor de ambas. Esta estructura también se llama proyecto-funcional o matricial.

En una estructura mixta habrá por ejemplo:

Un jefe de recursos del análisis, programación, sistemas, producción y varios jefes de proyecto. El jefe de recursos asignará personal de diferente especialización, de forma temporal, a cada uno de los proyectos. Cuando el proyecto finaliza, el personal se vuelve a integrar, dentro de su departamento, a las órdenes del jefe de recursos.

Existen además otros tipos en los que se entremezclan las estructuras anteriores con factores como el geográfico y el SBU (estructura orientada a negocios).

2.2. DISEÑO.

Los tipos de diseño más extendidos son los siguientes:

• Apuntado.

En el modelo apuntado hay un número elevado de niveles en la pirámide jerárquica. Es el caso de la Administración en el que desde el presidente del gobierno al jefe de grupo hay 14 niveles.

En este tipo de modelo se producen grandes rigideces a la hora de la circulación de la información.

• Plano.

En el modelo plano existen pocos niveles en la pirámide jerárquica lo que hace que las organizaciones con este tipo de estructura sean mucho más flexibles y operativas que las anteriores.

En la moderna teoría de la organización se propugna por la disminución de niveles, lo cual es muy difícil de conseguir en las organizaciones antiguas con estructuras apuntadas, ya que en la mayoría de ellas las retribuciones son función del nivel jerárquico.

- **Basado en la línea.**

Suelen ser organizaciones jóvenes y pequeñas que tienen que dedicar todos sus recursos a la producción. En ellas o el staff no existe o es muy pequeño.

- **Con orientación a staff.**

Las organizaciones antiguas y grandes suelen tener una tendencia a la creación de unidades de staff, justificándolas en la absoluta necesidad de estudiar una serie de cuestiones que las unidades de línea, por su propia naturaleza, no podrían hacer por tener que dedicar todo su tiempo a la producción. En las organizaciones aristocráticas, burocratizadas y decadentes las unidades de staff llegan a crecer desmesuradamente, llegando a superar incluso a las de línea.

Hay que señalar, no obstante, que las unidades de staff, limitadas y eficientes, pueden ser de una enorme ayuda para la organización.

Tradicionalmente se ha dicho que en un centro de tecnologías de la información debe haber una unidad staff dedicada al estudio de nuevos productos software y hardware y de nuevos servicios ya que las unidades de análisis y programación; y las de sistemas y producción, al estar, en general, desbordadas de trabajo, no pueden dedicar tiempo a estudiar aquellos aspectos que interesan al centro. Sin embargo, esto no es del todo cierto, ya que aunque es cierto que hay que estar al corriente de la evolución del mercado de Tecnologías de la Información (una de las funciones de los directivos de Tecnologías de la Información) si no se tienen en cuenta cuestiones como: estudio de oportunidad de introducción de nuevas tecnologías, mejora en los niveles de servicio y calidad, mejora en la eficiencia y productividad tanto por los TIC como por los departamentos que utilizan TIC, implicación del resto de la organización y gestión del cambio; esta unidad puede quedarse reducida a una simple unidad generadora de informes sin ningún valor añadido.

2.3. SISTEMA DE FUNCIONAMIENTO.

Desde el punto de vista del funcionamiento se pueden destacar las siguientes posibilidades:

- **Jerárquico.**

Las comunicaciones siguen siempre las líneas jerárquicas que marcan la estructura piramidal de la organización. La mayoría de las comunicaciones, por no decir todas, se producen de jefe a subordinados y de subordinados a jefes. Las comunicaciones colaterales están muy restringidas.

- **Reticular.**

Son mucho más flexibles y eficientes, ya que las comunicaciones entre las unidades y empleados de la organización no tienen por qué seguir exclusivamente las líneas de mando jerárquicas. Las comunicaciones son de todos con todos, sobre todo por niveles. Esto hace que muchos problemas se resuelvan a nivel horizontal sin que tengan que intervenir las líneas de mando convencionales, las que

entrarán sólo en funcionamiento cuando las comunicaciones reticulares de nivel horizontal no puedan dar resueltas las cuestiones que se planteen entre las diversas unidades de dos líneas jerárquicas diferentes.

- **Formal.**

En las organizaciones formales las comunicaciones suelen estar muy formalizadas y documentadas de acuerdo a normas estrictas. Lo que no se comunique por las vías formales establecidas no existe.

Las reuniones también tienen una preparación muy formal y muy reglada con convocatorias anticipadas, órdenes del día, entregas de documentación para la discusión y el debate.

- **Informal.**

Hay organizaciones más informales, sobre todo las jóvenes y pequeñas, que suelen prescindir casi totalmente de los formalismos. Esto tiene la ventaja de la agilidad y flexibilidad de funcionamiento, pero también graves inconvenientes cuando las organizaciones empiezan a tener un tamaño considerable.

- **Centralizado.**

- **Descentralizado.**

3. ORGANIZACIÓN DE UN CENTRO DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN.

Cada departamento de Sistemas de la Información presenta unas características distintas dado que son distintas sus historias, sus tamaños y la naturaleza concreta de los requerimientos de sus usuarios. Por ello no puede ni debe darse una descripción de un departamento de Sistemas de Información ideal sino proporcionar los elementos que puedan permitir definir su organización y su estructura en cualquier caso. Generalmente, la estructura de un departamento TIC será una situación mixta de las estructuras vistas anteriormente.

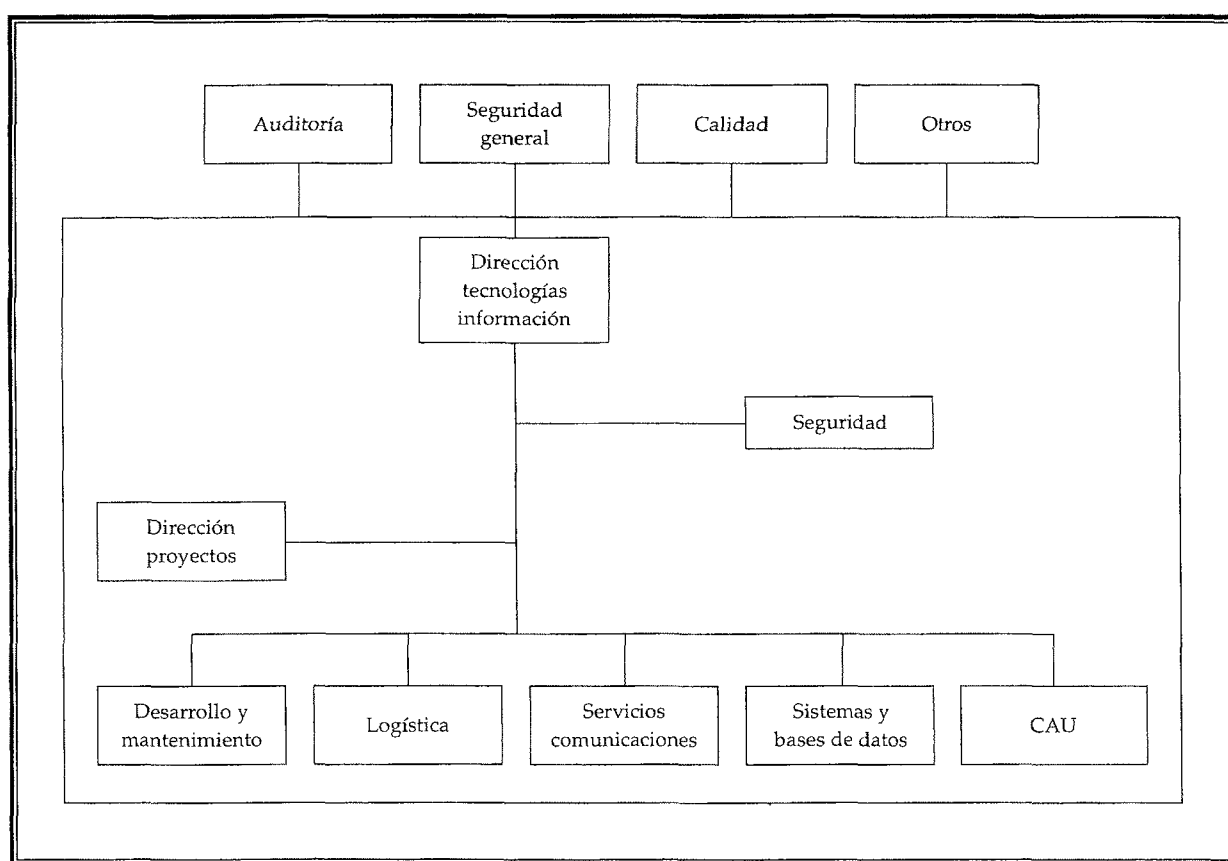
Si analizamos el problema desde una perspectiva diacrónica, esto es, analizando la evolución en el tiempo, vemos que la organización y sus funciones han cambiando sustancialmente a lo largo del tiempo en un proceso influenciado tanto por la evolución de las tecnologías que han debido controlar y utilizar, como por las propias necesidades del mercado que han generado profundas reorganizaciones del modelo empresarial y por tanto de su estructura.

La experiencia de las grandes organizaciones recopilada por organizaciones consultoras como Gartner Group ha puesto de manifiesto la conveniencia de organizar los departamentos de Sistemas de Información por función y no por tecnología. El argumento básico parte de las características de la formación necesaria y de la conveniencia de proporcionar un servicio integrado. La idea que subyace es que un buen analista lo es tanto en un entorno como en otros sobre todo en la época de las herramientas multiplataforma y que, por ejemplo, en la gestión de la Red no es conveniente aislar el soporte de las redes de área local de las extendidas pues cada vez más el tráfico atraviesa varias veces de ellas. Esta circunstancia, unida a la necesidad de realizar tareas de planificación más intensas, generó el modelo que hemos expuesto. Pero además a los condicionantes técnicos se superpuso un nuevo modelo de mercado.

Durante los 90 se ha consolidado un modelo empresarial que fue anunciado por Peter Drucker caracterizado por un proceso denominado «flattening». En resumen, se traduce en un aplanamiento de las organizaciones debido por una parte a la necesidad de tener un tiempo de respuesta más rápido para tomar las decisiones adecuadas que requiere el mercado y, por otra parte, en aprovechar la potencia de los Sistemas de Información para elaborar información de dirección y para transmitir instrucciones. Con ello es posible sustituir 2/3 de los niveles situados en las líneas intermedias.

Por otra parte se ha visto conveniente distribuir las decisiones por la organización dando autonomía a las unidades de negocio (Business Units) que disponen de presupuesto independiente y autonomía para perseguir sus objetivos dentro de los estándares señalados por la organización.

Teniendo en cuenta, otra vez, los condicionantes anteriores, podríamos definir, desde un punto de vista conceptual especificando las entidades generales, una estructura de un Departamento de Sistemas y Tecnologías de la Información de la siguiente forma:



A partir de ahora definiremos y desglosaremos cada uno de los componentes de un Centro TIC. Mencionar, ahora, que todo Centro TIC tiene interrelaciones con el mundo exterior tales como:

- Auditoría, que no es parte del Centro TIC, pero que definirá los diferentes controles a los que se debe ajustar.
- Calidad: el Centro TIC deberá ajustarse al Plan de Calidad de la Organización a la que pertenece.

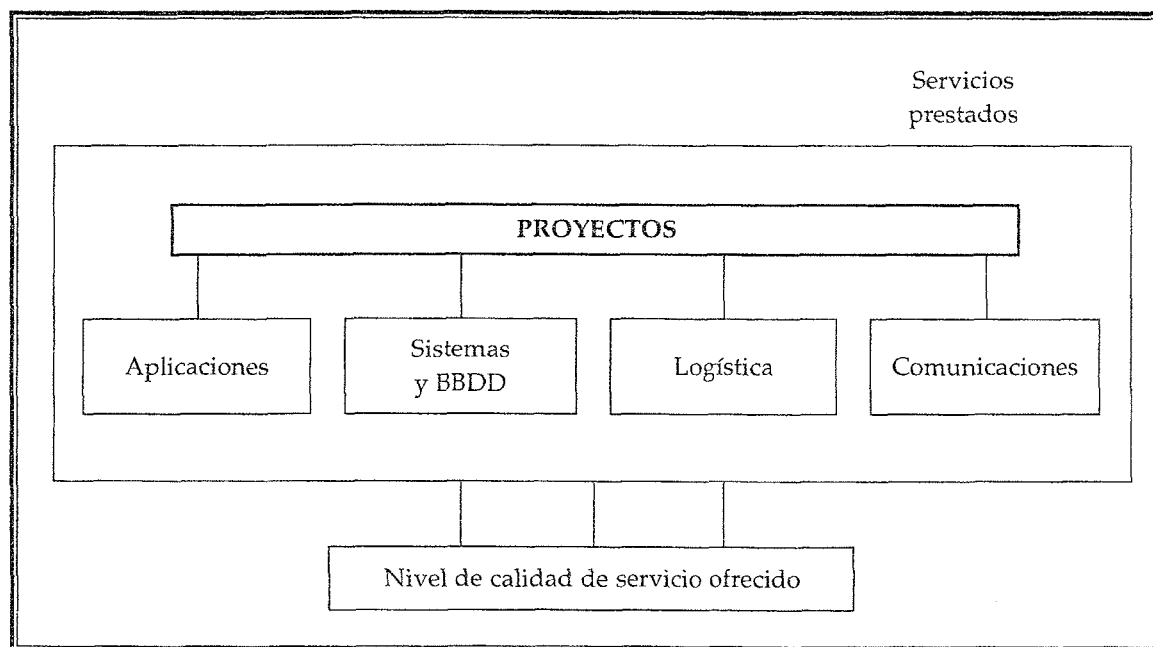
- Seguridad: aunque hay un área de seguridad, ésta deberá estar relacionada con todo lo que se especifique en el Plan General de Seguridad de la Organización.
- Otros: aquí entrarían empresas o proveedoras de servicios externas; departamentos de Contratación, Recursos Humanos, Legislación a cumplir, etc. En el ámbito de la Administración General del Estado no podemos olvidar la relación que debe existir con otras organizaciones que de acuerdo a la competencia delegada por nuestro marco jurídico sus decisiones pueden tener influencia en las actuaciones del Centro TIC (en este ámbito ningún Organismo es independiente o está aislado).
- Todas las áreas del centro TIC deberán ofrecer unos niveles adecuados de servicio.

4. DIRECCIÓN DE PROYECTOS.

En el esquema anteriormente definido, no se debe confundir Desarrollo o ingeniería del software con el desarrollo de nuevos proyectos, ya que un proyecto engloba más aspectos aparte del mencionado (puede englobar comunicaciones, bases de datos, seguridad, planificación, control presupuestario, control de calidad, gestión, etc.). En términos generales el trabajo de Desarrollo y Mantenimiento será un componente más de un proyecto.

En este caso, la relación que existe entre dirección de proyectos y el resto es el de una organización proyecto-funcional o mixta.

El esquema podría ser el siguiente:



Ciertos servicios prestados pueden asociarse o descomponerse en proyectos que, desde un punto de vista general, sus componentes serán aplicaciones, sistemas y bases de datos y comunicaciones, y necesitarán de toda una infraestructura logística para su correcto funcionamiento.

Los proyectos se deben realizar en un plazo finito y determinado.

En la dirección de proyectos también habrá que tener en cuenta:

- Será el máximo responsable de las relaciones con los usuarios dentro de su proyecto.
- Estimación de costes.
- Descomposición del proyecto en diferentes tareas.
- Planificación de las distintas tareas.
- Control de ejecución de las tareas.
- Asignación de responsables para cada tarea.
- Asignación y gestión de recursos para cada tarea.
- Corrección de desviaciones.
- Control presupuestario.
- Establecimiento de un plan de calidad del proyecto y controles de calidad.
- Ejecución de Auditorías.
- Diseño de los planes de formación tanto para los componentes del proyecto como para los usuarios.
- Estudio de las tendencias tecnológicas y productos del mercado.
- Deberá coordinarse con los demás directores de proyectos en establecimiento de normas y metodologías a seguir en los proyectos.

El perfil del director del proyecto debería ser:

- Fuertes conocimientos de sistemas y tecnologías de la Información: arquitecturas, tecnologías, etc.
- Alta capacidad de negociación. Expresiones tales: «esto no se puede hacer», deben ser destruidas.
- Fuertes conocimientos del mercado de Tecnologías de la Información.
- Alta capacidad de gestión de recursos humanos y presupuestarios.

En el ámbito de la Administración Pública deberá conocer el Marco Jurídico correspondiente (Ley de Contratos del Estado, Ley de Función Pública, etc.)

Hay organizaciones que recaen la dirección de proyectos en los usuarios demandantes del servicio. Es obvio que en todo proyecto la implicación del usuario es fundamental, pero la dirección técnica

ca es responsabilidad del Centro TIC, siendo responsabilidad de los usuarios una correcta especificación funcional de tal forma que la solución propuesta resuelva su problemática. Cada uno debe actuar en su parcela.

Los proyectos también pueden ser internos, para el centro TIC. Éstos deberán seguir las mismas reglas y pautas que los proyectos para usuarios

5. DESARROLLO Y MANTENIMIENTO.

En el área de desarrollo y mantenimiento se tiene como función fundamental el desarrollo de aplicaciones y mantenimiento de las mismas a través de las funciones de análisis y programación.

La organización dentro de esta área de desarrollo es una de las que mayor número de combinaciones de tipos de organización admite: sectorial, funcional, mixta, etc. La tendencia es que esté orientada a proyecto-funcional, ya que cada vez más, se realizan proyectos que utilizan no una, sino varias tecnologías. Cada vez que se quiera lanzar un proyecto se buscará personal que reúna distintos perfiles (decisión del director del proyecto que pertenece a Dirección de Proyectos), se integrarán y formarán parte de un equipo de proyecto que lleve a cabo el desarrollo del nuevo sistema; una vez terminado el proyecto, estas personas quedarán disponibles para formar parte de otros proyectos. Para subir a producción el nuevo sistema (decisión que adoptará el director del proyecto correspondiente de acuerdo con los demás implicados), se seguirán unas normas de promoción de versiones comunes para todos los proyectos.

La ventaja de esta estructura es que facilitará la integración de personal externo en cualquier proyecto, especialmente procedente de proveedores o empresas externas; y que cualquier sistema que se quiera incorporar, será un proyecto más. No se debe perder la vocación que existe actualmente hacia los entornos o lenguajes, pero esta orientación debe ser más vertical. Además habrá que tener en cuenta la orientación funcional de los proyectos.

En términos generales podríamos decir que se deberán tener conocimientos de:

- Arquitecturas y plataformas tecnológicas; J2EE; Microsoft .NET; CORBA; ERP; E-learning; sistemas multimedia; gestores de contenidos; gestores de expedientes; Sistemas Web, Cliente / Servidor, etc.
- Metodologías de desarrollo: metodologías de análisis y diseño estructurado; orientación a objetos: Métrica, UML, Eurométodo. Reingeniería de procesos.
- Técnicas de prototipado rápido.
- Herramientas CASE: orientadas al diseño estructurado o a orientación a objetos: Rational/Rose, Certificados digitales y sistemas de firma electrónica en lo que afecte a sus aplicaciones.
- Lenguajes de programación.

También deberán conocer los entornos de sistemas, bases de datos y comunicaciones en la medida que puedan tener influencia en sus aplicaciones.

Las principales tareas de esta área son:

- Análisis.
 - Estudio del sistema de información preexistente.
 - Diagnóstico del sistema preexistente.
 - Diseño racional y normalizado del nuevo sistema de información.
 - Determinación del modelo conceptual de datos.
 - Determinación del modelo lógico de datos, lo cual implica definir para cada tabla de datos los atributos o campos de la tabla.
 - Determinación de las cadenas de proceso.
 - Determinación de procesos.
 - Descripción generalizada de cada proceso.
 - Descripción funcional del sistema de confidencialidad.
- Diseño y construcción.
 - Diseño físico del modelo de datos.
 - Descripción de cada proceso.
 - Diseño de menús.
 - Diseño de pantallas.
 - Diseño de informes de salida.
 - Organigrama de detalle de cada proceso en el que figuren las unidades de tratamiento.
 - Determinación de las unidades elementales de tratamiento.
 - Esquema de detalle de cada unidad de tratamiento (programa).
 - Descripción procedural de cada unidad de tratamiento (programa).
 - Determinación de juegos de ensayo.
 - Determinación del sistema de cargas iniciales de datos.
- Mantenimiento: está encargado del mantenimiento de los sistemas de desarrollo a los siguientes niveles:
 - Correctivo, mantenimiento debido a errores en el sistema.
 - Perfectivo, mantenimiento debido a la detección de algún tipo de mejora o nueva funcionalidad.
 - Adaptativo, mantenimiento debido a la obsolescencia o necesidad de unificación de sistemas.

6. SEGURIDAD.

Tradicionalmente este campo ha estado entroncado dentro del área de sistemas, como una parcela más de su trabajo. Sin embargo, dada la importancia y complejidad que ha adquirido, así como su influencia, no sólo en los diferentes proyectos, sino en desarrollo y también en buenas prácticas por parte de los usuarios, esta área ha adquirido una entidad propia que origina que no esté imbricado en ninguna de las áreas tradicionalmente consideradas.

El área de Seguridad no puede actuar de forma independiente de las políticas generales de seguridad definidas en el ámbito de la organización global a la que pertenece (empresa, ministerio, organismo, etc.). Será la encargada de ejecutar estas políticas así como de la puesta en marcha de sistemas, procedimientos o proyectos que tendrán incidencia en todas las parcelas y proyectos TIC.

Las funciones más importantes del área de seguridad son: definición de proyectos de seguridad; análisis y gestión de riesgos; definición de procedimientos de seguridad; ejecución de lo dispuesto por la normativa vigente al respecto; identificación de incidentes de seguridad; documentación y formación tanto interna como a usuarios.

En este campo de la formación también deberán encargarse de la formación a los usuarios de sistemas TIC en el ámbito de la seguridad: buenas prácticas, etc.

Las tareas en esta área son:

- Análisis y gestión de riesgos:
 - Identificar amenazas que acechan al sistema de información (activos).
 - Determinar vulnerabilidad del sistema ante esas amenazas.
 - Estimar el impacto o grado de perjuicio de una inseguridad permanente.
 - Obtener información cuantitativa del riesgo que se corre.
 - Basada en el resultado obtenido en el análisis de riesgos.
 - Permite seleccionar e implantar salvaguardas de seguridad.
 - Conocer, prevenir, impedir, reducir o controlar riesgos identificados.
 - Reducir al mínimo su potencialidad o sus posibles perjuicios.
- Definición de procedimientos de seguridad:
 - Identificación y autenticación de la persona que accede a la información. Se necesitarán adecuados controles de acceso.
 - Integridad de la información.
 - Confidencialidad.

- Disponibilidad.
 - No repudio.
 - Adecuada identificación de ficheros y tratamientos de datos personales y su inclusión en la base de la Agencia de Protección de Datos.
 - Todo aquello que la normativa vigente respecto a seguridad esté establecido.
- Definición de proyectos de seguridad:
 - Los servicios de conexión única (Single Sign-On) deben convertirse en un componente muy importante de los estándares de seguridad de la organización, ayudando a extender la aplicación de los certificados digitales y la identificación segura.
 - La Infraestructura de Clave Pública (PKI) debe ser la tecnología efectiva para alcanzar los estándares necesarios de firma electrónica y garantizar la confidencialidad, autenticidad, integridad y no repudio de la información almacenada y transmitida vía Internet/Intranet.
 - Los Servicios de Directorio son almacenes de información acerca de entidades de red, como aplicaciones, archivos, impresoras y usuarios, que proporcionan una manera consistente de nombrar, describir, localizar, acceder, administrar y asegurar información acerca de esos recursos.
 - Securitización de Clientes: es fundamental definir las políticas que permitan blindar todo tipo de equipos y terminales de los usuarios de la organización global; como manera de proteger los sistemas frente a los ataques externos, e internamente evitar que los usuarios puedan acceder a servicios a los que no tienen acceso.
 - Identificación de incidentes de seguridad: será importante mantener auditorías y registros de accesos, y operaciones realizadas en nuestros sistemas de información, así como monitorización y registro de anomalías en el funcionamiento de los mismos.

7. LOGÍSTICA.

Esta otra parcela de trabajo que tradicionalmente ha sido propia del área de sistemas. Pero con la aparición de los PCs, la instalación de sistemas en centros periféricos con la complejidad que origina en la gestión de inventario, así como la ejecución de tareas de carácter administrativo le ha conferido una personalidad propia que actuará de soporte y ayuda al resto de las áreas que componen el Centro TIC.

Esta área se puede dividir en tres:

- Infraestructuras: control, mantenimiento y adecuación de las instalaciones base del centro de sistemas TIC.
- Administración: archivo, biblioteca y de todo el papeleo que se genera en cada una de las actividades del centro TIC.
- Gestión de almacén. Inventario y Control de Suministros: correcta catalogación del material presente y reposición cuando baja de unos niveles prefijados.

8. SISTEMAS Y BASES DE DATOS.

El área de sistemas es otra de las áreas que está sufriendo cambios hoy en día. Tradicionalmente se ha dicho que es la encargada de mantener el correcto funcionamiento del sistema operativo, software base, software de aplicaciones y hardware. Y aunque lo sigue haciendo, el problema es que estos conceptos han adquirido otra dimensión.

Las áreas de sistemas, al igual que las de desarrollo, empezaron a sufrir transformaciones con la aparición de los sistemas gestores de bases de datos, PCs, sistemas distribuidos e Internet. Si a esto añadimos la aparición de gestores de contenidos, ERPs (Enterprise Resource Process), sistemas de gestión documental, XML, SSO (Single Sign On), E-learning, etc. y, especialmente, proyectos que ya no tienen la tipificación de ingeniería del software y que exigen fundamentalmente la participación del personal de sistemas, podemos observar que su complejidad e importancia dentro una organización ha crecido de forma impresionante. Es más, hay organizaciones que al no tener desarrollo propio han optado por hacer desaparecer esta área potenciando la de sistemas. Dentro del ámbito de la Administración Pública, se observa una fuerte tendencia a externalizar el desarrollo, pero sistemas sigue dependiendo del personal propio, eso sí, con apoyo de empresas externas.

Por otro lado, esta área aunque es todavía parte importante en la implantación de sistemas de seguridad, va perdiendo capacidad decisoria en este campo pasando a áreas específicas en la materia.

Tradicionalmente la organización de esta área ha sido sectorial basada en la tecnología y funcional. Y aunque esto sigue siendo así, en los proyectos donde se exige la introducción de nuevas tecnologías y los rápidos cambios que se producen en éstas, este modelo está empezando a resquebrajarse.

Las cuatro grandes subáreas (desde un punto de vista funcional) en las que se puede subdividir el área de sistemas podrían ser:

- Sistemas Operativos, Software Base y Sistemas Corporativos: encargada del mantenimiento y mejora continua de los sistemas de información centrales de la organización.
- Microinformática: se encarga de todo lo relacionado con el mundo del PC.
- Bases de Datos: gestión de sistemas de bases de datos.
- Integración de Sistemas: sistemas que deben comunicarse entre sí ya se ejecuten sobre la misma plataforma o distinta.

En organizaciones con sucursales o departamentos fuera de las oficinas centrales se pueden encontrar sistemas basados en servidores de ficheros e impresión y en el caso de organizaciones que han optado por sistemas distribuidos, también pueden tener sistemas gestores de bases de datos, sistemas documentales, etc. Aunque la gestión y administración tanto de usuarios, sistemas y seguridad deben estar centralizadas, será necesario tener personal en las delegaciones periféricas que seguirán los procedimientos marcados por las oficinas centrales.

9. COMUNICACIONES.

Esta área en cuanto a soporte a datos tiene su origen, en una buena parte de las organizaciones, en el área de sistemas, sin embargo, la parte de telefonía o voz no. Con la centralización de los recursos corporativos (tanto en voz como en datos); acceso a través de Internet por parte de los ciudadanos, empresas o

proveedores, y otras unidades de la organización a los mismos; así como la adopción de las competencias de telefonía, ha supuesto que el correcto diseño en cuanto a topología y ancho de banda, y una correcta planificación de las necesidades de comunicaciones se hayan convertido en elementos críticos en cualquier organización, hasta el punto de ser una de las áreas que más presupuesto consume.

Otro aspecto importante es la liberación de los servicios de telecomunicaciones hasta el punto que éstos se deben adquirir en un mercado de libre competencia, terminando el monopolio de la operadora dominante. La valoración de diferentes opciones tecnológicas de distintas operadoras se ha convertido en una nueva necesidad dentro de los Centros TIC.

Todo lo anterior le ha hecho adquirir personalidad propia dentro de un Centro TIC.

Esta área se encarga de los servicios de voz y datos basados en diferentes tecnologías tanto a nivel local (dentro de un edificio) como a nivel de área extendida (WAN).

El principal problema con la que se encuentra esta área es la dificultad a la hora de planificar las necesidades de comunicación de una organización especialmente en el entorno WAN. Es tarea de los directores de proyecto, área de sistemas y desarrollo poder proporcionar datos sobre el flujo de datos en una WAN para poder dimensionar las correspondientes líneas de comunicación.

Sus funciones principales son:

- Programar necesidades en medios de telecomunicaciones.
- Análisis, diseño y construcción de los sistemas de comunicaciones.
- Gestión de los elementos de comunicaciones.
- Instalación y mantenimiento de los elementos de comunicaciones.
- Explotación técnica para asegurar los enlaces internos y externos de las Unidades.
- Definición de niveles y calidad de servicio.
- Implantación de sistemas de seguridad de acuerdo a las directrices marcadas por el área de seguridad.
- Monitorización de las líneas de comunicación.
- Resolución de los problemas de comunicaciones.
- Establecimiento de contratos de alquiler de circuitos y mantenimiento con las distintas operadoras de telecomunicaciones.

Además tenemos que añadir el despegue de nuevos servicios de telecomunicaciones de radio o telefonía móvil como:

- Telefonía móvil automática: GSM, GPRS y DC-1800 y a la espera del UMTS.
- Servicios WAP.

- Radio difusión sonora digital: con posibilidad de transmitir datos e imágenes.
- Sistema de telefonía de acceso de radio: LMDS: establece el bucle de abonado de telefonía sin el tendido físico de cables.

Por otro lado, como en el resto de los casos, la formación, documentación y establecimiento de normas y estándares son parte importante de sus funciones.

10. CENTRO DE ATENCIÓN A USUARIOS.

Todos los proyectos o servicios ofrecidos a los usuarios tienen incidencias. Uno de los problemas del Centro TIC es ser capaz de gestionar éstas de tal forma que:

- Resuelva la incidencia.
- No se consuman todos los recursos del centro TIC, al poder recibir llamadas todas las áreas del centro.

La idea es unificar en un único punto todas las recepciones de incidencias ya sean de hardware, software, seguridad, comunicaciones, de aplicaciones, tipo funcional, etc. Por otro lado, deberá ser el punto de entrada desde donde se le suministrará información al usuario de los distintos procedimientos a seguir.

Este punto único de contacto suministrará el acceso a los niveles apropiados de los servicios y proveerá de soporte técnico esencial para utilizar estos servicios de una forma eficiente y eficaz. Se constituirá en una interfaz única entre los usuarios finales y el centro TIC. Este punto único recibe el nombre de Centro de Atención a Usuario (CAU) o infocentro.

Los principios que debe regir el CAU son los siguientes:

- Mejora continua del servicio proporcionado. Para llevarlo a cabo hay que disponer información sobre los niveles de servicio.
- Proveer de un único punto de contacto al usuario final que sirva de enlace con otras áreas.
- Servirá para detectar información sobre los usuarios a fin de complementar las necesidades no cubiertas: formación, fallos de desarrollo, etc.
- Actuar como fuente de conocimiento gracias a la documentación sobre las soluciones aportadas a las incidencias.

El CAU dará respuesta a cualquier tipo de incidencia que le sea reportada, tanto técnica como funcional. No siempre será quien resuelva realmente la incidencia.

10.1. CICLO DE UNA INCIDENCIA.

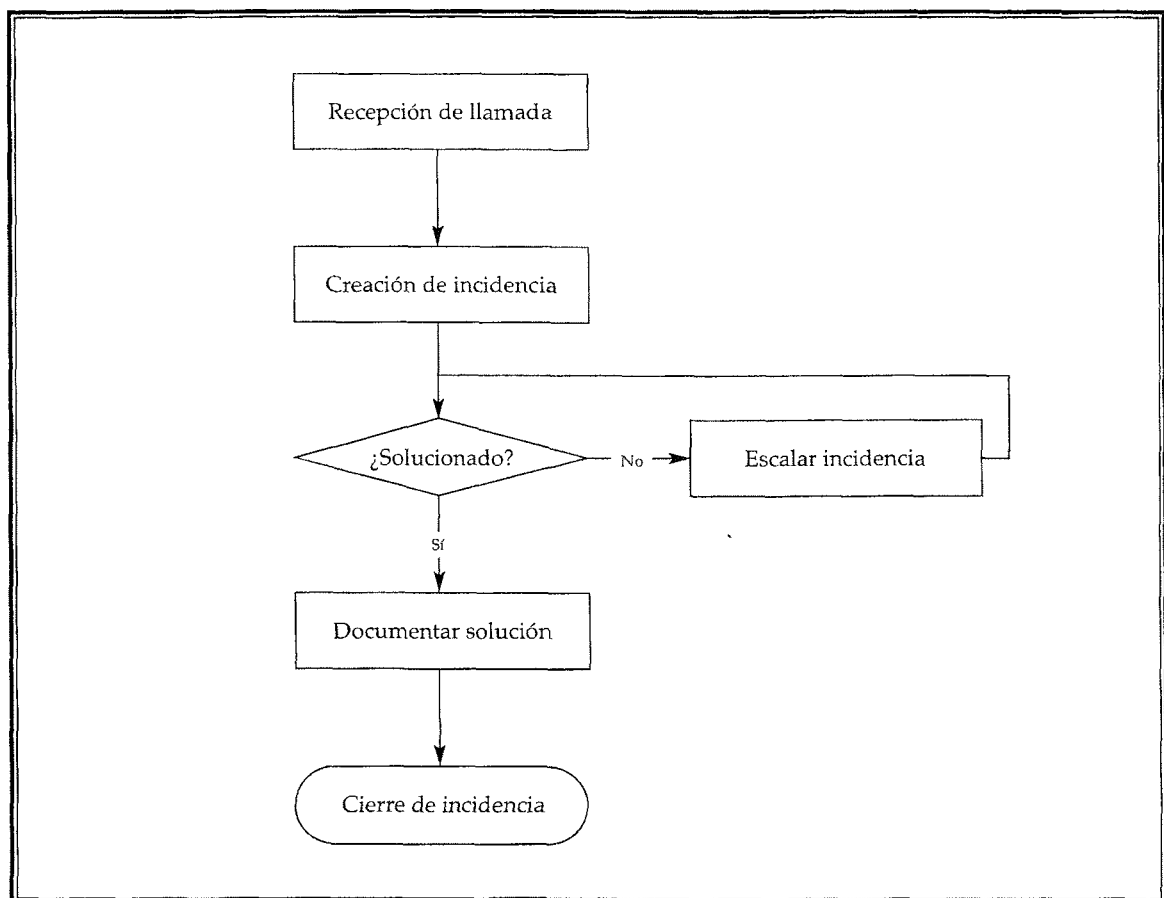
Desde que se produce una incidencia hasta que se resuelve, ésta sigue un ciclo tal y como podemos ver en la figura.

La incidencia se produce generalmente a través de una llamada telefónica, aunque también podría ser a través de un correo electrónico, o por medio de un sistema gestor de incidencias basado en WEB, que permitiría al usuario rellenar un formulario con los datos de su problema. La recepción de la incidencia se efectúa en el CAU, donde anotarán los datos del usuario y las características del problema a resolver.

Una vez recepcionada la incidencia, pueden suceder dos situaciones:

- Se resuelve la incidencia en el mismo CAU. Con lo que se cerrará la incidencia y se documentará la solución.
- El CAU no resuelve la incidencia y la escala a otro nivel que puede ser una de las áreas del Centro TIC. Será el área escalada la encargada de asignar un responsable para la resolución del problema. Una vez que el responsable ha detectado la solución la reportará al CAU, quien se pondrá en contacto con el usuario. Posteriormente, documentará la solución y cerrará la incidencia.

Algunas organizaciones más tecnificadas poseen un gestor de incidencias de tal forma que cuando el CAU escala la incidencia, el responsable asignado por el área afectada, se pone en contacto con el usuario. Una vez resuelta, documenta la solución, que será introducida en el gestor de incidencias y se cerrará la solución. De esta forma el CAU también está informado de la resolución y forma.



10.2. ESTRUCTURA A TRES NIVELES.

A la hora de gestionar y resolver una incidencia se establecen tres niveles de gestión:

- Nivel 1: corresponde al mismo Centro de atención a Usuarios o CAU. Se encarga de recoger la incidencia, convenientemente caracterizada con los datos del usuarios y descripción del problema. Si puede resolverla, lo hará documentando la solución y cerrando la incidencia. Si no la puede resolver la escalará al nivel 2, identificando qué área es la más apropiada para resolverla.

El nivel 1 se encargará del almacenamiento, caracterización y explotación de toda la información y soluciones relacionadas con las incidencias recibidas.

- Nivel 2: corresponde a las otras áreas del Centro TIC: desarrollo y mantenimiento, sistemas y bases de datos, seguridad, dirección de proyectos, etc. El área afectada nombrará un responsable de resolver la incidencia que será quien se ponga en contacto con el usuario y una vez resuelta, documentará la solución y se lo reportará al CAU para el cierre correspondiente.

El nivel 2 deberá tener acceso a la base de incidencias ya que la incidencia reportada puede haberse producido anteriormente o puede deberse a una solución incorrecta de un caso anterior.

- Nivel 3: este nivel lo constituyen los proveedores externos y/o empresas de mantenimiento. Aunque generalmente la incidencia llegará hasta este nivel cuando no se ha podido resolver en nivel 2, no es descartable que venga directamente del nivel 1 en el caso de una clara identificación por parte del CAU (caso de avería de un monitor con el que existe un contrato de mantenimiento). Una vez resuelta la incidencia se reportará al CAU la solución, el motivo y éste la cerrará.

Lo que se pretende con esta estructura es que la mayor parte de las incidencias se resuelvan en el CAU, dejando a los especialistas las incidencias más difíciles o complejas.

El CAU deberá llevar un registro de incidencias y generará estadísticas sobre tipos de incidencias más repetidas y departamentos más afectados. La información obtenida se utilizará para descubrir posibles necesidades, formación o procedimientos de usos mal llevados a la práctica.

10.3. RELACIONES CON LOS CENTROS DE LA PERIFERIA.

En el caso de organizaciones con oficinas en la periferia se seguirá la misma tónica descrita anteriormente. Esto puede resultar especialmente duro para aquellos centros periféricos que tienen personal informático que se les obliga a introducir un nivel más en la resolución de su incidencia:

- Nivel 1: CAU.
- Nivel 2: personal informático del centro periférico.
- Nivel 3: otras áreas del centro TIC.
- Nivel 4: proveedores externos.

En este caso, las incidencias a los proveedores externos también pueden llegar directamente del personal informático de la periferia, aunque éstos deberán reportar la solución al CAU.

Aunque pueda parecer añadir más «burocracia», si se tiene un adecuado sistema de gestión de incidencias, se podrá utilizar todo el conocimiento de la organización, ya que a fin de cuentas hay incidencias comunes en todos los sitios, reduciendo ostensiblemente los tiempos de resolución y dejando al personal informático de la periferia dedicado a otras tareas.

11. VULNERABILIDADES Y RIESGOS.

11.1. CONCEPTO DE VULNERABILIDAD.

La vulnerabilidad se refiere a la probabilidad de que ocurra una amenaza sobre un activo, siendo los activos aquello que se quiere proteger: máquinas, datos, etc. Su medida no se hace de forma directa sino que se basa en estadísticas e históricos.

Cuando no se tienen medidas de la propia empresa, se recurre a medidas y estadísticas de organizaciones similares a la nuestra.

Es obvio que su amenaza tiene impacto sobre un activo, éste es vulnerable a esa amenaza, con lo que habrá que tomar las distintas medidas de tipo físico y organizativo para minimizar el impacto o evitarlo totalmente.

11.2. RIESGOS POTENCIALES.

Para la identificación de los riesgos potenciales a los que está expuesta la Función Informática de una Organización, lo más adecuado es hacer una clasificación atendiendo a su origen, distinguiendo los accidentales de los intencionados.

Entre los de origen accidental se deben considerar, sobre todo, los siguientes:

- Desastres naturales.
- Vendavales, seísmos, rayos, etc.
- Incendios.
- Inundaciones.
- Averías en los equipos propios del Centro de Proceso de Datos.
- Averías en las instalaciones eléctricas o interrupciones en el suministro.
- Averías de climatización.
- Perturbaciones electromagnéticas.
- Errores en la introducción, transmisión y utilización de los datos.

Entre los de origen intencionado, en los que no se excluyen parte de los ya mencionados, se señalan como los más frecuentes:

- Fraudes.
- Sabotajes.
- Sustracción de algún elemento del Sistema.
- Huelga y marcha de personal estratégico.
- Difusión o salida incontrolada de información al exterior.

Frente a estos riesgos potenciales, cabe adoptar cualquiera de estas posturas:

- Aceptar el riesgo, confiando en su baja probabilidad de ocurrencia.
- Transferir el riesgo, limitándose a la contratación de los correspondientes seguros. Esta medida, por una parte, no palía todo el daño causado, al ser algunos efectos (precisamente los más costosos) imposibles de reemplazar y, por otra, no repone la información perdida.
- Evitar el riesgo. Conlleva la elaboración y puesta en marcha de un Plan de Seguridad Informática, cuyas medidas de carácter preventivo minimicen la probabilidad de ocurrencia de un siniestro.

Normalmente se opta por una situación mixta de las anteriores, donde el factor a considerar es la relación coste/ganancia que obtiene implementando medidas preventivas.

A partir de ahora, consideraremos que se opta por la última opción.

12. INSTALACIONES.

En este apartado repasaremos algunos de los aspectos a tener en cuenta a la hora de diseñar un centro de proceso de datos.

12.1. LOCALIZACIÓN DEL CENTRO DE PROCESOS DE DATOS. ASPECTOS A CONSIDERAR.

El sitio elegido para un centro de proceso de datos debe cumplir una serie de características esenciales, alguna de ellas parecerán obvias pero debemos citarlas en este estudio, las características referentes a la seguridad del mismo constituyen el bloque principal.

Los posibles eventos naturales también deben ser tenidos en cuenta: sitios con riesgo de inundación (cerca del cauce de los ríos), inconvenientes como el polvo, ruptura de canalizaciones, caídas de tensión, y muchos otros efectos.

Otro tema a tener en cuenta es la correspondiente coordinación con el plan de seguridad del propio edificio. Hay que estudiar cómo el plan de seguridad del centro de sistemas de información se ve afectado, o puede afectar al plan general de seguridad del edificio o recinto.

Aparte de lo dicho anteriormente hay una serie de factores habituales que hay que considerar antes de decidir la ubicación del centro de proceso de datos.

- Características de las máquinas a instalar: otro aspecto es el peso de los equipos que queremos instalar, especialmente porque este peso se concentra en un área reducida. Ésta ha sido tradicionalmente una de las razones por las que se han instalados las máquinas centrales o corporativas en los sótanos, pero con la disminución de peso y tamaño de los sistemas actuales, no debe ser considerado el único criterio.
- Diseño del centro de proceso de datos: el centro de proceso de datos no debe ser visible desde el exterior. Se deben construir instalaciones de forma discreta y minimizar instalaciones sobre su propósito, evitando signos obvios (afuera y dentro del edificio), que identifiquen la presencia de actividades cuya seguridad se desea. No se debe identificar en directorios telefónicos ni en edificios. Típicamente, el centro de proceso de datos se debe separar en una serie de zona como: entrada de datos, entrada/salida, telecomunicaciones, almacenamiento, operación, soporte, etc. Para que esta división por zonas sea efectiva, ésta debe ser desarrollada durante la planificación inicial del centro, y tener previstas las necesidades futuras, de tal manera que la evolución del mismo no ponga en compromiso el nivel de seguridad.
- Vigilancia del centro de proceso de datos: un sistema de circuito cerrado de televisión juega un papel muy importante en el plan de seguridad de un centro de proceso de datos. Sin embargo, este punto es uno de los más costosos del plan de seguridad, sin embargo la justificación de su costo a largo plazo es muy fácil si tenemos en cuenta la cantidad de personal de vigilancia que nos ahorramos con este sistema. Los detectores de movimiento son otra herramienta muy útil a la hora de prevenir actividades no permitidas en lugares ocultos como pueden ser determinadas partes de la sala de ordenadores o ciertos despachos. De nuevo la discreción debe ser tenida en cuenta al ser situados estos detectores.
- Incendios.
 - La mayoría de los muros de los centros de proceso de datos deben tener una resistencia al fuego de al menos dos horas, deben también ser aislantes al vapor para mantener unas condiciones medioambientales controladas.
 - El vidrio debe ser evitado todo lo posible en la sala, ya que las puertas y ventanas de vidrio no ofrecen suficiente protección contra el fuego, aparte el vidrio aumenta la visibilidad de la sala, con lo que disminuye su seguridad.
 - El diseño de un sistema adecuado de protección contra incendios debe basarse en una serie de factores: la velocidad y precisión del sistema automático de detección, la velocidad y precisión del sistema de extinción, y la provisión de un sistema eficaz de alarmas para mantener la seguridad del personal.
 - El sistema de detección automático es la forma más rápida y efectiva de darse cuenta de que un incendio está ocurriendo. Los detectores de ionización o fotoeléctricos son los más difundidos, aparte pueden ser complementados con detectores de temperatura o cualquier otro que sirva para este propósito.
 - El sistema de alarma contra incendios debe ser distinto de los demás sistemas de alarma, y debe avisar al personal de que se ha producido un fuego, para que éstos puedan tomar las medidas oportunas.

- Otros factores. Por último, los centros de proceso de datos para su normal funcionamiento dependen de multitud de factores, como pueden ser: el sistema de aire acondicionado, sistemas de generación y distribución de electricidad, entre otros. Los avances producidos en estos campos nos permiten en la gran mayoría de casos incluir estos sistemas en lugares seguros del centro de proceso de datos. Sin embargo, hay otros que no queda más remedio que situarlos fuera del edificio, por ejemplo, las torres de refrigeración, transformadores, etc. Ya que dependemos totalmente de estos elementos, la seguridad diseñada para el centro debe incluir todos estos elementos.

Un elemento esencial del diseño de la seguridad es la posibilidad de monitorizar y controlar todos los sistemas, subsistemas y componentes que forman parte del sistema de seguridad. Este control puede efectuarse desde una consola central de seguridad que debería ser el destino de todos los lectores de tarjetas, sensores de alarma y cámaras del circuito cerrado. Desde esta consola, el personal adecuado, puede verificar el estado del sistema y tomar las medidas pertinentes.

12.2. SEGURIDAD CONTRA INCENDIOS.

Indudablemente, la seguridad contra incendios es una cuestión importantísima en la planificación de la estructura de un centro de proceso de datos, además tiene un papel fundamental entre las medidas de seguridad físicas del mismo. Sin embargo, puesto que la explicación de este tema es algo obvio, en este apartado vamos a tratar de darle un enfoque distinto, tratando de desmontar una serie de ideas erróneas existentes tradicionalmente en esta materia.

Como cualquier otra materia, una buena práctica de seguridad contra incendios depende de una aplicación ordenada de técnicas y métodos cuidadosamente desarrolladas por ingenieros de seguridad contra incendios a lo largo del tiempo. Los jefes de sala y demás personal competente en esta materia cometerían un grave error si sólo basaran sus medidas de seguridad contra incendios en consejos de profesionales en esta materia.

A continuación expresaremos algunas ideas erróneas acerca de la protección contra el fuego que se presentan tradicionalmente en los centros de cálculo:

- Los ordenadores deben instalarse en zonas a prueba de fuego.

Esta idea está basada en un pequeño engaño. El hecho es que la asociación nacional de protección contra el fuego prohíbe el uso del término «a prueba de fuego» en sus propias publicaciones. Esto es así porque la frase en sí carece de significado: ningún material o edificio puede ser considerado «a prueba de fuego». Esta idea puede provenir de considerar lo mismo «a prueba de fuego» que incombustible.

Esta primera idea errónea nos sirve para demostrar la importancia de pensar en la seguridad contra incendios como un número de acciones que deben ser tomadas en conjunto.

No es suficiente que el edificio sea «resistente al fuego» sino que es también importante controlar los materiales inflamables que existen así como los métodos de detección y extinción de incendios.

- El Halón es un sistema de extinción de incendios ideal.

La mayoría de los gestores de seguridad están familiarizados con el Halón (un agente de extinción de incendios muy difundido en todos los centros de proceso de datos). Almacenado en for-

ma líquida a alta presión, es expulsado en forma de gas sobre el fuego, cuando éste es detectado. El Halón trata de apagar el fuego interfiriendo con la reacción química por la que se produce la combustión. Asumiendo que se dispone de una concentración de Halón apropiada (entre el 5 y el 7%), el fuego se extinguirá rápidamente.

Aunque el Halón puede ser considerado como un elemento extremadamente atractivo para la extinción de incendios en habitaciones con elementos críticos o muy caros, sin embargo, debemos tener en cuenta algunos de sus inconvenientes. El primero de ellos es que el Halón es muy caro, normalmente puede ser cuatro veces más costoso que un sistema de extinción automático basado en agua para edificios nuevos, es un poco más barato en edificios ya existentes puesto que el área a proteger es menor.

Una vez descargado el Halón debe ser recargado, el coste de esta recarga será aproximadamente el 40 por 100 del coste de instalación inicial. Como consecuencia de esto, las personas encargadas de la instalación deben ser conscientes del coste de la recarga. También debemos hacer énfasis en el procedimiento de respuesta a la detección de incendios, que habitualmente lleva consigo un considerable retraso en la descarga del Halón (hasta que la presencia de fuego es verificada realmente). Puede ser una contradicción instalar un sistema de extinción de incendios muy caro y sin embargo éste ser ineficiente debido a un sistema de detección demasiado tardío y «celoso».

La operación de un sistema de extinción basado en Halón depende de una cadena muy complicada de eventos. Primero el fuego tiene que ser detectado (de manera automática o manual), a continuación se transfiere el control al sistema de Halón (normalmente suena una sirena indicando que el Halón se descargará en un minuto). Durante este minuto los conductos de ventilación deben ser cerrados así como todas las puertas y ventanas, el aire acondicionado también debe ser parado y el personal evacuado. A continuación el sistema de Halón abre las válvulas para dejar salir el Halón de las botellas o recipientes en los que se encuentra, éste se dispersa por toda la habitación para localizar el foco del fuego para extinguirlo (éste debe encontrarse en la concentración adecuada para que sea efectivo). Si alguno de todos estos eventos falla, el sistema de extinción es ineficaz.

Una vez liberado el gas, se debe esperar un período de tiempo bastante amplio para que el fuego sea completamente extinguido o bien que la temperatura de la sala haya bajado lo suficiente, sólo entonces podremos ventilar la sala, si lo hacemos antes, corremos el riesgo de que el fuego se reproduzca y nos encontremos en la difícil situación de tener un fuego y ya hubiéramos agotado el Halón de nuestra instalación (en algunas instalaciones se instala un segundo sistema de respaldo, pero esto aumenta el coste significativamente).

Finalmente, se tiene la sospecha (o evidencia) de que el Halón no es tan inofensivo como se creía. Experimentos de laboratorio han demostrado que el Halón en concentraciones relativamente altas (12% o más) puede producir problemas de corazón. Si el Halón no apaga el fuego y se calienta por encima de 900° F, tiende a descomponerse en elementos altamente tóxicos.

Por todo lo visto anteriormente, aunque el Halón en condiciones normales y baja concentración es un gas inerte y sin peligro, a la hora de planificar el sistema de extinción de incendios se deben tener en cuenta todos estos peligros y debe ser realizada por personal especializado.

- Los detectores de humos son el mejor sistema de extinción de incendios.

Ésta es una de las confusiones más habituales, obviamente los detectores de humos no constituyen por sí solos un sistema de extinción de incendios, es muy corriente la confusión entre los sistemas de detección y extinción de incendios, los detectores constituyen el primer grupo. Sin

embargo, hay que hacer notar que un conjunto eficaz de detección de incendios constituye un eje fundamental en el que basar toda nuestra infraestructura contra incendios.

- El agua es el mayor enemigo del centro de proceso de datos.

Esta idea está basada en la curiosa línea de razonamiento que evitaba usar agentes de extinción de incendios que pudiera dañar el origen del fuego. Un ejemplo de esta idea ocurrió en una planta nuclear de EE.UU., en la que un fuego estuvo activo durante seis horas y media hasta que el encargado permitió el uso del agua que acabó con el fuego en quince minutos.

La experiencia ha demostrado que el objetivo más importante a la hora de combatir un fuego es extinguirlo lo más rápidamente posible en lugar de muchas veces preocuparse por el efecto que pudiera tener el agente de extinción usado en los bienes que queremos proteger. Si ponemos en marcha un sistema con algún agente que pudiera resultar perjudicial, quizás podamos tener algún desperfecto al producirse un incendio en la parte afectada. Sin embargo, si no usamos un agente eficaz el fuego podría propagarse a otras partes del edificio y los daños podrían ser mucho mayores.

Un ejemplo lo tenemos en una fábrica de papel de EE.UU. en la que se decidió no poner un sistema de extinción de incendios basado en agua porque ésta dañaría el papel, se produjo un incendio y el sistema instalado se demostró ineficaz con lo que no sólo se perdió todo el papel sino que la estructura del edificio resultó seriamente dañada.

- Los sistemas de extinción secos son mejores que los basados en agua.

Para empezar un sistema de extinción basado en agua se basa en unos sensores de temperatura que al alcanzar un determinado nivel (generalmente 165° F), se dispara un mecanismo por el que se deja caer sobre el área afectada una fina nube de agua que se encarga de extinguir el fuego.

Los sistemas «secos» se utilizan fundamentalmente en lugares donde la congelación del agua de las conducciones pudiera dañar el sistema de extinción, en este caso se basan en aire comprimido que se mezcla con el agua a la hora de actuar sobre el fuego, lo que contribuye a que el agua no se congele en las canalizaciones (re llenas con aire comprimido).

Los sistemas «secos» tienen fundamentalmente dos desventajas, la primera es su mayor complejidad y la segunda viene del hecho de que las canalizaciones al estar llenas de aire comprimido se produce un retardo hasta que el agua comienza a actuar sobre el fuego, y ya hemos visto lo importante que era actuar sobre el fuego cuanto antes.

A pesar de estas desventajas el sistema «seco» ha sido muy utilizado en las salas de ordenadores ya que ese retardo era aprovechado para evaluar la gravedad de la situación, si se comprobaba que era una falsa alarma se cerraba el paso del agua. El principal argumento para utilizar el sistema «seco» era el daño que se podría producir en caso de una apertura accidental de una boca. En primer lugar, si un fuego es lo suficientemente grande como para abrir una boca, éste producirá un mayor daño que el que pueda producir el agua de esa boca. Además, estas bocas son lo suficientemente fiables como para poder pensar que si una de estas bocas vierte el agua de manera accidental es porque la misma ha sido manipulada sin cuidado alguno.

- Los esfuerzos en protección contra incendios se deben centrar en la sala de ordenadores.

Existen dos razones para tener un nivel alto de seguridad en la sala de ordenadores, la primera es la protección de los bienes informáticos de la empresa (aunque este primer motivo se puede

minorar con la contratación de un seguro) y la segunda, la continuidad del servicio (quizás la principal). Hoy en día es imposible la continuidad de la mayoría de las empresas sin la función informática, así pues debemos tomar todas las medidas para evitar que cualquier acto voluntario o no pueda interrumpir la función informática, entre estos hechos están los incendios. Existe una tendencia a centrar toda la seguridad contra incendios en la sala, esto es un gran error.

Un ejemplo de esto ocurrió en Massachusetts, en una empresa la sala de ordenadores se encontraba en la tercera planta de un edificio de estructura de acero sin sistema de detección de incendios aparte del existente en la sala. Un incendio comenzó en la primera planta, éste no fue demasiado importante, sin embargo, sí se produjeron gases tóxicos y altamente corrosivos que por diversas canalizaciones llegaron al tercer piso. Los ordenadores no estuvieron expuestos a altas temperaturas, pero fueron seriamente dañados por este humo corrosivo.

Así, a la hora del diseño de la política de extinción de incendios se deben tener en cuenta los efectos que pudieran tener en la sala de ordenadores los fuegos producidos en otras partes del edificio, especial atención hay que prestar a las canalizaciones entre plantas, ya que hay que buscar el total aislamiento entre las distintas plantas de un edificio.

12.3. SEGURIDAD DE LAS CONDUCCIONES.

En los edificios de oficinas de hoy en día, en los que parece instalarse la moda de los espacios abiertos y sin obstáculos interiores, las canalizaciones de electricidad, teléfono, datos, etc., deben realizarse por el suelo (o falso suelo). Estas canalizaciones en la mayoría de los casos se producen de una manera incontrolada y desordenada por debajo del suelo, haciendo posible mover un ordenador de un lugar a otro de la sala sin coste alguno.

Para poder satisfacer esa necesidad de movilidad, todos los cables y conducciones necesarias son incluidas en unas conducciones especiales de carriles paralelos de acero por debajo del suelo. El diseño de estas conducciones puede variar de unas instalaciones a otras, pero básicamente consisten en una serie de carriles donde alternan cables de electricidad con carriles que llevan los cables de datos, y una serie de registros a lo largo de la misma planta, donde el personal pertinente pueda verificar o controlar el funcionamiento, a tramos se presentan una serie de rosetas donde poder efectuar las conexiones.

Diseñadas específicamente para edificios de nueva construcción, este sistema de canalizaciones en el suelo proporciona mayor seguridad que las conducciones por el techo, falso suelo o cualquier otro tipo de canalización. Pero, sin embargo, este tipo de canalizaciones no son del todo seguras; normalmente las mismas canalizaciones dentro de la misma planta deben dar servicio a departamentos que tratan datos sensibles y a otros que no los tratan, con el correspondiente riesgo de que cualquier persona pueda acceder a una roseta de conexión y realizar alguna conexión fraudulenta por la que datos sensibles se pongan en manos indebidas. Un mayor nivel de seguridad lo proporcionan las canalizaciones que separan físicamente las canalizaciones eléctricas y de datos no sensibles de las que llevan datos sensibles, aparte también se mejora el aislamiento electromagnético.

Este tipo de canalización en lugar de contener dos carriles, como los vistos anteriormente, contienen tres carriles de acero; el primero contiene cables de electricidad, el segundo cables de comunicaciones no confidenciales, y el tercero, aislado físicamente de los otros dos, contiene cables de comunicaciones confidenciales. Aunque el mismo sistema de distribución da servicio a todo el edificio, el acceso al tercer carril está reservado a aquellos despachos o localizaciones que lo requieran, y para ello estarán equipados con una roseta especial. Así, todos los despachos contienen una roseta estándar, que previenen que un empleado «desleal» acceda a datos sensibles de manera factible (podría hacerlo tala-

drando el suelo, con la correspondiente capa de acero, y el ruido necesario para llevarlo a cabo), y otros despachos llevan instalada una roseta especial para acceder a datos sensibles.

El aislamiento de los cables eléctricos y de datos ordinarios de aquellos que necesitan una mayor confidencialidad, nos permite un nivel de seguridad corporativo aceptable, sin incurrir en los costes adicionales de instalar un sistema de distribución redundante en el mismo edificio. Además, es posible realizar tareas rutinarias de mantenimiento de la instalación eléctrica sin afectar para nada a aquellas comunicaciones críticas.

Los comerciales en esta área citan como una de las causas principales de cambio de edificio en las compañías la obsolescencia del sistema de canalizaciones. En algunos de ellos el sistema antiguo puede ser actualizado con algunas extensiones, pero la situación actual en la que el cambio de despacho y el cambio de equipos es algo habitual, complican estas actualizaciones más si cabe.

Un último aspecto a tener en cuenta a la hora de elegir un sistema de canalizaciones adecuado es el mundo en el que nos movemos, en el que los requerimientos avanzan a velocidades vertiginosas, y capacidades que hoy en día nos parecen inalcanzables serán rutina dentro de poco. Un sistema de canalizaciones que pueda recoger este avance a esta velocidad es fundamental para una correcta evolución de nuestro centro de cálculo.

12.4. CONTROL DE ACCESOS.

El control de los accesos es un aspecto fundamental en la seguridad de un centro de proceso de datos. Todas las personas en contacto con el sistema de proceso de datos deben tener un motivo para poder hacerlo (principio de legitimidad). Un sistema en el cual el control de acceso se basara en personal de vigilancia que controle el acceso a determinados sitios no es del todo seguro (este personal se podría distraer o podría ser sobornado).

Una alternativa muy válida la constituye los sistemas de control de acceso electrónicos. El sistema se activa cuando el usuario presenta un código (a través de un lector de tarjetas o directamente por un teclado), si este código es válido, la puerta controlada es abierta automáticamente. Cada puerta puede usar distintos controladores y éstos ser programados para aceptar unos u otros códigos. Estos códigos pueden ser cambiados mediante algún procedimiento.

Una solución más sofisticada la constituye un sistema donde es posible la monitorización de los accesos y el control desde un punto central. Este sistema está constituido por lectores, controladores y otros periféricos, éstos se pueden conectar mediante líneas dedicadas o telefónicas.

El lector es el punto en el cual el usuario presenta el código para ser validado. Cada lector puede tener acceso directo al controlador o se pueden utilizar multiplexores para permitir el acceso de varios lectores por el mismo canal. El controlador tiene la función de procesador central de información, donde el código introducido por el usuario se compara con el juego de códigos válidos (guardados normalmente en una memoria RAM).

Los lectores y multiplexores pueden compartir inteligencia con el controlador y así, funcionar como controladores remotos. Los códigos autorizados se programan en la memoria a través del controlador al que pueden conectarse alguna pantalla e impresora para proporcionar esa información. A estos sistemas centralizados a veces se les llama sistemas on-line mientras que a los sistemas compuestos por lectores independientes se les llama off-line.

Uno de los temas que hemos tratado era el medio por el cual el usuario introducía el código en el sistema. El método más corriente de hacer esto era mediante una tarjeta de banda magnética o con microchip incorporado, que también podría incluir una fotografía del empleado y podría servir como identificación del mismo.

Cuando utilizamos tarjetas, el código puede ser guardado en éstas a través de una banda magnética, un circuito electrónico o bien un núcleo magnético incluido dentro de la tarjeta. El método de la banda magnética es el más utilizado y el más barato, pero el método del núcleo magnético es el más difícil de duplicar. El código puede ser también incluido en forma de patrones ocultos y sólo visibles a través de determinados métodos ópticos, de tal manera que a simple vista la tarjeta no presenta ningún código visible. En este caso los sensores son ópticos en lugar de magnéticos.

Los sistemas de proximidad utilizan un sensor que emiten y reciben una señal a través de frecuencias de radio. El código es introducido manteniendo una tarjeta cercana al sensor, los circuitos de la tarjeta modulan una señal de una forma determinada, que el sensor traduce en el código de que se trate.

Adicionalmente se le puede requerir que introduzca un código previamente memorizado por el empleado a través de un teclado. El claro inconveniente es que el código puede ser olvidado o escrito en lugares obvios de encontrar por alguien que ponga el más mínimo empeño. Sólo si el código introducido por el usuario coincide con el incluido en la tarjeta se le permite el acceso, en caso de que haya discrepancia se le permite introducir otro código un número limitado de intentos.

El último método lo constituye un periférico de alta seguridad que se basa en sistema biométricos como lector de las huellas de los dedos y su posterior comparación con los patrones previamente introducidos en el sistema de las huellas de las personas a las que se les permite el acceso; *scanners* oculares, etc. La fiabilidad de este tipo de dispositivos, así como de cualquier otro basado en las características morfológicas de las personas, es muy alta.

El tamaño de almacenamiento de los sistemas centralizados hacen posible tener un alto grado de seguridad, asignando un código a cada uno de los empleados.

Con este sistema, como podemos individualizar cada puerta y cada usuario dentro del sistema, se pueden crear distintos niveles de seguridad, de manera que algunos usuarios tengan acceso a la sala del ordenador mientras que otros no lo tengan. La configuración básica tendría un nivel de acceso (a todos los empleados se les permite entrar en todos los sitios), en el extremo opuesto cada empleado tendría su propio perfil de acceso.

El acceso también puede ser restringido por tiempo en lugar de por espacio. Se podrían crear distintas zonas horarias de tal forma que un empleado, en un momento determinado, tendría acceso a un lugar en concreto, mientras que en otra franja horaria no lo tendría.

12.5. SENSORES Y ALARMAS.

Otra de las consideraciones que debemos hacer a la hora de planificar nuestro centro de proceso de datos, se formula sobre la base de un buen conocimiento de algunos de los sistemas de alarma así como los sistemas de sensores disponibles.

- Sensores de temperatura.

La sala de ordenadores es un lugar que debe ser vigilado constantemente y de manera precisa ante posibles cambios en la temperatura que podrían variar el normal funcionamiento de los equipos, la mejor manera de hacer esto es mediante unos sensores que nos permite conocer la temperatura de las distintas partes de la sala, éstos pueden ser colocados en distintos lugares (techo, suelo o ambiente) para tener una visión más precisa. El funcionamiento del equipo de aire acondicionado/refrigeración de la sala está en estrecha relación con estos sensores; si la temperatura sube mucho, la refrigeración se pone en marcha, y se parará en caso contrario.

- Sensores de humedad.

Al igual que ocurre con la temperatura, en la sala de ordenadores deben vigilarse los cambios de humedad para el correcto funcionamiento de los equipos, el sistema de refrigeración lleva incluido un subsistema de humidificación, muy relacionado con estos sensores.

- Sensores de agua.

Normalmente la sala de ordenadores lleva consigo un falso suelo, en este falso suelo se incluyen estos sensores para detectar de una manera rápida las posibles fugas de agua en la sala.

- Alarma de acceso no permitido.

Algunas instalaciones al producirse una identificación no válida en el sistema de acceso en lugar de cerrar el paso, dejan libre el paso, pero hacen sonar una alarma en otro lugar, para posteriormente el personal de seguridad tratar de identificar al intruso.

- Alarma de mal funcionamiento en la refrigeración.

Cuando se produce un aumento considerable de la temperatura sin llegar a sospechar que se puede tratar de un incendio, al igual que al disminuir la humedad relativa de manera considerable, se disparará una alarma, estas dos alarmas indican un mal funcionamiento del sistema de refrigeración de la sala. Se encuentran normalmente en un panel en la sala de los operadores que está en una localización próxima a la sala de ordenadores.

12.6. SISTEMAS DE CABLEADO.

El sistema de cableado con que se dota a un edificio es un componente fundamental de la infraestructura del mismo. La aparición de los sistemas de cableado estructurado se basan en la necesidad estratégica que tiene una organización de considerar sus requerimientos en materia de comunicaciones a largo plazo. La vida útil del cableado está aproximadamente en 20 ó 25 años mientras que la del hardware o software no supera los cinco años, por ello parece evidente la necesidad de dotar a la organización de una infraestructura capaz de adaptarse lo mejor posible a todos los cambios tecnológicos que suceden.

Los requisitos que se le exigen a un sistema de cableado son:

- Capacidad de crecimiento, que permita añadir nuevos componentes al sistema.
- Capacidad de absorber nuevas tecnologías de forma que los componentes a añadir al sistema de cableado sean los mínimos.

- Alto grado de flexibilidad para permitir la movilidad del personal dentro del mismo edificio.
- Sistema fiable con las mínimas interrupciones posibles y un coste de reparaciones razonables tanto en tiempo como en dinero.
- Fácil identificación y gestión de los circuitos de información.

12.6.1. Cableado estructurado.

Por cableado estructurado se entiende un sistema de distribución integral de comunicaciones (voz y datos) basado en la normalización de los cables, conectores y adaptadores de todas las comunicaciones.

Un cableado estructurado cuenta con cables, rosetas de conexión, distribuidores de planta, etc., normalizados e interconectados de modo que puedan cubrir las necesidades y requisitos de todos los posibles usuarios, y a ser posible durante toda la vida útil del edificio.

El sistema de cableado ofrece una jerarquía que permite llevar esto a la práctica:

1. Subsistema de campus: permite interconectar edificios en el entorno local de un campus.
2. Subsistema troncal: interconecta las distintas plantas del edificio, convirtiéndose en la espina dorsal del mismo.
3. Subsistema horizontal: partiendo de los cuadros de distribución de planta llega a las rosetas o puntos de conexión donde el usuario conecta su terminal.

Así pues, la tipología básica es en estrella, independientemente de la tipología de la red de datos que se pretenda instalar; todas las tipologías son adaptables a ésta mediante los correspondientes baluns.

A continuación realizaremos un repaso a algunos de los elementos que componen los subsistemas anteriores:

- Punto de conexión:

Para el usuario, el punto de conexión son las rosetas, en las que se encuentran conectores hembra RJ11 (seis contactos), RJ45 (ocho contactos para cables UTP) o RJ49 (para cables STP). Las rosetas de conexión para cables de voz son el RJ11, no obstante ésta es sustituida por la RJ45 cuando se produce intercambio de datos.

Para evitar posteriores recableados, es muy conveniente dimensionar adecuadamente el número de rosetas por despacho, y como regla general, se toma la medida de cuatro a seis metros cuadrados por puesto.

- Cableado horizontal:

Lo constituye el segmento que une las rosetas con el armario de distribución de planta. Debe ser apropiado para transmitir datos y telefonía. Se consigue mediante el uso de cables normalizados UTP (par trenzado sin apantallar) o STP (par trenzado apantallado).

Este mismo cableado se utiliza para conectar la roseta con el equipo específico de que se trate, para ello se dispone de latiguillos estandarizados, terminados en un conector RJ45. En aquellos equipos que no dispongan de conector RJ45 y sí coaxial, se utilizará un BALUN para transformar las impedancias.

- Cableado vertical:

El cableado vertical o troncal se considera la espina dorsal del sistema, y realiza la conexión entre las distintas plantas del edificio.

Este subsistema puede ser tan sólo una extensión física de los cables que llegan a los cuadros de distribución de planta hasta el armario principal del edificio, o se puede constituir otra red diferenciada que conecte los distintos armarios de distribución de planta.

En el primer caso se utilizarían cables de pares que dan continuidad al sistema horizontal, y en el segundo se trata de otra red local que dispondrá de otro cableado en función de la tecnología empleada.

13. DIMENSIONAMIENTO DEL EQUIPAMIENTO FÍSICO. PLANIFICACIÓN DE LA CAPACIDAD.

13.1. DEFINICIÓN.

Es un proceso sistemático para conocer y predecir el conjunto de recursos (instalaciones, máquinas, equipos, etc.) necesarios para atender la carga de trabajo esperado en el futuro. La planificación de la capacidad, determina las necesidades de recursos para suministrar el nivel de servicio requerido, actual y futuro. Para ello es necesario definir los objetivos de nivel de servicio del usuario.

Los objetivos en el tiempo de la planificación de capacidad son:

1. Planificar los recursos necesarios.
2. Mejorar las técnicas de proyección de las necesidades y de la capacidad.

La planificación de la capacidad debe comprender, corregir y controlar todo aquello que desvirtúe la operación correcta del sistema y está muy relacionada con muchas de las funciones de la gestión de instalaciones, tales como:

- Rendimiento.
- Explotación.
- Problemas.
- Cambios.
- Recuperación.
- Seguridad.
- Informes.

Como conclusión, podemos decir que una planificación de la capacidad de un sistema debe dar:

- Visión ordenada del sistema.
- Información de la carga actual.
- Medida del rendimiento actual y del consumo de recursos.
- Proyección de la carga futura.
- Predicción del rendimiento esperado.
- Evaluación de las configuraciones futuras.

13.2. NECESIDAD DE LA PLANIFICACIÓN.

Cada vez es más necesario realizar una buena planificación de la capacidad de los sistemas informáticos ya que estamos en una etapa en que el crecimiento de proceso de datos es muy rápido en las empresas, esto es debido a que actualmente todas las organizaciones tienden a planes más agresivos que dan lugar a:

- Dar servicio a un mayor número de usuarios.
- Sistemas más importantes para la Empresa.
- Búsqueda de mayores beneficios.
- Necesidad de implementar rápidamente los nuevos planes.

La preponderancia de sistemas en línea (ON-LINE), cuyos beneficios son considerables, dan lugar a los siguientes condicionantes:

- Tienden a tener un crecimiento más acelerado.
- No se pueden desplazar a horas de menos carga de trabajo.
- Consumen más recursos.
- Crean mayor dependencia.
- Manifiestan inmediatamente los problemas en el tiempo de respuesta.

Utilizar nuevas alternativas para el desarrollo de aplicaciones futuras que mejoran la productividad, consumen un gran número de recursos y hacen muy difícil el prever su impacto en el sistema tales como:

- Manejadores de Base de Datos relacionales Lenguajes de 4.^a generación.
- Nuevas herramientas de ayuda a los Sistemas de desarrollo.

- Sistemas CAD-CAM.
- Sistemas corporativos.
- Etcétera.

Un mayor gasto en Proceso de Datos.

Planificar el crecimiento de Proceso de Datos por parte de la dirección.

Asegurar el cumplimiento de los convenios de nivel de Servicio y de rendimiento del sistema.

Para dimensionar los sistemas atendiendo a las consideraciones descritas no valen soluciones parciales como se desprende de los siguientes ejemplos:

1. Si se considera como posible solución el aumentar la memoria real, sólo es efectivo, si existe mucha paginación, ya que no mejora el consumo de CPU.
2. Si se toma como posible solución el aumentar la velocidad de proceso de la CPU, se pueden producir cuellos de botella en otros elementos del sistema, por ejemplo: en la entrada/salida.

Bien entendido que hay que adoptar soluciones globales, es necesario hacer un crecimiento planificado de los recursos del sistema de información, con objeto de tener un crecimiento evolutivo. Si no se planifica, la carga de trabajo se verá frenada al llegar al límite de los recursos, dando lugar a un crecimiento reprimido.

Cuando después de un crecimiento reprimido se amplían los recursos del sistema se produce una demanda latente, que es el trabajo que estaba frenado por falta de recursos, dando lugar a un crecimiento no gradual. La demanda latente es la base de dos leyes fundamentales de proceso de datos:

1. La carga de trabajo se expande hasta ocupar la capacidad existente.
2. No existe nunca suficiente espacio en disco.

Esta demanda se va creando durante los períodos de saturación de los recursos informáticos y a medida que las necesidades de proceso continúan creciendo. Cuando están disponibles las nuevas capacidades, esta demanda se carga rápidamente en el sistema. Por ello, una parte esencial de la planificación de los recursos informáticos es la consideración de la demanda latente.

Todo lo anteriormente expuesto nos lleva a que debemos adelantarnos a los problemas, en un ambiente constante de cambio, ya que no se puede llegar a tener un sistema en su nivel de saturación, se necesitan sistemas balanceados, para lo cual, es totalmente necesario realizar estudios de planificación de capacidad, considerando tanto el hardware como el costo (overhead) que lleva asociado el software que debe satisfacer las necesidades de los usuarios locales y remotos, los cuales requieren una respuesta a su demandas como si fueran los únicos usuarios de sistema. Estas consideraciones nos hacen comprender que planificar el comportamiento de un sistema, no es una tarea sencilla, ya que ha de tenerse en cuenta mucho y variados aspectos del hardware, software y de las aplicaciones que se van a llevar a cabo.

14. FACTORES A CONSIDERAR.

En la planificación de la capacidad de un sistema se deben tener en cuenta los siguientes factores:

- Características de la carga de trabajo.
- Utilización de los recursos.
- Evaluación del sistema.

14.1. CARACTERÍSTICAS DE LA CARGA DE TRABAJO.

El análisis inicial de la carga de trabajo, que soporta un Centro de Proceso de Datos genera un perfil gráfico que muestra las características de trabajo de ese Centro en particular. Dicho perfil genera una figura general donde se combina la carga y el tiempo de CPU medido en horas, transacciones, o cualquier otro factor que se ajuste lo más posible a la situación. Sin embargo, para una mayor utilidad, deben analizarse de forma específica, tanto la carga como el tiempo.

Para analizar las características de la carga de trabajo en el sistema actual hay que determinar los siguientes aspectos:

1. Reparto del trabajo a lo largo del día, determinar cuáles son las horas más representativas, de forma que se pueda establecer el origen y volumen de los puntos de carga.
2. Requisitos de los trabajos a realizar, para lo cual hay que determinar:
 - La relación de transacciones por minuto.
 - La relación de paginación.
 - La utilización de los distintos recursos.
 - Cuál ha de ser el tiempo de respuesta.

A la hora de tomar medidas de un sistema existente se plantea el problema de cuándo se puede considerar que el comportamiento del sistema es característico del mismo.

Idéntico problema se plantea cuando se deben buscar los datos para introducirlos en un modelo que evalúe el comportamiento del sistema sometido a una carga determinada. El común denominador a estos problemas reside en determinar las magnitudes que caracterizan la carga del sistema. A continuación se exponen algunas de las que se usan con mayor frecuencia:

- Tiempo de CPU por trabajos.

Es el tiempo total de CPU necesario para ejecutar un trabajo (programa, transacción, etc.) en un sistema determinado. Evidentemente es función directa del número de instrucciones a ejecutar para realizar un trabajo y del volumen de datos procesados.

- Número de operaciones de E/S por trabajo.

Es el número total de operaciones de entrada/salida que requiere la ejecución de un trabajo. Dicho número conviene desglosarlo según el dispositivo, el archivo, etc., sobre el que se realicen.

- Características de la operación de E/S por trabajo.

Hacen referencia al soporte (cinta, disco...) y, en el caso de discos, la posición que ocupa el archivo sobre el que se efectúan. Todo ello tiene una influencia directa en el tiempo necesario para realizar una operación de entrada/salida.

- Tiempo entre llegadas.

Es el tiempo entre dos requerimientos sucesivos para un servicio del sistema o de uno de sus dispositivos. En muchos casos se utiliza su inversa, que es la frecuencia de llegada que cuenta las peticiones de servicio que se producen por unidad de tiempo.

- Prioridad.

Es la que el usuario asigna a cada uno de los trabajos que somete al sistema.

- Memoria necesaria.

Es la que requiere un trabajo determinado para su ejecución. Puede ser constante (memoria real) o variable (memoria virtual paginada o segmentada), según la gestión que el sistema operativo haga de la memoria.

- Localidad de las referencias.

Es el tiempo en el que todas las referencias a memoria hechas por un trabajo permanecen dentro de una página (segmento) o conjunto de páginas (segmentos). Si se considera la ejecución de un programa como una sucesión de referencias a memoria, la localidad del programa será tanto mayor cuanto más tiempo esté dentro de la página (segmento) o un conjunto de páginas (segmentos) considerado. Ésta es la aparente contradicción de medir una magnitud ligada a espacio (localidad) mediante un tiempo.

- Tiempo de reflexión del usuario.

Es el tiempo que el usuario de un terminal de un sistema interactivo necesita para generar una nueva petición al sistema, es decir, el tiempo de pensar más el de teclear.

- Número de usuarios simultáneos.

Es el número de usuarios interactivos que trabajan simultáneamente sobre el mismo sistema en un instante dado.

- Intensidad del usuario.

Es la relación entre el tiempo de proceso requerido por una petición y el tiempo de reflexión del usuario.

14.2. UTILIZACIÓN DE LOS RECURSOS.

Una función de la planificación de la capacidad es comprender la utilización de cada subsistema, por medio de medidas.

La indicación de la capacidad de un recurso viene dada por el tiempo que requiere para completar un servicio.

El tiempo total de respuesta a la solicitud de un servicio viene dado por el tiempo de servicio del recurso y su tiempo de espera.

Bajo el punto de vista de la planificación de capacidad, una instalación será vista como un conjunto de recursos interrelacionados. Cuando se planea el uso de recursos hay que realizar algunos supuestos. No es práctico esperar un 100 por 100 en la utilización de la capacidad total de un dispositivo; por tanto es necesario calcular para cada grupo de dispositivos unos márgenes de rendimiento y capacidad razonables, con el fin de poder planear las ampliaciones de recursos.

El margen de seguridad se determina evaluando la capacidad óptima y haciendo una estimación razonable de la capacidad práctica.

En el momento en que la carga de trabajo haga que un recurso alcance o entre en el margen de seguridad, el trabajo se realizará con un alto nivel de riesgo y será necesario tomar alguna determinación, antes de que sea necesaria una acción correctora.

14.3. EVALUACIÓN DEL COMPORTAMIENTO DE UN SISTEMA.

Se lleva a cabo por medio de un conjunto de variables, cuyos valores nos dan una evaluación del comportamiento del sistema. Estas variables se pueden agrupar en dos clases:

1. Las que hacen referencia al comportamiento del hardware y el software del sistema.
2. Las que hacen referencia a cómo el usuario ve que el sistema se comporta con respecto a él.

Sin embargo, teniendo en cuenta que el comportamiento de un sistema es función primordialmente de su carga, las variables que caracterizarán dicho comportamiento dependen del uso a que está destinado.

A continuación se hace una breve descripción de variables que habitualmente se utilizan para evaluar el comportamiento de un sistema:

- Throughput.

Es la cantidad de trabajo útil ejecutado por unidad de tiempo en un entorno de carga determinado (normalmente se mide en trabajos por hora o en transacciones por segundo).

- Capacidad.

Es la máxima cantidad de trabajo útil que se puede realizar por unidad de tiempo en un entorno de carga determinado.

- Tiempo de respuesta.

Es el tiempo transcurrido entre la entrega de un trabajo o una transacción al sistema y la recepción del resultado o la respuesta.

- Factor de utilización de los componentes.

Es el porcentaje de tiempo durante el cual está siendo utilizado un componente del sistema informática (CPU, canal, dispositivo de E/S, etc.).

- Solapamiento de componentes.

Es el porcentaje de tiempo durante el cual dos o más componentes del sistema están siendo utilizados simultáneamente.

- Overhead.

Es el porcentaje de tiempo que los distintos dispositivos del sistema están siendo utilizados en áreas del sistema, no directamente imputables a ninguno de los trabajos en curso.

- Frecuencia de paginación.

Es el número de fallos de página que se producen por unidad de tiempo en un sistema de memoria virtual paginada.

- Frecuencia de swapping.

Es el número de programas sacados de memoria por unidad de tiempo a causa de falta de espacio en ella o para permitir su reorganización para recuperar espacio en ella.

Atendiendo a las mediciones realizadas sobre el comportamiento de sistema, puede ser conveniente realizar una serie de ajustes en determinados parámetros del Sistema Operativo, algunos de los que pueden modificarse con facilidad, con objeto de mejorar el comportamiento global del sistema, se detallan a continuación:

- Tamaño del quantum.

Es la cantidad de tiempo de uso ininterrumpido de la CPU que un sistema de tiempo compartido asigna a los diferentes trabajos. En ciertos sistemas no existe uno sino varios quantum para las distintas prioridades internas de los distintos trabajos, por lo que no es un solo quantum el que hay que modificar sino buscar un equilibrio adecuado entre todos ellos.

- Prioridad interna.

Es el nivel de prioridad interna que recibe un programa en función de la prioridad externa asignada.

- Tamaño de la participación de memoria.

Es la cantidad fija de memoria principal asignada a una cola de trabajo.

- Tamaño de la ventana.

Es el intervalo de tiempo durante el cual se toman medidas para determinar el conjunto de trabajos de un programa en un entorno de memoria virtual paginada que usa esa política. Evidentemente según el período de tiempo durante el que se tome medidas para determinar el conjunto de trabajos, éste varía y, por lo tanto, el valor medio del conjunto de trabajo estará afectado por los valores que intervengan en su cálculo.

- Máxima frecuencia de paginación.

Es la frecuencia máxima de fallo de página permitida, a partir de cuyo instante se efectúa la suspensión de alguno de los trabajos en curso para evitar el excesivo «overhead» que se pueda generar.

- Número de usuarios simultáneos.

Es el máximo número de usuarios de terminales permitidos por el sistema.

15. ACTIVIDADES A REALIZAR.

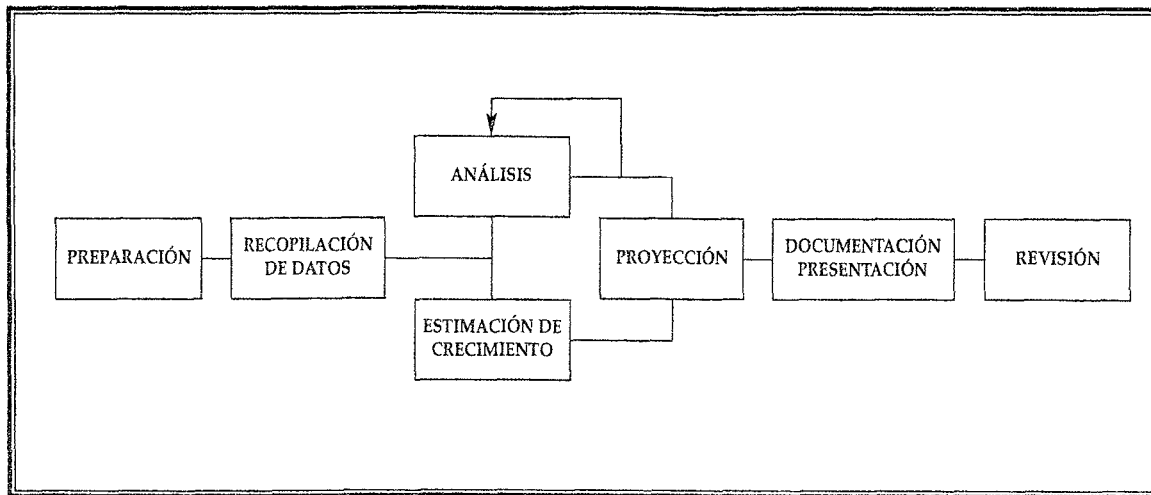
Para planificar la capacidad de un Sistema Informático se deben realizar los siguientes trabajos:

1. Análisis de la carga y capacidad actual, para lo cual es necesario hacer una recopilación de datos.
2. Análisis de la carga futura considerando el crecimiento vegetativo, los nuevos servicios, posibles contingencias, etc.
3. Proyección de la capacidad futura.
4. Identificación de diferencias o desviaciones.
5. Documentar el plan, formalizando los requerimientos de capacidad.
6. Aprobación por parte de la dirección.
7. Revisión y control del plan.

Estos trabajos se deben realizar analizando las áreas siguientes:

- Procesador central: CPU.
- Almacenamiento: Discos.
- Comunicaciones: Red de Teleproceso.

El siguiente gráfico nos muestra las distintas fases que se deben seguir:



16. METODOLOGÍAS DE PLANIFICACIÓN DE LA CAPACIDAD.

Existen diversas metodologías usadas para hacer una planificación de la capacidad de los sistemas informáticos y se pueden agrupar de la siguiente forma:

- Reglas basadas en la experiencia.
- Métodos analíticos, como son:
 - La proyección lineal.
 - La teoría de colas.
- Simulación.
- Bench-mark.

16.1. REGLAS BASADAS EN LA EXPERIENCIA.

Son reglas generales de fácil uso sacadas de la experiencia cotidiana donde el sentido común y el ojímetro tienen un papel relevante. No hay que menospreciar estas reglas, ya que como es sabido, el ámbito del ojímetro abarca leyes bien comprobadas y conocidas, como las de Murphy y Parkinson.

Generalmente están basadas en:

- La experiencia.
- Características particulares de equipos o productos.
- Mediciones efectuadas en situaciones «Típicas».

Su principal desventaja es que no son sensibles a casos particulares, pero tienen a favor, que sirven de ayuda y complementan al resto de las metodologías.

Como ejemplos de estas reglas podemos citar:

1. La utilización de una línea no debe exceder del 40 por 100.
2. La utilización de la CPU para sistemas en línea no debe exceder del 90 por 100 en horas pico.
3. Una línea puede comenzar a experimentar problemas de tiempo de respuesta cuando su utilización es mayor que el 70 por 100.

16.2. PROYECCIÓN LINEAL.

Es un método sencillo y fácil de aprender. Tiene validez matemática cuando se estima la utilización de recursos por lo que frecuentemente se usa para realiza proyecciones de CPU, sin embargo, no se puede aplicar para explicar fenómenos de comportamiento no lineal, como por ejemplo el tiempo de respuesta.

El siguiente ejemplo sirve de muestra de una proyección lineal:

En un sistema que actualmente tiene 15.000 transacciones en línea en la hora punta, con un consumo de CPU del 40 por 100, ¿cuál será la utilización de CPU para 30.000 transacciones?

SOLUCIÓN: $\% \text{ CPU} = 30.000 \times 40 / 15.000 = 80$

16.3. TEORÍA DE COLAS.

Esta metodología utiliza fórmulas matemáticas a veces complicadas. Se aplica a fenómenos de espera y requiere que estén establecidos los niveles de servicio que deben darse. Para aplicarla hay que ajustar el modelo haciendo una proyección del comportamiento pasado y actual del sistema, por lo que necesita un mayor conocimiento de las características propias del mismo, utilizando distribuciones probabilísticas (Poisson, Erlang, etc.) y determinando los factores que afectan al rendimiento.

La teoría de Colas se basa en el tiempo de servicio y el tiempo de cola de cada componente del sistema, ya que cada unidad de trabajo que se ejecuta en un sistema informática usa los componentes del mismo, por cierta cantidad de tiempo que se denomina tiempo de servicio. Cuando hay más de un usuario compartiendo el mismo recurso, se producen contenciones que son consecuencia del tiempo de espera de un usuario para poder usar un recurso que está siendo utilizado por otro. Cuanto mayor sea el tiempo de utilización de ese recurso por otros usuarios, mayor será el tiempo que tiene que esperar para poder utilizarlo el primer usuario. La cantidad de tiempo extra empleado en esperas se calcula usando un parámetro llamado factor de cola.

El tiempo que una tarea emplea en un dispositivo del sistema, ya sea usándolo o esperando utilizarlo, se denomina tiempo de respuesta del dispositivo y es calculado como el producto del tiempo de servicio por el factor de cola.

$$Tr = Ts \times Fq$$

El factor de cola no es nunca inferior a la unidad, y será mayor cuanto mayor sea la contención en el recurso. Cada recurso del sistema puede tener un factor de cola distinto, puesto que éste depende directamente del nivel de utilización del dispositivo. Para valores de utilización cercanos al 100 por 100 el factor de cola crece considerablemente, por lo que los dispositivos con alta utilización con verdaderos cuellos de botella del sistema.

16.4. SIMULACIÓN.

Esta metodología se basa en la utilización de programas para simular la realidad. Al igual que la teoría de colas es aplicable a fenómenos de espera y requiere que estén establecidos los niveles de servicio, de igual forma necesita una proyección del comportamiento del sistema. Tiene la ventaja de que puede resolver problemas complicados de teoría de colas más fácilmente, pero puede llegar a consumir gran cantidad de recursos, debido al costo imputable a los programas, que se encargan de simular una situación de carga de trabajo análoga a la esperada.

16.5. BENCH-MARK.

Es una metodología bastante frecuente para comparar diferentes sistemas informáticos frente a una carga característica de una instalación concreta que permite realizar mediciones en el ambiente real. La comparación se efectúa, básicamente, a partir del tiempo necesario para la ejecución.

Las principales dificultades que se plantean radican en determinar la carga característica y en valorar el aprovechamiento que hacen los programas de las peculiaridades de los distintos software utilizados. La preparación de un Bench-Mark requiere realizar gran cantidad de trabajo previo al comienzo del mismo y generalmente se utiliza un software especial para generar las transacciones que debe soportar el sistema.

BIBLIOGRAFÍA

- Temario de las pruebas selectivas para ingreso en el Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado. ASTIC.
- Plan de Sistemas de Información de la Junta de Castilla y León. Dirección General de Telecomunicaciones. Consejería de Fomento de la Junta de Castilla y León 1998.
- Plan de Empleo Informático de la Junta de Castilla y León. Consejería de Presidencia de la Junta de Castilla y León 1999.
- Software Engineering. Pressman, Roger S. 2001. Edition: 5.
- Master en Sistemas y Tecnologías de la Información. INAP 2001.
- Restructuring the Information Technology Organization. Keith R. Nelson and Richard W. Davenport. Central Michigan University 1995.
- Plan Director de Telecomunicaciones de la Junta de Castilla y León. Dirección General de Telecomunicaciones. Consejería de Fomento de la Junta de Castilla y León 2002.

- Curso Selectivo Cuerpo Superior de Sistemas y Tecnologías de la Información, IX promoción. INAP 2002.
- Temario de las pruebas selectivas para ingreso en el Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado. ASTIC.
- Temario de las pruebas selectivas para el acceso, por promoción interna, al Cuerpo de Gestión de Sistemas e Informática de la Administración del Estado. Ministerio para las Administraciones Públicas.
- Metodología Magerit. Ministerio para las Administraciones Públicas.
- Guía de la Seguridad de los Sistemas de Información para Directivos de las Administraciones Públicas. Ministerio para las Administraciones Públicas.
- Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades. Ministerio para las Administraciones Públicas.
- Planificación de los Sistemas de Información. Curso selectivo Cuerpo Superior de Sistemas y Tecnologías de la Información del Estado (IX promoción).



