UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

ESCUELA UNIVERSITARIA

DE

INGENIERÍA TÉCNICA DE TELECOMUNICACIONES

TRABAJO FIN DE CARRERA

- **TITULO**: *EVALUACIÓN Y DISEÑO DE UN SISTEMA REAL DE SEGURIDAD INFORMÁTICA*

- **ESPECIALIDAD**: *EQUIPOS ELECTRÓNICOS*

- **AUTOR**: *HERLINDA HERNÁNDEZ PERERA*

- **TUTOR**: *CARMEN NIEVES OJEDA GUERRA*

- **FECHA**: *MAYO 1995*

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

ESCUELA UNIVERSITARIA

DE

INGENIERÍA TÉCNICA DE TELECOMUNICACIONES

TRABAJO FIN DE CARRERA

PRESIDENTE SECRETARIO VOCAL

TUTOR AUTOR

Calificación

APROBADO (6,T)

Índice

1 - Introducción

El presente trabajo está realizado sobre el Servicio de Informática perteneciente a la Secretaría General Técnica de la Consejería de Sanidad y Asuntos Sociales de la Comunidad Autónoma Canaria.

En este estudio se pretenden analizar los aspectos que intervienen en la Seguridad de los Sistemas Informáticos en general, para luego particularizarlos para el Servicio de Informática de la Consejería de Sanidad y Asuntos Sociales.

Los tareas que se han realizado para llegar a esta presentación son:

- recopilación de información acerca del Sistema
- definir objetivos
- determinar la planificación de objetivos
- desarrollar una descripción general del entorno
- identificar áreas críticas
- evaluación de riesgos
- diseño del proyecto de mejora
- presentar el proyecto a la Dirección del Servicio

En un Sistema Informático, con el fin de asegurar la integridad de la información contenida en él, se precisa describir las directrices necesarias y los mecanismos capaces de satisfacerlas para lograr dicho fin. Dependiendo de los mecanismos utilizados y su grado de efectividad, se puede hablar de Sistemas seguros o inseguros.

Se mantienen, por su interés, algunas debilidades que en el día de hoy han sido resueltas.

La metodología utilizada en este estudio ha llevado a diferenciar las siguientes fases:

- ***FASE DE ESTUDIO DEL SISTEMA REAL:*** Se parte de un desarrollo de la descripción general del sistema. Determinando el entorno tecnológico.

- ***FASE DE DEFINICIÓN DE LAS DIRECTRICES:*** Se comienza haciendo un balance de los requerimientos y mecanismos necesarios para poseer una buena seguridad informática, tanto de los equipos como de los programas y datos.

- ***FASE DE RECONOCIMIENTO DE DEBILIDADES Y ANÁLISIS DE RIESGOS :*** Tras la revisión del estado actual de la organización existente, los procedimientos de trabajo, los controles informáticos, los controles de seguridad de acceso (físicos y lógicos), y el estado de las instalaciones, se hacen constar las debilidades encontradas. Además se intenta evaluar el riesgo que supone cada debilidad encontrada.

- ***FASE DE MECANISMOS Y ACCIONES CORRECTORAS :*** Se propone, para cada debilidad, las soluciones que se consideran más oportunas. Para abordar una solución organizada desarrollar una serie de proyectos, que atenderán a cada área estudiada.

- ***FASE DE PROPUESTA DE MEJORAS DEL SISTEMA:*** Se analizan las opciones que resulten estratégicas para el servicio. Se presentan alternativas de proyecto, que ofrecen ventajas para el desarrollo de la evolución del servicio. Se detallarán las funciones y los métodos de trabajo para incrementar la seguridad y la productividad, permitiendo una mejor gestión del departamento.

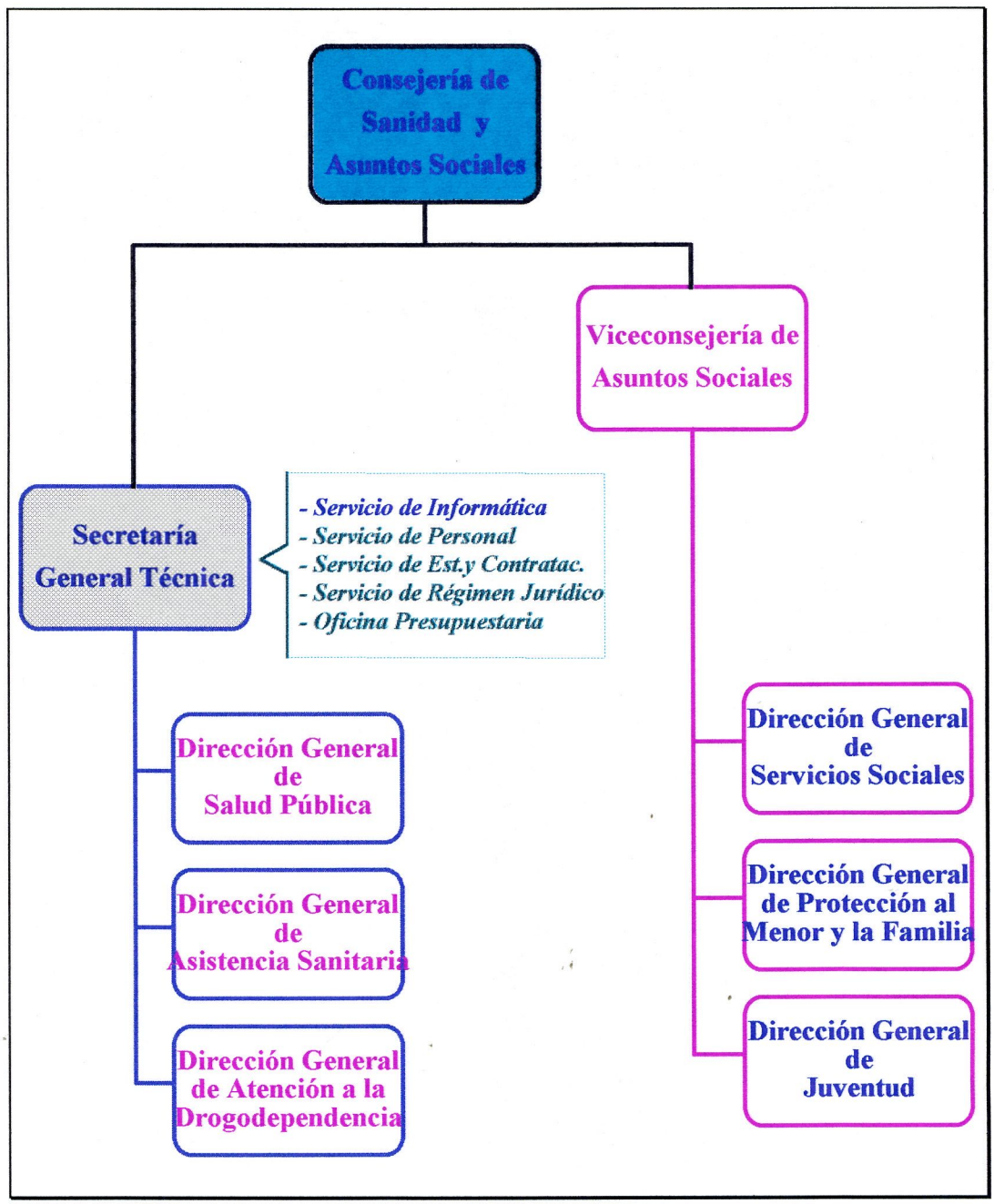
- ***FASE DE BALANCE, GRADO DE EJECUCIÓN Y PRESUPUESTO:*** Se exponen unos cuadros comparativos de las debilidades encontradas y los mecanismos o acciones correctoras, así como la valoración y el grado de prioridad recomendado. En cuanto al coste económico, se mantienen tarifas de enero del presente año, pero aún sin actualizar.

2 - Panorama General de la Infraestructura del Sistema

2.1.- DESCRIPCIÓN GEOGRÁFICA DEL SISTEMA

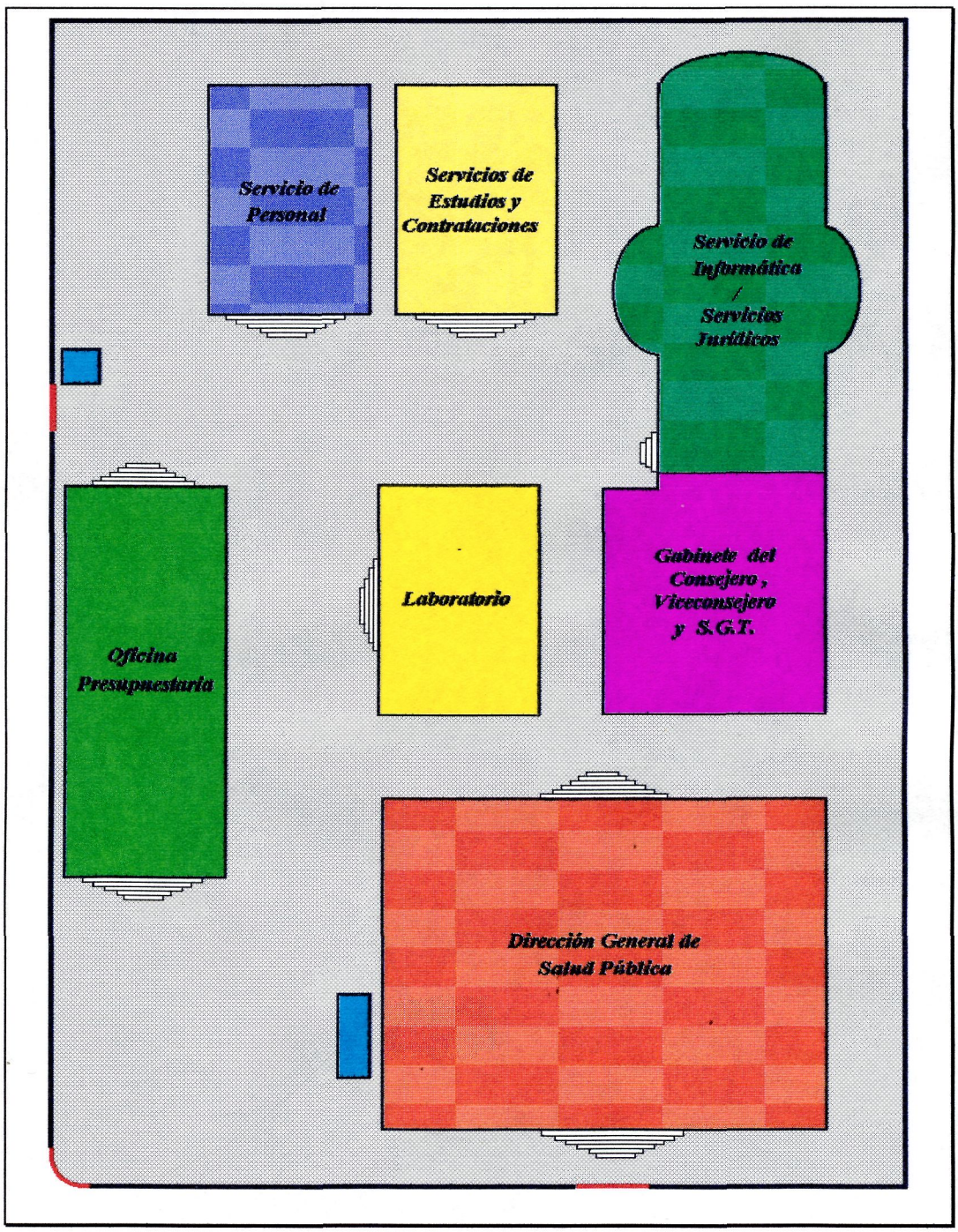
2.1.1.- DESCRIPCIÓN GENERAL

La Consejería de Sanidad y Asuntos Sociales está compuesta por los siguientes departamentos que se relacionan en el organigrama siguiente :



2.1.2.- **SITUACIÓN GENERAL**

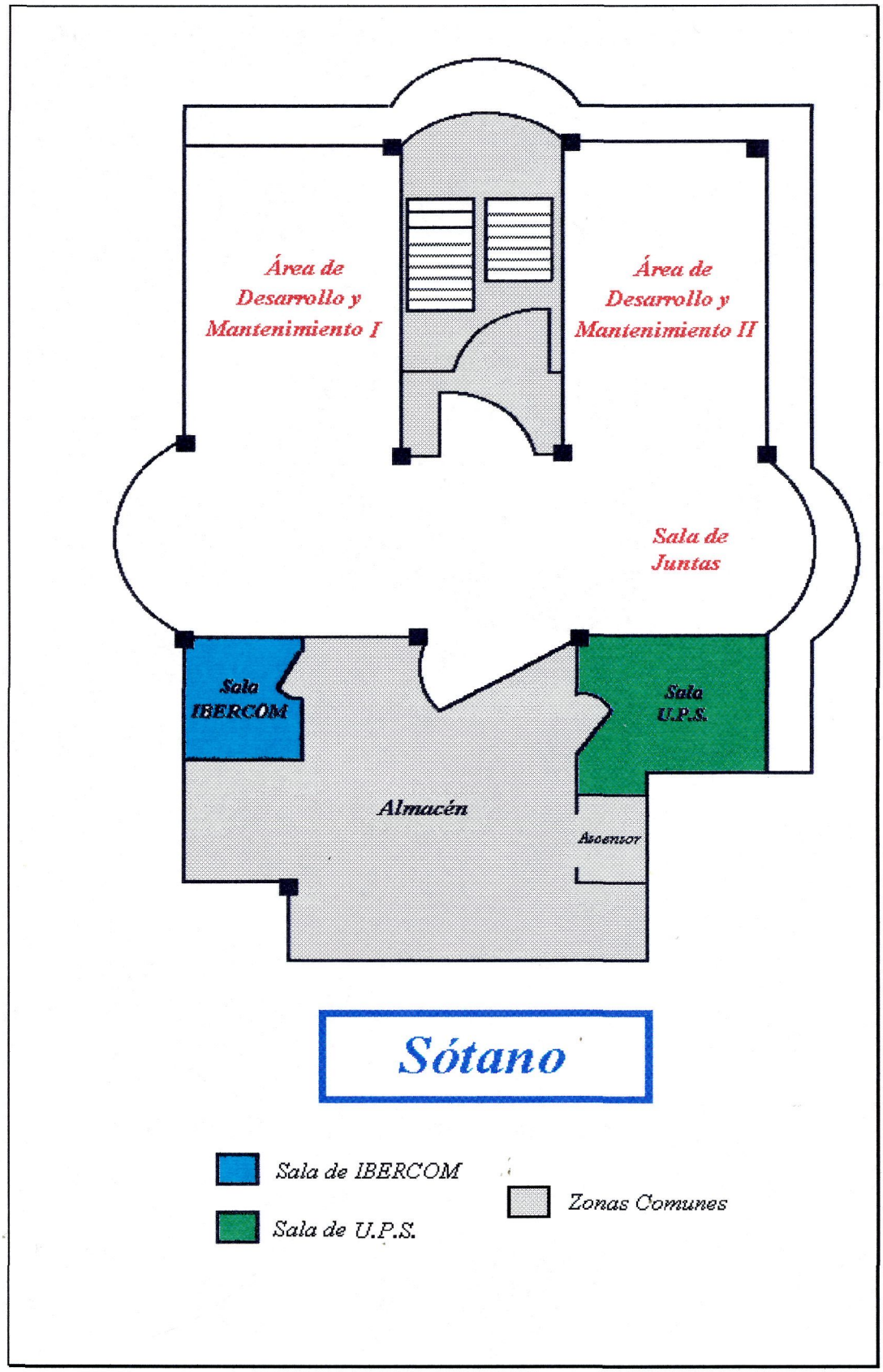
La Consejería de Sanidad y Asuntos Sociales se encuentra situada en la Rambla General Franco, 53 de Santa Cruz de Tenerife. El recinto está compuesto de la siguiente estructura :

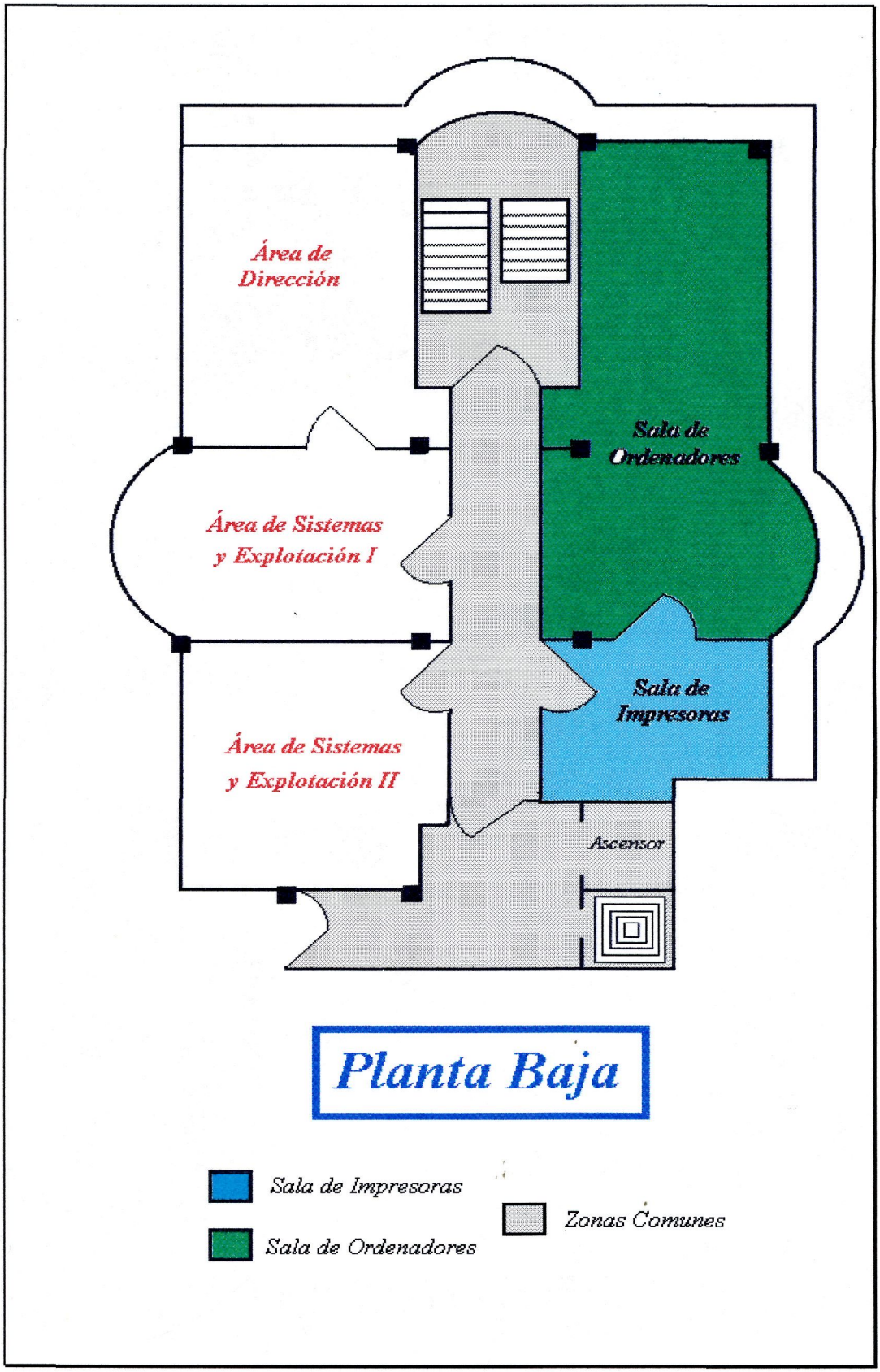


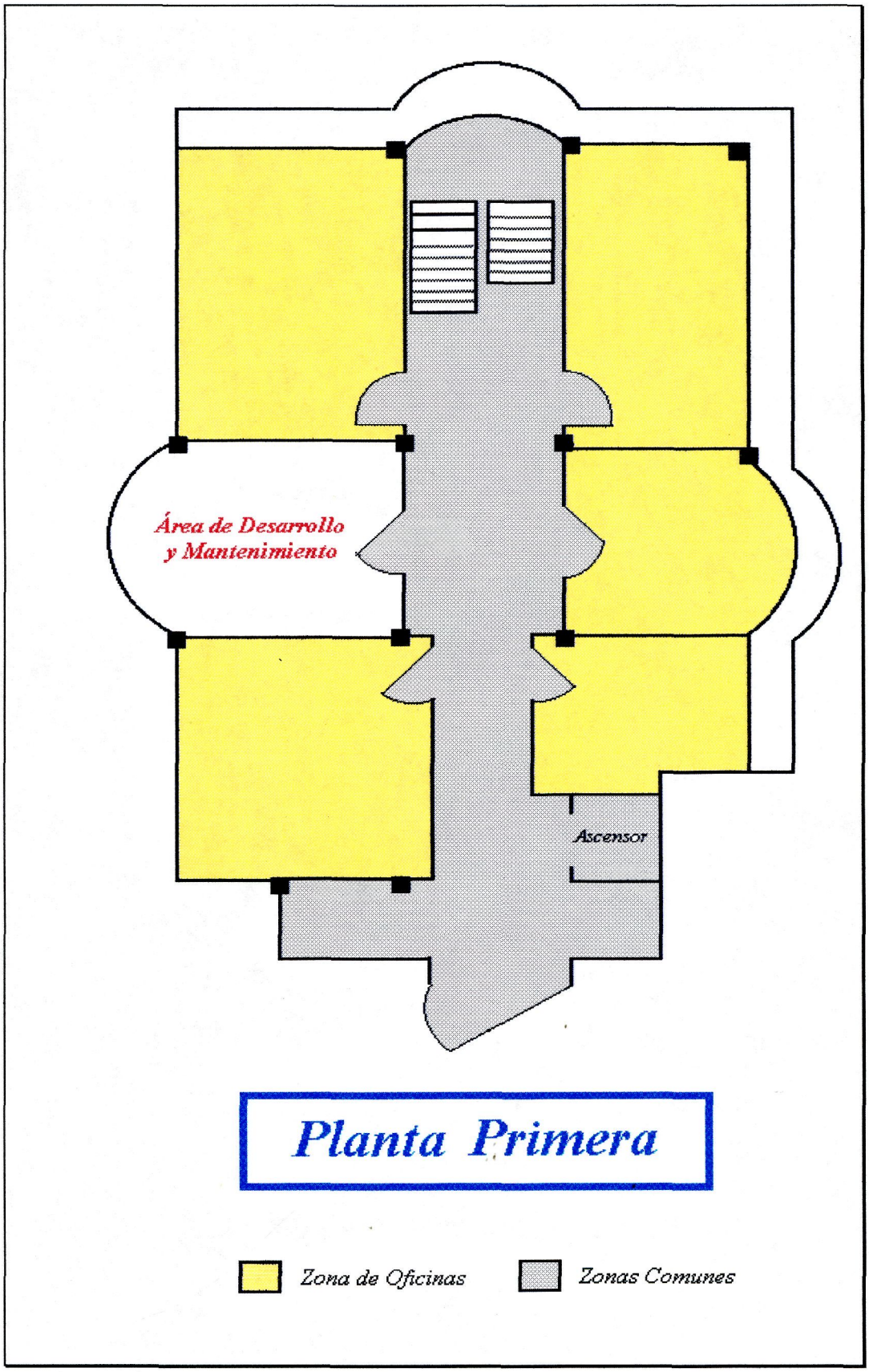
2.1.3.- SITUACIÓN DEL C.P.D. EN EL EDIFICIO

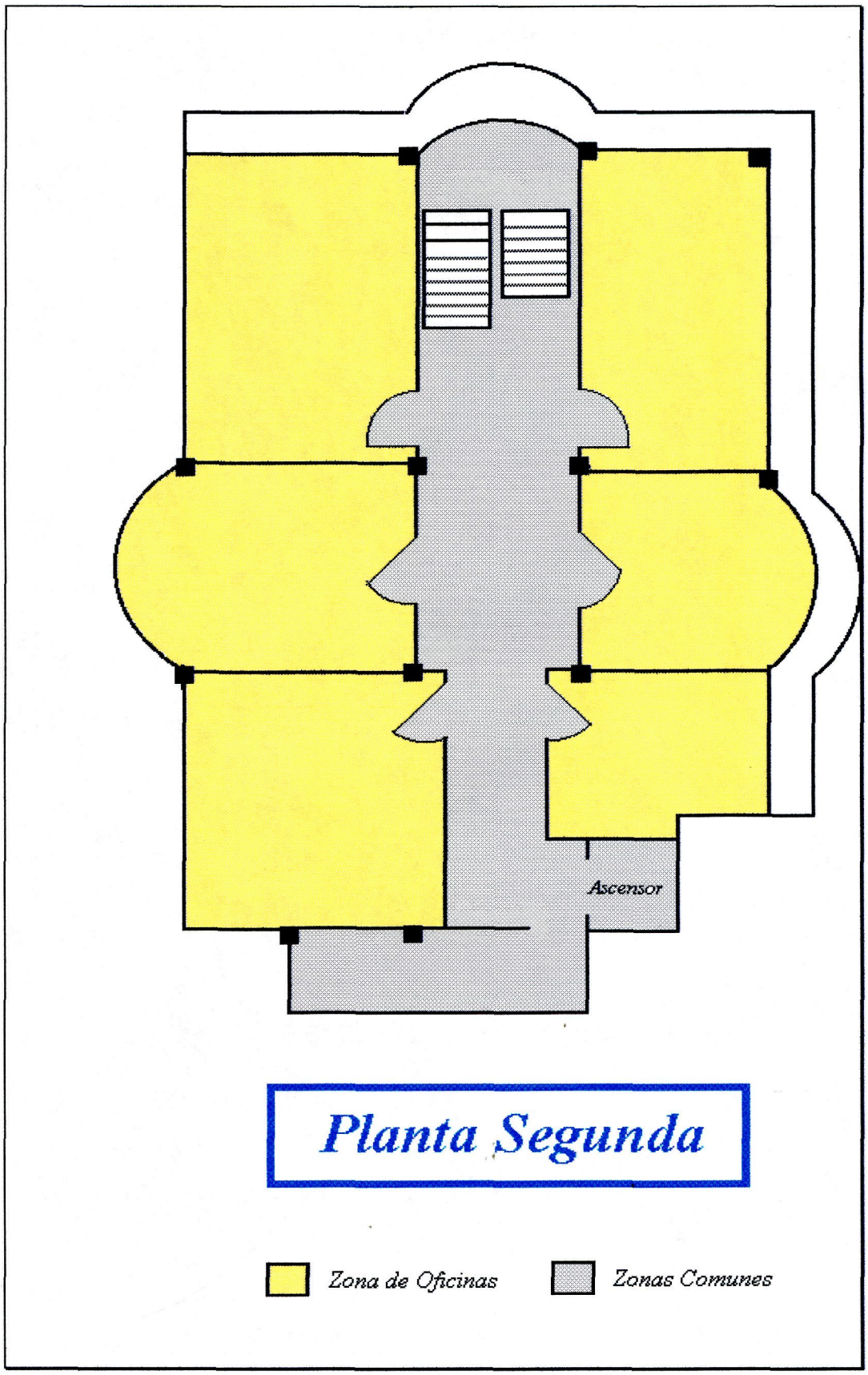
El Centro de Proceso de Datos se encuentra situado en un edificio de cuatro plantas, que comparte con otros departamentos adscritos a la Secretaría General Técnica :

- ***Sótano*** :
  - Área de Desarrollo I del Centro de Proceso de Datos
  - Área de Desarrollo II del Centro de Proceso de Datos
  - Sala de Juntas del Centro de Proceso de Datos
  - Sala de IBERCOM, perteneciente al Centro de Proceso de Datos
  - Sala de U.P.S., perteneciente al Centro de Proceso de Datos
  - Almacén, de uso común para todo el Edificio
- ***Planta Baja*** :
  - Área de Dirección del Centro de Proceso de Datos
  - Área de Sistemas y Explotación I del Centro de Proceso de Datos
  - Área de Sistemas y Explotación II del Centro de Proceso de Datos
  - Sala de Ordenadores, perteneciente al Centro de Proceso de Datos
  - Sala de Impresoras, perteneciente al Centro de Proceso de Datos
  - Gabinete del Consejero
- ***Planta Primera*** :
  - Área de Desarrollo y Mantenimiento del Centro de Proceso de Datos
  - Servicio de Régimen Jurídico
  - Dependencias del Secretario General Técnico
  - Dependencias del Viceconsejero de Asuntos Sociales
- ***Planta Segunda*** :
  - Servicio de Estudios y Contrataciones
  - Gabinete de Prensa









2.2.- GENERALIDADES DEL SISTEMA

2.2.1.- INTRODUCCIÓN

- **Procesadores IBM ES/9000 9121**

Los IBM Enterprise System/9000 (ES/9000) constituyen la gama de ordenadores más amplia ofrecida en una sola familia de procesadores. Fundamentada en las tecnologías más avanzadas de IBM y su reconocida arquitectura de sistemas, esta potente familia logra un crecimiento que se multiplica por 120 desde los sistemas más pequeños montados sobre bastidor, hasta los ordenadores para su uso general más alto de la gama.

La era abierta con los sistemas ES/9000 constituye un paso más en el compromiso adquirido por IBM de mejora continua de sus productos, incorporando avances tecnológicos significativos basados en una arquitectura ya reconocida, diseñada para lograr la integración de la empresa y proporcionar soluciones a las necesidades específicas de negocio tanto de hoy como del futuro.

- **Una plataforma homogénea y vías de crecimiento definidas**

La familia ES/9000, basada en arquitectura Enterprise Systems Architecture/390 (ESA 390) de IBM, proporciona una plataforma común para el conjunto de sus 28 modelos de procesadores. Este potencial de desarrollo sin

precedentes con vías de crecimiento claramente definidas permite una excepcional granularidad de capacidad de proceso a través de toda la familia.

Mediante la utilización de un diseño y tecnología punta, los procesadores ES/9000 introducen las ventajas de la arquitectura ESA/390 de los entornos operativos Virtual Storage Extended Extended/Enterprise System Architectura (VSE/ESA), Virtual Machine/Enterprise System Architectura (VM/ESA), Multiple Virtual Storage/Enterprise System Architectura /MVS/ESA) y Advance Interactive Executive/Enterprise Systema Architectura (AIX/ESA). Mayor rendimiento y disponibilidad son beneficios adicionales que proporciona esta familia de procesadores.

La familia ES/9000 ofrece posibilidades aún más amplias a través de un conjunto de potentes funciones opcionales, como el dispositivo de proceso vectorial, el dispositivo criptográfico integrado o la implantación de la arquitectuta Enterprise System Conection Architectura (ESCON) de IBM, basada en la utilización de tecnología de fibra óptica con velocidades de transferencia de datos de hasta 10 MB/seg, así como canales paralelos con capacidad de transferencia de hasta 4,5 MB/seg.

Estas avanzadas funciones y dispositivos están diseñadas para abrir nuevas perspectivas de desarrollo de aplicaciones.

La familia IBM ES/9000 incluye diez procesadores refrigerados por aire en armario independiente, los modelos 180, 190, 210, 260 y 320 son o no procesadores; los modelos 440 y 480 son procesadores diádicos. El modelo 490 es un multiprocesador de dos vías. El modelo 570 es un multiprocesador de tres vías

multiprocesador de tres vías y el modelo 610 es un multiprocesador de cuatro vías. Los cambios de modelo dentro de este grupo se realizan sencillamente.

Estos modelos ofrecen unas mejoras importantes en el rendimiento, por ejemplo el rendimiento del modelo 610 es casi dos veces el de un modelo 480, y más de 3,5 veces el de un modelo 320. Además, funciones avanzadas que anteriormente estaban limitadas a los modelos ES/9000 refrigerados por agua, ahora están disponibles en estos modelos ES/9000.

- **Mejoras de diseño**

La familia ES/9000 continúa nuevas dimensiones en potencial de proceso, y dispone a su empresa para un crecimiento de capacidad de proceso sin precedentes.

Las mejoras de diseño incluyen:

- Enterprise System Architecture/390
- Canales paralelos de 4,5 Mb/seg.
- Arquitectura de canal ESCON de IBM hasta 10Mb/seg.
- Mejoras específicas para VM
- Amplia memoria del procesador
- Memoria expandida de hasta 2GB
- Hasta 96 canales
- Procesor Resource/System Manager (PR/SM)
- Dispositivo vectorial
- Procesadores diádicos

- Dispositivo ESCON de Distancia Extendida (XDF)
- Función Disponibilidad del Procesador
- Protección de Memoria del Subsistema
- Multiprocesadores

Los últimos avances en tecnología y empaquetamientos son el sello de los procesadores ES/9000 refrigerados por aire (frame). Estos incluyen una fiabilidad superior, mayor disponibilidad y un servicio más sencillo, resultando todo ello en unos requerimientos ambientales menores.

- **Funciones y dispositivos avanzados**

La familia ES/9000 ofrece una completa relación de funciones avanzadas, que incluye:

ESA/390: Los usuarios de los modelos ES/9000 refrigerados por aire pueden sacar provecho de todas las capacidades del sistema operativo MVS/ESA. También soportan los sistemas operativos VSE/ESA, AIX/ESA y VM/ESA.

PR/SM: Es una función estándar de todos los procesadores ES/9000 que permite que varios sistemas operativos se ejecuten simultáneamente. Los modelos refrigerados por aire (frame) pueden crear siete particiones lógicas con un alto grado de aislamiento. PR/SM permite realizar trabajos simultáneamente, como producción, prueba y migración, en entornos separados de un mismo sistema físico.

Flexibilidad de configuración de memoria: Los modelos en frame ofrecen hasta dos gigabytes (GB) de memoria del procesador. La memoria central puede configurarse con un mínimo de 16 Mb y un máximo de 512 Mb; o hasta 2 Gb de memoria expandida a tiempo de IML (Initial Machine Load).

Opciones de canal: Los ES/9000 disponen tanto de canales ESCON como paralelos. Los canales ESCON proporciona una velocidad de transferencia de 10 MB/seg. y una distancia máxima de conexión de 9 kilómetros , o con el Dispositivo de Distancia Extendida (XDF) un máximo de 60 kilómetros; ambas opciones utiliza dos directores ESCON. La combinación de canales ESCON y/o paralelos permite conectar diferentes unidades de E/S; así como los veloces dispositivos de IBM.

Mejoras específicas: Los modelos refrigerados por aire frame ofrecen mejoras específicas para el sistema operativo VM/ESA, así como para el DB2 Sort. Estas mejoras contribuyen a mejorar el rendimiento del sistema y las aplicaciones.

Gestión multisistema: La nueva familia de procesadores ES/9000 da un importante paso hacia adelante hacia un mayor control de configuración de sistemas múltiples.

Las opciones de conexión, mejoradas con la utilización de la fibra óptica, permiten conexiones entre centros de procesos de datos, así como de sistemas situados en el mismo local.

Dentro de un centro de procesos de datos, las posibilidades de conexión mediante ESCON permiten la configuración de un complejo de sistemas (Sysplex), dando la posibilidad de realizar balances de carga y recuperación entre sistemas. Las configuraciones de sistemas múltiples que requieran una coordinación horaria extremadamente precisa, pueden utilizar la función IBM Sysplex Timer para asegurar la interconexión entre sistemas interconectados.

Función Vectorial Integrada: La función opcional de Vector proporciona un elemento de ejecución para procesar programas vectorizados. Instrucciones vectoriales nuevas mejoran el tiempo de respuesta a los usuarios finales de aplicaciones con muchas operaciones numéricas. Existen muchas aplicaciones vectorizadas disponibles que abarcan un amplio rango de soluciones técnicas y científicas.

Modelos Multiprocesador: El diseño de los nuevos modelos multiprocesador 490, 570 y 610 amplia las vías de crecimiento de la línea actual de productos 9121, y ofrece también un mayor rendimiento y disponibilidad.

Mejor diseño: Un procesador I/O independiente incorporado en todos los modelos gestiona todas las actividades relacionadas con el canal, liberando así el procesador central para realizar otras tareas y mejorando el rendimiento global del sistema.

Función de disponibilidad del procesador: En los modelos 440 a 610 esta función minimiza el impacto de muchos de los errores en el Procesador Central (CP) que anteriormente no eran recuperables en sistemas con dos o más CPs. Esto

se consigue mediante el cambio del programa en ejecución desde el CP a otro CP operativo.

Gestión de Reconfiguración Dinámica : La función de Reconfiguración dinámica en los modelos refrigerados por aire (frame) funciona en conjunción con el nivel adecuado del sistema operativo MVS/ESA para permitir la configuración dinámica del sistema I/O. Canales, unidades de control, dispositivos pueden ser añadidos o retirados sin la necesidad de power on reset e IPL (Initial Program Load). Ello significa una contribución importante a la mejora de la disponibilidad del sistema.

2.2.2.- CONCEPTOS GENERALES

• ***Medios de transmisión***

Los posibles medios de transmisión o soportes físicos para el envío de la señal se pueden clasificar en grandes grupos que son:

- **Magnéticos**: No son propiamente medios de transmisión sino un medio de almacenamiento de información (cintas, diskettes)

- **Cables**: Su materia suele ser el cobre, el aluminio o aleacciones entre ellos. El criterio más habitual para clasificarlos es el ancho de banda.

- Cable de par normal: utilizado principalmente en telefonía, para distancias cortas y bajas velocidades. Ancho de banda del orden de 10 Khz.

- Cable de par trenzado: disminuye la posibilidad de acoplo entre pares cercanos. Ancho de banda del orden de 10 Khz pero de mayor calidad que el anterior.

- Cable de par trenzado y apantallado: incorpora una malla de hilos cruzados que le protege de las radiaciones indeseadas. Permite más velocidad y más distancia. Ancho de banda del orden de 1 a 20 MHz.

- Cable coaxial: compuesto de alma central de cobre, una capa aislante y una malla metálica de apantallamiento. Existen muchos tipos en función de sus dimensiones y características mecánicas. Ancho de banda del orden de 10 y 100 Mhz.

- **La radio**: Utiliza como medio físico la atmósfera, en la zona del espectro entre los 30 Khz y los 300 Mhz. Fundamentalmente se emplea como soporte de los medios de difusión como radio y televisión. En alcances cortos hay más posibilidades al utilizar la parte alta del espectro. En comunicaciones de datos se utiliza poco. Son la base de la telefonía móvil.

- **Microondas**: Similares a la radio, pero utilizan la parte alta del espectro en la zona de 1 a 300 Ghz. Utilizan la atmósfera como medio físico y una red de antenas receptoras y transmisoras. Necesitan repetidores cada 50 Km aproximadamente y sus señales se transmiten en línea visual directa. Su mayor problema es su dependencia con las variaciones atmosféricas.

- **Satélites**: Básicamente consisten en una antena dotada de un transponedor o conversor. Reciben en una frecuencia y transmiten en otra. Para poder utilizarlos necesitan estar situados en órbitas geoestacionarias (36000 Km) y tener una separación mínima de un grado aproximadamente para no interferirse. Su número está limitado a un máximo de 360. Tiempos de propagación muy altos, del orden de 250 a 300 mseg. Cubren áreas muy extensas por lo que son idóneas para comunicaciones de difusión. Trabajan con un ancho de banda del orden de los 500Mhz para cada transponedor. Necesitan de una estación de tierra con antenas complejas.

- **Fibras ópticas**: Son conductores adecuados para la transmisión de señales con un ancho de banda correspondiente a las señales luminosas (de 10Mhz a 1000Ghz.). Son el medio de transmisión del futuro, por su gran capacidad, su inmunidad a las interferencias y su materia prima (plásticos o vidrios compuestos) que las hacen inmunes a la corrosión. La mayor dificultad radica

en adaptar las señales a esos márgenes de frecuencia, que se hace a partir de diodos led o láser. Su utilización es cada vez mayor como sistema de enlace en las redes básicas de transporte.

- ***Cable Coaxial de Banda Base***

El cable coaxial se usa frecuentemente en la red de telefónica, en aplicaciones que requieren prestaciones muy similares a las de una red de área local.

Hay dos tipos de cables coaxiales: el de banda base y el de banda ancha. Aunque están construidos de forma similar, en instalación y aplicación son diferentes.

En el caso de banda base, el hilo conductor central está rodeado de una malla muy fina de hilos de cobre. El espacio que queda entre el hilo y la malla está aislado para separar los dos conductores y mantienen las propiedades eléctricas. Todo el cables está cubierto por un aislamiento de protección para reducir las emisiones eléctricas.

El cable tiene un diámetro aproximado de 0,94 mm.

El cable transporta una sola serial digital a una velocidad de transmisión muy alta, de 10 a 12 megabytes por segundo. La frecuencia de transmisión es relativamente baja. Los bits se ponen directamente en el cable sin modulación alguna.

Para convertir un cable en una red hacen falta los siguientes dispositivos:

1) Transceptores: Unidades de interfaz de la red que proporcionan la inteligencia necesaria para leer las direcciones de un mensaje y para otras funciones orientadas a la red.

2) Derivadores de cable: Conectan el cable de transceptor al cable principal.

3) Repetidores: Amplifican la señal a medida que los mensajes pasan de una sección del cable a otra.

El cable principal de la red se instala dentro de un portacables, que a su vez se puede instalar bajo el suelo, dentro de las paredes o en el techo. Se dejan tomas en cada oficina para facilitar la conexión de estaciones de la red.

Las características de las redes de cable coaxial de banda base son:

- *Restricciones de aplicación:* La mayoría de las redes de cable coaxial de banda base limitan la distancia entre estaciones y el número de éstas.

-*Topologia:* Se usa frecuentemente para redes dispuestas en bus.

- *Fiabilidad:* Se puede calificar entre bueno y excelente.

- *Vulnerabilidad*: El cable en sí es bastante fuerte y resistente.

- *Posibilidad de interfases*: Es sensible a los ruidos. No es recomendable para instalaciones donde se producen niveles muy altos de interferencias eléctricas.

- *Seguridad*: La seguridad es un grave problema, porque el cable puede actuar como una antena, emitiendo señales constantemente, lo que permite la recepción no autorizada de las señales. La señal interferida puede interferir en sistemas de radiodifusión, televisión, etc.., que se encuentren cerca de la red.

- ***Velocidad de transmisión***

Existen tres tipos de velocidad diferentes:

-Velocidad de modulación: es el número de estados de la señal eléctrica en la unidad de tiempo. Se mide en Baudios por segundo y está ligada totalmente a las características del canal y a la técnica modulada empleada.

-Velocidad de transmisión de información: mide el número de bits por segundo que pasan a través del canal. La relación con los Baudios dependerá del número de estados diferentes que soporte la señal eléctrica portadora.

Bits por segundo = N x Baudios por seg.

(N = logarítmo en base 2 del núm. posibles de estados de la señal)

-Velocidad de transferencia de información: es el número de bits útiles, descontando errores y redundancia, que son capaces de pasar a través del canal. El objetivo último de un sistema de comunicaciones debe ser el maximizar esta velocidad.

- ***Tipos de señales***

Al tratar con la información lo primero que se hace es convertirla en "señal" para transmitirla a través del canal de comunicaciones. La señal se clasifica en dos grandes grupos en función de su valor en el tiempo:

- Señales analógicas: tienen en el tiempo una forma continua análoga al proceso que tratan de representar (el sonido, la voz, la imagen..)

- Señales digitales: en el tiempo tienen una forma discontinua y se basan normalmente en un código o conjunto finito de símbolos (información escrita, los datos numéricos...).

- ***Adaptación de la señal al medio***

Dado que las señales pueden ser analógicas o digitales, no siempre coincide el tipo de señal con el canal de transmisión, en estos casos es necesario realizar una modificación o adaptación de una al otro. Se presentan cuatro casos:

- Conversión analógica a analógica: necesaria por ejemplo para aprovechar el ancho de banda de los canales telefónicos. Se conoce como Modulación y la realizan los Moduladores.

- Conversión analógica a digital: necesaria por ejemplo para el envío de voz por un canal digital. Se conoce como Digitalización o Codificación y la realizan los Codec.

- Conversión digital a analógica: necesaria por ejemplo para el envío de datos por un canal telefónico. Se conoce como Modulación y la realizan los Modems.

- Conversión digital a digital: necesaria para acceso a canales digitales. Se conoce como Adaptación o Conversión de protocolo y la realizan los Adaptadores o Conversores.

- ***Modems***

Son los elementos frontera o interfaz entre el equipo de datos y la red. La parte del equipo informático que se conecta al modem recibe el nombre de ETD (equipo terminal de datos), mientras que el modem se conoce como ETCD o ECD (equipo terminal de circuito de datos).

La función que les da el nombre es la Modulación, introducir en el canal una señal alterna, que se llama "Portadora", a la que se modifica algunos de sus parámetros (amplitud, frecuencia o fase) de acuerdo con la señal de datos.

Son dispositivos que han ido evolucionando mucho a lo largo del tiempo, presentando una gran variedad de nuevas funciones como son:

- funciones de marcación, almacenamiento de números de teléfono y respuesta automática

- funciones de corrección de errores y sistemas de transmisión sofisticados

- control y adaptación a la calidad de la línea siendo capaces de variar su velocidad, de acuerdo a la calidad en tiempo real

- permite la gestión de líneas múltiples en un sólo enlace

- ***Concentrador***

Es un equipo que comparte varios canales de entrada mediante un programa, que adjudica todo el canal de salida, a uno de entrada, bajo demanda del usuario.

- ***Control de línea***

Es el conjunto de procedimientos operativos, comandos y señales de control que permiten a un sistema de comunicaciones gestionar la transmisión, en series de bits, en un canal de comunicaciones.

- ***Servicio***

Comunicación entre capas de distinto nivel.

- ***Protocolo***

Conjunto de reglas sintácticas y semánticas que determinan el comportamiento de unidades funcionales en el establecimiento de la comunicación. Se emplea en la comunicación entre dos capas pares remotas.

- ***Red de comunicación***

Conjunto organizado de recursos (nodos, enlaces, terminales) que permiten la interconexión de usuarios remotos para el intercambio de información.

- Nodos: elementos de conmutación y encaminamiento
- Enlaces: canales de comunicación entre nodos
- Terminales: elementos que dan entrada a los usuarios finales

- ***Red de Comunicación de Datos (RCD)***

Enfocada a la transmisión de información entre equipos informáticos, dando lugar a un diálogo entre ellos y al acceso a recursos informáticos desde localizaciones remotas.

Se pueden clasificar en:

- Redes WAN (Wide Area Network): Redes de Área Extensa. Tienen una cobertura ilimitada en distancia. Cubren las necesidades de acceso remoto a host centrales desde cualquier localización geográfica. Emplean habitualmente, los servicios de las redes telefónicas, al ser estas de cobertura mundial.

- Redes MAN (Metropolitan Area Network): Redes de Área Metropolitana. Son de reciente aparición. Dan una cobertura entre 3 y 50 Km, enmarcándose su ámbito en campus, complejos industriales o áreas metropolitanas.

- Redes LAN (Local Area Network): Redes de Área Local. Son de reciente difusión, a raíz de la aparición de los ordenadores personales. Aunque fueron

concebidas para la comunicación entre PCs, su versatilidad y potencia las ha convertido en redes nativas para todo tipo de procesadores. Abarcan distancias desde 1 m hasta unos 3 Km, posibilitando la conexión rápida y flexible de cualquier tipo de equipo informático.

Entre las características que poseen destacan:

- Alta velocidad
- Medio de transmisión común y uniforme
- Comunicación directa entre cualquier par de nodos
- Simplificación de cambios

Hay tres maneras de ampliar una LAN:

- *REPETIDORES*: Conexión a nivel físico en el mismo segmento. Ayuda para limitación de distancias en un segmento.

- *BRIDGES*: Conexión a nivel MAC, entre dos segmentos. Ayuda para limitación de distancias, de número de nodos, y en caso de carga de la red local.

-*GATEWAYS*: Conexión a nivel presentación, entre redes distintas. Conversión de protocolos y reformateo de tramas.

- ***Arquitectura de Comunicaciones***

Es un conjunto de reglas que gobierna la interconexión e interacción de los componentes de un sistema. Existen dos tipos de arquitecturas:

- Arquitecturas propietarias: creadas por fabricantes y que tienen como característica principal el afrontar problemas de comunicación concreto. Son, en general, incompatibles entre sí. Tienen una dependencia bastante fuerte con el hardware del fabricante concreto.

Ejemplos: SNA de IBM
DNA de Digital

- Arquitecturas estándares: definidas por organismos internacionales y que tienen como característica principal el estar destinadas a romper el aislamiento de las distintas marcas de fabricantes. No dependen en absoluto de un hardware en concreto.

Ejemplo: OSI definida por la Organización Internacional de Estandarización (ISO), es la más importante

NOTA: Las normas OSI (Open Sistems Interconnection) consisten en un modelo en siete niveles o categorías, que garantiza una comunicación eficiente dentro de una red de área local y entre redes diferentes. Cada uno de los niveles está destinado a proveer un servicio para el nivel inmediatamente superior.

La Organización Internacional de Normalización ISO (International Standars Organization) ha desarrollado unas normas para interconexión de sistemas abiertos (OSI).

Conceptos de esta arquitectura:

- USUARIO FINAL: Todos aquellos que sean origen o destino de información. No son conocidos por la red.

- UNIDAD LÓGICA (LU): Son los intérpretes o intermediarios entre la red y los usuarios finales. Estarán situadas allí donde estos vayan a acceder a la red. Una de las características más importantes de las LUs es la exclusividad de su nombre y dirección en la red. Se implanta por medio de software.

- UNIDAD FÍSICA (UF): Para posibilitar el manejo de los componentes físicos de la red SNA en cada una de las máquinas que la forman se define un elemento que se encarga de controlar los recursos de la máquina, denominada PU. Tienen dirección exclusiva en la red. Se implanta por medio de software.

- SYSTEM SERVICES CONTROL POINT (SSCP): Está situado en el procesador central con la función de coordinar y controlar el funcionamiento de toda la red definida. Está situado en la cúspide de la estructura de la red SNA, centralizando toda la gestión y operación de la red.

- SESIONES: Tanto el funcionamiento interno de la red como la transmisión de datos entre usuarios finales se realizan por medio de conexiones lógicas temporales, entre los correspondientes elementos de la red (SSCP, PU, LU). Estas conexiones se denominan SESIONES y

posibilitan el diálogo entre los recursos que las establecen. Existen dos tipos de sesiones:

- *Sesiones de Servicio*: necesarias para el funcionamiento de la red.
  - Sesiones SSCP-PU
  - Sesiones SSCP-LU

- *Sesiones de Trabajo*: para intercambio de información entre usuarios finales.
  - Sesiones LU-LU

- SUBÁREAS: Partes en que está dividida la red SNA. Estas partes constan de un procesador central, o host, o controlador de comunicaciones junto con los controladores de terminales que de ellos dependan. Cada subárea tiene definido un número único en la red, lo que permite crear un esquema de direccionamiento para identificar de forma unívoca cualquier punto de la red.

- DIRECCIONES: Con base en la división de la red en subáreas se construye el direccionamiento de la red SNA. Cada elemento (PU o LU) tiene un número exclusivo dentro de su subárea, que unido a la exclusividad del número de subárea, hace que la dirección de red sea única.

- RUTAS: Es el camino a través de la red. Una ruta en SNA está definida entre subáreas, y se basa en tres conceptos:

Grupo de Transmisión (GT): define un grupo de líneas entre dos máquinas adyacentes como un sólo enlace lógico.

Ruta Explícita (ER): define un camino físico unidireccional entre dos máquinas dadas, adyacentes o no.

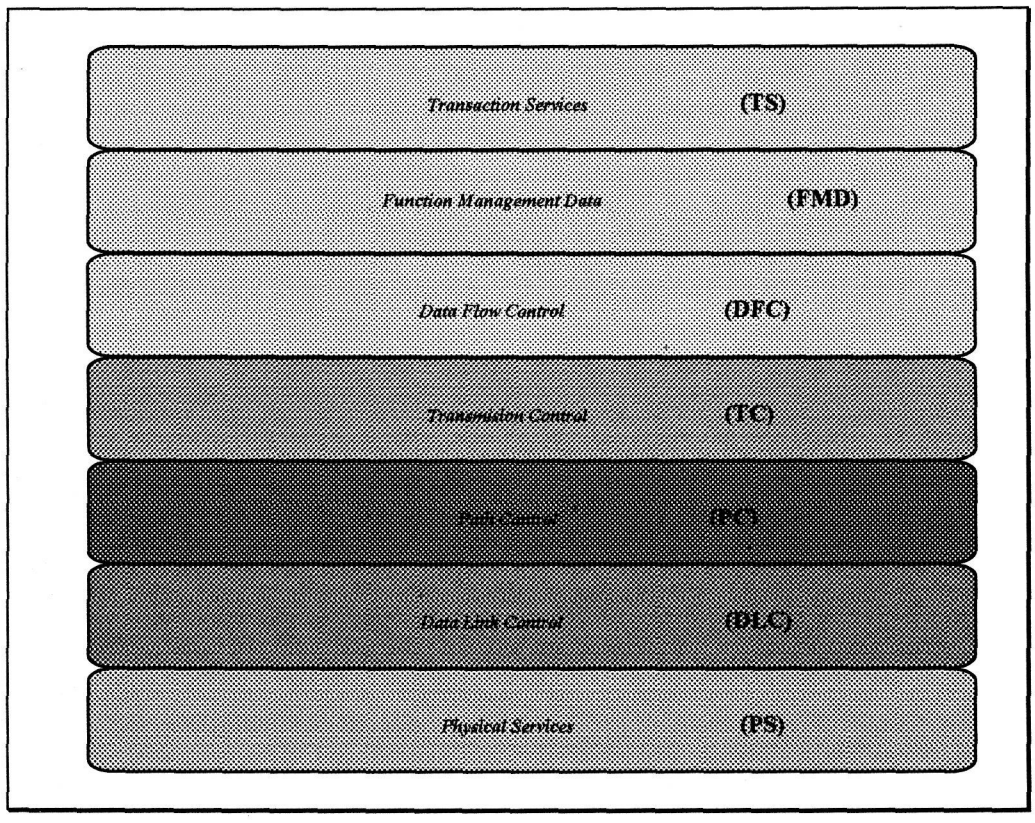
Ruta Virtual (VR): define un camino lógico entre dos máquinas, adyacentes o no, junto con una prioridad de tráfico y un mecanismo de control de flujo.

- MENSAJES/NIVELES: El flujo de información en una red SNA se estructura en mensajes que son de dos clases:

Peticiones: Contienen datos de usuario final o comandos de red.

Respuestas: Son mensajes de reconocimiento de una petición.

La arquitectura SNA define una estructura jerárquica consistente en siete niveles. Cada nivel cumple con una función específica.

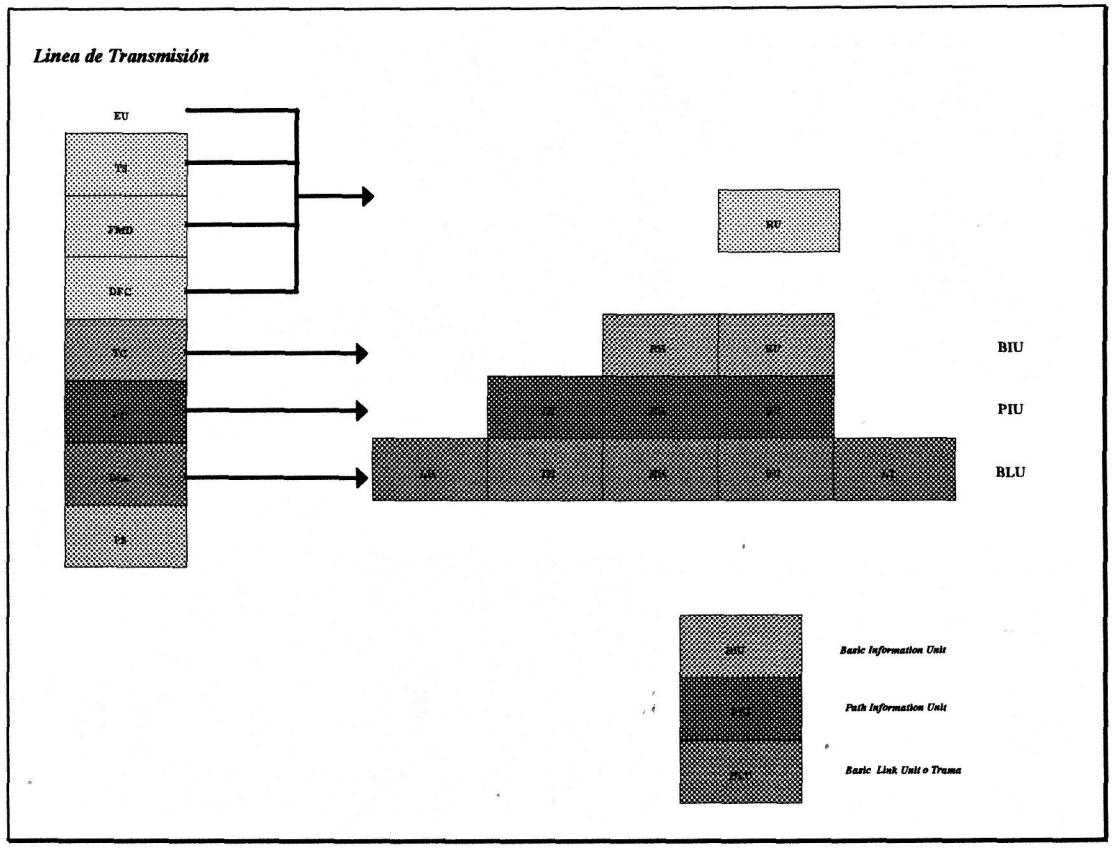


Para que estos mensajes se puedan transmitir en la red, será necesario emplear una información de control adicional a medida que sea necesaria. Esta información de control se estructura en:

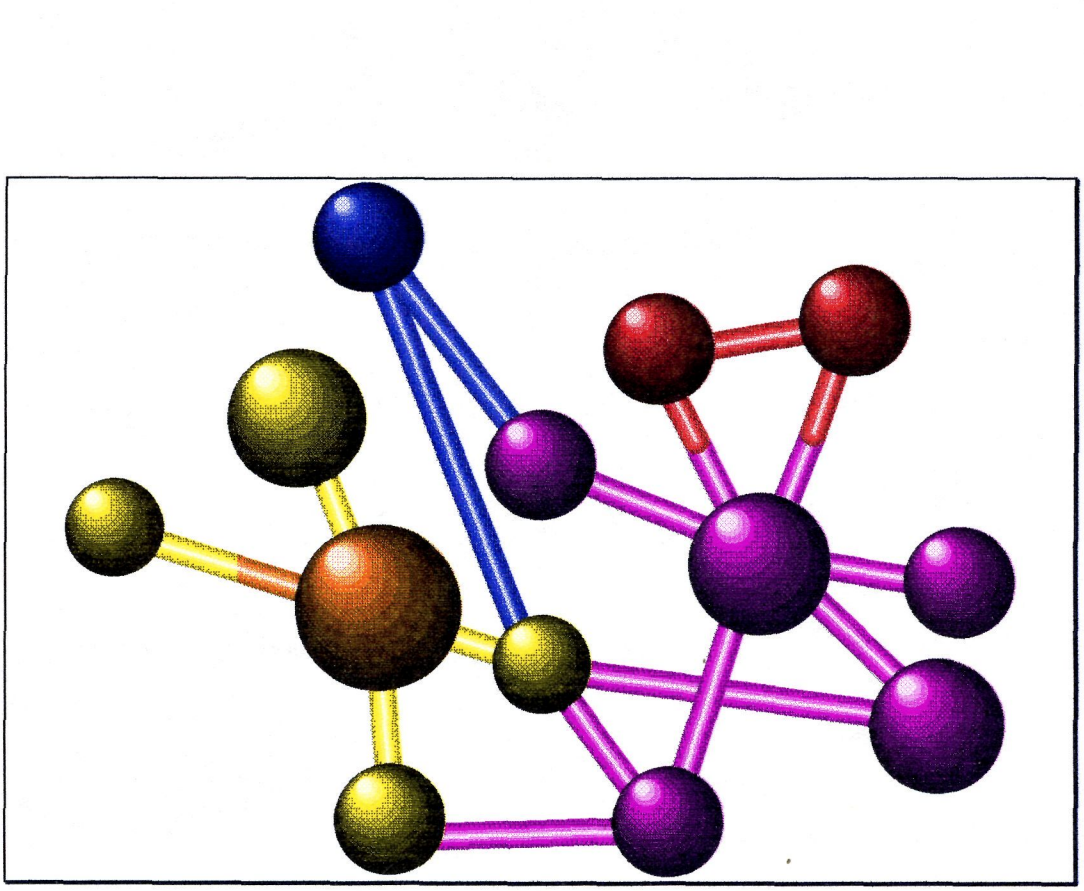
- Request/Response Header (RH)

- Transmission Header (TH)

- Link Header y Link Tailer (LH y LT)



Recientemente, IBM ha sustituido cinco programas de gestión de red residentes en el SNA, por un solo programa nuevo, el NetView. Este proporciona un sistema centralizado de gestión que realiza diagnósticos en protocolos de SNA, sesiones de comunicación, y procedimientos de contabilidad de red. También presenta visualmente las alertas de diagnóstico de la red, y determina los fallos de componentes de la misma. El NetView puede monitorizar también el tráfico X.25 en el entorno SNA. Un nuevo programa de IBM, el X.25 SNA Interconnection, permite a las redes SNA transportar datos con arreglo a los protocolos X.25 de conmutación de paquetes.



- ***Red ETHERNET***

Es una de las redes locales más conocidas y populares, desarrollada por XEROX.

Las estaciones de la red ETHERNET están conectados por un cable coaxial de banda base utilizando el protocolo CSMA/CD.

CSMA/CD: Es un método de contienda (protocolo). Método de acceso a la línea basado en que el primero que llega es el primero que la utiliza. Protocolo de acceso múltiple por detección de portadora con detección de colisiones. Establece las normas para cuando dos personas comienzan a hablar al mismo tiempo. Las dos dejan de conversar y esperan a que la otra continúe hablando, la primera que comience a hablar será la que tenga la palabra.

Además de saber si alguien está utilizando el canal antes de comenzar a transmitir, se comprueba si se ha producido una colisión, y si es así, se detiene la transmisión. El mensaje se vuelve a emitir al cabo de unos instantes.

Puesto que la estación comprueba si la línea está libre antes de y durante la transmisión, el número de colisiones es relativamente bajo y, por tanto, el rendimiento es mayor.

Como en todos los métodos de contienda, el canal es un medio de transmisión sin control central. El acceso al canal está controlado por las propias estaciones.

Las estaciones se conectan a la línea principal por medio de un módulo interfaz de red. El interfaz se encarga de dar formato a los mensajes y de transmitirlos. Estos se presentan en paquetes de longitud fija, en los cuales están contenidos los datos de las estaciones emisora y receptora, además de otra información. El tamaño del paquete está compuesto de 256 bytes, aunque las especificaciones técnicas permitan paquetes que van desde 72 byte hasta 1256 bytes.

Las estaciones contienen mecanismos de reconocimiento de dirección, que se usan para identicar y aceptar los paquetes. Todas las estaciones tienen asignadas una dirección de 48 bytes. Por tanto, cuando se cambia una estación de un lugar a otro de la red,. se pueden reconfigurar completamente con un mínimo de cambios en el sistema operativo.

Los datos se transmiten a una velocidad de 10 megabytes por segundo a una distancia máxima de dos kilómetros y medio. En una red que cubra una distancia de 500 m, no se pueden conectar más de 100 estaciones.

La red Ethernet se utiliza ampliamente debido a su alto grado de eficacia, que ronda el 97 por ciento, como a la amplia gama de productos comerciales que son incorporables a la red. Buena muestra de ellos son los productos que permiten en la actualidad el uso del sistema operativo UNIX directamente en la red y el anuncio de que se dispondrá de interfaces X.25 y SNA lo que permitirá su interfuncionamiento con redes públicas de paquetes y con la red de IBM.

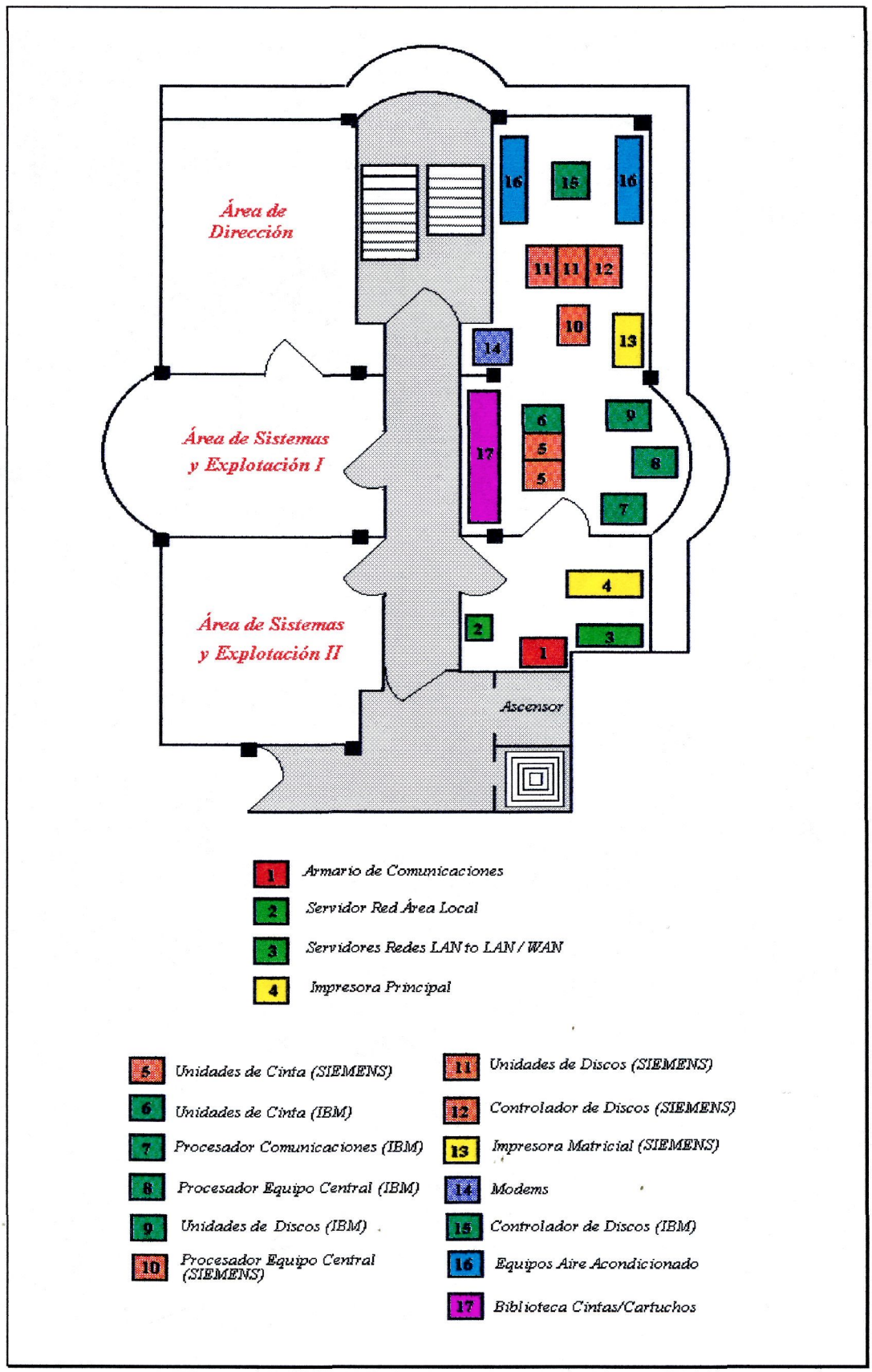
2.2.3.- CARACTERÍSTICAS GENERALES

El sistema es un IBM de la familia ES/9000. La configuración existente se basa en:

- 1 procesador del equipo central ES/9121 modelo 190 de 8 MIPS de potencia con 64 MB de memoria central ampliables a 512 MB
- 2 unidades de disco 9345-B22 con una capacidad de 3 GB cada uno
- 2 unidades de disco 9345-B12 con 2 GB cada uno
- 1 unidad de cinta 3490-C11, con cargador automático de cartuchos y dispositivo de compresión de datos
- 1 impresora principal 3825 modelo láser con velocidad de impresión de hasta 58 ipm
- 2 procesadores de comunicaciones 3745 preparados para conexión de 8 líneas de hasta 19.200 bps y una línea de 64 kbps
- una red Ethernet por provincia (S/C de Tenerife y Las Palmas)
- 1 servidor de comunicaciones (Gateway) bajo OS/2 en cada provincia
- 15 ordenadores personales para tareas de terminal y servidor de comunicaciones

- 195 ordenadores personales para uso como terminal
- 22 impresoras matriciales
- 69 impresoras láser para conexión a los ordenadores personales
- 2 Sistemas Operativos:
  - VM/ESA
  - AIX/ESA
- un Gestor de Base de Datos ADABAS de Software A.G.
- una Herramienta de Desarrollo que es el lenguaje de programación de cuarta generación NATURAL
- Cableado PDS 1061 de AT&T
- tomas normalizadas RJ-45 para voz y datos
- UPS

A continuación se muestra el gráfico de la distribución de los equipos dentro de la sala de ordenadores, especificando cada uno de ellos:



2.3.- ORDENADOR CENTRAL

2.3.1.- PROCESADOR DEL EQUIPO CENTRAL

La configuración de base es un sistema ES / 9121 modelo 190 de 8 MIPS de potencia con 64 MB de memoria central ampliables a 512 MB.

Forma parte de la familia ES/9000, por lo que soportan la arquitectura ESA/390 que incorpora las últimas innovaciones en utilización de memoria, conectividad y cálculo técnico. Bajo esta arquitectura, se puede trabajar en diversos entornos operativos como MVS/ESA, VM/ESA, VSE/ESA, o el más reciente AIX/ESA. Esta riqueza de entornos puede coexistir simultáneamente en una misma máquina mediante la función estándar PR/SM, que también permite trabajar con sistemas operativos S/36 y XA.

La arquitectura ESCON está basada en tecnología de fibra óptica y la soportan todos los modelos de la familia ES/9000, y por tanto los modelos 9121. Ofrece velocidades de transferencia de hasta 10 MB/s y distancias de conexión de hasta 9 Km, ó 60 Km con ESCON XDF que se basa en un interfaz láser con fibra monomodo. Además ESCON ofrece una nueva visión en la gestión de los recursos de entrada/salida de la empresa, permitiendo cambios sencillos de las configuraciones.

Los procesadores 9121 ofrecen mayores rendimientos y aportan nuevas funciones como PS/SM, canal ESCON, canal paralelo 4,5 MB/s y vector.

La memoria instalada varía desde 64 MB hasta 2048 MB. Parte de la memoria instalada puede ser utilizada como memoria expandida. Esta mejora el tiempo utilizado en operaciones de E/S y CPU. Se pueden obtener beneficios económicos mediante la inversión en memoria expandida pues ésta retrasa en el tiempo la necesidad de cambio a un modelo más potente.

La porción de memoria instalada dedicada a memoria central se realiza a tiempo de IML. Los valores posibles son 16 MB, 48 MB, 64 MB, 96 MB, 128 MB, 192 MB y 256 MB. La diferencia entre memoria instalada y memoria central se dedica automáticamente como memoria expandida.

La arquitectura ESA/390 está diseñada para trabajar con grandes cantidades de datos almacenados eficientemente en diversos soportes físicos, El HSB (High Speed Buffer) proporciona datos al procesador a gran velocidad.

La arquitectura ESA/390 junto a los procesadores ES/9000 9121 permiten realizar inversiones balanceadas en recursos de CPU, memoria central / expandida y DASD, ofreciendo una gestión transparente al usuario.

La arquitectura ESA ofrece los espacios de datos y los hiperespacios. Un espacio de datos puede alcanzar 2 GB y sólo contiene datos. Su ventaja reside en el uso eficiente y transparente del soporte físico (central, expandida, DASD) y la facilidad de acceso común por programas en distintos espacios de direcciones.

Los espacios de datos pueden verse como una extensión de los espacios de direcciones, en los que se restringe su uso a datos y no programas, y se facilita el acceso a ellos desde múltiples espacios de direcciones.

Los hiperespacios alcanzan también los 2 GB y sólo contienen datos. Se diferencian de los espacios de datos en que su soporte físico es memoria expandida y DASD, y no memoria central.

Modelo refrigerado por aire.

El volumen de transacciones/minuto soportado por este modelo es de:

- 820 tr / minuto simples (validaciones de tarjeta de crédito)
- 405 tr / minuto medias (apunte en c.c.)
- 90 tr / minuto complejas (reserva aérea)

El procesador 9121 trae un programa para la definición de unidades de entrada/salida llamado IOCP (Input/Output Configuration Program).

Incorpora un sistema integrado (IOSP) de ayuda al diagnóstico, tanto local como remoto mediante el Remote Support Facility (RSF), que incluye una tarjeta adaptadora multiprotocolo a la que se conectan la pantalla monocroma IBM 8503, el modem IBM 5853 y opcionalmente hasta cuatro terminales IBM 3151 y dos impresoras proprinter 4201/4202.

Los canales son asignados a cada partición lógica de modo exclusivo por lo que no pueden ser compartidos. La comunicación entre particiones lógicas puede realizarse mediante DASD compartidos, CTC ya sea mediante IBM 3088 o directa con canales ESCON, o conexión VTAM mediante IBM 37xx.

La función de protección de memoria del subsistema es una función de hardware. Esta función permite que la zona de código y bloques de control del

subsistema posea una clave de memoria diferente a la zona de aplicaciones de usuarios. Mediante esta función se mejora la disponibilidad del sistema impidiendo que aplicaciones con fallos de programación lleven abajop el sistema. Además se facilita la detección del problema en la aplicación mejorando así la productividad.

2.3.2.- UNIDADES DE DISCO

El subsistema de discos IBM 9340 está formado por elementos de almacenamiento montados en bastidor que ofrecen rendimiento, capacidad de crecimiento granular y una significativa reducción en la superficie ocupada por la máquina.

El IBM 9340 presenta considerables ahorros en costes operativos comparando con los productos anteriores de IBM. Usando avances tecnológicos como un nuevo y más pequeño conjunto de discos y cabezas de lectura (Head Disk Assembly HDA), circuitos de tecnología avanzada y empaquetamiento de los componentes mejorado. El subsistema 9340 está diseñado para mejorar su fiabilidad, disponibilidad y mantenimiento para conseguir un entorno de operación continuada.

El subsistema 9340 se compone de o bien un módulo de unidad de control 9341 y módulos de disco 9345 montados en un bastidor 9309, o bien de una unidad de control 9343 con módulos de disco 9345 montados en su propio bastidor.

El módulo de discos 9345 utiliza platos de 5,25 pulgadas montados en un HDA (subconjunto de platos, cabeza de lectura/grabación y mecanismos de acceso), de gran capacidad y poca demora de rotación.

La alta densidad de grabación y la rápida velocidad de rotación de los discos 9345 reducen el tiempo de latencia e incrementan la velocidad de transferencia del dispositivo al buffer a 4,4 MB/seg.

Se disponen de dos unidades de disco 9345-B22 con una capacidad de 3G cada uno y dos unidades 9345-B12 con 2G cada uno. La capacidad total es de 10G. El controlador de los discos IBM 9343-CO2 es un dispositivo independiente de estos, con dos vías de acceso para conexión al procesador por canales independientes.

2.3.3.- UNIDADES DE CINTA

El subsistema de cintas magnéticas 3490E modelos C10, C11 y C22, forman parte de la familia de 3490E, y están diseñadas para aumentar significativamente el rendimiento y la capacidad del cartucho.

Nota: la letra "E" significa Capacidad Mejorada, es decir, que graban y leen en formato de 36 pistas y bidireccional.

Las unidades van montadas en bastidor y están dirigidas para sistemas intermedios.

Se dispone de una unidad 3490-C11 con una boca de acceso, dispositivo cargador automático de cartuchos (ACL) y dispositivo de compresión de datos, que da a los cartuchos una capacidad media de hasta 2'4 GB.

Existe posibilidad de cambio en los modelos de C10 a C11 y de C11 a C22.

La velocidad de transferencia es de 4'5 Mb/seg con una conexión a canal independiente.

Los modelos C11, C12 y C22 son completamente compatibles con los modelos existentes, utilizando ambos el sistema de cartuchos de cinta de capacidad mejorada.

El dispositivo de capacidad mejorada (36 pistas, formato de grabación bidireccional) que en los cartuchos de capacidad extendida proporciona una capacidad de 800 Mb por cartucho.

2.3.4.- **IMPRESORA PRINCIPAL**

La impresora de páginas IBM 3825 es una impresora conectable a canal direccionable. Todos los puntos (APA) de no impacto, hojas sueltas, e impresión por doble cara que proporciona en alta calidad.

Posee un software necesario para la impresión de formularios y preimpresos con tecnología AFP (Funciones Avanzadas de Impresión) de IBM.

Utiliza un proceso electrográfico, en una gran variedad de tamaños de papel, para imprimir a una velocidad de hasta 58 impresiones por minuto.

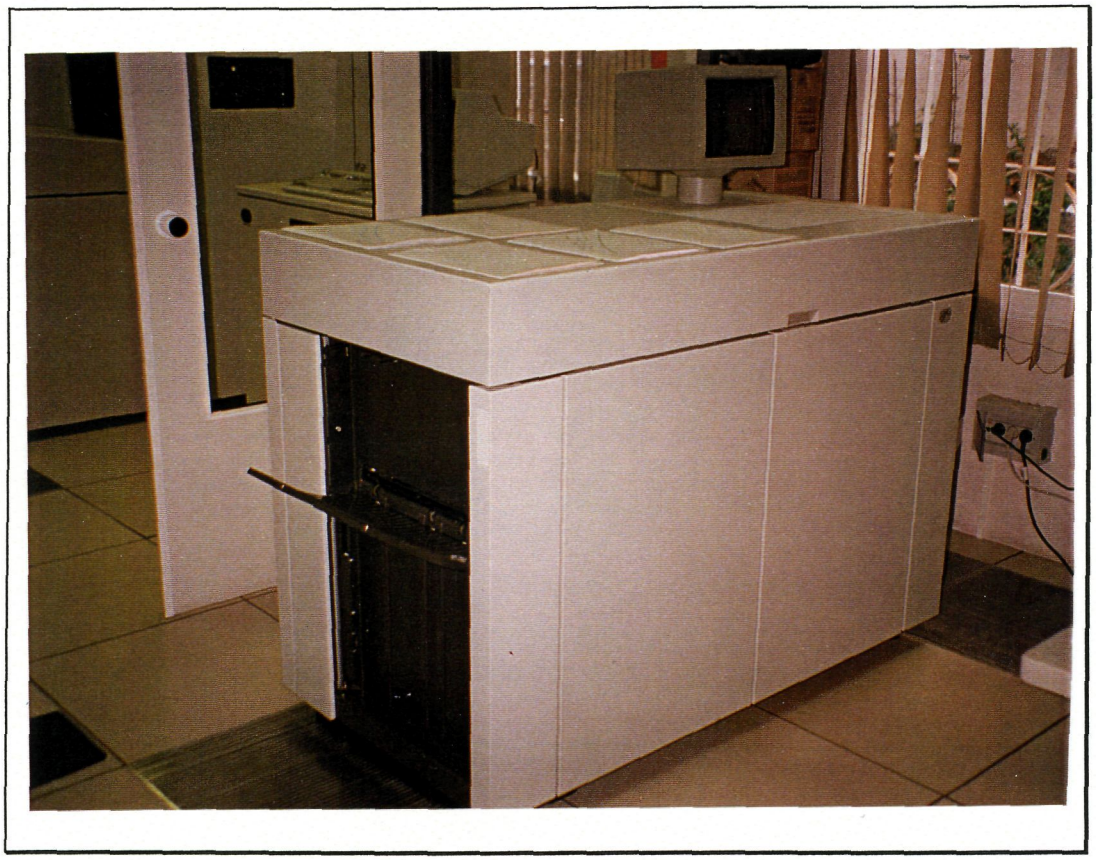
La impresora de páginas IBM 3825 se une a la creciente familia de impresoras de Funciones Avanzadas de Impresión (AFP) de IBM, formada además por la impresora de páginas IBM 3820, los subsistemas de impresión IBM 3800 modelos 3 y 5, la impresora de páginas 3827 y la impresora de páginas IBM 3835.

El soporte de Funciones Avanzadas de Impresión para la impresora de Páginas IBM 3825 existe bajo los Sistemas Operativos IBM MVS, VSE y VM.

La impresora de Páginas IBM 3825 puede utilizarse para imprimir etiquetas autoadhesivas en papel xerográfico en tamaños A4 o carta.

La impresora de Páginas IBM 3825 puede utilizarse para imprimir documentos con código de barras.

La impresora de Páginas IBM 3825 puede conectarse a una red SNA vía el IBM Tokeng Ring o una línea SDCL usando el Remote PrintManager en un entorno MVS con PSF/MVS.



2.3.5.- **PERIFERIA**

Se compone de:

- 15 ordenadores personales para tareas de terminal y servidor de comunicaciones

- 195 ordenadores personales para uso como terminal

- 22 impresoras matriciales y 69 laser para conexión a los ordenadores personales

- Una red local ETHERNET por provincia. En cada una de dichas redes existe un Servidor de Comunicaciones (GATEWAY) bajo OS/2.

- Las estaciones de trabajo están dotadas del programa Personal Comunication 3270, y ejecutarán una emulación 3270 que les permita conectarse al HOST.

2.4.- CONTROLADORES DE COMUNICACIONES

2.4.1.- PROCESADORES DE COMUNICACIONES

El Controlador de Comunicaciones IBM 3745 gestiona el flujo de datos entre terminales y ordenadores centrales. Puede conectarse local o remotamente a ordenadores IBM 43xx, 937x o 30xx.

Las características principales son:

- alta disponibilidad, gracias a una tecnología muy fiable y un mantenimiento mejorado
- control de comunicaciones a un coste adecuado para redes pequeñas o intermedias
- rendimiento aumentado, del orden de 4,5 veces del IBM 3720
- conectividad ampliada, con conexión de ordenadores, líneas de velocidad bajo y media (hasta 256 Kbps), enlaces de 2 Mbps y redes locales en anillo.
- gestión simplificada, ya que el controlador de comunicación IBM 3745 ha sido diseñado para una utilización y modificación sencilla, facilitando el crecimiento de las redes.

La unidad del Controlador de Comunicaciones es un IBM 3745 con modelo 170 en Tenerife y 160 en Las Palmas. Estas unidades están configuradas de modo que puedan soportar ampliaciones de hasta 30% de líneas o terminales. Están equipadas con 8 líneas de 19.200 bps y de 1 línea de 64 Kbps. Además incorporan disco duro y posibilidad de carga y operación remota.

2.4.2.- **CONEXIÓN SIEMENS-IBM**

La conexión del equipo SIEMENS y el sistema IBM está garantizada. Dicha conexión se lleva a cabo a través de los controladores de comunicaciones de IBM y de SIEMENS y de un producto de sotware llamado TRANSIT CD, que dispone de un módulo para la conversión de protocolos TRANSDATA a SNA, y viceversa.

Las impresoras SIEMENS no se pueden utilizar directamente, ya que no son físicamente conectables, pero se pueden utilizar conectadas a un ordenador personal si se usan herramientas de transformación de ficheros.

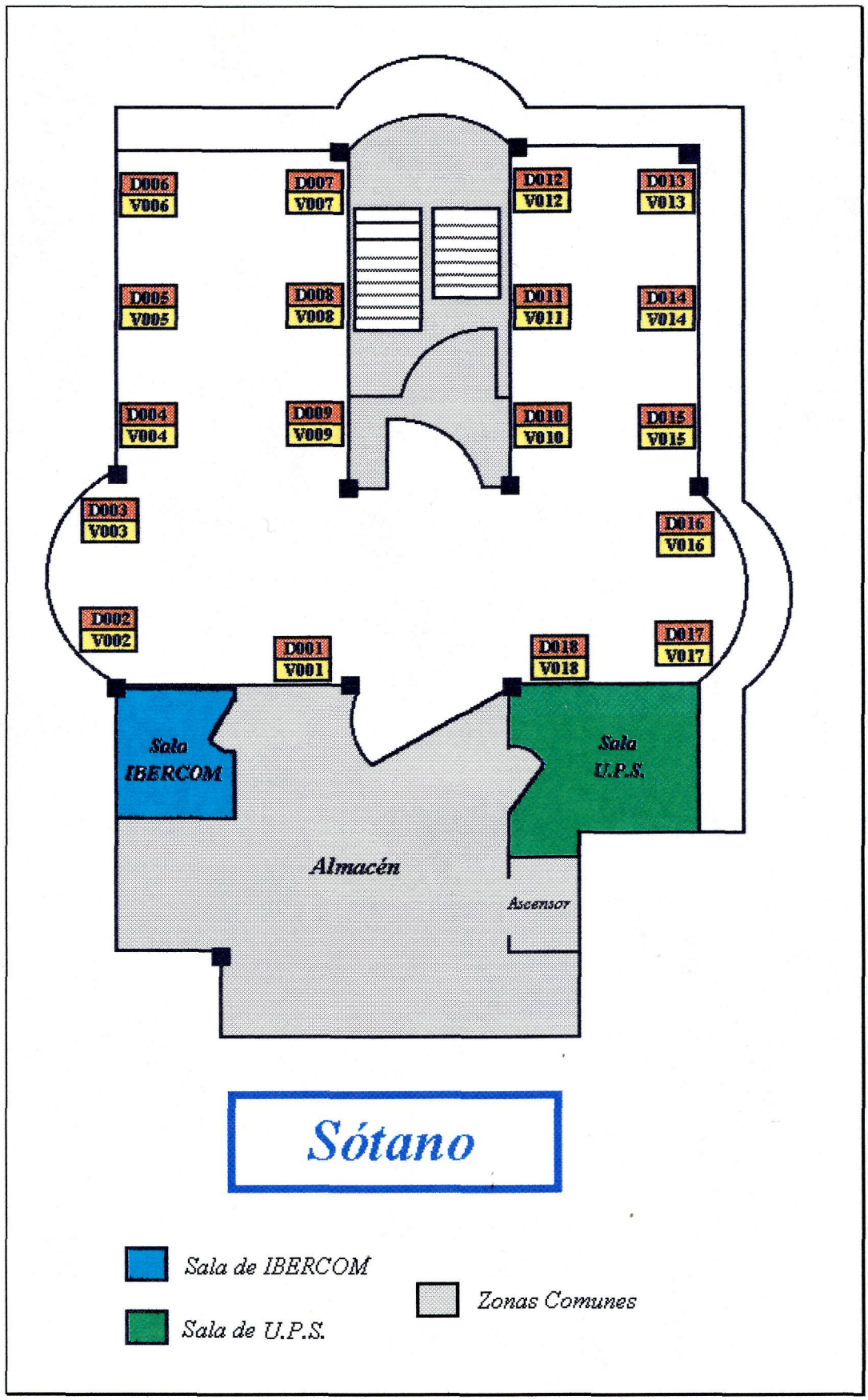
En los puestos terminales se podrá elegir el entorno de trabajo desde los mismo puestos, ya que se contemplan los dos entornos en las respectivas tarjetas de emulación que se instalan en los equipos terminales.

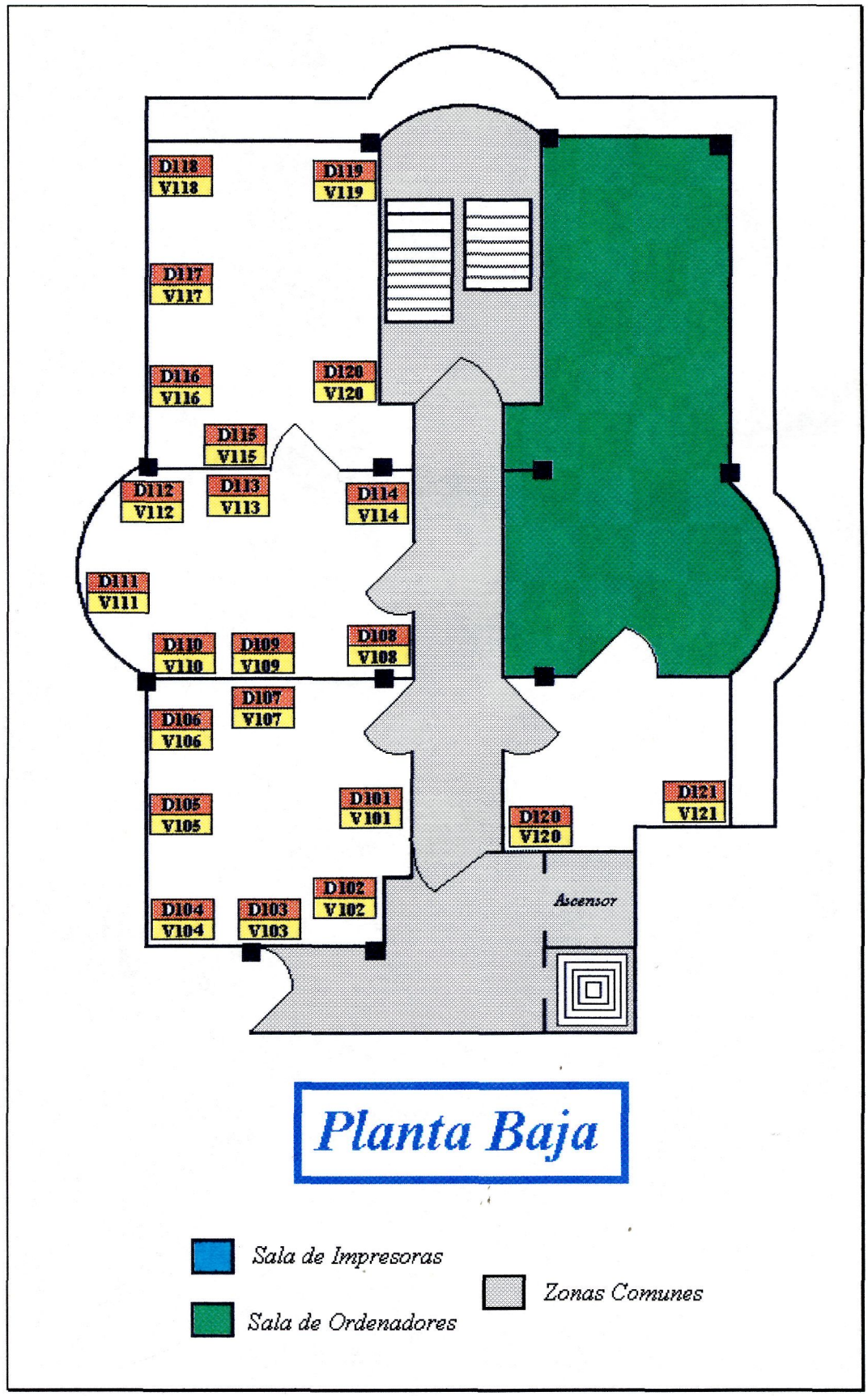
2.4.3.- INFRAESTRUCTURA Y ACONDICIONAMIENTO

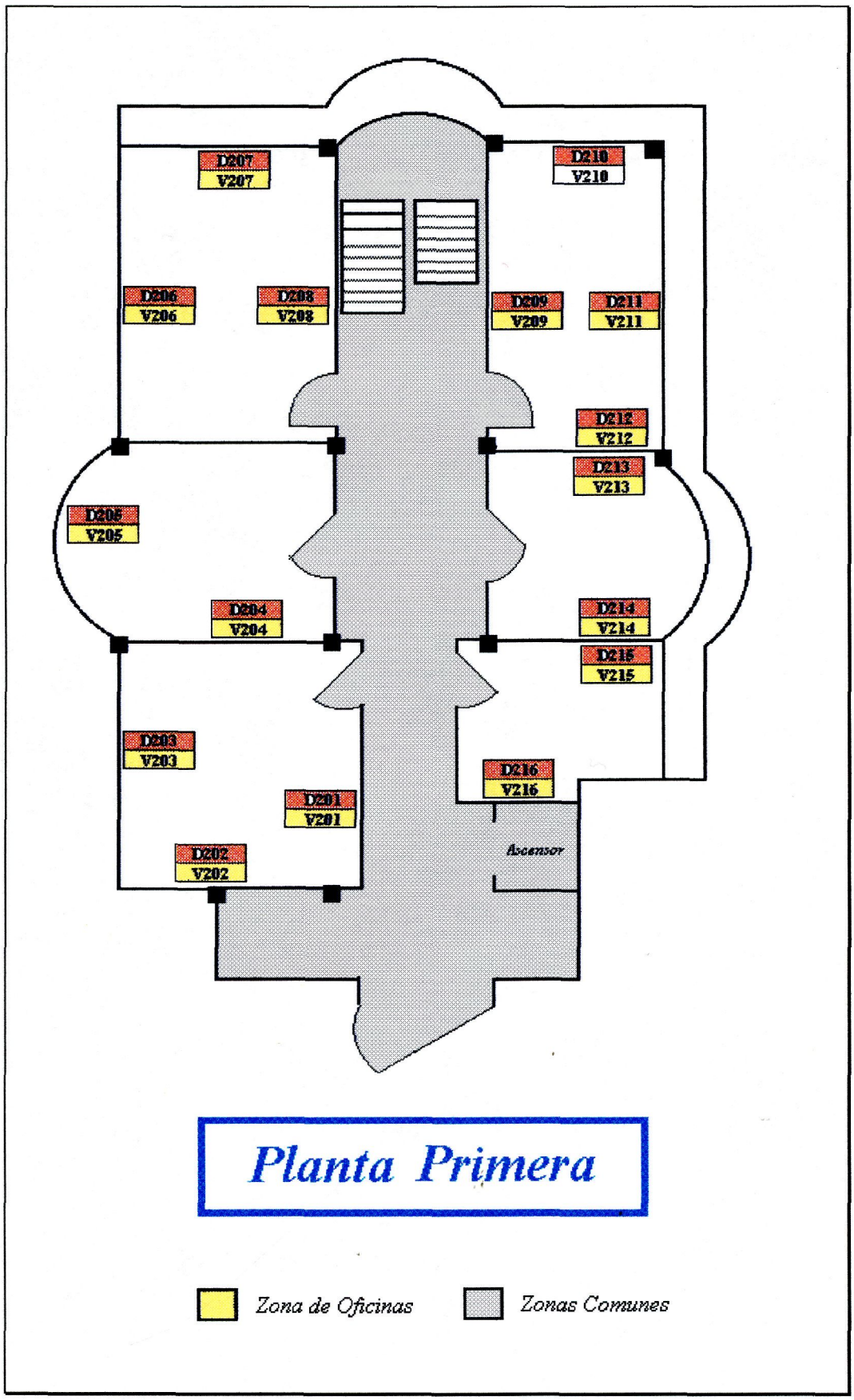
Las especificaciones de la infraestructura de voz, datos y corriente son las siguientes.

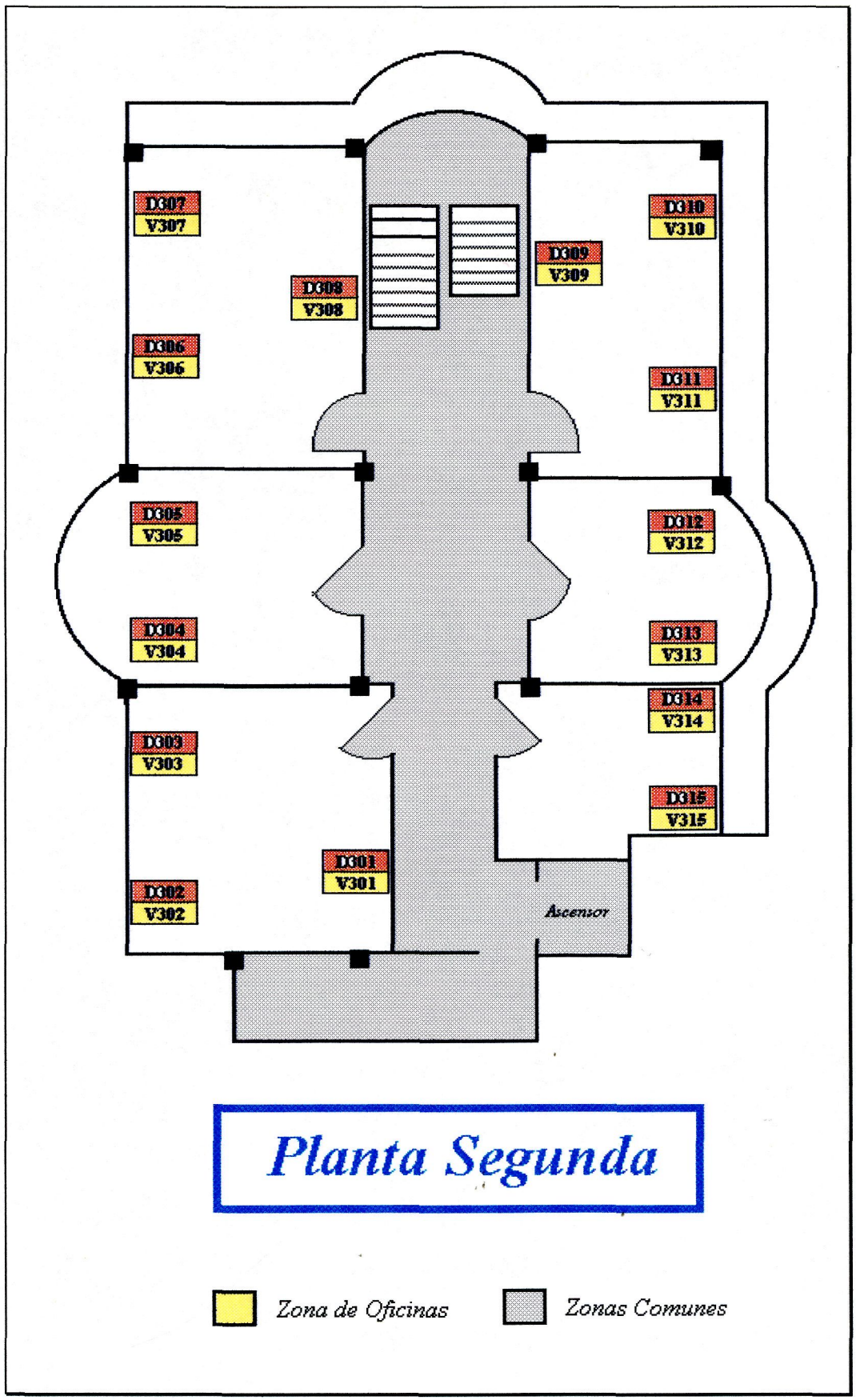
- Cableado PDS 1061 de AT&T
- Toma normalizadas RJ-45 para voz y datos
- Bastidores necesarios para la ubicación de concentradores modulares, para dotar de 500 puestos de trabajo con una topología 10 Base/T.
- Cableado soporta una red ETHERNET con velocidad de hasta 10MB/seg.
- UPS
- Sistemas de Aire Acondicionado
- Subsistema de Tierra
- Cuadros de corriente y cuadros de alarmas

La estructura del cableado del edificio se presenta a continuación, con los puntos de cableado referentes a voz y datos correspondiente. Se distinguen cada una de las plantas señalando las zonas de cobertura informática y diferenciándolas del resto.









2.5.- EQUIPO LÓGICO

2.5.1.- SISTEMA OPERATIVO

En el sistema residen dos Sistemas Operativos, que son:

- **VM/ESA:** incluye otros productos como soporte AFP para las impresoras, soporte de conexión X25,..
- **AIX/ESA**: es el producto de IBM en la plataforma Enterprise System

Ambos pueden ejecutarse concurrentemente, de manera independiente, mediante el dispositivo PRSM. Puede crear 7 particiones lógicas con un alto grado de aislamiento. Por tanto, permite realizar trabajos simultáneos en entornos separados de un mismo sistema fisico.

El VM/ESA es un Sistema Operativo con multiproceso de IBM, para ordenadores medianos y grandes. El multiproceso permite que varios usuarios de un Sistema compartan los recursos del mismo, trabajando de forma interactiva. De esta forma, cada usuario piensa que son los únicos que están trabajando.

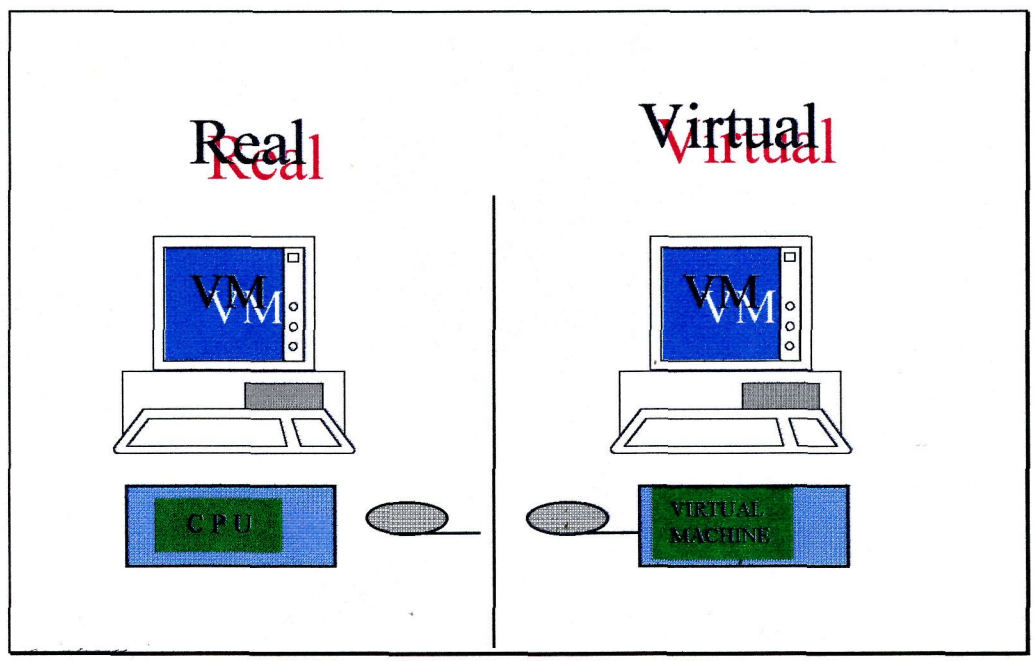
La función de un Sistema Operativo es el manejar los recursos de los dispositivos fisicos de la instalación, para que ni los programas ni los usuarios tengan que controlar las características de cada uno de ellos.

El VM/ESA controla los recursos de un sistema real de ordenadores: CPU, memorias y dispositivos de E/S, de forma que están disponibles para muchos usuarios al mismo tiempo.

Hay un concepto intrínsecamente unido al VM, es el de "*máquina virtual*". A cada usuario de VM se le asigna una máquina virtual individual, y una parte del VM "*multi-programa*".

El VM tiene un programa llamado *planificador*, que resuelve situaciones conflictivas, por el uso de recursos entre los usuarios. El sistema intenta que todos los usuarios tengan acceso a todos los recursos que necesiten de la instalación.

Una instalación puede decidir que máquinas virtuales tienen procesos del mismo tipo, pero en general el VM toma esta decisión de forma interactiva. Favorece a los usuarios con procesos triviales, por ejemplo aquellos que solo se mueven a lo largo de un fichero, frente a los que realizan procesos más complejos, como la ejecución de un programa que calcule inversión de matrices.



El Sistema Operativo VM tiene varios componentes:

- el ***Programa de Control*** CP (Control Program), que actúa como un simulador de hardware: es el que controla los recursos del ordenador real, distribuyéndolos entre las máquinas virtuales, incluyendo la memoria central y la propia CPU como recursos del sistema. El Cp se carga en las direcciones más bajas de la memoria real en tiempo de IPL del sistema. Controla la paginación y el proceso de planificación. El Cp maneja las comunicaciones entre las máquinas virtuales.

- el ***Sistema Conversacional*** CMS (Control Monitor System)

- el IPCS o DVF o ***Sistema de Control de Errores de Software***

- el ***Sistema de Control de Grupos*** o GCS: es un sistema operativo de máquina virtual, que permite a un sistema VM manejar, por sí mismo, productos de una red de telecomunicaciones con arquitectura SNA

- el ***Sistema de Comunicaciones*** o RSCS, es el RJE del VM

- el ***TASF*** (Transparent Services Access Facility): permite a los usuarios de un sistema VM comunicarse con otras máquinas virtuales, dentro de un grupo de sistemas VM interconectados.

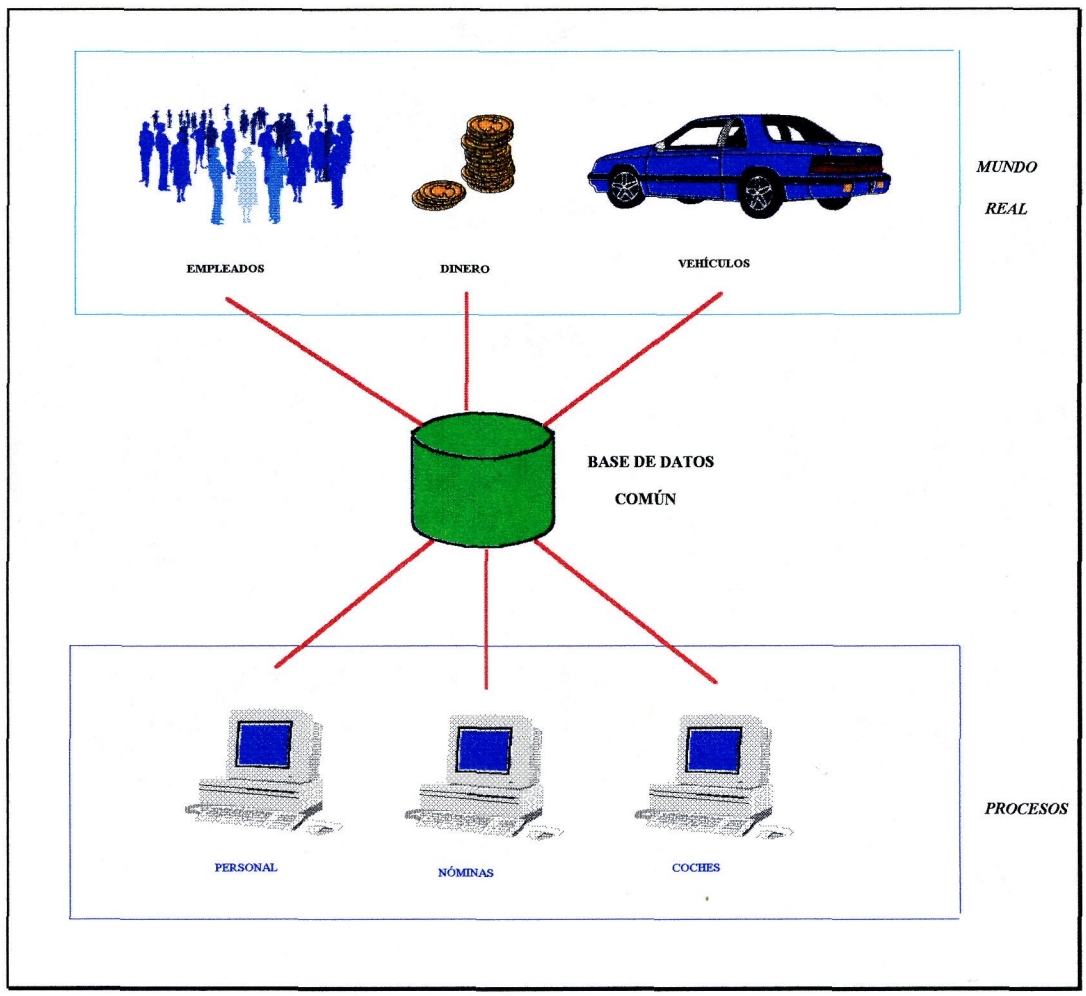
El VM soporta una variedad muy grande de dispositivos periféricos. Algunos dispositivos no soportados por el VM, pueden controlarse desde una máquina virtual donde está cargado un supervisor que sí los soporta. Por ejemplo, el diskete

3540 es un dispositivo de E/S que se puede controlar desde una máquina virtual, donde se está ejecutando el Sistema Operativo VSE.

La configuración de cada posible máquina virtual en el Sistema se define como *directorio*. La memoria de una máquina virtual no siempre reside en la real del ordenador. Parte de ella se almacena en un disco (DASD). El CP puede detectar, si una determinada máquina virtual necesita usar un área de su memoria que esté en ese momento en el disco. Si es así la llevará a la memoria real del ordenador y la dejará allí hasta que deje de utilizarse. Entonces el CP devolverá dicha área al disco. Este proceso es lo que se denomina *paginación*.

2.5.2.- **BASE DE DATOS**

La Base de Datos utilizada en el Sistema, es ADABAS. Este modelo de almacenamiento de la información, está basado en su centralización bajo una estructura común que permita su manipulación de modo coherente pero flexible, eliminando las redundancias al máximo.



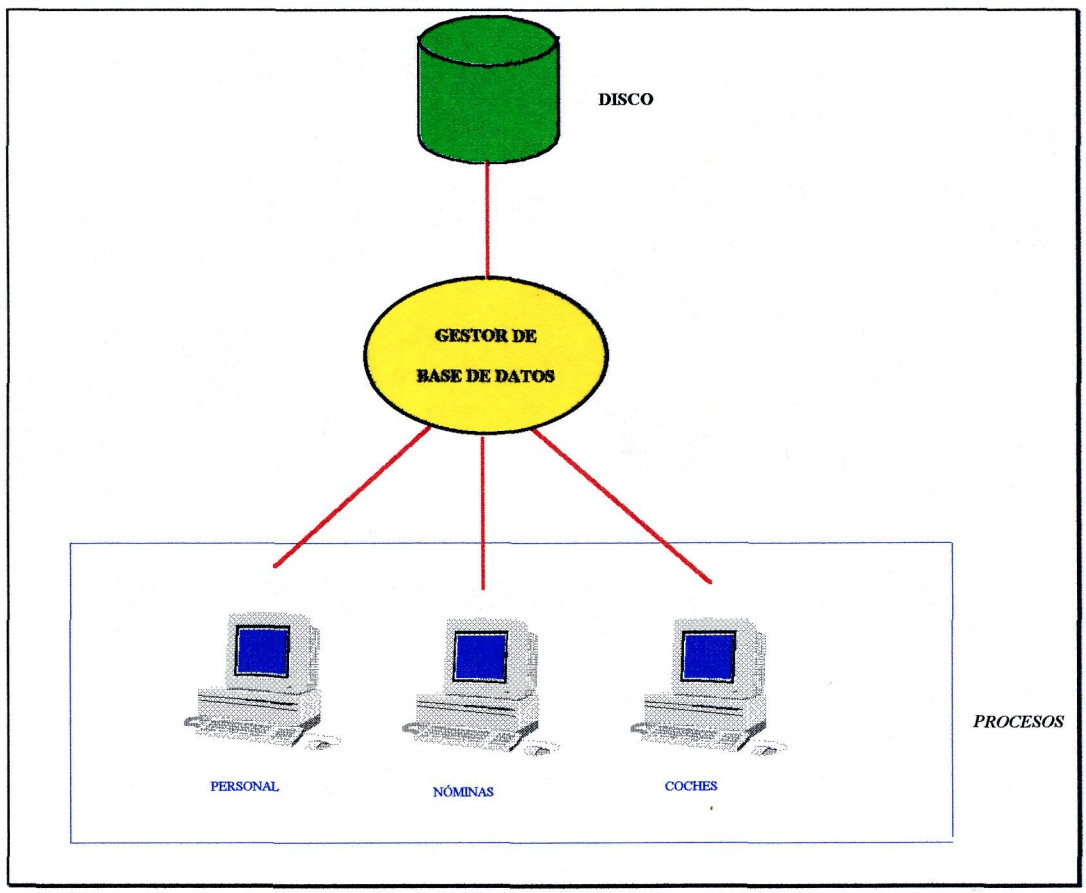
Con este enfoque de Base de Datos, se consiguen dos puntos favorables :

- ***Diseño de datos independiente de las Aplicaciones***
  - Reducción de la Redundancia
  - Flexibilidad

- ***Almacenamiento centralizado de los Datos***

  - Proceso Paralelo
  - Reduce las inconsistencias

Este conjunto de datos almacenados en disco, se encuentran a disposición de una o varias aplicaciones, mediante el control que realiza el *"Gestor de la Base de Datos"*.

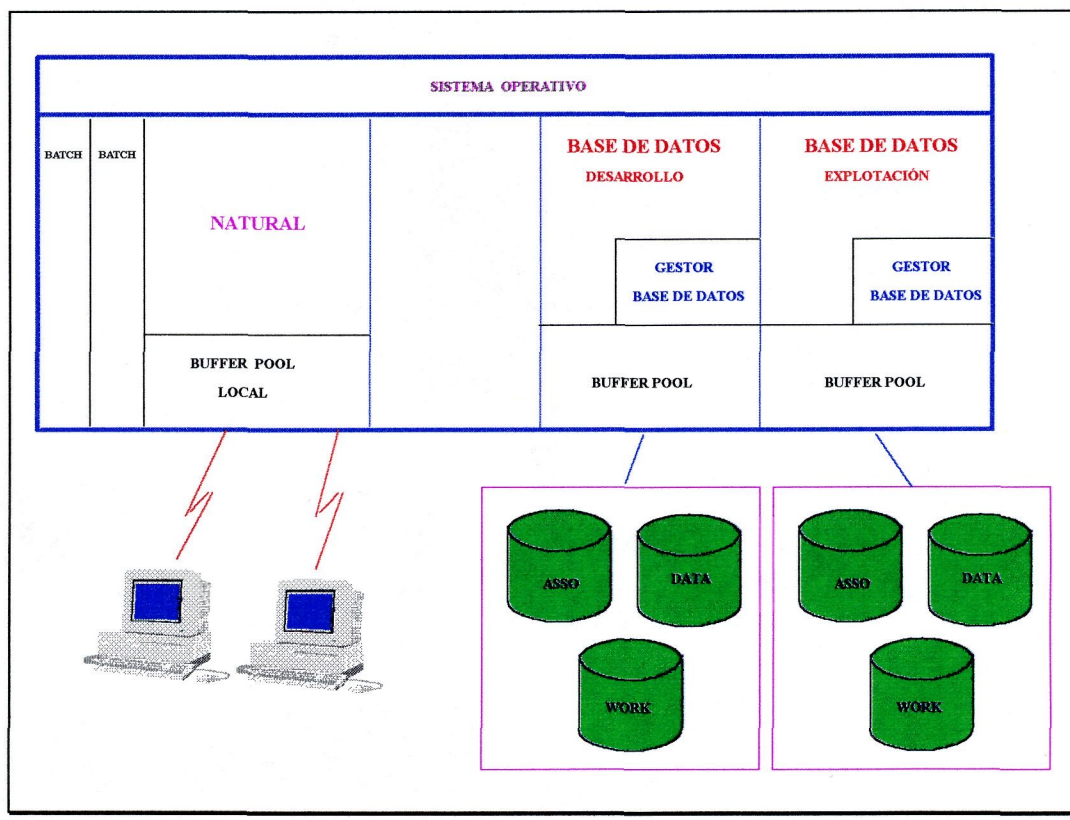


El Gestor de la Base de Datos es un proceso separado (único para cada Base), que :

- Interpreta y resuelve las peticiones de los usuarios
- Gestiona y controla su uso en paralelo

- Controla y optimiza el método de acceso a los datos

En este Sistema existen dos Bases de datos : "Desarrollo" para la programación y pruebas, y "Explotación" para el Usuario Final. Existe la posibilidad de definición de hasta 253 Bases de Datos y hasta 255 Ficheros en cada una.



Cada Base de datos está compuesta por tres Data-Set :

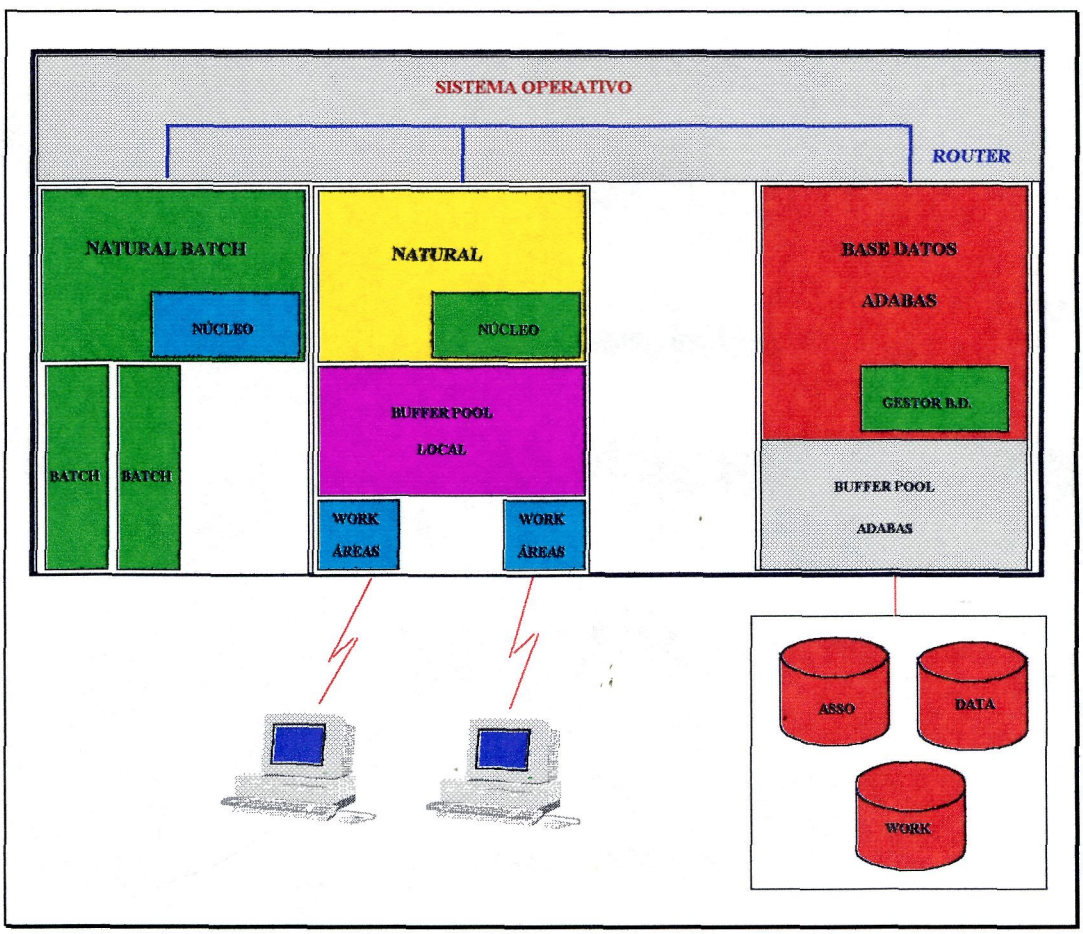
- ***ASSO (Asociador)*** : Contiene la información lógica necesaria para acceder a los datos.
- ***DATA (Area de Datos)*** : Contiene los datos de los distintos archivos comprimidos.
- ***WORK (Area de Trabajo)*** : Contiene la información intermedia (utilidades)

2.5.3.- HERRAMIENTAS DE DESARROLLO

El Lenguaje de Programación utilizado en el Sistema, es NATURAL. Es un sistema de desarrollo de cuarta generación y contiene los siguientes elementos :

- ***Procesador de Comandos*** : Evalúa y procesa comandos.
- ***Compilador*** : Valida sintaxis de programas fuente. Compila el código fuente en objeto.
- ***Optimizador*** : Reemplaza partes del código objeto por instrucciones en Assembler.
- ***Procesador de Ejecución*** : Carga y ejecuta objetos.

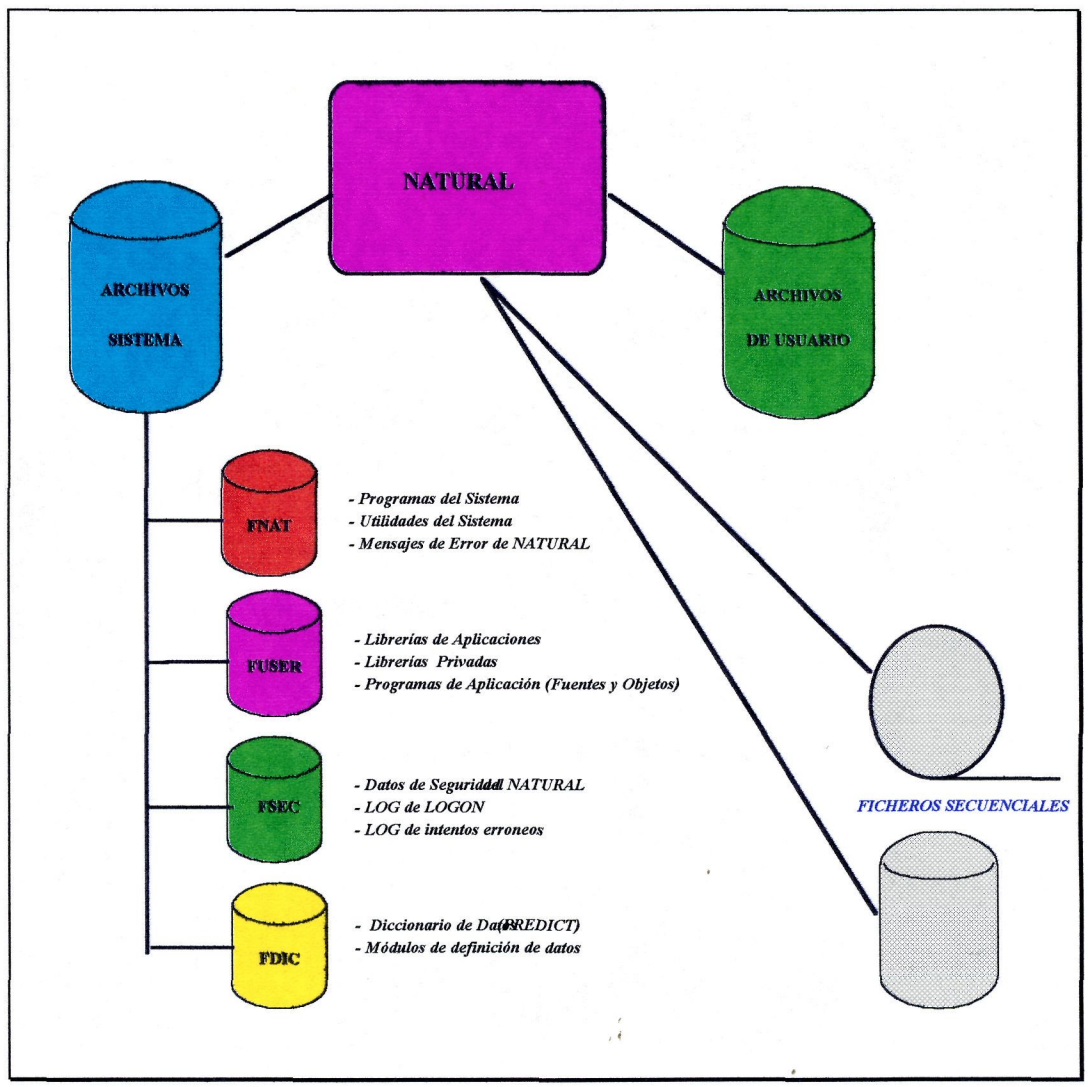
La Arquitectura del NATURAL tiene la siguiente estructura :



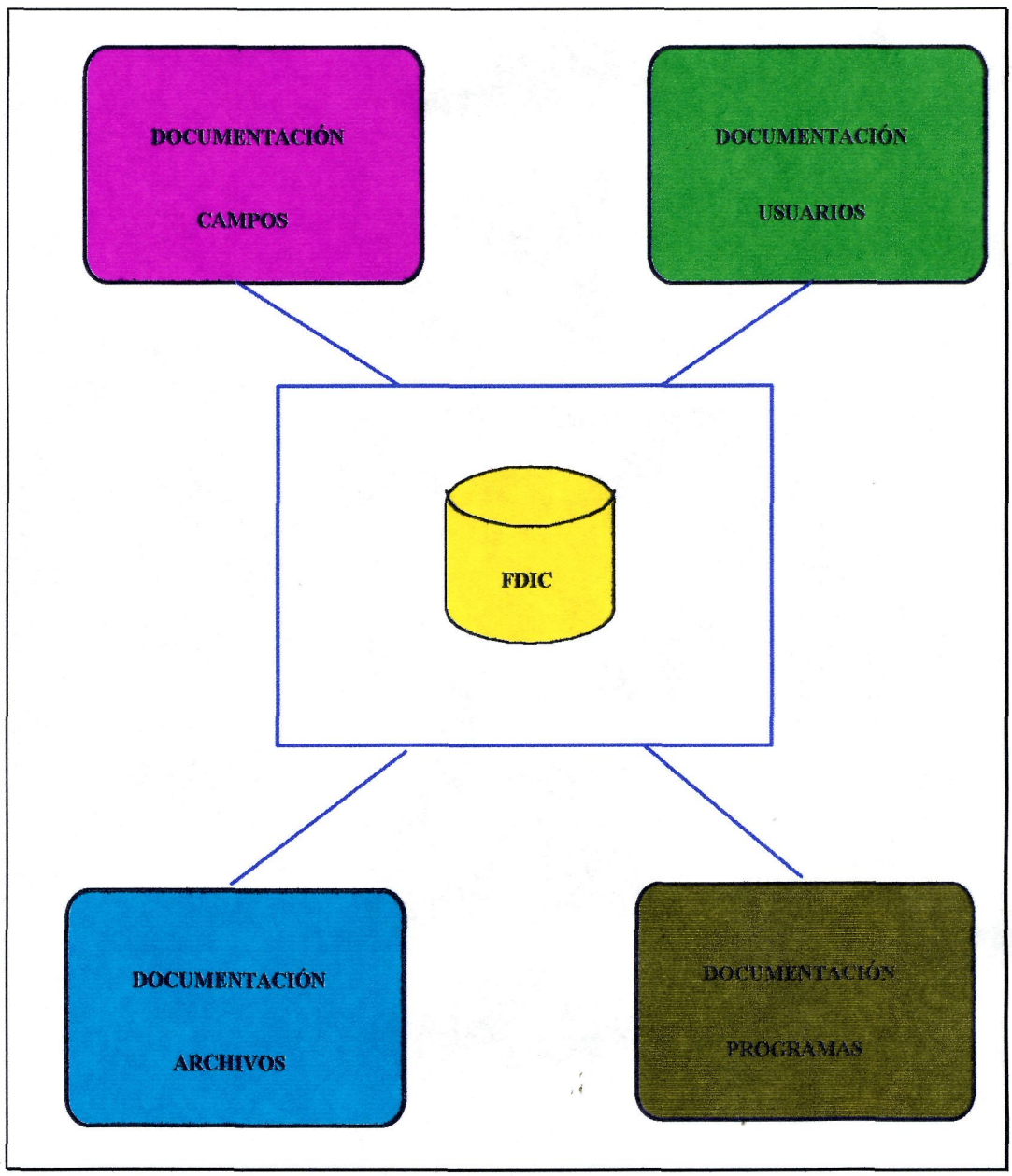
Para el uso del NATURAL es necesario que se encuentren disponibles todos los archivos definidos para dicho sistema de desarrollo, y éstos son:

- Archivos de Usuario

- Archivos del Sistema.



PREDICT es un Diccionario de Datos activos para administradores de Bases de Datos, administradores de datos y desarrolladores de aplicaciones que necesitan gestionar información relativa a datos y programas. Es un sistema interactivo con capacidad para crear, mantener y listar información en un entorno on-line.



2.5.4.- **OFIMÁTICA**

Los productos de ofimática que se encuentran instalados en el Sistema, so de entorno Windows:

- Windows para Grupo de Trabajo
- Word
- Excel
- Correo Electrónico

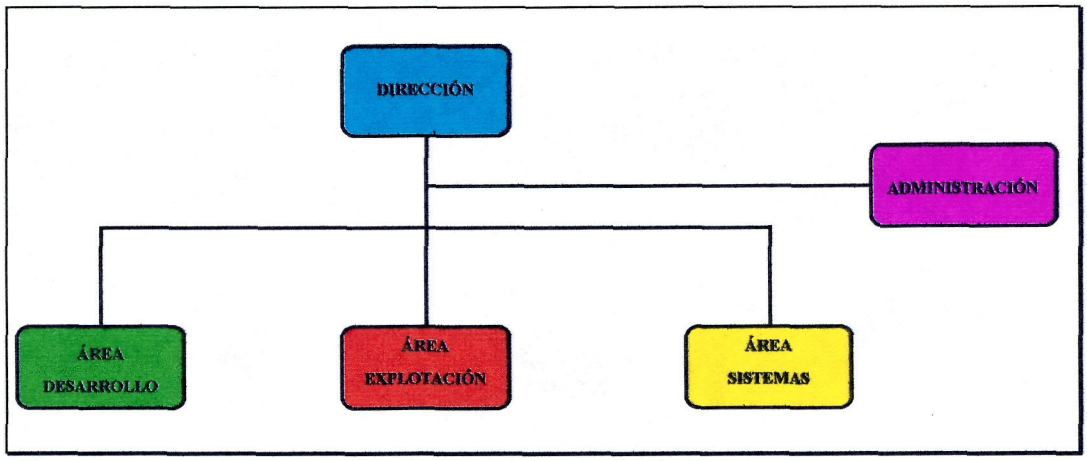
Estos productos engloban las funciones de correo, transferencia de ficheros, editores de Texto, bases de datos, hojas de Cálculo, etc.

Todos ellos son de reciente incorporación con sus licencias correspondientes, ya que con anterioridad se encontraban en estado de "peligro" en lo que se refiere a seguridad informática debido a productos "pirateados".

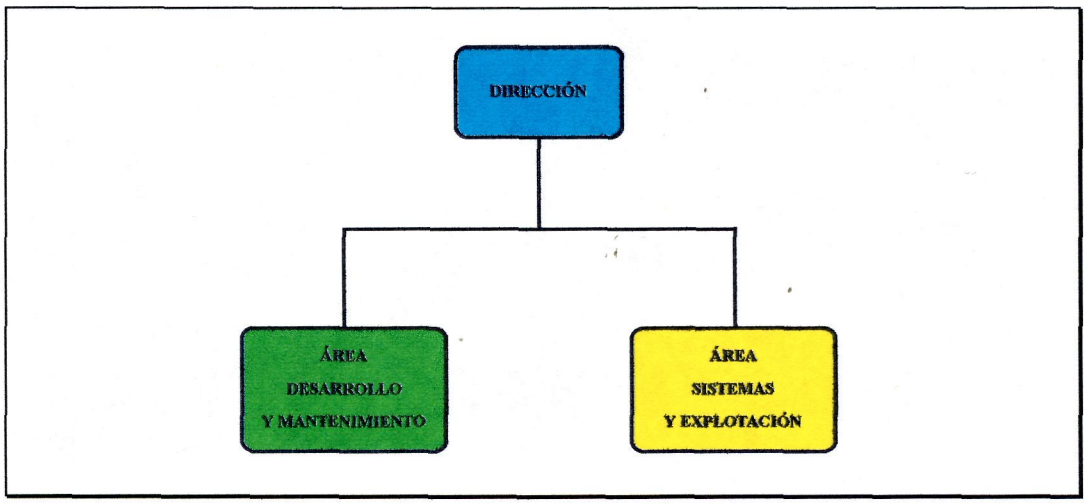
2.6.- RECURSOS HUMANOS

2.6.1.- ESTRUCTURA ORGANIZATIVA

El Centro de Proceso de Datos está compuesto por las siguientes Áreas que se relacionan en el organigrama siguiente :

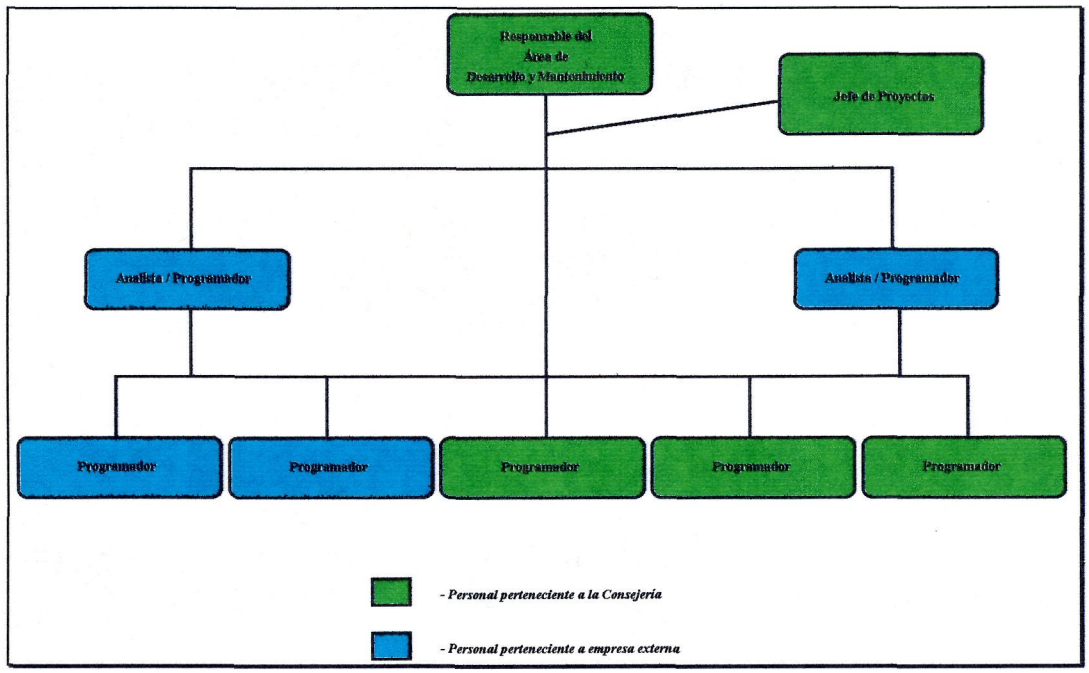


Debido a la falta de Recursos Humanos, este C.P.D. no tiene definida un Área de Explotación ni de Administración, pero sí ha asumido sus funciones, repartiéndolas entre el resto de los departamentos. Por ello, han sido renombrado las que existen, quedando el organigrama de la siguiente manera :

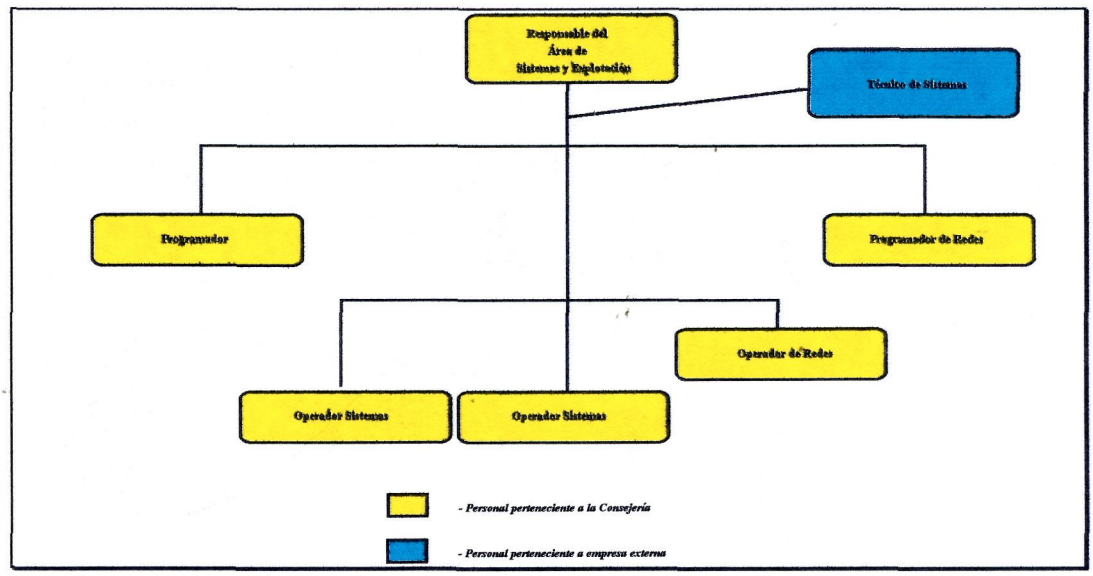


2.6.2.- **PLANTILLA ACTUAL**

El Área de Desarrollo y Mantenimiento se encuentra constituida por el siguiente personal :



El Área de Desarrollo y Mantenimiento se encuentra constituida por el siguiente personal :



2.6.3.- DESCRIPCIÓN DE FUNCIONES

- ***Dirección***

  - Asesorar al Secretario General Técnico sobre cualquier solicitud.
  - Interpretar las necesidades y la política de las Direcciones Generales.
  - Elaborar el Plan estratégico de Hardware, Software, Comunicaciones y Personal Informático.
  - Controlar y coordinar las funciones de las Áreas de Desarrollo y Mantenimiento y Sistemas y Explotación.
  - Participar en la elaboración y aprobar los planes de formación del personal.
  - Realizar la propuesta de Plan Anual y elaborar el presupuesto del Servicio.
  - Proponer la contratación de los equipos de infraestructura para el Centro de Proceso de Datos.
  - Elaborar los Pliegos Técnicos de Contrataciones Informáticas.

- ***Área de Desarrollo y Mantenimiento***

  - Organizar y coordinar reuniones con los usuarios para la realización de las definiciones funcionales de los nuevos Proyectos a acometer y solicitudes de modificación de los existentes.
  - Evaluar el desarrollo o las modificaciones de los Proyectos, su complejidad y sus tiempos de ejecución.
  - Controlar el cumplimiento de los plazos previstos para el desarrollo y puesta en marcha de los Proyectos.

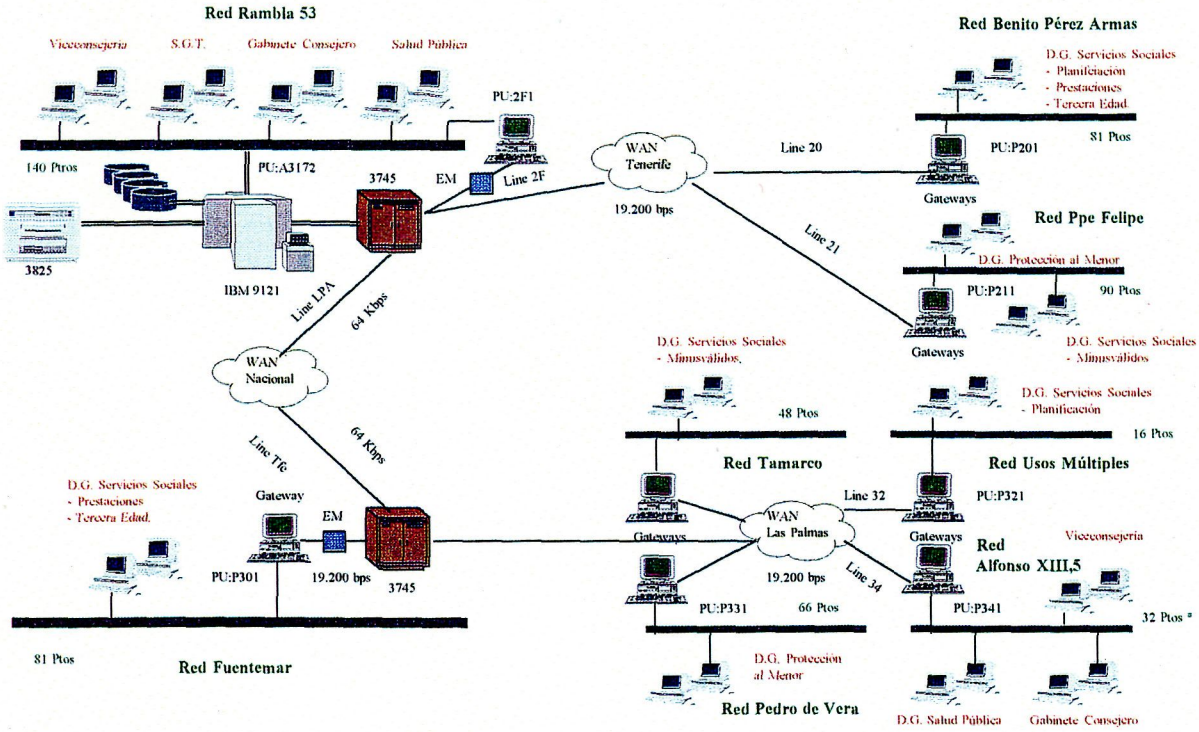
- Comprobar que las aplicaciones realizadas, reúnen las condiciones funcionales solicitadas por el usuario, y funcionan correctamente.
- Definir los entornos de trabajo, tanto de desarrollo como de explotación.
- Supervisar y realizar el paso de los módulos terminados a Explotación.
-Organizar y coordinar las demostraciones necesarias para los usuarios, y darle formación y soporte en los proyectos a su cargo.
- Definir seguridades de acceso a usuarios, aplicaciones y ficheros.
- Elaborar la definición de metodologías de Desarrollo y Mantenimiento en cuanto a análisis, diseño y codificación de módulos, así como supervisar la correcta utilización de los mismos.
- Ejecutar aquellos procesos ocasionales o periódicos necesarios para la explotación de Aplicaciones, que debido a su gran consumo de recursos, no pueden ser ejecutados por el usuario.
- Realizar el Análisis Funcional, Orgánico, Programación y mantenimiento de los Proyectos encomendados.
- Aplicar los Lenguajes, Utilidades y los Estándares de nomenclatura y programación.
- Mantener reuniones periódicas para elaboración de planificaciones.
- Cumplir con los planes de formación asignados.

- ***Área de Sistemas y Explotación***

- Mantener relaciones con los proveedores del entorno de Sistemas, con el fin de evaluar la necesidad y rentabilidad de los producto.
- Definir, junto con el resto de las Áreas, los equipo necesarios para la implantación de aplicaciones.

- Analizar las necesidades de crecimiento informático a medio y largo plazo, así como la previsión de saturación de almacenamiento en los discos.
- Instalar y mantener el Software de base.
- Monitorizar y ajustar el rendimiento del Sistema y de las comunicaciones.
- Diseñar todas las soluciones de interconectividad entre sistemas y redes de comunicaciones.
- Instalar y mantener el Software de comunicaciones en el ordenador central y controladores de comunicaciones.
- Programar y poner a punto rutinas y módulos del Software de base, para que puedan ser utilizadas por los operadores.
- Encender y apagar el ordenador central, las comunicaciones y las bases de datos.
- Atender a los mensajes de consola.
- Ejecutar las copias de seguridad (backup).
- Ejecutar la operatoria de administración de periféricos.
- Instalar los ordenadores personales y el software correspondiente, mantenerlos y chequearlos periódicamente.
- Asesorar al usuario sobre el hardware y software instalados.
- Cumplir con los planes de formación asignados.

2.7.- DIAGRAMA DE LA RED DE COMUNICACIONES SNA



3 - Definición de las Directrices

3.1.- SEGURIDAD FÍSICA

Seguridad Física incluye todos los mecanismos dirigidos a asegurar el Sistema Informático sin que el propio Sistema intervenga en el mismo. También es denominada como Seguridad Externa.

En un Sistema Informático todos los mecanismos de seguridad tienen que complementarse entre sí, de tal forma, que si una persona logra saltarse alguna de las protecciones, se encuentre con otras que le hagan el camino difícil.

A) **Seguridad Física**

Engloba aquellos mecanismos que impiden a los agentes físicos la destrucción de la información existente en el Sistema.

Se trata de eliminar los posibles peligros que originen los agentes físicos o la presencia física de personas no autorizadas:

- ***Protección contra Desastres*** : Consta de elementos de prevención, detección y eliminación que actúan contra incendios, humos, sobretensiones, fallos en el suministro de energía, etc.

  También es necesario controlar la temperatura y limpieza del medio ambiente en que se encuentran los equipos, instalación de aire acondicionado,

falso suelo, ventilación y, en definitiva, tomando en consideración todo aquello que pueda causar cualquier problema en la instalación.

- ***Protección contra Intrusos*** : Desde el punto de vista físico, es necesario establecer mecanismos que impidan el acceso físico de las personas no autorizadas a las instalaciones. Suele llevarse a cabo mediante puertas de seguridad con apertura por clave o llaves especiales, identificación de las personas por tarjetas de acceso o por reconocimiento de la voz, huellas digitales, etc.

B) **Seguridad de Administración**

Engloba aquellos mecanismos más usuales para impedir el acceso lógico de personas físicas al Sistema. Este acceso puede realizarse a través de un terminal del Sistema o bien desde otro Sistema por medio de una red de comunicación a los que estén conectados ambos sistemas.

- ***Protección de Acceso*** : Se trata de un mecanismo para el control de los intentos de entrada o acceso al Sistema, de tal forma que permita la conexión cuando un usuario lo solicite y pase el control correspondiente, rehaciendo el intento en aquellos casos en que la identificación del supuesto usuario no sea satisfactoria.

Uno de los mecanismos más usuales es la introducción de una Palabra Clave (PASSWORD) para la identificación del usuario. La fórmula más extendida es la de pedirle su nombre de usuario (USERNAME) y a

continuación la palabra clave, tal que el mecanismo accede al archivo correspondiente para contrastar los datos recibidos y aceptar o rechazar el intento. Esta palabra clave se debe grabar en los archivos de administración del Sistema codificada o encriptada para que no sea fácilmente reconocible por cualquier persona.

Los intentos fallidos de acceso deben de ser registrados por el Sistema, con el fin de que el Administrador del Sistema pueda estudiar cada cierto tiempo si se está o no intentando transgredir la seguridad del Sistema.

El Sistema debe dotar al Administrador del Sistema, para que en cualquier momento, se pueda realizar un alta o una baja de un usuario, asignándole en el primer caso, ademas de un USERNAME, la correspondiente contraseña o PASSWORD inicial. Mientras que el USERNAME es público, la PASSWORD no lo es, siendo recomendable su cambio cada cierto tiempo.

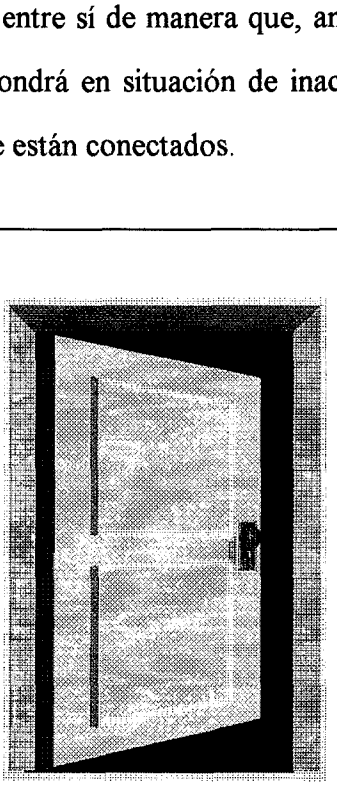
Cuando es tecleada la PASSWORD en un terminal para su acceso al Sistema, no deberá aparecer en la pantalla como ocurre con el resto de los datos que se teclean, para así conservar el secreto de la misma.

Al proceso de petición de entrada a un Sistema, contestación a las preguntas de identificación, contrastación de los datos recibidos y dar el correspondiente acceso, se denomina LOGIN. Así mismo al proceso de despedida del Sistema, se le denomina LOGOUT.

- ***Seguridad Funcional*** : Engloba aspectos relativos al funcionamiento del Sistema y a la seguridad que se pretende tener de las instalaciones.

Uno de los aspectos es la seguridad en la transmisión de datos. En las lineas de transmisión de datos existen diversos problemas de seguridad debido a lo fácilmente violables que son dichas líneas. Existen mecanismos tales como compactación de datos o criptografía.

El otro aspecto es la seguridad del correcto funcionamiento del Sistema. Existen mecanismos que, ante situaciones de mal funcionamiento, consiguen recuperar y controlar el entorno, protegiendo fundamentalmente la información. Este tipo de mecanismos se basa en la instalación de dos o más computadoras conectadas entre sí de manera que, ante el mal funcionamiento de una de ellas, éste se pondrá en situación de inactivo, tomando el control cualquiera de los otros que están conectados.



3.1.1.- UBICACIÓN DEL EDIFICIO

La inmensa mayoría de los edificios administrativos no están proyectados para una función informática. En la actualidad los técnicos van tomando conciencia de este tipo de instalaciones y, poco a poco, se encaminan hacia una nueva tecnología informática.

En la mayoría de los casos, el edificio se encuentra ya construido, por tanto, hay que darle forma, proyectar su interior y exigir que cumpla unas condiciones mínimas de trabajo, en cuanto a la instalación de equipos informáticos se refiere.

El progresivo desarrollo e implantación de las nuevas tendencias informáticas, implica una transformación en le forma tradicional de realizar el trabajo. Informática y Ofimática se dan cita, permitiendo integrar en un solo sistema todos los procesos y movimientos, tanto mecánicos como humanos, y ello obliga, sin lugar a dudas a una reorganización total de los elementos estructurales.

La automatización ha variado por completo el concepto de oficina. Esta revolución consiste en un renovado concepto de espacio y de instalaciones. Se trata de dar forma a un espacio dentro del cual puedan desarrollarse libremente y de forma rápida el ciclo de gestión burocrática y administrativa, sin retrasos que frenen la eficacia productiva.

Los elementos simples de los que debe contar un edificio moderno, que vaya a albergar en su interior un Sistema Informático, están divididos en tres zonas bien diferenciadas:

- Zona del Ordenador

- Zona de Oficinas y Despachos
- Zona de Servicios comunes

Una construcción / readaptación de un edificio con estas características, por motivos de seguridad externa, deberá estar exento de edificios colindantes o anexos.

Por otro lado, no deberá estar situado en un Área Industrial que, por su actividad, desprende gran cantidad de polvo al exterior, ya que esto podría afectar considerablemente y de forma perjudicial a los ordenadores. También deberá tenerse en cuenta, que la presencia de determinadas industrias pueden crear campos magnéticos o eléctricos de alta frecuencia, que podrían producir saltos y/o rayas en las pantallas, así como el borrado total o parcial de los soportes magnéticos, cintas, cartuchos, discos flexibles, etc. Por ejemplo, la proximidades a una emisora de radio o radar, produciría un campo magnético intenso.

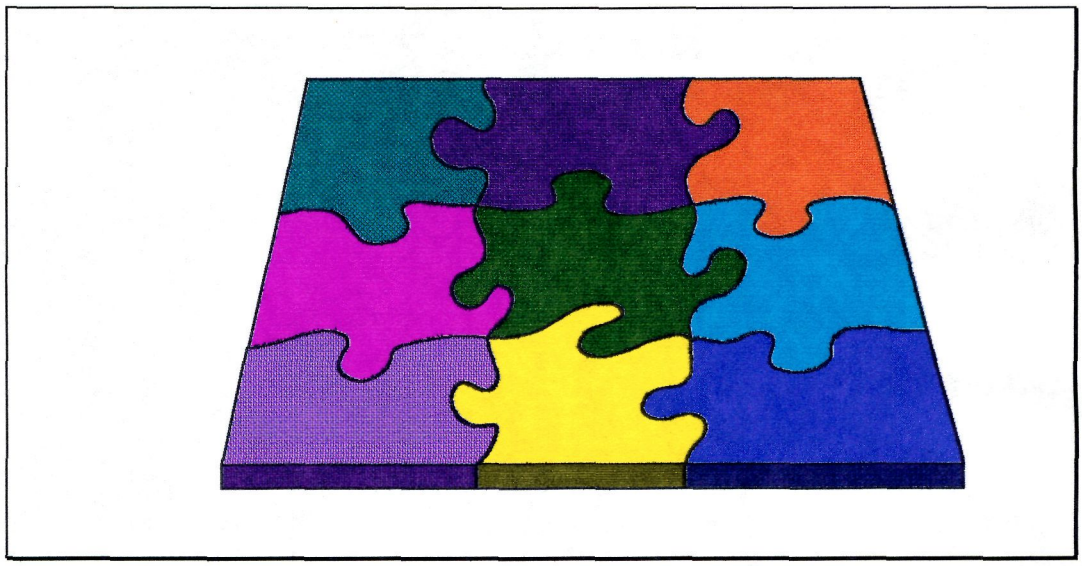
No es aconsejable proyectar el edificio en altura, debido a que se perderá diafanidad y extensión horizontal, muy importante para la instalación de los ordenadores.

Si se dispone de terreno, lo aconsejable es realizar la edificación lo más extensa como sea posible horizontalmente. Se conseguirán resultados más eficaces en cuanto a diafanidad, luminosidad, sincrorresistencia, posible evacuación y seguridad.

La construcción del edificio deberá comprender :

- Estructuras resistentes

- Suministros de energía eléctrica
- Instalaciones
- Seguridad



3.1.2.- UBICACIÓN DEL C.P.D.

Un Centro de Informática no puede ser instalado como cualquier oficina, sino que el trato debe ser más técnico, teniendo que considerar aspectos tales como la elección de la situación de la Sala de Ordenadores, los materiales a utilizar, los equipos de protección contra incendios, los equipos de aire acondicionado, así como los sistemas eléctricos.

La situación para las Salas de Ordenadores es un local resistente al fuego. Además, no debe situarse encima, debajo o adyacente a áreas donde se manipulen, fabriquen o almacenen materiales inflamables o explosivos.

En cuanto a la seguridad del suelo, techo y paredes, sería necesario que:

- las paredes serán de material incombustible y construidas desde el suelo real hasta el techo real.

- en caso de que el recinto de los ordenadores tuviera paredes exteriores adyacentes a un edificio susceptible de incendio, se procurará instalar ventanas irrompibles (que mejorarán la seguridad del personal y del propio ordenador), o también pueden instalarse unas "bocas de agua" sobre las ventanas para protegerlas con una cortina de agua en caso de incendio.

- el falso techo deberá ser de un material incombustible o, por lo menos, resistente al fuego.

- el falso suelo debe ser de materiales incombustibles o resistentes al fuego. También es importante que el espacio creado entre el falso suelo y suelo real, permanezca siempre limpio.

- las áreas de almacenamiento de material informático, deberán ser impermeables.

- Se deberá instalar un sistema de drenaje en el suelo. Es conveniente que el suelo real presente una ligera inclinación hacia un desagüe, para conseguir una buena previsión en caso de inundaciones fortuitas o provocadas, cuya humedad afectaría a los equipos informáticos.

- No deberán existir interferencias electromagnéticas, ya que esto podría producir alteraciones y vibraciones en pantallas y máquinas.

3.1.3.- SALIDAS DE EMERGENCIA Y PLANES DE EVACUACIÓN

En caso de inminente peligro (incendios, humos, sobretensiones, etc.), para la seguridad de las personas de los Centros de Procesos de Datos, deberá existir una vía central de evacuación que sea de acceso inmediato y transparente. Se deben minimizar los recorridos desde cualquier punto del edificio para su rápido desalojo. Además se deberán colocar carteles orientativos y croquis de evacuación, necesarios para que la misma se realice lo más rápidamente posible.

Para el buen funcionamiento del Sistema, se debe realizar la instalación de un grupo de continuidad para la alimentación eléctrica. Para los casos de un fallo de energía eléctrica, se instalarán luces de emergencia alimentadas con baterías que iluminan el área de evacuación inmediatamente.

Cualquier incidencia que ocurra en el recinto, se encuentre o no fuera de las horas de trabajo del personal, deberá activar inmediatamente la alarma correspondiente en un centro de control vigilado por personal destinado a este fin.

Deberá realizarse un estudio de las posibles situaciones de emergencia y evacuación planteables, para la definición de las normativas y procedimientos a seguir en casos reales y en simulacros. Así mismo deberá realizarse un plan de entrenamiento a las personas que trabajan en el edificio, mediante cursos, charlas, proyecciones y maniobras de simulación y de evacuación necesarias.

3.1.4.- SEGURIDAD EN EL ACCESO AL RECINTO

En cuanto a la seguridad contra intrusos desde el punto de vista físico, deberá establecerse una limitación de acceso al recinto, mediante rejas y otras protecciones en ventanas.

Además deberá existir un centro de vigilancia y seguridad en la/s entrada/s del recinto, donde se procederá a la identificación de las personas que entran al recinto. Se deberá llevar un control exhaustivo de la persona que entra en un parte de visitas, indicando la hora de entrada, la de salida y a qué dependencia se dirige. Una vez se autorice a la persona el acceso al recinto, se le asignará una tarjeta de identificación que deberá llevar en lugar visible.

Así mismo se deberá llevar un registro de los maletines, paquetes o bultos que porta la persona que accede al recinto, mediante algún equipo existente en el mercado, para evitar el riesgo de acciones delictivas.

También se debería instalar una cámara de circuito cerrado en la/s entrada/s, para ayudar en la identificación de la persona.

3.1.5.- SEGURIDAD EN EL ACCESO AL C.P.D.

En cuanto a la seguridad contra intrusos desde el punto de vista físico, deberá establecerse una limitación de acceso al Centro de proceso de datos, mediante rejas, protecciones en ventanas, así como puertas de seguridad en cada una de las entradas. Es recomendable que la/s puerta/s de acceso, dispongan de cerradura eléctrica, tarjetas magnéticas con clave de acceso, teclados con claves de acceso, huellas digitales, o bien otro tipo de mecanismo de características similares.

Se deberá realizar un estudio de los posibles niveles de acceso a las distintas dependencias del Centro de Proceso de Datos (Sala de Ordenadores, Sala de Impresoras, Área de almacenamiento de material informático, etc.), para la separación de dichas dependencias mediante algún control de seguridad, ya sea con vigilancia o puertas de seguridad de las características descritas anteriormente.

3.1.6.- **SEGURIDAD DEL C.P.D.**

Se deberán tener en cuenta los siguientes aspectos:

- *Tratamiento del Suelo* : Los Ordenadores necesitan además de una fuente de alimentación eléctrica, un innumerable "ovillo" de cables, para que funcionen. También son necesarios un sinfín de conexiones de todo tipo para la transmisión de datos, intercomunicación entre ellos, conexión de pantallas, etc. Estos cables de interconexión no pueden trazarse por encima del suelo, porque forzosamente impedirían comunicar fácilmente por la sala. Por ello, surge la necesidad de sobre-elevar el suelo y canalizar todos los cables por debajo de éste, además de que sirva como aislante de las distintas corrientes inducidas que, sin lugar a dudas, generan.

  Lo que se consigue con el falso suelo, se puede resumir en tres puntos fundamentales:

  - permitir cambios en la situación de las unidades.
  - proporcionar seguridad al personal
  - como "plenum" de aire acondicionado

  La solución que mejores resultados ofrece actualmente es el denominado "falso suelo de acceso libre", que consiste en unos "pedestales" regulables, en los cuales se apoya una estructura que permite encajar de manera sólida las baldosas. La regulación de estos pedestales es importante para el correcto nivelado del falso suelo.

No deberán cruzar la Sala de Máquinas conducciones de agua, excepto las específicas del aire acondicionado.

- *Tratamiento de las Paredes* : Deberá cumplir que no sea reflectante y no desprenda polvo. En cuanto al color, deberá ser de un tono claro.

- *Tratamiento del Techo* : El revestimiento del forjado superior, se realizará con un falso techo, que además puede servir de plenum para el aire acondicionado y para ocultar las interconexiones de los equipos eléctricos o los de alarma, y el trazado de las conducciones de extinción de incendios.

  Se deberán evitar las planchas de escayola tradicional, ya que desprende gran cantidad de polvo. Se deberá tener en cuenta que el coeficiente de inflamación de las placas sea mínimo, así como la absorción acústica, que es muy importante para la transmisión de ruidos.

  Lo que fundamentalmente debe cumplir un "falso techo" en una Sala de Ordenadores, se resume en tres puntos:

  - ausencia de polvo.
  - no combustible
  - absorción acústica

- *Tratamiento de la Altura de la Sala* : Es uno de los factores fundamentales a tener en cuenta para la elección de la planta donde se ha de situar la Sala de Ordenadores.

La altura comprendida entre el "falso techo" y el "falso suelo", deberá ser de unos 3 metros y, en ningún caso, inferior a 2'5 metros, según las condiciones de seguridad e higiene.

- *Tratamiento de las Puertas* : Deberán abrir hacia afuera y sus dimensiones deberán adaptarse al tráfico de la maquinaria.

- *Tratamiento del Aislamiento Acústico* : En la sala de ordenadores, generalmente no se exigen niveles acústicos acusados, debido a que es poco el personal que realiza allí un trabajo que requiera un nivel de concentración alto, pero es conveniente amortiguarlo.

  La sala de ordenadores el corazón del edificio, en el cual son naturales las palpitaciones sonoras. No obstante, generalmente se separa las máquinas más ruidosas, como impresoras, reproductoras y aquellas que comportan elementos de rotación. Una fuente generalizada de ruido la constituyen las salidas de aire acondicionado. Ello obliga a especificar niveles máximos admisibles para tales salidas.

  La técnica acústica consiste en reducir la propagación del ruido por diversos métodos : apantallamiento, absorción o combinación de ambos.

- *Tratamiento del Aislamiento Térmico* : La necesidad de ambientación de temperatura de un edificio depende evidentemente del poder aislante de su cerramiento, pero también de su situación y diseño.

En verano, las paredes acumulan el calor del exterior, radiándolo al interior y creándose, por la diferencia de temperaturas unas corrientes de convección causantes de algunas incómodas sensaciones que la refrigeración no logrará hacer desaparecer totalmente. Por tanto, deberá aislarse en la medida de lo posible, para que la climatización pueda rendir a pleno ritmo.

El aire acondicionado es un estándar obligatorio para cualquier oficina de hoy en día. Al margen de proporcionar un aire limpio, ventilación adecuada, control de la temperatura, dotar de aire acondicionado a una oficina sirve también para la eliminación del polvo y ruidos externos, ya que las ventanas se mantendrían cerradas durante todo el tiempo.

Para mantener en general un ambiente físico agradable, se debe contar con tres factores fundamentales:

- Temperatura : deberá oscilar entre los 20°C y los 24°C.
- Ventilación : deberá oscilar entre 12 m^3 y 15 m^3 de aire.
- Humedad relativa : deberá oscilar entre 45% y 55%.

La potencia frigorífica total de los equipos autónomos debe estar sobredimensionada respecto a las necesidades de la sala de ordenadores, de forma que al quedar eventualmente fuera de servicio un circuito (por avería de cualquiera de sus componentes), el resto de la instalación sea capaz de mantener las condiciones de la sala.

La distribución del aire climatizado para los ordenadores, se deberá efectuar a través del falso suelo. De esta manera, se forma en la misma

superficie del suelo un sistema flexible y seguro que permite el tratamiento de aire para el recinto. La aportación de aire exterior filtrado y tratado, tiene como finalidad la renovación del aire para el confort de las personas y para la creación de una sobre-presión en la sala.

El aire acondicionado, deberá se independiente para la Sala de Ordenadores. Dicho sistema debe tener una alarma en el área habitual de mantenimiento del edificio, para advertir al personal de servicio de una emergencia. Las canalizaciones para el aire acondicionado, deben ser de material incombustible. Así mismo, las canalizaciones para otras áreas que pasen por la Sala de ordenadores, deben contener compuertas con fusibles térmicos en cada pared de la Sala. Los filtros utilizados en el sistema de aire acondicionado deben ser de material incombustible o, como mínimo, de material auto extinguible.

- *Cuadros y Sistemas de Emergencia* : Dentro de la Sala de Ordenadores deberá instalarse un cuadro eléctrico general, lo suficientemente amplio para posibles modificaciones. Deberá poseer distribución de fuerza a posibles máquinas con acometida trifásica, además de neutro y tierra dotado de contacto general; diferencial de alarma y pulsadores en serie de corte de corriente de emergencia, todo ello identificado en el propio cuadro de acceso a la sala y en la salida de emergencia que actúa sobre el contador.

  La alimentación a dichos cuadros deberán proceder de la Unidad de Alimentación Ininterrumpida (UPS) y estar debidamente protegidas. Las canalizaciones para acometidas de corriente a los cuadros deberán ser lo suficientemente amplias para permitir posibles cambios.

Los pulsadores de corte de corriente de los cuadros de los ordenadores y del cuadro general de climatización, deberán estar situados dentro de la Sala de Ordenadores y dotado de contador general, pulsadores en serie identificados, de corte de corriente general de emergencia (para poner fuera de servicio a toda la instalación) en el propio cuadro. Deberá ademas, situarse otro interruptor junto a la puerta de acceso a la Sala, y otro más en la salida de emergencia actuando sobre el contador.

- *Equipo de Alimentación Ininterrumpida (UPS)* : Para la obtención de un alto grado de fidelidad en el suministro de energía a la Sala de Ordenadores, deberá realizarse la instalación de un equipo de Alimentación Ininterrumpida. Esto es debido a que la energía suministrada por las compañías de energía presenta numerosos fallos al cabo del año, como son los fallos que en consumos normales no se aprecian, pero sí afectan al ordenador, y fallos detestables fácilmente.

  El Sistema de Alimentación deberá estar formado por los siguientes elementos:

  - rectificador
  - grupo de baterías
  - inversor
  - bypass electrónico
  - sistema de sincronismo
  - controles e indicadores visuales y acústicos

  Las baterías podrán estar instaladas en una sala independiente o bien en un armario contiguo a la UPS.

El sistema de bypass estático sin corte permite transferir la carga desde el grupo de continuidad a la red, en caso de producirse un sobrecarga. De esta manera, el rectificador tomará la energía de la red transformándola en tensión continua; el inversor, a su vez, creará una tensión alterna estable que no dependerá de los fallos de tensión, ya que en caso de que la red falle, la energía será suministrada a través de las baterías y podrá cubrir tales fallos con una autonomía mínima.

La UPS cubre perfectamente la totalidad de los fallos de la red sin que la carga se percate de ello, asegurando un trabajo continuo y sin problemas de pérdida de información.

- *Seguridad contra Incendios* : Las salas de ordenadores deberán estar dotadas de detección de ambiente, "falso suelo" y "falso techo", mediante detectores iónicos-ópticos y extinción automática con Halón 1301, en ambiente y "falso suelo" como mínimo, calculada para una inundación con este gas en una proporción del 5% del volumen de la sala. Dicho hidrocarburo es utilizado para la extinción automática de incendios, especialmente en Salas de Ordenadores, ya que no deja residuos ni afecta al funcionamiento de los equipos eléctricos e informáticos, y además no es tóxico para el ser humano.

  En el resto del edificio, se deben instalar suficientes extintores portátiles de dióxido de carbono, recomendado para el equipo eléctrico. Estos extintores deberán estar correctamente señalizados y fácilmente accesibles para el personal.

Al margen del uso de extintores portátiles como agentes primarios de extinción , se aconseja colocar una boca de agua con manguera a una distancia efectiva del ordenador. Ésta sólo se utilizará como agente extintor secundario, debido a que el agua afecta de manera muy grave a los ordenadores.

3.1.7.- SEGURIDAD DEL PERSONAL INFORMÁTICO

Para el logro de una buena seguridad, tanto física como lógica, se deberá implantar una política de control del personal que presta sus servicios en el Centro de Proceso de Datos (tanto interno como de empresas subcontratadas), de tal forma que contemple los siguientes aspectos, necesarios para la integridad y privacidad de la información manejada en dicho servicio:

- incompatibilidades familiares en puestos de trabajo directamente dependientes

- establecimiento de un procedimiento formal de denuncias e investigación

- solicitud de referencia personales, en los casos en que proceda, al realizar nuevas contrataciones, subcontratados o traslados

- en el caso de empresas, hacer un procedimiento de clasificación y homologación de las mismas

- identificación del personal permanentemente visible

- evaluaciones periódicas del rendimiento

- evaluaciones periódicas del trabajo desarrollado

- evaluaciones periódicas de la evolución profesional

3.1.8.- SEGURIDAD DE LA INFORMACIÓN

En cuanto a la seguridad contra intrusos desde el punto de vista del acceso al Sistema, se deberán establecer mecanismos de control de los intentos de entrada o acceso al Sistema, de tal forma que permita la conexión cuando un usuario lo solicite y pase el control correspondiente, rehaciendo el intento en aquellos casos en que la identificación del supuesto usuario no sea satisfactoria.

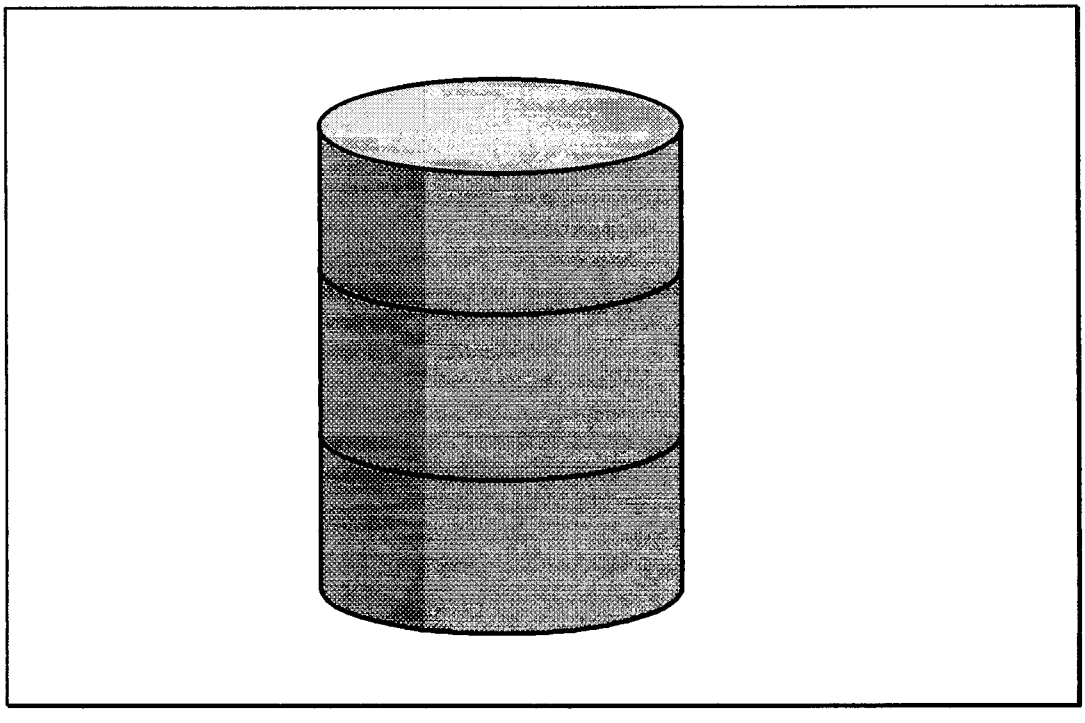
Uno de los mecanismos más usuales es la introducción de una Palabra Clave (PASSWORD) para la identificación del usuario. La fórmula más extendida es la de pedirle su nombre de usuario (USERNAME) y a continuación la palabra clave, tal que el mecanismo accede al archivo correspondiente para contrastar los datos recibidos y aceptar o rechazar el intento. Esta palabra clave se debe grabar en los archivos de administración del Sistema codificada o encriptada para que no sea fácilmente reconocible por cualquier persona.

Además, deberá elaborarse un organigrama alternativo, en el que cualquier puesto de responsabilidad específica, tenga previsto un técnico como suplente, para los casos de ausencias. Así mismo, deberá tenerse en cuenta esta definición de puestos claves para la planificación del período vacacional.

3.2.- SEGURIDAD LÓGICA

Seguridad Lógica incluye todos los mecanismos dirigidos a asegurar el Sistema Informático, siendo el propio sistema el que controla dichos mecanismos. También es denominada como Seguridad Interna.

La finalidad principal de los Sistemas Informáticos, es la del tratamiento de la información que se almacena permanentemente en las Bases de datos. La pérdida o alteración no deseada de dicha información, causaría trastornos que podrían ser irreparables en algunos casos.



3.2.1.- SEGURIDAD LÓGICA SOBRE EL SISTEMA

El punto más importante para el logro de una buena seguridad, es dotar al Sistema de un mecanismo para el control de los intentos de entrada o acceso al Sistema, de tal forma que permita la conexión cuando un usuario lo solicite y pase el control correspondiente, rehaciendo el intento en aquellos casos en que la identificación del supuesto usuario no sea satisfactoria.

Uno de los mecanismos más usuales es la introducción de una Palabra Clave (PASSWORD) para la identificación del usuario. La fórmula más extendida es la de pedirle su nombre de usuario (USERNAME) y a continuación la palabra clave, tal que el mecanismo accede al archivo correspondiente para contrastar los datos recibidos y aceptar o rechazar el intento. Esta palabra clave se debe grabar en los archivos de administración del Sistema codificada o encriptada para que no sea fácilmente reconocible por cualquier persona.

El Sistema deberá dotar al Administrador del Sistema, para que en cualquier momento, se pueda realizar un alta o una baja de un usuario, asignándole en el primer caso, ademas de un USERNAME, la correspondiente contraseña o PASSWORD inicial. Mientras que el USERNAME es público, la PASSWORD no lo es, siendo recomendable su cambio cada cierto tiempo.

Cuando es tecleada la PASSWORD en un terminal para su acceso al Sistema, no deberá aparecer en la pantalla como ocurre con el resto de los datos que se teclean, para así conservar el secreto de la misma.

Al proceso de petición de entrada a un Sistema, contestación a las preguntas de identificación, contrastación de los datos recibidos y dar el correspondiente acceso, se denomina LOGIN. Así mismo al proceso de despedida del Sistema, se le denomina LOGOUT.

Los intentos fallidos de acceso deben de ser registrados por el Sistema, con el fin de que el Administrador del Sistema pueda estudiar cada cierto tiempo si se está o no intentando transgredir la seguridad del Sistema.

3.2.2.- SEGURIDAD LÓGICA SOBRE LOS DATOS

No se incluye entre las funciones de un Servicio de Informática, la de mantenimiento de la Información y responsabilidad directa sobre ella. La información es propiedad y responsabilidad de los Usuarios que la producen, y debe de quedar siempre así. La Dirección de Sistemas de Información, sólo proporciona las herramientas para recogerla, almacenarla y difundirla, y es la responsable del buen funcionamiento de dichas herramientas y de la seguridad, confidencialidad y fiabilidad de la información, según criterios establecidos por sus propietarios.

Deberá existir, por lo tanto, un administrador de la Base de Datos, que asumirá la responsabilidad sobre la integridad y privacidad de los datos del Sistema.

- *Control de las Bases de Datos y Archivos* :
  - Instalación del Software
  - Mantener el Software actualizado
  - Realización del plan de Hardware y Software a corto y largo plazo
  - Control de la seguridad de las Bases de Datos y los Archivos
  - Control y uso de las utilidades
  - Definición y control de datos
  - Monitorización de rendimientos y ajustes
  - Procedimientos de Copias de Seguridad y de Recuperación
  - Planificación de Copias de Seguridad

- *Control de Usuarios* :
  - Procedimientos de autorizaciones
  - Procedimientos de seguridad
  - Estándares y formas de uso

- *Control de Documentación* :
  - de utilidades y procedimientos de backup y recovery
  - de definición de Base de Datos y Archivos
  - de Manuales de Software

Una cuestión que tiene gran importancia para los administradores de las Bases de Datos, es el desarrollo de un programa cuidadosamente planeado para las Copias de Seguridad (Backup) de las Bases de datos. Deberá hacerse diariamente, y se deberán realizar sobre soporte magnético, almacenándose en dependencias alejadas del Sistema y en armarios protegidos.

La documentación del Administrador, deberá contener toda la información necesaria de las rutinas y procedimientos de recuperación para que puedan ser consultados en cualquier momento por el personal de explotación que lo necesite.

Debido a que los sistemas de información no son inmunes a problemas que puedan conducir a la pérdida accidental de los datos, se debe tener en cuenta esto para la preservación de los datos de los archivos y de transacciones , tanto en la fase de diseño como durante la toda la vida del sistema.

Existen tres causas potenciales de la pérdida de datos:

- debido al procesamiento incorrecto de los datos o a un error del operador

- debido a las fallas del software de las aplicaciones
- debido a los desastres naturales, como incendios, inundaciones o terremotos, así como las fluctuaciones y fallos súbitos en la energía eléctrica durante el procesamiento del sistema.

Para solucionar estas pérdidas de información, y garantizar la integridad de los datos, existen los métodos de respaldo. Estos consisten en duplicar el conjunto original de datos. Existen varios métodos, para mantener estas copias de respaldo:

- Generación de archivos maestros
- Vaciado de archivos maestros
- Copias imágenes del registro

3.2.3.- SEGURIDAD LÓGICA SOBRE LAS APLICACIONES

El sistema deberá integrar un mecanismo de seguridad, que proteja la información registrada y restrinja los accesos a la misma mediante perfiles personalizados de usuario. De esta manera se garantizará la confidencialidad de los datos que genere, evitando posibles fugas de información.

Todos los accesos a los recursos y datos de los ordenadores deben estar perfectamente controlados, de manera que ninguna persona pueda acceder a información o herramienta a las cuales no esté autorizado.

Las validaciones de las transacciones, se llevan a cabo junto con los procedimientos de identificación del usuario. Se requieren varios niveles de identificación del usuario, para proteger totalmente al Sistema de la pérdida accidental de datos o del uso no autorizado.

Al entrar el usuario al sistema, se lleva a cabo el primer nivel de identificación. Esto se realiza por medio de una contraseña individual que los identifica de forma única. Además, habrá que especificar niveles adicionales de protección que soliciten a los usuarios demostrar que tienen la autorización.

Las password son uno de los elementos más importantes de la confidencialidad, y por eso debe existir una normativa que formalice tanto la codificación, como el mantenimiento de las mismas. De este modo, debe existir una mentalización de todo usuario sobre la confidencialidad de los códigos y claves de acceso.

Es necesaria la realización de una normativa sobre la gestión de los accesos de los usuarios : altas, bajas o modificaciones, y de obligada ejecución y cumplimiento una vez sea comunicada una incidencia sobre alguno de los usuarios por el órgano correspondiente.

Es importante que exista una normativa sobre la confidencialidad de la información. Es fundamental restringir lo más posible el acceso directo a la información reservada. Un foco peligroso es el Personal Informático descontento, dado de baja o despedido. Antes de salir de la empresa, podría realizar cualquier actividad nociva para los datos. Es conveniente controlar especialmente a estas personas, en los que se refiere a su acceso a la información de valor para la empresa.

Los sistemas informáticos, deben de cumplir unas normas de confiabilidad y de confidencialidad de los datos. Por ello deben de cumplir las siguientes normas :

- *Unicidad* : la información es actualizada por las unidades que la generan y se comparte con el resto, de forma que se evita la redundancia y se favorece la coordinación administrativa, garantizando la coherencia de dicha información.

- *Uniformidad* : la información se somete a idénticos tratamientos independientemente de la unidad en la que se recojan.

- *Accesibilidad* : toda la información recogida, se recupera por múltiples vías de acceso, y se preserva de la forma más conveniente y ágil para el usuario, en función de sus necesidades y la definición de su perfil. De

manera que el sistema es una herramienta eficaz para el control y mejora de la gestión, que permite la optimización de recursos y la mejora en los servicios.

- *Seguridad* : el sistema integra un mecanismo de seguridad que protege la información registrada y restringe los accesos a los mismos, mediante perfiles personalizados de usuario y sus correspondientes competencias garantizando la privacidad de la información.

3.3.- SEGURIDAD EN LAS TELECOMUNICACIONES

3.3.1.- SEGURIDAD FÍSICA

La función principal de las telecomunicaciones, es compartir información con otros usuarios. Por ello, es necesario proteger la información para que no se utilice de forma no autorizada.

A medida que un sistema aumenta, son cada vez más importantes la seguridad y privacidad de los datos; por tanto, es necesario y casi obligatorio, disponer de los dispositivos precisos para proteger esa información.

La misma tecnología que hace posible compartir la información y hacerla más productiva, puede destruir toda esa información. Si se desea mantener la información, es necesario proteger los datos y los programas contra fallos del equipo, errores de los programas o de los usuarios, o causas humanas o naturales, bien sean accidentales o deliberadas.

Es necesario una normativa para la prevención de aquellas acciones que puedan atentar contra la seguridad. Al mismo tiempo, esta seguridad tampoco debe restringir el trabajo de los usuarios.

En la mayoría de los sistemas, es suficiente una seguridad restringida, pero para ello es necesario la definición de una serie de medidas :

- *Medidas para la Seguridad Física* :

- Control del acceso a la zona donde se encuentran los equipos.
- Control ambiental de la zona donde se encuentran los equipos.
- Planificación para evitar accidentes.
- Prevención contra incendios y otros desastres.

- *Medidas para la Seguridad de la Información* :
  - Hacer copias de seguridad de los Datos.
  - Posibilidad de reconstruir la información.
  - Hacer copias de seguridad del Software.
  - Disponer de equipos de reserva.
  - Definición de claves de acceso.

Los usuarios de la red, han de estar identificados ante el Sistema. Éste permitirá acceder a los datos para los que el usuario tenga autorización. El control de acceso, se logra por medio de los siguientes métodos :

- *Claves de Acceso (Passwords)* : Es la más sencilla de las técnicas de control. El usuario ha de conocer la clave de acceso adecuada para poder entrar en la red y para tener acceso a determinados ficheros. Las claves de acceso se deben asignar y cambiar frecuentemente.

- *Tarjetas de Identificación y llaves de acceso* : Estos disponen de una pequeña memoria que contiene una identificación y una serie de algoritmos de autorización. Cuando el usuario introduce la tarjeta en un lector que está unido a la estación, el ordenador comprueba la validez de la identificación. Si la Tarjeta es válida, el ordenador inicia el proceso de acceso.

- *Sistema Operativo* : Controla el acceso a los datos, programas y dispositivos, mediante unas Tablas en las que se encuentran todos los usuarios junto con el tipo de acceso. Cada vez que el usuario solicita una información, el sistema comprueba en la tabla si está autorizado y el tipo de autorización.

En cuanto al control del acceso a la zona donde se encuentran los equipos, hay que destacar que las puertas del local deberán estar cerradas, las ventanas y puertas deberán estar protegidas por alarmas antirrobo, y se deberá identificar a todos los visitantes que entren en el lugar.

La información y el Software, han de guardarse en habitaciones cerradas, las estaciones deberán estar ancladas a la mesa y los diskettes se han de guardar cerrados con llave dentro de los cajones de la mesa o dentro de un fichero.

En cuanto al control ambiental de la zona donde se encuentran los equipos, el aire acondicionado se ha convertido en una necesidad. Además se deberá llevar el control del aire y la humedad.

3.3.2.- SEGURIDAD LÓGICA DEL SISTEMA

Deberá existir un administrador de las Telecomunicaciones que asumirá la responsabilidad plena de la Gestión las comunicaciones: Existen tres áreas principales:

- *Seguridad* : Consistirá en la asignación de contraseñas a los usuarios, el establecimiento de grupos de ellos y creación de informes acerca de la utilización real de las comunicaciones. Esta última tarea es esencial, porque los supervisores han de poder identificar a las personas que hayan venido accediendo a un directorio.

- *Rendimiento* : Puesto que los usuarios nuevos u ocasionales pueden experimentar dificultades con funciones de rutina, como la entrada (LOGIN), los supervisores, deberán de ayudarles estableciendo unos sencillos procedimientos o "rutinas" a seguir.

  Otro área del rendimiento de las comunicaciones es la observación permanente de las estadísticas de tráfico de la red, así como el hacer uso de ciertos medios o herramientas para contribuir al control del Sistema y al logro del máximo rendimiento.

- *Mantenimiento* : Esto no significa necesariamente la reparación física de los componentes defectuosos de la red, aunque la mayoría de las supervisiones de Sistemas grandes, lleva efectivamente un inventario de los componentes básicos para su sustitución inmediata en caso de avería.

Finalmente, los administradores necesitan llevar diarios de operaciones que faciliten la localización y el seguimiento de todos los cambios ocurridos en la red. Este libro o diario de operaciones debe guardarse bajo llave cuando no se esté utilizando.

Otro punto a tener en cuenta dentro de la seguridad de las telecomunicaciones, es la disponibilidad de Hardware de reserva. Es conveniente disponer de recursos secundarios, ya que en caso de una avería, el Sistema puede volver a ponerse en marcha, una vez reemplazado el dispositivo defectuoso, de tal manera que no se vea afectado el servicio prestado al usuario.

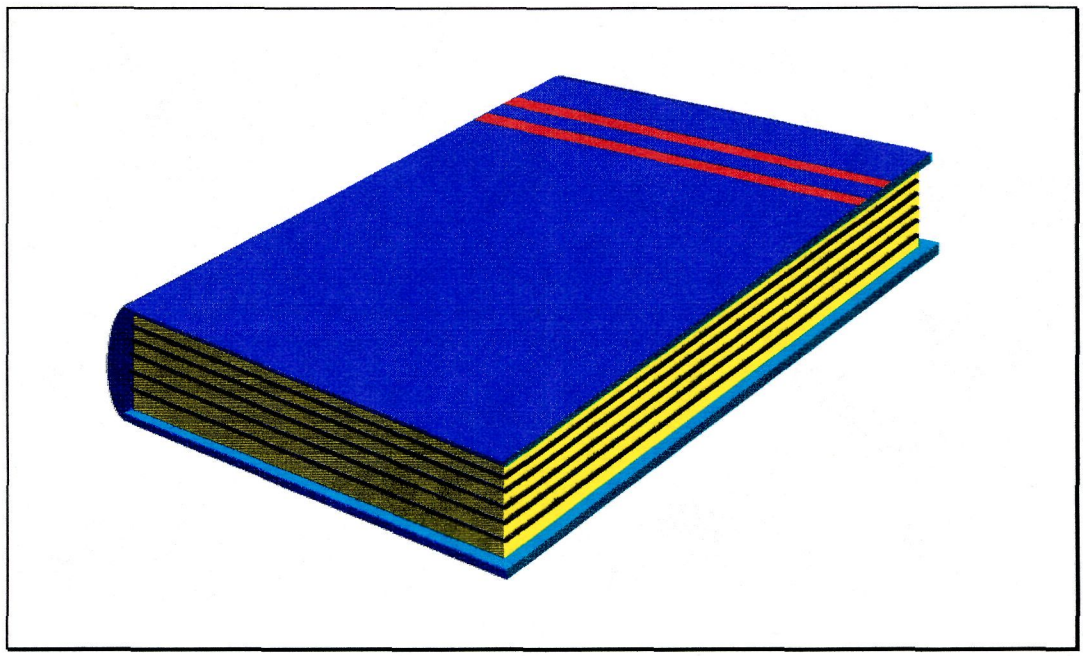
Uno de los puntos más importantes de un buen sistema es su documentación; cuanto mejor sea la documentación, más fácil será instalar y mantener el Sistema.

La documentación ha de ser una descripción completa de la Red, incluyendo las estaciones, los periféricos, los cables y otros dispositivos. La documentación del Administrador, deberá contener toda la información necesaria para mantener la Red. Habrá de incluir las guías de operación de todo el equipo, los códigos y mensajes de error del Sistema, las guías de localización de problemas, etc.

Una buena documentación deberá incluir ejercicios, prácticas e instrucciones paso a paso de todas las situaciones, además de una ayuda relativa al contexto con información resumida que le sirva al operador para salir de una situación determinada sin tener que recurrir a los manuales.

Además, la información de los manuales, ha de ser fácil de localizar, bien sea por medio de un índice de contenido o por cualquier otro método. Las

instrucciones de conexión y desconexión del Sistema y los comandos más importantes, deberán resumirse en una guía de referencia.



3.3.3.- SEGURIDAD LÓGICA DE DATOS

Una cuestión que tiene gran importancia para los administradores de las Telecomunicaciones, es el desarrollo de un programa cuidadosamente planeado para las Copias de Seguridad (Backup) de la Red. Deberá hacerse diariamente, pero en la mayoría de los Sistemas de Software exige el backup sólo de aquellos archivos que hayan sufrido modificaciones desde el último backup (mediante la hora de dichos archivos). Estos se deberán realizar sobre soporte magnético, almacenándose en dependencias alejadas del Sistema y en armarios protegidos.

La documentación del Administrador, deberá contener toda la información necesaria de las rutinas y procedimientos de recuperación para que puedan ser consultados en cualquier momento por el personal de explotación que lo necesite.

Por otro lado, para evitar el acceso a los datos durante la transmisión, lo que ocasionaría problemas de fiabilidad y de confidencialidad de la información, es recomendable la utilización de procedimientos de encriptación de la información. Este sistema de seguridad codifica todos los caracteres de un fichero, es decir, los cambia empleando un determinado algoritmo, de forma que no se pueda entender.

La mayoría de los sistemas de encriptación emplean una clave que consta de una clave de acceso o de números aleatorios, que se usa como base para codificar y decodificar los datos. Estos pasan por una serie de transformaciones y sustituciones, hasta que quedan irreconocibles, de modo que si se pierde la clave, los datos ya no se pueden decodificar. La instalación de un sistema de codificación se puede realizar mediante Hardware especial de codificación conectado a las lineas de comunicación, o Software implantado en cada estación.

Existen varios factores que influyen en la necesidad de la implantación de un sistema de encriptación de datos:

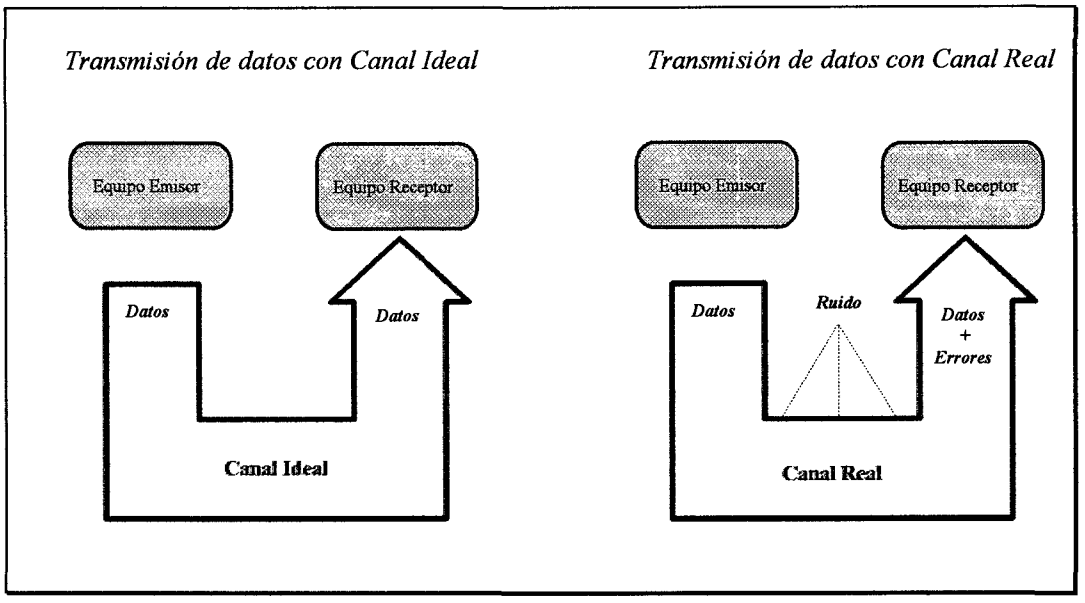
- El grado de importancia de la información : cuanto más valiosa, más necesario será su encriptación.

- El coste : el Software de codificación no es muy caro, pero necesita mucha memoria y tiempo para encriptarla. Por el contrario, el Hardware de codificación es bastante caro.

- El tiempo : el Software de codificación suele ser bastante lento, lo que reduciría el rendimiento de las comunicaciones. Siempre es posible utilizar Hardware de comunicación, que es varias veces más rápido que el Software.

Otro punto a tener en cuenta es la fiabilidad de la transmisión de los datos. La transmisión de datos es una actividad del mundo real en la que los procesos no siempre tienen el carácter ideal que se les ha asignado.

Uno de lo principales problemas que se presentan en los procesos de transmisión de datos, está relacionado con el hecho de que el medio de transmisión juega un papel activo en todo el proceso. Los medios de transmisión influyen introduciendo un elemento importante del proceso de comunicación : el ruido, que es el conjunto de todas las interferencias, de cualquier clase, que van a deteriorar la calidad de una transmisión, llegando hasta el extremo de generar errores que la dificulten o incluso la impidan.



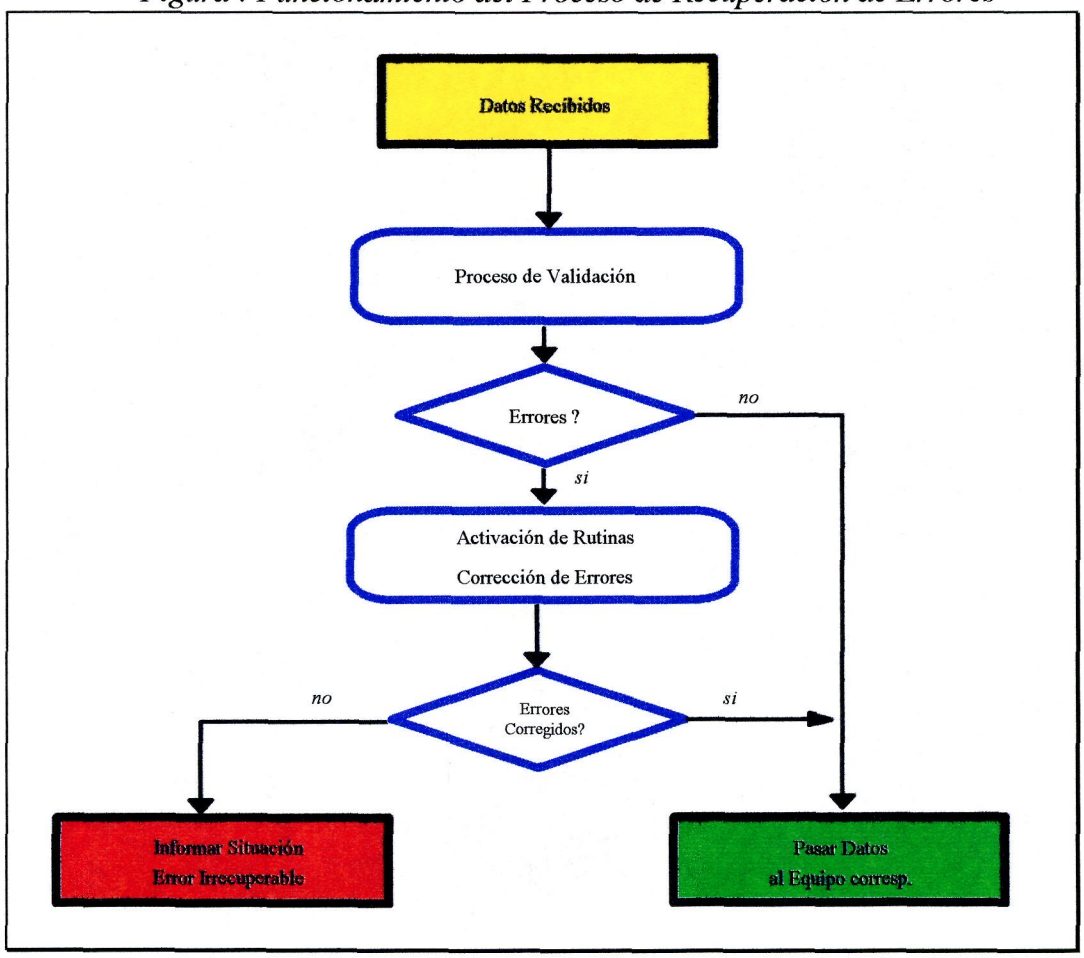
Cuando se diseña un equipo de transmisión o de conmutación de datos no se pueden tener en cuenta todos los factores que van a influir en su funcionamiento. El diseño debe tener un carácter lo suficientemente general y el diseñador o equipo de diseñadores deben atenerse a unos plazos y unos presupuestos determinados. Por todo ello se hace necesario introducir un elemento adicional en el proceso de comunicación de datos: los Sistemas de Control de Errores.

Dado que se sabe que en todo proceso de transmisión y recepción de datos existe una cierta probabilidad de que aparezcan errores, es importante dotar a los equipos involucrados en el proceso, de medios para:

- Detectar la presencia de errores y, por tanto, rechazar los datos afectados por los mismos.
- Corregir esos errores.

La idea fundamental de los equipos de recuperación frente a los errores, es la de conseguir que la comunicación resulte un proceso exento de errores.

Figura : Funcionamiento del Proceso de Recuperación de Errores



Cuando un equipo de comunicación de datos, detecta y corrige un error, se dice que ha sido *capaz de recuperarse frente a una situación de error.* La capacidad de recuperación de errores de los equipos de comunicación de datos, es una medida importante de su calidad.

Los sistemas de recuperación frente a situaciones de error, constan de dos módulos independientes:

- *Módulo de Detección de Errores* : que estará supervisando todo el proceso de la comunicación y validando todos los datos que vaya recibiendo.
  - Uso de la paridad
  - Uso de códigos de Redundancia Cíclica

- *Módulo de Corrección de Errores* : que entrará en funcionamiento cada vez que el módulo de Detección de Errores así lo indique.
  - Sistemas de Corrección hacia adelante
  - Sistemas de Corrección hacia atrás

3.3.4.- SEGURIDAD LÓGICA DE APLICACIONES

El sistema deberá integrar un mecanismo de seguridad, que proteja la información registrada y restrinja los accesos a la misma mediante perfiles personalizados de usuario. De esta manera se garantizará la confidencialidad de los datos que genere, evitando posibles fugas de información.

El método más sencillo es el de las Claves de Acceso o (PASSWORD). El usuario ha de conocer la clave de acceso adecuada para acceder al Sistema y a las aplicaciones permitidas. Estas claves se deben cambiar frecuentemente.

El Sistema, en el momento de la conexión del usuario, tras su identificación asigna el perfil correspondiente a dicho usuario, garantizando el acceso de las personas previamente definidas, destacando las siguientes funciones:

- definición de todos los aspectos de restricción de uso, de forma que todos ellos pueden ser asignados o no a un usuario.

- definición de usuarios, cuyo perfil de seguridad, se basa en la restricción o no de ciertos módulos.

- posibilidad de asignar un nivel de acceso a cada usuario, y a su vez, relacionarlo con el nivel de seguridad de ciertos procesos.

3.4.- CONTROL SOBRE LA EXPLOTACIÓN DEL SISTEMA

3.4.1.- SEGURIDAD FÍSICA DE SOPORTES MAGNÉTICOS

La inmensa cantidad de información procesada en el Centro de Proceso de Datos implica la existencia de gran número de soportes magnéticos para almacenarla convenientemente.

La información es el bien más importante que posee la entidad, y por ello necesita de unas medidas de seguridad específicas.

El almacenamiento de soportes magnéticos debe ser adecuado, en un lugar que reúna las condiciones de control precisas para los soportes magnéticos, tales como humedad, temperatura, y las medidas de seguridad adecuadas para evitar pérdidas o robos.

Las cintas deben estar en una sala específica para soportes magnéticos, separada de la que contiene los ordenadores, y las únicas personas que deben acceder a dicha sala, serán los que realicen la labor de bibliotecarios, con lo cual se consigue que el acceso este controlado.

Los soportes magnéticos deben poseer una etiqueta externa numérica o alfanumérica, que permita clasificarla y referenciarla adecuadamente, sin que por ello se suprima una adhesiva que indique el contenido.

Las cintas deberá ser clasificadas en base a esa etiqueta externa, y deberán ser solicitadas referenciándola por la misma.

La existencia de un gestor automático de soportes magnéticos facilita, en gran medida, la labor el bibliotecario para mantener un inventario actualizado de soportes, donde conste si está o no disponible, y en su caso de no ser así, el contenido y la vigencia del mismo. Este software puede adquirirse a una firma externa, pero podría también desarrollarse a medida según las necesidades del servicio.

Este gestor automático de soportes magnéticos debe ser de uso exclusivo del personal de la biblioteca y de los preparadores, o planificadores de tareas de explotación.

Todos los ficheros almacenados en soporte magnético, cinta o cartucho, que se conserven como seguridad, deben poseer etiquetas de cabecera, que el propio software pueda comprobar en el caso de que exista un error de los operadores al montar un soporte no adecuado.

El inventario de soportes magnéticos debe ser controlado de forma automática por los bibliotecarios, realizándose las altas, bajas y modificaciones en tiempo real, cuando se comunique la utilización o liberación de una cinta. Con este inventario se evitarán problemas de pérdida de soportes o almacenamiento de información no útil.

3.4.2.- SEGURIDAD LÓGICA SOBRE EL SISTEMA

En una instalación de Procesos de Datos de cualquier envergadura es fundamental que todos los procesos de explotación estén bien documentados, tanto documentación en papel sobre manuales manejables, como en comentarios que autodocumenten los procesos y faciliten su consulta diaria.

En particular, los procedimientos de explotación, por su naturaleza, deben tener una documentación muy clara y completa. La importancia de estos procedimientos no radica tanto en la perioricidad de su utilización como en la propia función que realizan.

Deberá establecerse un calendario dentro de los procesos de explotación diaria, en el que se contemple las pruebas de los procedimientos, de manera que se pueda garantizar su funcionamiento en el caso de que fuera necesario.

Este calendario deberá elaborarse para posteriormente incorporarse al los planes de explotación.

Deberá existir una copia de seguridad de toda la documentación generada en esta área. Esto resulta de gran ayuda, evitando pérdidas irrecuperables, recurrir a fuentes originarias para recuperar manuales, además de la pérdida innecesaria de tiempo.

Por otro lado, debería llevarse un libro o cuaderno de incidencias, a modo de diario de problemas, en el que se reflejen todas las incidencias acaecidas, la hora y la fecha, la causa que la motivó (en caso de conocerse), las acciones correctoras

y los efectos ocasionados por dicha incidencia, dejando constancia de si se solventó o no, y en que fase de resolución se halla, para documentar a la persona que lo consulte.

Este libro deberá ser consultado por el Jefe del Sala de cada turno, y formará antes de que se proceda al relevo por el turno siguiente.

Será de responsabilidad directa del Jefe de Explotación, o de la persona en quien se delegue, el mantener una biblioteca de documentación de todas las aplicaciones y programas existentes en el ámbito de explotación, y exigir que junto con el traspaso de un módulo nuevo o modificado a explotación, se envíe la documentación correspondiente. De esta forma, se garantizará la actualización de la documentación de las aplicaciones en explotación.

3.4.3.- SEGURIDAD LÓGICA SOBRE TAREAS DE EXPLOTACIÓN

La planificación de los trabajos en procesos *batch* es una de la labores más importantes del entorno de explotación, y por lo tanto, de las más peligrosas. Deberá realizarse la adquisición de un producto software adecuado o, en su defecto, desarrollar uno que se adapte a la instalación y que cubra las necesidades actuales.

La planificación deberá conllevar la comprobación a posteriori de la realización de todos los trabajos planificados, y de su correcta planificación, por parte de los técnicos que realicen la labor de supervisión. Para ello, es de gran utilidad la revisión exhaustiva del *log* de actividad, donde queda constancia de aquellos trabajos procesados, y si han finalizado correctamente, además se puede comprobar si se ha repetido indebidamente algún proceso. Es por ello que el log debe tener un período de retención alto, de manera que en cualquier momento se pueda acudir a él para localizar una situación concreta, o la causa de un error manifestado con cierto retraso.

Deberá crearse una normativa para la codificación de nombres, tanto de programas como de jobs, que los identifiquen claramente y les asigne una aplicación sin necesidad de recurrir a diccionarios o documentación anexa.

Deberá llevarse un libro de incidencias, en el cual, el operador refleje todo tipo de incidencias y las causas que las provocaron, así como las acciones correctoras en cada caso. De esta forma, además de un registro adecuado de los hechos acontecidos, se poseerá un manual al cual recurrir en caso de que se presenten

situaciones repetidas, Posteriormente, pueden realizarse estudio en base a las incidencias y elaborar estadísticas concretas.

A continuación se exponen las tareas que se recomienda seguir:

- *planificación de la carga diaria*: consiste en la determinación, preparación y adecuación de los procesos diarios, de los trabajos a ejecutar. Para esta tarea el planificador/preparador se apoya en la información contenida en el manual de explotación.
- *manipulación de discos, cintas o cartuchos*: Por un lado, el planificador define y prepara, desde el día anterior, los soportes físicos a manipular, y por otra, los operadores manipulan en el momento de ejecución de las cadenas, dichos soportes. Para ello, ambos deben tener conocimiento de los flujos de los procesos, así como de las vigencia de las distintas versiones de los ficheros, información contenida en los documentos de descripción de procesos y ficheros.
- *desencadenamiento de procesos*: esta tarea consiste en el lanzamiento de los distintos trabajos, de acuerdo con la planificación elaborada previamente.
- *tareas de recuperación y reincido del sistema:* durante las ejecuciones de los trabajos puede existir incidencias que obliguen a tomar determinadas acciones por parte del personal de operación, a dichas incidencias corresponden unos procedimientos de recuperación y rearranque que estarán plasmados en la correspondiente documentación del sistema.
- *procedimientos de emergencia:* en la explotación de sistemas pueden darse situaciones en las que, debido a causas externas al sistema, no se disponga de la funcionalidad completa. En este tipo de situaciones los

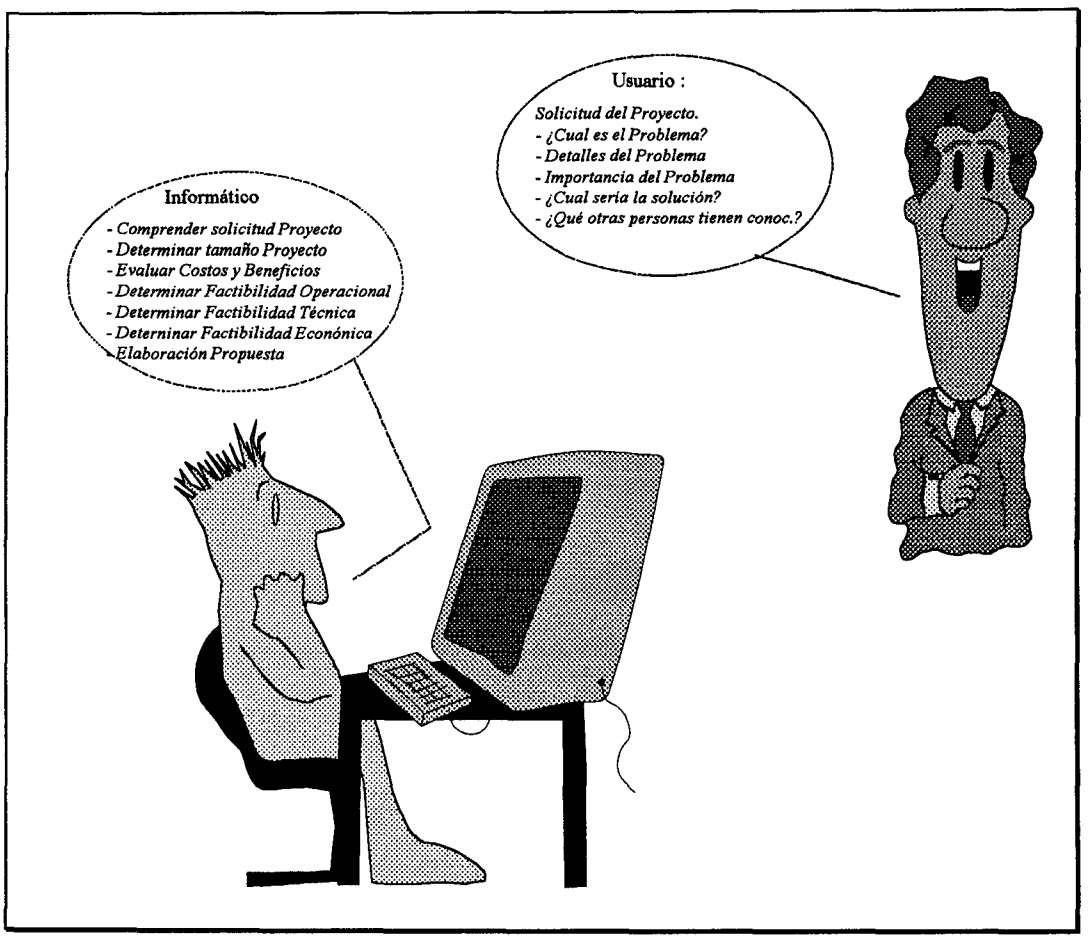
procedimientos de emergencia contemplan los pasos que deben ser dados si el sistema va a estar indisponible total o parcialmente por un tiempo.

- *comprobación de ejecuciones*: mediante esta tarea el personal de explotación verifica la correcta ejecución de los trabajos procesados. Los puntos de control necesarios deberán estar documentados.
- *control de entrega de informes*: sirviéndose de la documentación del sistema preparada a tal efecto, el planificador realiza las comprobaciones pertinentes para asegurar la correcta edición y distribución de todos los informes previstos.
- *mantenimiento de históricos y copias de seguridad*: mediante esta tarea el personal de explotación asegura la correcta realización de las copias de seguridad, así como la elaboración de históricos, de acuerdos con los requerimientos del sistema, descritos en la documentación del mismo.

3.5.- CONTROL SOBRE DESARROLLO Y MANTENIMIENTO DE APLICACIONES

3.5.1.- ESTUDIOS DE VIABILIDAD

La propuesta de proyecto presentada por los usuarios, es un elemento crítico para emprender el estudio de un Sistema de Información. Aunque el formato de dicha solicitud cambia dependiendo de la necesidad, debe de existir una normativa general sobre la clase de información que deberá contener.



En la propuesta, el solicitante identifica dónde necesita la asistencia y proporciona los detalles. En ella se deberá indicar :

- Identificación del Problema
- Detalles del Problema
- Importancia del Problema
- Solución al Problema, según el solicitante
- Indicación de otras personas que tengan conocimiento del problema

Si se va a desarrollar un Sistema por cualquiera de las estrategias de desarrollo, primero es necesario revisar la solicitud del Proyecto. La elección de una estrategia de desarrollo es un aspecto secundario; lo importante es determinar si la solicitud merece o no la inversión de recursos en un proyecto de Sistemas de Información.

La finalidad de la investigación preliminar es evaluar las solicitudes del proyecto. Es la reunión de información que permite emitir un juicio respecto a la factibilidad del proyecto propuesto.

En la investigación preliminar o el Estudio de Viabilidad, se deberán satisfacer los siguientes objetivos:

- Aclaración y comprensión de la solicitud del Proyecto : los datos recogidos durante la investigación se reúnen por medio, principalmente de dos métodos:
  - Revisión de los Documentos de la organización
  - Conducción de entrevistas

- Determinación del tamaño del Proyecto.

- Evaluación de los Costos y Beneficios de diversas opciones.

- Determinación de la Factibilidad del Proyecto, es decir, la posibilidad de que el sistema sea de utilidad para la organización. Se estudian tres pruebas de factibilidad :

  - *Factibilidad Operacional* : los proyectos propuestos únicamente tienen beneficio cuando logran ingresar al grupo de sistemas de información que satisfacen los requerimientos de la organización.

  - *Factibilidad Técnica* : los proyectos propuestos debe de cumplir con unas condiciones de garantías tecnológicas, de capacidad de datos, de exactitud, confiabilidad, facilidad de acceso y seguridad de datos.

  - *Factibilidad Financiera y Económica* : un Sistema que puede ser desarrollado desde el punto de vista técnico y que, además, sería utilizado si se llega a instalar, debe ser una buena inversión para la organización. Los beneficios financieros deberán igualar o exceder a los costos.

  Para ser considerada como factible, la propuesta deberá pasar todas las pruebas, de lo contrario, el proyecto no será factible.

3.5.2.- **CONTROL DE PROYECTOS**

El control y seguimiento de los proyectos es fundamental, y debe ser realizado de forma continua, en todos los proyectos del Área de Desarrollo.

Este problema, que lleva a algunos Servicios de Informática, a prescindir de todo tipo de medida del trabajo de Desarrollo, no debe hacerles renunciar a obtener unas medidas mínimas que permitan adoptar medidas correctoras y mantener los planes con desviaciones aceptables. Estas unidades de medida utilizadas, no tienen un valor exacto pero pueden obtenerse aproximaciones muy valiosas.

De entre los parámetros que pueden obtenerse, los más interesantes para un Servicio de Informática son :

Parámetros de Servicio	- Calidad - Plazo
Parámetros Económicos	- Costo - Rendimiento
Parámetros de Planificación	- Cantidad de Trabajo realizado - Cantidad de Trabajo pendiente

Las medidas más utilizadas son :

- *Para Desarrollo de Aplicaciones* :

  - **Calidad** : Indica el grado de acabado de la Aplicación en el período de tiempo medido. Este medida debería complementarse con una apreciación subjetiva, realizada por un Analista (distinto al Responsable de Desarrollo), acerca del Consumo de Recursos, Mantenibilidad, Documentación, etc.

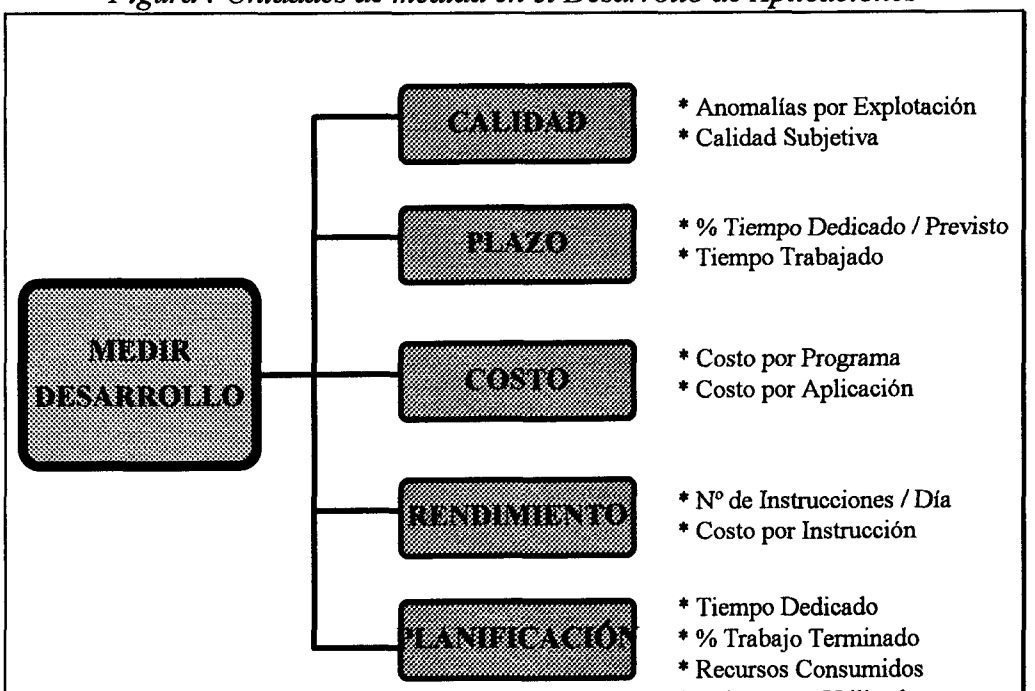
  - **Plazos** : Da una idea del tiempo medio que se tarda en atender una petición, cuando se trata de trabajos planificados o bien, para trabajos puntuales.

  - **Costo** : Tiene como componentes el tiempo de Desarrollo y los Recursos de Explotación.
  Una vez obtenidos los datos por Programa o por Aplicación, puede realizarse una clasificación, que muestre claramente dónde se consume la porción de recursos más importante.

  - **Rendimiento** : Permite una cierta evaluación de la eficacia de los Programadores, de los Lenguajes de Programación, de los Equipos de trabajo o de la propia Instalación con relación a otros.

  - **Planificación** : Permite una orientación sobre el esfuerzo de Desarrollo pendiente y, en consecuencia, el plazo y costo finales previsibles.

Figura : Unidades de medida en el Desarrollo de Aplicaciones



- *Para Explotación de Aplicaciones* :

  - **Calidad** : Puede aplicarse al conjunto de anomalías ocurridas en la explotación de los trabajos o desglosarse por causas. También puede limitarse a las anomalías detectadas por los Usuarios (Cantidad Real) o extenderse también a las detectadas y corregidas antes de la entrega de resultados (Calidad Final).

  - **Plazos** : Se suele medir en períodos de tiempo dados (diario, acumulados mensual y anual) para cada Transacción, para cada Aplicación y para el conjunto.

- **Costo** : La medida del Costo de Explotación está muy ligada al Sistema Operativo con el que se trabaje y, más en concreto, a las facilidades de medida que el propio Sistema Operativo aporte. Los parámetros que normalmente se utilizan se refieren a cada trabajo concreto (un Programa, una Aplicación, una Transacción, etc.).

Por otro lado, se determinan unos valores estándar en ptas./unidad que permiten calcular los costos.

Algunos Sistemas hacen una evaluación conjunta de la utilización de todos los recursos asignando un peso uno y proporcionan un parámetro único que denominan . "Unidad de Servicio".

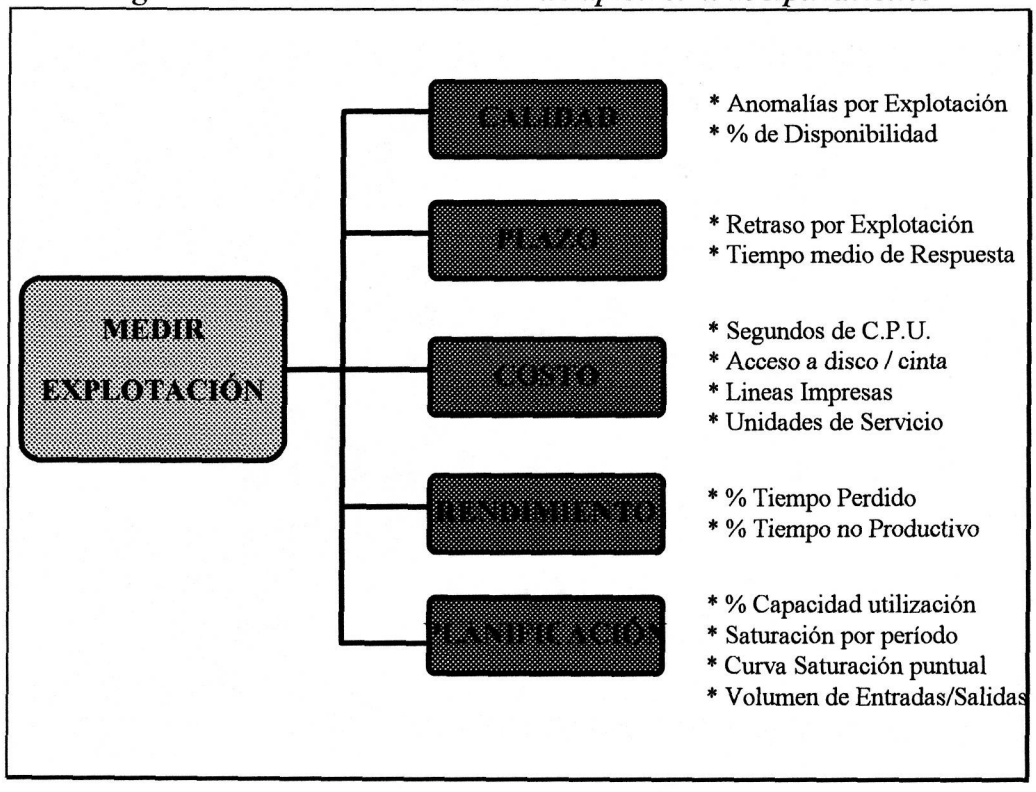
Al igual que los anteriores, debe calcularse aparte el valor estándar de una Unidad de Servicio.

- **Rendimiento** : Las medidas de Rendimiento en Explotación, están orientadas a medir pérdidas por anomalías y explotaciones inútiles y pérdidas por trabajos internos del Servicio de Informática.

- **Planificación** : Permite una orientación sobre el grado de utilización de la capacidad total del Ordenador. Deberá ser establecida previamente con ayuda de la experiencia y del propio fabricante. La Capacidad total debe tomarse en el sentido de "la máxima alcanzable en la práctica" y no "la teórica anunciada por el Proveedor".

Esta medida sirve para analizar las previsiones de saturación media del equipo. Puede verse desvirtuado por la existencia de períodos de carga reducida (por ejemplo los turnos de tarde y noche), por lo que habrá de obtenerse por períodos separados e incluso por períodos muy cortos para obtener el grado de saturación puntual.

Figura : Unidades de medida en la Explotación de Aplicaciones



Para la realización de todas estas medidas que hacen posible el control y seguimiento de los proyectos es fundamental, la utilización de Herramientas, que deberán de ser implantadas en el Servicio de Informática y de las que se desarrollará una normativa de uso obligado para todos los técnicos.

A continuación se enumeran algunas de las herramientas de medida tanto para Aplicaciones en Desarrollo como de Explotación:

- *Parte Diario de Anomalías de Explotación* : Será elaborado por el Servicio de Informática e informado por los responsables de las anomalías. Permite establecer su número y tipo.

- *Diario de Explotación* : Este diario es proporcionado normalmente por el propio Sistema Operativo. Relaciona todos los trabajos realizados y su consumo de recursos. Si el Sistema Operativo no proporciona esta información, deberá ser elaborada por los operadores, tomando como uso de recursos el tiempo de presencia en el Ordenador.

- *Diario de Trabajos solicitados a Desarrollo* : En este diario se anotará la Fecha de Petición de cada trabajo, una descripción breve del mismo y anotaciones adicionales sobre el grado de dificultad, situación, plazo previsto, etc.

- *Diccionario de Programas* : En él se recogerá para cada Programa de la instalación, entre otras cosas, el número de Instrucciones que lo componen, su Identificación, el Lenguaje de Programación, Aplicación a la que pertenece, Programador que lo desarrolló, etc.

- *Control de Producción del Área de Desarrollo* : Deberá recoger. de cada persona todos los tiempos dedicados al nivel de Aplicación, Programa y Actividad Específica.

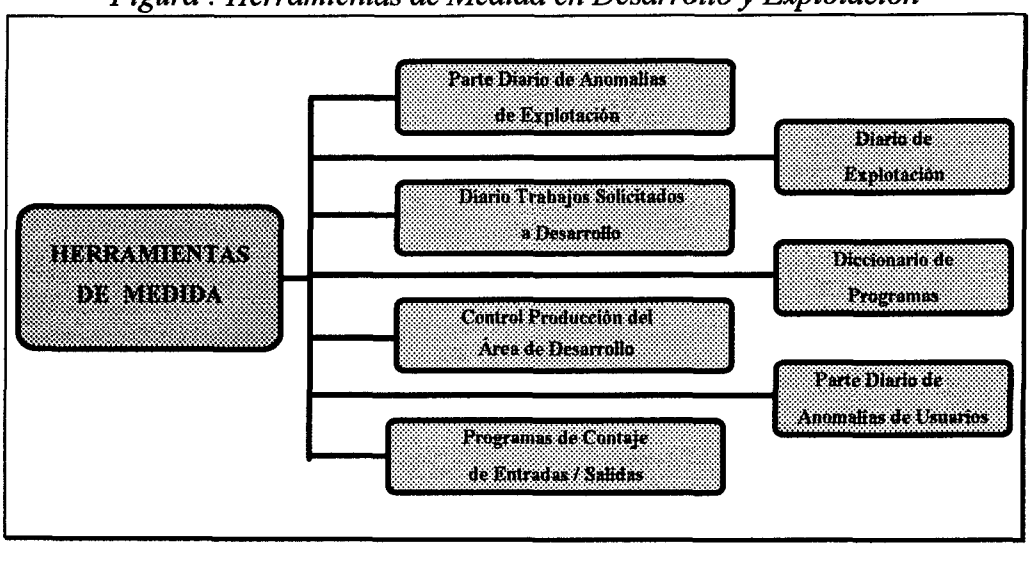
  Si el número de personas es elevado, puede incluso desarrollarse una aplicación interna para este fin. El problema más importante para obtenerlo reside, en obligar a todas las personas a que realicen su declaración y conseguir que ésta sea medianamente correcta.

- *Parte Diario de Anomalías de los Usuarios* : Para las explotaciones de procesos batch, estos partes deberán recoger todas las anomalías que detecten los usuarios, tanto en la calidad de los resultados, como en el

plazo de entrega. Para las explotaciones de aplicaciones en tiempo real, deberán recoger los tiempos de no disponibilidad, incidente y tiempos de respuestas anómalos.

- *Programas internos para medir datos* : Serán elaborados por el Servicio de Informática para medir el número de datos de entrada y de elementos de salida (lineas impresas, registros de un fichero, hojas de un impreso, etc.). Estos programas, suelen incorporarse a cada Aplicación.

Figura : Herramientas de Medida en Desarrollo y Explotación



Una vez realizada la actividad de Medir, a continuación se obtienen conclusiones acerca del trabajo medido. Para deducir las conclusiones sobre los resultados de una medida, es preciso poder compararlos con valores de referencia que previamente hayan sido establecidos como "Aceptables". Dichos valores de referencia, son denominados ***estándares.***

Cada instalación de Proceso de Datos es diferente de las demás: cambian los equipos instalados, los Sistemas Operativos, los Lenguajes de Programación, las

responsabilidades, la experiencia de los técnicos, etc. Como consecuencia, los estándares de referencia son diferentes y deben establecerse en la propia instalación.

Los estándares varían con el tiempo. Su mejora se incluye entre los objetivos de la Dirección de Informática.

La comparación de los resultados logrados en los distintos Departamentos de la Dirección de Informática con los estándares esperados, puede provocar tres tipo se actitudes:

- alerta ante unos resultados decididamente inadecuados para el nivel de servicio comprometido con los usuarios.

- confianza cuando dichos resultados son satisfactorios y no existen perspectivas o necesidad de mejorarlos aún más.

- Deseos de mejora, bien porque el grado de satisfacción no sea completo, bien porque existen caminos claros para lograr dicha mejora sin perjudicar la rentabilidad de la actividad mejorable.

Tanto el primer caso como el tercero, propician la aplicación de medidas correctoras, pero mientras las del primero tienen un carácter de urgencia, de acción inmediata carente a veces del proceso de estudio y planificación necesarios, las otras pueden enfocarse como proyectos de mejora y permiten acudir al mercado de software en busca de la herramienta que permitirá alcanzar el grado de mejora buscado.

Existen algunos caminos posibles de mejora de los distintos parámetros reflejados en el sistema de medidas y estándares :

- *Para Desarrollo de Aplicaciones* :

  - **Calidad** : Existen en el mercado gran número de productos que disminuyen el trabajo de Desarrollo aumentando a la vez la fiabilidad de los programas desarrollados:
    - Generadores de Informes
    - Manejadores de Librerías
    - Software de Aplicaciones concretas
    - Recogida de datos on line
    - Gestión y acceso a Bases de Datos
    - Generadores de Transacciones
    - Lenguajes de 4ª Generación

  - **Plazo y Rendimiento** : Las mismas ayudas a la Calidad, introducen mejoras en el plazo. Terminales e incluso ordenadores dedicados exclusivamente al proceso de Desarrollo, son también ayudas importantes que pueden justificarse con volúmenes de desarrollo elevado.

  - **Costo** : Ayudan las mismas herramientas mencionadas para la Calidad, Plazo y Rendimiento, aunque debe hacerse la salvedad de que en general, el uso de herramientas de Desarrollo más potentes puede acarrear un aumento en los costos de prueba de Programas y, más aún, en los de Explotación de las Aplicaciones.

- **Planificación** : Los errores de cumplimentación del Plan de Desarrollo, suelen deberse más a defectos de la propia Planificación que a la mala utilización posterior de los recursos. Planificar un proyecto en sus etapas iniciales origina grandes errores por la gran cantidad de variables que se desconocen.

- *Para Explotación de Aplicaciones* :

- **Calidad** : La mejora de la Calidad en la Explotación, puede conseguirse por alguno de los caminos siguientes :
  - mejora en los Procedimientos de Explotación
  - mejora en las Normas de Control de Calidad
  - mayor implicación de los operadores en su trabajo

La colaboración de Soporte de Sistemas es fundamental en el primer camino. Una de sus actividades principales es, justamente, la elaboración de procedimientos y software de ayuda a la Explotación.
En la mejora de las Normas de Control de Calidad, la mayor participación corresponde a los Departamentos de Diseño y Desarrollo.

- **Plazo y Rendimiento** : Los retrasos en la entrega de resultados se deben a :
  - Problemas de Hardware : sólo se solucionan con un buen sistema de mantenimiento y con equipos de backup.
  - Problemas de Sistema Operativo : se solucionan reduciendo al máximo el número de cambios en el Sistema y a la realización de pruebas exhaustivas en cada cambio.

- Problemas de Aplicaciones : se solucionan con cualquiera de las opciones de la Calidad en el Desarrollo.

- **Costo** : Los costos de Explotación vienen condicionados por la calidad del trabajo de Desarrollo. Existen en el mercado analizadores de aplicaciones que alertan sobre el exceso de consumo de recursos. Una buena medida, sigue siendo también hacer que Desarrollo revise y optimice aquellos programas que consumen gran número de recursos.

- **Planificación** : La curva de saturación de los equipos instalados, debe proyectarse continuamente en función del plazo previsible para la renovación de los equipos.

3.5.3.- CONTROL DE DESARROLLO DE APLICACIONES

En un Servicio de informática, debe adoptarse una normativa establecida por la organización y de obligado cumplimiento, para la realización de cualquier desarrollo de un sistema informático.

Los objetivos del diseño de sistemas son muy amplios y afectan a aspectos, tanto de la aplicación como de la organización en la que será implantado dicho sistema. Por consecuencia, no ha de sorprender el hecho de que los grupos de sistemas de información mejor manejados, también mantengan estándares para el desarrollo de sistemas. Las especificaciones de diseño, se establecen dentro del marco fijado por estos estándares:

- *Estándares para Datos* : Normas para asignar a los datos y especificar su longitud y tipo. Estos serán utilizados por todas la aplicaciones desarrolladas por el grupo de sistemas de información. Con frecuencia estarán contenidos en el Diccionario de Datos.

- *Estándares de Codificación* : Abreviaturas y designaciones formales para describir actividades y entidades dentro de la organización.

- *Estándares Estructurales* : Normas sobre cómo estructurar el software del Sistema : dividir el software en módulos, para la codificación estructurada y la relación existente entre los componentes del sistema.

- *Estándares de Documentación* : Descripciones de las características del sistema, de la relación entre componentes y de las características de

operación que pueden ser revisadas para conocer los detalles de la aplicación.

Con el objeto de garantizar que la aplicación cumpla con los estándares, muchas organizaciones cuentan con un grupo de control de calidad, que tiene la responsabilidad de revisar todas las especificaciones de diseño de sistemas de información, así como el propio sistema una vez terminado.

Existen también estándares a seguir en cuanto al diseño de cualquier sistema informático:

- *Diseño de Controles* : Los analistas de sistemas, deberán anticipar los errores que se cometerán al introducir los datos en el sistema o al solicitar la ejecución de ciertas funciones. Algunos errores no tienen importancia ni consecuencias, pero otros pueden ser tan serios que podría ocasionar el borrado de datos o el uso inapropiado del sistema. Aunque exista sólo la más mínima probabilidad de cometer un error serio, un buen diseño de sistemas de información ofrecerá los medios para detectar y manejar un error.

  Los controles de entrada proporcionan medios para :
  - asegurar que sólo los usuarios autorizados tengan acceso al sistema
  - garantizar que las transacciones sean aceptables
  - validar los datos para comprobar su exactitud
  - determinar si se han omitido datos que son necesarios

- *Diseño de Procedimientos* : Los procedimientos especifican qué tareas deben efectuarse al utilizar el sistema y quienes son los responsables de llevarlas a cabo.

  Entre los procedimientos importantes, se encuentran :
  - Procedimientos para entrada de datos : métodos para la captura de datos de las transacciones y su ingreso en el sistema de información.
  - Procedimientos durante la ejecución : pasos y acciones emprendidos por los operadores del sistema, y en ciertos casos, por los usuarios finales, que interactúan con el sistema para alcanzar los resultados deseados.
  - Procedimientos para el manejo de errores : acciones a seguir cuando se presentan resultados inesperados.
  - Procedimientos de seguridad y respaldo : acciones para proteger el sistema y sus recursos contra posibles daños.

  Estos procedimientos deberán formularse por escrito y formar parte de la documentación del Sistema en su paso a Explotación.

- *Diseño de especificaciones para Programas* : En ellas se describen cómo transformar las especificaciones de diseño del Sistema (salidas, entradas, archivos, procesamiento y otros) en Software de computadora.

  El diseño del software de computadora es importante para asegurar que :
  - los programas producidos lleven a cabo todas las tareas y lo hagan de la forma establecida.
  - la estructuración del software en módulos permita su prueba y validación para determinar si los procedimientos son correctos.

- las modificaciones futuras se puedan realizar en forma eficiente y con un mínimo de interrupción en el diseño del sistema.

3.5.4.- CONTROL DE LA EXPLOTACIÓN DE APLICACIONES

El final del desarrollo de una aplicación, lo marcan las pruebas de aceptación. Éstas son independientes de las pruebas que el equipo de Desarrollo realizan para probar sus trabajos. En las pruebas de aceptación participan tanto personal informático como usuarios finales.

La formación a Usuarios finales es previa a la puesta en marcha de la aplicación. En su transcurso, los usuarios deberán conocer los nuevos procedimientos de trabajo, las salidas (listados y documentos) de la aplicación, la corrección de errores, etc.

Al terminar un nuevo sistema y estar listo para el paso a explotación, es necesario llevar a cabo una serie de tareas, tales como verificar que el nuevo sistema está operativo, eliminar el antiguo, formar a los usuarios, desarrollar el manual de mantenimiento, instalar el sistema en explotación, comprobar el perfil de los usuarios finales que tendrán acceso al mismo, dar de alta los privilegios al nuevo sistema,...

Para el paso a explotación deberá presentarse la siguiente documentación:

- *Inventario de Ficheros:* consiste en una relación de los ficheros que utiliza el sistema, incluyendo una breve descripción del contenido funcional de los mismos.
- *Descripción de Ficheros*: para cada fichero existe un documento en el que se detallan las características del mismo.

- *Inventario de Programas*: consiste en una relación de todos los programas del sistema, con un breve descripción del objetivo de los mismos.
- *Descripción de Programas*: consiste en una información detallada de los objetivos de cada programa, incluyendo el flujo del proceso correspondiente, con los ficheros utilizados y los informes emitidos,..
- *Inventario de Pantallas*: consiste en una relación de todas las pantallas de la aplicación, en el cual se incluye la identificación funcional de las mismas.
- *Descripción de Pantallas*: para cada pantalla de la aplicación se facilita una información que comprende la representación gráfica de la misma.
- *Inventario de Informes*: consiste en una relación de todos los informes emitidos por la aplicación, incluyendo número de copias, destinatarios y perioricidad.
- *Descripción de Informes*: para cada informe existe un documento, que consiste en la representación gráfica del mismo, así como las indicaciones necesarias para su verificación y control.
- *Inventario de Tablas*: consiste en una relación de todas las tablas que contienen datos a utilizar como parámetros de la aplicación.
- *Descripción de Tablas*: para cada tabla se editará un documento con los valores específicos correspondientes a cada parámetro.

3.5.5.- CONTROL DE MANTENIMIENTO DE APLICACIONES

Debe considerarse la adopción de una normativa que, oficial y comúnmente aceptada por el Área de Desarrollo y Mantenimiento, marque las pautas a seguir en la prueba de programas o aplicaciones.

La adopción de esta norma eliminará los problemas existentes en este ámbito, como son errores de programas en explotación por haberse probado deficientemente, o la utilización de datos reales para las pruebas, con la pérdida de confidencialidad que ello ocasiona.

Esta norma contemplará la creación de modelos completos de ensayo que, para cada programa, estudien todas las posibilidades existentes. Se realizarán a medida de la aplicación, y debido a sus características propias, deberían ser guardados como parte integrante de la documentación.

Los programas deberán ser probados individualmente una primera vez, y luego dentro del marco total de la aplicación, para la comprobación del interface entre dichos programas. Todo ello, previo su traspaso a explotación.

Se recomienda, en cuanto a las pruebas de calidad, que se contemplen cuatro niveles:

- *Prueba:* Ejecutar un programa con la intención de hallar errores
- *Verificación*: Ejecutar un programa en un simulacro para detectar errores
- *Validación*: Uso del software en una ambiente no simulado
- *Certificación*: Garantía del correcto funcionamiento

Las estrategias de prueba se refieren a las pruebas de la lógica del programa y las pruebas de las especificaciones del proceso. En cuanto a los niveles de prueba se deberán realizar pruebas parciales, de carga máxima, de almacenamiento, de procedimientos, y del tiempo de ejecución.

Se recomienda la creación de una librería de prueba con datos desarrollados para realizar las pruebas de la totalidad de un sistema, que por otro lado, deberá conservarse durante toda la vida del sistema, ya que para el mantenimiento posterior también sería de gran utilidad.

Los datos de salida deben de sufrir un proceso de conciliación con los de entrada, no sólo a nivel de trámites generales, sino también a datos concretos, incluso si estos proceden de cálculos. Para ello, podrán realizarse comprobaciones muestrales sobre elementos convenientemente extraídos de la población total.

En el caso de que se produzcan errores, o no corresponda su funcionamiento con el especificado, deberá procederse a una recodificación. Todo estos pasos deben de estar documentados con firmas antes del paso a explotación.

De todo esto, se desprende que debe existir una intensa colaboración entre los departamentos u organismos usuarios y el Área de Desarrollo y Mantenimiento. Esta permanente colaboración debe normalizarse mediante unos procedimientos formalmente establecidos, que determinen responsabilidades y marquen pautas de realización.

Esta colaboración entre usuarios y desarrollo debe empezar en la fase de diseño conceptual y esquemas directores del proyecto, donde ambas partes

firmarán los puntos acordados y los plazos a cumplir, fijándose las necesarias reuniones posteriores para que, una vez elaborado el Análisis Funcional, sea conjuntamente discutido, aprobado y firmado. Desde ese momento empieza la fase de elaboración de cuadernos de carga, que darán origen al Análisis Orgánico y su correspondiente codificación.

La colaboración y respaldo de los desarrollos que se aborden, que comienza desde la fase de concepción del diseño preliminar, debe continuar en la fase de análisis, y finalizar en la de pruebas. En todas ellas debe estar implicado directamente el usuario, firmando aquello que se vaya acordando, incluyendo las pruebas.

Una vez finalizada esta fase, existirá una prueba global y conjunta, hecha por el usuario y por el equipo de desarrollo. Una vez realizada, y comprobado que se ciñe a lo descrito, será aprobada y firmada por las dos partes, guardándose el juego de ensayos utilizado, como soporte documental de la aplicación, incluyendo los resultados obtenidos.

De esta forma, se evitarán posibles problemas que surjan a raíz de retrasos en al implantación, o por la no formalización en un documento de las necesidades previamente manifestadas por el usuario.

Toda instalación informática medianamente grande, debe contar con unos trámites de colaboración debidamente reglamentados, obteniéndose con ello un beneficio para ambos interlocutores.

Por otra parte, en cuanto al mantenimiento de programas de aplicaciones en explotación, deberán conservarse las normas referentes al desarrollo de las mismas, además de llevar un control especial para el posterior paso a explotación de la nueva versión del programa, documentando las modificaciones y adjuntando las pruebas realizadas.

Se recomienda que se disminuyan las responsabilidades del personal externo perteneciente a la empresa de servicios de un modo paulatino, incorporando personal propio en la plantilla y proporcionando nuevos desarrollo a los primeros. De esta forma, se controlaría un poco la dependencia que existe actualmente hacia ellos.

Por otro lado, se deberán mejorar las condiciones de seguridad con respecto al personal externo, en los términos de organización, normativas y procedimientos, y en general, dándoles un tratamiento especial.

Sería aconsejable realizar un control sobre el personal externo de la empresa de servicios, de modo que se realice un seguimiento de las tareas que desarrollan, exigiendo un plan de actuación a corto y medio plazo. Además se deberían solicitar unos partes de control que fueran más detallados que los actuales, y un desvío de los proyectos encomendados, con las causas que lo han motivado.

3.6.- CONTROL SOBRE LA OFIMÁTICA Y LA MICROINFORMÁTICA

3.6.1.- NORMATIVA DE LOS EQUIPOS

Uno de los puntos importantes dentro del manejo de equipos de microinformática, es la necesidad de que exista una normativa de protección en la seguridad de los datos.

Se deberá convertir esta normativa en política interna de la empresa y todos los empleados deberán seguirlas forzosamente.

Existen dos tipos de Métodos de Protección :

- *Medidas Preventivas* : que se deben seguir desde el principio, cuando se adquiere el ordenador o cuando existe la plena seguridad de la no existencia de algún virus informático.

  Normativas sobre el Sistema Operativo :

  - Utilizar siempre un Sistema Operativo fiable
  - Hacer copia en diskette del Sistema Operativo
  - No grabar un Sistema Operativo de diskette dudoso en el Disco Duro
  - Apagar y volver a arrancar un ordenador ajeno con el diskette propio
  - No trabajar con diskettes originales
  - Comprobar la envoltura de los productos de software adquiridos

Normativas sobre el Disco Duro :

- No utilizar el Disco Duro como único lugar de almacenamiento
- Comprobar los diskettes antes de copiarlos en el Disco Duro
- Proteger los Discos contra escritura
- Realizar copias de seguridad periódicamente
- Hacer un sistema rotativo de copias
- Tener bajo control los discos de procedencia ajena

Normativas sobre Redes :

- Elegir convenientemente la clave de acceso a la red
- Adoptar medidas preventivas en las empresas fabricantes de software
- No manejar virus informáticos

- *Medidas de Contingencia* : que se deben tomar en el mismo momento en que se detecte el problema.

  - Conservar la calma
  - Desconectar totalmente el ordenador
  - Encender el ordenador con otra copia de seguridad
  - Hacer copias de seguridad de los ficheros de datos y los no ejecutables
  - Dar nuevo formato el disco infectado
  - Comprobar los discos originales con programas detectores
  - Recomponer el disco con los programas originales
  - Volver a copiar la información, si no está infectada de virus informáticos
  - Volver a comprobar los discos con programas detectores
  - Probar todos los discos utilizados con anterioridad al problema
  - Avisar a otros usuarios, si se ha detectado virus, de peligro de infección

3.6.2.- SEGURIDAD FÍSICA DE LOS EQUIPOS

No todas las violaciones que se producen en los Sistemas Informáticos, se deben a accesos no permitidos, sino que puede producirse por muy diversas causas. Entre éstas, con el progreso de la informática, aparece el "Software mal intencionado", es decir, pequeños programas que poseen una gran facilidad para reproducirse y ejecutarse, cuyos efectos son destructivos y el daño, en la mayoría de los casos, es irreversible. En términos populares, se ha denominado "Virus Informático".

Existen cuatro métodos de contagio de virus informáticos entre distintos equipos :

- El medio más susceptible de contagio, lo constituyen las copias ilegales de software que circulan entre los usuarios.

- El segundo foco de contagio, lo constituyen unos programas de uso común, por los que bien se paga una pequeña cantidad en concepto de manual o de derechos de autor simulados ("Shareware"), o bien no se paga nada por ellos ("Freeware).

- El tercer foco de esparcimiento, lo componen las redes públicas de ordenadores. Si bien no son una fuente muy común de virus de equipos, si constituyen un nido abundante. Además la transcendencia de las epidemias es mucho mayor, al ser más abundante el número de ordenadores afectados.

- El último foco de contagio, se está realizando con fines de chantaje, utilizando diskettes con vistosa presentación, y son enviados por correo a empresas y organismos oficiales. Su contenido puede hacer referencia a demostraciones de nuevos productos o bien a información técnica de algún tema de actualidad. Bajo una presentación aparente, se esconde un programa contaminante que, en algún momento, informa al usuario de su presencia y de los posibles efectos en el caso de que no se pague una cantidad por el antídoto.

Por estos motivos se hace imperiosa la necesidad de que exista una normativa de protección en la seguridad de los datos, y ésta se deberá convertir en política interna de la empresa y todos los empleados deberán seguirlas forzosamente.

Ente los Métodos de Protección, destacan :

- *Medidas Preventivas* : que se deben tomar cuando se adquiere el ordenador o cuando existe la plena seguridad de no estar infectado.
  Dentro de estas medidas se puede realizar otras dos subdivisiones :
  - Medidas Preventivas, que evitan que el ordenador se contagie.
  - Medidas Detectoras, que averiguan si el ordenador o los programas que se utilizan, están infectados o no.

- *Medidas de Contingencia* : que se deben tomar en el mismo momento en que se detecta el virus, para evitar su mayor propagación.

El primer tipo de medidas (Preventivas), no se debe seguir cuando se tenga duda o conocimiento de la existencia de algún virus en la memoria del ordenador o

en alguno de los discos, ya que esto no haría sino propagar más su infección. En tal caso, se debe pasar directamente al segundo grupo de medidas (de Contingencia), y seguirlas en el mismo orden en el que aparecen. Las medidas a seguir en cada caso y el orden ya han sido descritos en el Apartado anterior (3.6.1.)

Obligar a los usuarios a utilizar Software original y evitar el trasiego de diskettes de la oficina al domicilio particular, supone una disminución del riesgo de contagio en los equipos.

Otra forma de protección contra virus informáticos, consiste en la instalación de un Programa Protector del Disco Duro. Su función es la de prevenir y proteger frente a posibles ataques contra el Disco Duro. Por ello, deberá utilizarse siempre que se vaya a trabajar con diskettes que contengan Software de procedencia dudosa.

Este programa puede incluirse en el Fichero de Autoarranque, con el fin de proporcionar protección al Disco Duro siempre que se reinicialice el Sistema.

3.6.3.- SEGURIDAD LÓGICA DE LA INFORMACIÓN

Es importante que exista una normativa sobre las copias de seguridad (Backup). Consiste en que cada cierto período de tiempo, se realice una copia del contenido de los archivos, de forma que si se destruyen éstos, sea posible la recuperación de los datos a partir de la última de las copias. La realización de las copias de seguridad deber ser una rutina obligatoria.

La fiabilidad de las copias de seguridad dependerá fundamentalmente de la periodicidad con que se realicen y el índice de actividad de los archivos, es decir, de la frecuencia en que se actualicen. Además deberán ser almacenados en dependencias alejadas del sistema y en armarios protegidos.

La realización periódica de copias de seguridad (Backups), es una medida bastante efectiva para la seguridad de los datos.

Las copias de seguridad van a desempeñar dos importantes funciones :

- por una parte, una labor restauradora de los datos en caso de daños sobre éstos.

- por otra parte, una labor de detección, porque permite la comprobación entre dos copias del mismo fichero de parámetros tales como: tamaño, atributos, fechas, etc.

También es importante que exista una normativa sobre la confidencialidad de la información. Es fundamental restringir lo más posible el acceso directo a la

información reservada. Otro foco peligroso es el Personal Informático descontento, dado de baja o despedido. Antes de salir de la empresa, podría realizar cualquier actividad nociva para los datos. Es conveniente controlar especialmente a estas personas, en los que se refiere a su acceso a la información de valor para la empresa.

Es necesaria la realización de una normativa sobre la gestión de los accesos de los usuarios : altas, bajas o modificaciones, y de obligada ejecución y cumplimiento una vez sea comunicada una incidencia sobre alguno de los usuarios por el órgano correspondiente.

3.6.4.- MANTENIMIENTO DE EQUIPOS

Para el control del parque ofimático, se deberá llevar un inventario actualizado de los ordenadores personales para, en caso de avería, poder sustituirlo inmediatamente. Se ha de llevar registro de los números de serie de los equipos, partes o informes de servicio técnico y márgenes de garantía.

Se deberán exigir las siguientes condiciones, en la formulación de ofertas tanto de Hardware como de Software, a las empresas distribuidoras:

- *Experiencia* :
  1) Historial de la compañía distribuidora.
  2) Experiencia en la instalación de equipos y productos.
  3) Referencias de clientes de instalaciones similares.

- *Servicio Técnico* :
  1) Número de técnicos de servicio formados en la fábrica.
  2) Capacidad para prestar servicio técnico a domicilio :
     a) Servicio de reparación o sustitución antes de transcurridas 24 horas.
     b) Capacidad de respuesta permanente (24 horas al día).
     c) Capacidad para responder antes de transcurridas 2 horas.
     d) Capacidad de existencia de piezas suficientes para la prestación de un servicio técnico adecuado.

- *Capacidad de demostraciones* :
  1) Con Software idéntico al pedido.
  2) Con Hardware idéntico al pedido.

3) Realización de pruebas patrón de referencia.

- *Enseñanza o formación* :

  1) Capacidad para dar formación básica de usuario.

  2) Capacidad para dar formación en todo el Software adquirido.

  3) Capacidad para dar formación sobre instalación del Software.

  4) ¿Cuánto se carga por la enseñanza o formación adicional?

  5) ¿Va incluido el apoyo telefónico en el precio de compra?

- *Si son necesarios varios vendedores, ¿quién asumirá las funciones?* :

  1) Enseñanza y formación del Hardware.

  2) Servicio Técnico del Hardware.

  3) Enseñanza y formación del Software.

  4) Servicio Técnico del Software.

- *Software nuevo de Aplicaciones* :

  1) Compatibilidad con el Software actual.

  2) Características necesarias.

  3) Enseñanza o formación necesaria.

4 - Debilidades y Riesgos detectados

4.1.- SEGURIDAD FÍSICA

4.1.1.- UBICACIÓN DEL EDIFICIO

El edificio se encuentra situado en la Rambla General Franco, una de las vías de mayor tráfico de la ciudad y colindante con un Centro Médico de bastante actividad, lo que lo hace desaconsejable para la ubicación de una instalación de este tipo.

En el mismo recinto del edificio, se ubican los laboratorios de análisis, por lo que además de los riesgos intrínsecos que conlleva, hay que añadir el hecho de que en dichos laboratorios se realicen las muestras de drogras incautadas por las fuerzas de seguridad, con los peligros que supone para todo el personal que tiene acceso al recinto.

Existe la probabilidad de que surjan actos delictivos con la aparición de violencia. Por ello, existe una vigilancia continua.

En el entorno al edificio, existen unos almacenes en los que se guarda mercancía peligrosa y con alto nivel de riesgo.

Además, el alto índice de tráfico que circula por los alrededores provoca problemas de acceso al edificio.

4.1.2.- **UBICACIÓN DEL C.P.D.**

El C.P.D. se encuentra situado en un edificio que se comparte con otros departamentos adscritos a la Secretaría General Técnica. La planta del sótano se encuentra dedicada al Servicio de Informática, pero la planta baja y la primera, son comunes para el personal de todos los departamentos. Esto obliga a permitir el paso de todo el personal por cualquiera de los pasillos en los que se ubican las dependencias de informática.

En el edificio del Servicio de Informática no existe en la actualidad una clasificación de aquellas áreas de acceso restringido, lo que provoca una libre circulación de personas por cualquiera de las dependencias del edifico, incluso personal externo y visitas.

Además de las áreas propias de un Centro de Procesos de Datos, se encuentran las dependencias donde se encuentran las maquinarias de mantenimiento de edificio, UPS, aire acondicionado, centralita de red de telefonía interna, etc.

La puerta de acceso desde el recinto del edificio al Servicio de Informática, no reúne las medidas de seguridad adecuadas. La puerta es de cristal, lo que facilita que una persona la pueda forzar, a pesar de ser doble no es utilizada por personal de seguridad para retener al visitante durante su identificación dentro del mismo edificio. Ambas puertas son utilizadas a diario por todo el personal perteneciente a la Secretaría General Técnica, y ajenos al Servicio de Informática. No se utiliza un mecanismo de apertura y cierre automático por parte de una persona situada en la conserjería del edificio.

Las paredes de la sala, en contra de lo que debería ser, se hallan recubiertas en ciertas partes, de materia inflamable y combustible como madera y tela, lo que facilitaría la propagación del fuego en breves instantes.. Lo mismo ocurre con las mamparas móviles que separan los diferentes despachos. Esto produciría la desaparición total del Centro de Procesos de Datos y la parada total de la actividad.

4.1.3.- SALIDAS DE EMERGENCIA Y PLANES DE EVACUACIÓN

Tanto en el edificio del Servicio de Informática como en cualquiera del recinto, no existen salidas de emergencia, a lo que se puede añadir la inexistencia de carteles indicadores que faciliten la evacuación en caso de necesidad. Esto implica un alto riesgo para el personal que trabaja en el edificio. La única salida existente es la puerta principal.

No existen planes de formación, en materia de seguridad, del personal que trabaja en la Consejería, de forma que no se sabe cuándo se debe evacuar, qué indica una alarma sonora, o si hay varias de diferentes tipos, qué significa cada una de ellas. Además no se conocen los tiempos de que se disponen en caso de sonar una alarma, y si deben utilizar escaleras o ascensores. No se realizan simulacros de evacuación del personal ni personal cualificado para dirigir las labores de evacuación.

Todo ello, puede provocar verdaderos desastres personales en el caso de que se plantee la situación real, ya que está totalmente demostrado que la improvisación y el desconocimiento en tales circunstancias sólo incrementa la confusión y el pánico de las personas. Además existe en la Consejería personal minusválido que lógicamente tendrían mayor problema en caso de desalojo, aumentando el riesgo por motivo de catástrofe.

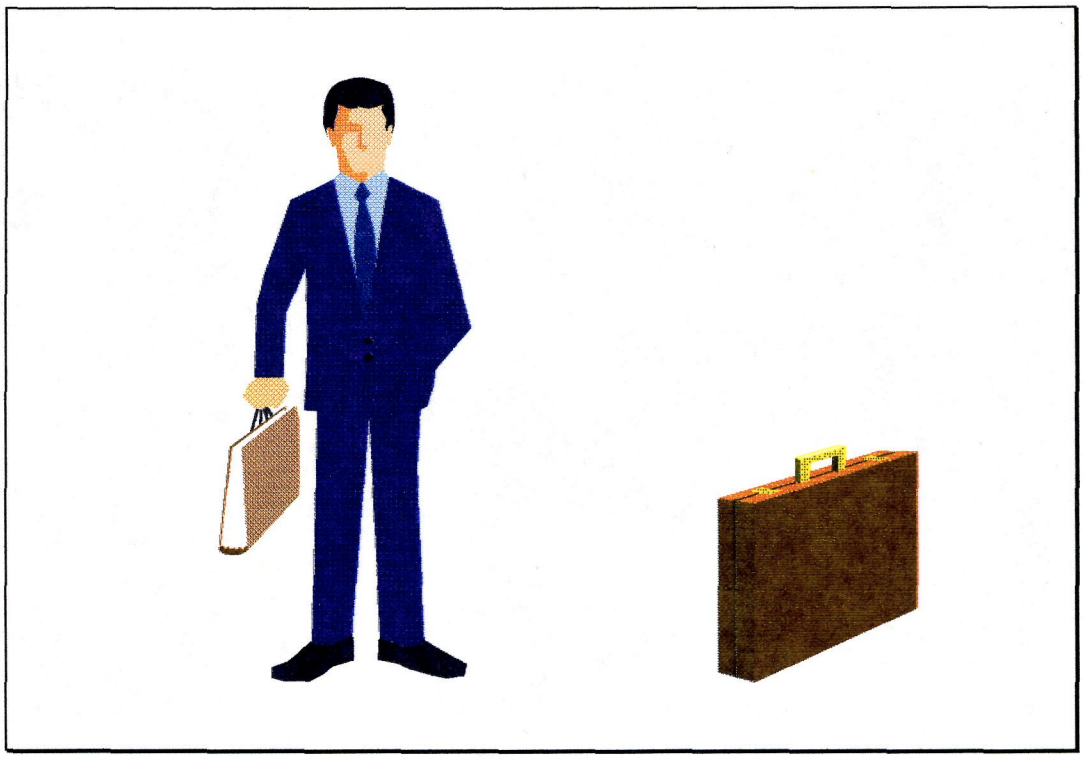
4.1.4.- SEGURIDAD EN EL ACCESO AL RECINTO

La identificación de las personas que entran al recinto se hace de forma visual, cotejándose, en caso de no ser funcionarios o laborales, con el listado de personal externo, o avisando a la persona que viene a visitarse. Una vez se supera este control visual, muchas veces desde el vehículo, el individuo que entra en la instalación no necesita ningún otro tipo de control.

De esta manera, cualquiera que supere los controles de identificación en la entrada al recinto, tendrá libertad para moverse por el edificio sin ningún tipo de restricción. A la salida de recinto, tampoco se avisará por si porta algún soporte magnético u otro objeto confidencial, con intención de sacarlo del edificio.

Por tanto, la deficiente identificación a la entrada al recinto, junto con otras deficiencias citadas, aumentan los riesgos de que accedan personas indeseables, y realicen acciones delictivas y fraudulentas, con un incuantificable valor, dada la diversidad de acciones.

No se realizan registros obligatorios sobre los maletines, bultos, materiales y paquetes que portan las personas que acceden al edificio, y por tanto, tampoco se realiza sobre aquellas que se dirijan al Servicio de Informática. Esto debe hacerse extensivo a los bultos, paquetes, material que se saca del Servicio, pudiendo ocasionar que personal mal intencionado aproveche esta debilidad para sustraer material o algún otro elemento que pudiera ocasionar trastornos, tanto económicos como de imagen de la Consejería de Sanidad.



El riesgo puede conllevar desde la desaparición de una cinta magnética, hasta la destrucción de documentación confidencial, e incluso la destrucción del Área de Informática.

4.1.5.- SEGURIDAD EN EL ACCESO AL C.P.D.

Aunque se dispone de mecanismos para el control del acceso del personal al Centro de Proceso de Datos, no se utilizan. Existen dos puertas de acceso a dicha sala que están permanentemente abiertas, y posibilitan el acceso a cualquier persona que se encuentre dentro del recinto.

En la misma sala existen otros elementos que obligan a tener las puertas de la misma abiertas. Este es el caso de los modems, multiplexores, impresoras, material de comunicaciones, cintoteca, etc. Por todo ello, se está asumiendo un riesgo alto de que ocurran circunstancias no deseadas como la desaparición de cintas o la manipulación de cualquier recurso por el personal no autorizado; o incluso, la colocación de algún elemento explosivo o incendiario que pasaría desapercibido, dada la inmensidad de la sala.

Las impresoras se encuentran dentro de la sala de ordenadores, con las deficiencias en cuestión de acceso ya enumeradas. De este modo, cualquier persona tiene acceso a las impresoras con entera libertad. No será necesario ningún tipo de identificación para acceder a las impresoras y tomar un listado. Estas deficiencias posibilitan la sustracción de listados importantes, y la visualización de información confidencial por parte del personal no autorizado. Este riesgo se incrementa con el proceso de Nómina por el personal informático, con lo cual se violan todas las confidencialidades que deben existir.

Además la inadecuada ubicación ocasiona un nivel de ruido muy incómodo para las personas que están permanentemente en la sala, como son los operadores, y generan, bastante polvo, que en la mayoría de los casos es invisible para el ojo

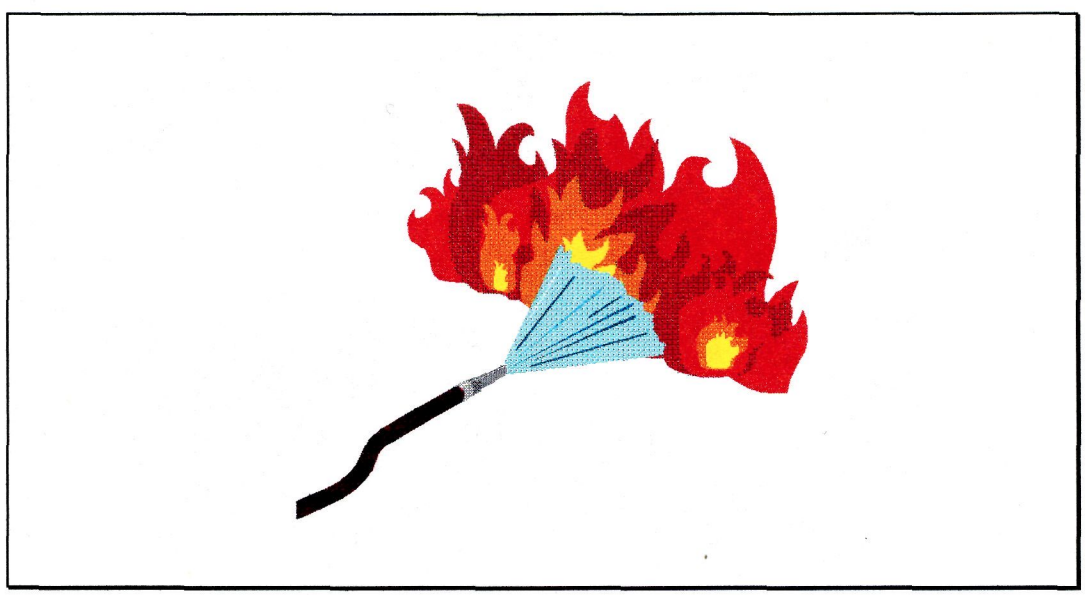
humano, y es desaconsejable en una sala en la que residen CPU's, discos y unidades de cinta, e incluso para el personal de explotación que trabaje en la misma sala.

Por otro lado, existe una máquina de café en el pasillo del C.P.D., con acceso a toda persona ajena al mismo, con lo que se agrava la circunstancia de seguridad informática. Además, es un lugar frecuentado para reunión y charla de compañeros de las oficinas colindantes.

4.1.6.- **SEGURIDAD DEL C.P.D.**

En las salas del sótano, donde se encuentran la sala de Desarrollo, la Sala de reuniones, los equipos de aire acondicionado, la centralita de la red de telefonía interna, las unidades de mantenimiento ininterrumpido, las baterías y los grupos electrógenos de emergencia, no se encuentran detectores de incendio.

Esto podría originar en caso de incendio, que se propague excesivamente antes de ser detectado por el reducido número de detectores existentes en el sótano, con la peligrosidad debido a la proximidad de otras máquinas, del almacén de papel, incluso de la sala de almacenamiento masivo de unidades.



En el sótano en el área dedicada a desarrollo, en muchas ocasionas se celebran cursos y presentaciones, por lo que dichas salas pueden estar ocupadas a cualquier hora.

Por otro lado, la actual estructura del pequeño edificio que alberga la central térmica, está posibilitando inundaciones en dicho edificio cuando llueve

copiosamente, dado que existe una inclinación del terreno que no permite más que una altura de 20 cm. de agua en el suelo a partir del cual rebosa y se introduce en la central térmica, obligándose a una detención del funcionamiento de la máquina allí ubicada..

Está máquina es la que garantiza la humedad en la sala de ordenadores, se dedica a fabricar vapor de agua para la sala. Por tanto, al no mantenerse los niveles de humedad necesarios, se debería detener los procesos informáticos activos, para que no afectara a los datos, con el coste que ello supondría. De igual manera, se podrían ver afectados los datos almacenados en las cintas y cartuchos que existen dentro de la sala, lo cual es imposible de ser valorado.

Otro aspecto importante resulta el permitir fumar en la cualquiera de las salas de informática sin tener ninguna medida de seguridad especial. Evidentemente, no puede ser clasificada como una causa muy grave, pero sí sintomática de la permisidad general existente. Tanto el humo como la ceniza de los cigarrillos son elementos nocivos para el hardware, y puede ocasionar deficiencias en los soportes magnéticos, que se manejan y almacenan dentro de la sala.

4.1.7.- SEGURIDAD DEL PERSONAL INFORMÁTICO

Actualmente no existe una cláusula de confidencialidad o secreto profesional en los contratos con el personal de empresas de servicios. Esto no ocasiona una pérdida de información, ni una pérdida económica, pero sí limita la posibilidad de exigir las responsabilidades oportunas o iniciar las acciones judiciales.

Tampoco existe un documento en el que se obligue a firmar a todo el personal que trabaje en la Consejería, tanto a nivel funcionario o laboral, como a nivel de personas subcontratadas.

Las propias personas que trabajan en la Consejería constituyen un factor de riesgo en sí mismo, al estar sujetas a condicionantes particulares imposibles de controlar. Por ello debieran existir ciertas medidas de seguridad para paliar en lo posible estos condicionantes. En el Servicio de Informática, se han detectado las siguientes debilidades:

- carencia de definición de incompatibilidades familiares en puestos de trabajo directamente dependientes
- no se solicitan referencias personales de aquellos nuevos contratados o subcontratados
- no se obliga a llevar la identificación personal permanentemente y en lugar visible
- no se realizan evaluaciones periódicas del rendimiento del personal ni del trabajo desarrollado.

4.1.8.- SEGURIDAD DE LA INFORMACIÓN

No existe una categorización de los datos en función de su confidencialidad. Esto es extensible tanto a datos elaborados como informes y comunicados de características especialmente confidenciales.

Toda instalación de proceso de datos de grandes dimensiones, que además conlleva unas labores administrativas importantes, se beneficia de múltiples maneras de una adecuada clasificación de la información, tanto para el intercambio con el exterior como para el establecimiento de restricciones internas. De no hacerlo así, se asumen riesgos innecesarios por la posible utilización de información de manera inadecuada o incluso fraudulenta, dañándose gravemente la imagen de la Consejería.

Este riesgo se ve incrementado por el considerable volumen de personal externo que colabora en las tareas informáticas. Este riesgo en sí no puede cuantificarse de una manera adecuada, dado que es algo intangible, pero debiera abordarse un estudio para evitarlo.

Existe el mismo tipo de restricción en cuanto al acceso lógico a los sistemas informáticos, tanto para el personal interno como para el externo. Los riesgos de la actual situación son evidentes. Cabría destacar la posible alteración de los datos y programas por personal externo de forma indiscriminada o el sacar información confidencial de las dependencias de la Consejería.

Por tanto, el riesgo es alto y de gran peligrosidad, pero es materialmente incuantificable.

Actualmente no existe un área dentro del Servicio que canalice las labores propias de una oficina de seguridad informática, si bien las funciones de seguridad lógica están siendo asumidas por personal del Área de Sistemas. Esto ocasiona que recaigan sobre las mismas personas labores y responsabilidades incompatibles. No pueden ser soportados por las mismas personas las labores de técnica de sistemas, con la responsabilidad que ello conlleva, con la labor de establecimiento de perfiles de seguridad y restricciones de acceso al sistema.

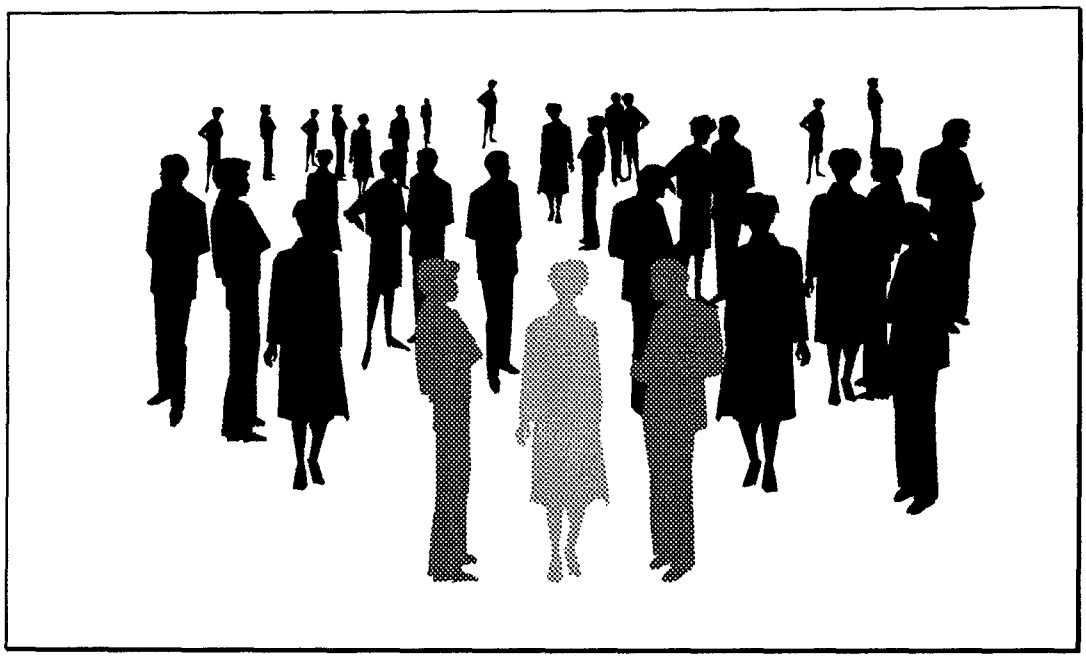
Los riesgos asumidos son altos, dado que se trata del personal cualificado de la instalación, teniendo acceso libre a todos los recursos, existiendo peligro de acceso indebido, hurto, destrucción, o manipulación de datos y programas del sistema.

Por otro lado, no existe una organigrama jerárquico alternativo, en el que se indique de manera individualizada las personas que deben ocupar un puesto en caso de ausencia del titular. Las personas que ejercen la labor en caso de necesidad, no conocen la problemática del puesto que van a desempeñar.

Además no se encuentran identificados aquellos puestos que denominados "claves" en la estructura, en los cuales se concentran gran número de responsabilidades, y cuya ausencia no puede ser remplazable. Esto pudiera ocasionar retrasos en ciertas autorizaciones, o en ciertas reuniones de trabajo, repercutiendo de manera directa en el servicio, al no estar presente la persona clave durante un período de tiempo, como pudiera ser una baja definitiva o una baja médica.

Los retrasos pudieran ser de importancia si la ausencia es de una persona con responsabilidades informáticas directas y muy concretas.

Todos estas debilidades conllevan un riesgo calificable pero no cuantificable.



4.2.- SEGURIDAD LÓGICA

4.2.1.- SEGURIDAD LÓGICA SOBRE EL SISTEMA

No existe un formalismo en las autorizaciones de modificación o cambio en el software de base, de manera que dichos cambios se realizan sin que quede constancia del hecho. Esto pudiera provocar situaciones no deseadas, como por ejemplo, que por error se realicen adaptaciones de ciertos módulos software para ceñirlos a la propia instalación, cuando dichos módulos habían sido desestimados por los responsables del Centro de Procesos de Datos, al no responder a unas características de funcionamiento determinadas. O bien si existe un problema de negligencia de un técnico, ésta no puede ser demostrable, ya que no existe una copia de la autorización ni del problema a solventar.

Por otro lado, no existe una comprobación de los módulos software base instalados. Se lleva un inventario manual de productos software que no es revisado ni actualizado con la frecuencia debida.

Una práctica habitual en todo centro de proceso de datos de gran envergadura, consiste en un inventario actualizado del software incluido en las librerías del sistema. En este servicio se ha detectado que no se lleva inventario para comprobar las librerías donde se encuentra el software de base activo, verificándose la versión, fechas y persona que lo implantó.

No existe una normativa formal que especifique de una manera clara y concreta la frecuencia con la que deben realizarse las copias de seguridad.

Actualmente se realizan dentro de la operativa normal de los procesos de salvaguarda, no existiendo una idea clara de en qué momento se debe salvar, qué vigencia debe tener la copia, y la necesidad de un duplicado en lugar de especial seguridad.

La carencia de esta normativa que indique frecuencia y marque calendarios, puede llevar a que en determinadas circunstancias, dichas copias no se realicen por alguna causa concreta, como un período punto de trabajo, y al intentar recurrir a una copia, ésta no exista, con la trascendencia que esto pudiera conllevar.

Existen facilidades para que cualquier usuario que pueda acceder a las librerías del sistema, realice una copia del cualquier módulo software, dado que no existen restricciones de copiado para ninguno de los elementos que componen el software del sistema. Esto pudiera ocasionar problemas, dado que una vez copiado, puede ser renombrado, y posteriormente utilizado con absoluta libertad.

Se da la circunstancia de que es el mismo personal el que realiza las labores propias de técnica de sistemas, y las de administración de la seguridad lógica de la instalación. Estas funciones debieran de realizarse por diferente personal.

A pesar de que existe un gran nivel de confianza entre el personal informático del Centro de Procesos de Datos, no es menos cierto que precisamente aquellas personas que realizan labores de técnica de sistema son las que constituyen un mayor riesgo, dado su nivel de calificación y los conocimientos específicos de la instalación. Es por ello que debe ser materia de control estricto la labor que realizan, sin que con ello se produzca una desconfianza personal, ni un encarecimiento del ambiente de trabajo.

El código de identificación y la password deben ser personales y confidenciales, de manera que toda persona que acceda al sistema sea responsable único y directo de aquellas operaciones que quedan registradas con su código de usuario.

Por otro lado, si un usuario olvida su password (del sistema) , el personal de sistemas accede a una consulta sobre el fichero de password, y la visualiza. Esto puede realizarse con frecuencia, siendo el único impedimento el desconocimiento de la existencia y uso del programa en cuestión. Todo ello se encuentra aún más fácil por la no encriptación del fichero de accesos y password. La actual situación no garantiza que personas no autorizadas accedan al programa que permite la visualización de las password y, por tanto, su posterior uso indiscriminado.

Cuando un usuario equivoca su password se le rechaza la conexión al sistema, pero no se realiza un seguimiento de todos los intentos fallidos. Además, cualquier persona conociendo el código de usuario de otra persona, puede intentar adivinar la password y posteriormente conectarse al sistema.

La medida de seguridad consistente en restringir el acceso de usuarios informáticos, desde terminales específicos, para evitar en un momento dado que se pueda acceder a ciertos recursos protegidos, habiéndose adivinado el código de usuario y password de acceso, no es utilizada en el centro de procesos de datos. Tampoco se está restringiendo el acceso de usuarios durante horarios previamente determinados, fuera de los cuales no se permite el acceso.

Los editores del sistema se encuentran sin protección específica, de manera que cualquier usuario puede editar cualquier librería o programa. De modo que

existe la posibilidad de que se modifiquen programas por parte de personas que ni siquiera debieran tener acceso.

Que cualquier programa de la instalación sea susceptible de ser alterado por personal no autorizado, es un riesgo innecesario que se está asumiendo. Los editores como parte integrante de todos los programas y ficheros, susceptibles de ser editados, quedan gravemente condicionados.

En el entorno existente, solamente hay protección de ciertos recursos mediante el RACF, es decir, no se establece la restricción de uso de cierta utilidad, sino que se protege el recurso sobre el cual se puede utilizar.

El uso incontrolado de utilidades del sistema puede tener gravísimas consecuencias, ya que puede alterar la información almacenada, modificar programas o incluso obtener copias de información confidencial. Pudiendo llegar incluso a procesar trabajos no autorizados con datos de trascendental importancia, llegando a ocasionar un caos informático inimaginable.

No se realiza como práctica habitual una revisión del LOG del sistema, ni de aquellos otros LOG específicos que se pudieran obtener de otros sistemas. Esto es de vital importancia para detectar posibles accesos no autorizados o procesamientos indebidos que lleven a una labor de corrección más que a una labor preventiva propiamente dicha

En dichos LOG puede quedar constancia de operaciones problemáticas o no autorizadas, así como la autoría de la misma y el puesto desde el que se realizó.

4.2.2.- SEGURIDAD LÓGICA SOBRE LOS DATOS

Existen usuarios que acceden al sistema compartiendo el código de identificación de usuario y la password de seguridad. Esto puede ocasionar riesgos al no quedar constancia de quién realiza unas funciones concretas, siendo generalmente personas con las mismas labores profesionales durante el mismo horario y turno de trabajo.

El código de identificación y la password deben ser personales y confidenciales, de manera que toda persona que acceda al sistema sea responsable único y directo de aquellas operaciones que quedan registradas con su código de usuario.

No existe una normativa de construcción de password que obliguen a que tenga cierta longitud y que no admita el carácter blanco. Esto facilita el que otras personas pueda adivinar la password de un usuario, mediante un algoritmo de generación de password. Esto es de gran relevancia en instalaciones como la que existe en este servicio, donde los niveles de seguridad son muy pobres.

No existe un mecanismo formal mediante el cual comunicar a los administradores de seguridad de la instalación, la baja de un usuario informático o el cambio de destino, de modo que tanto su código como su password, sean cancelados o adaptados a su nueva situación. De modo que pueden ser utilizados por otras personas, pudiendo ocasionar ciertos daños, premeditadamente o no, y que no puede seguirse de forma adecuada una acción correctora de los problemas causados y una acción sancionadora, si fuera procedente de la persona autora de los hechos.

No se toma la medida de precaución consistente en comprobar el contenido de los ficheros de datos, bien exhaustivamente, bien mediante un proceso de extracción muestral de un conjunto de registros representativos y completos. Este procedimiento sería de gran interés en instalaciones como la presente con falta de controles que garanticen la fiabilidad de los datos almacenados en los ficheros.

Esta carencia incide en la falta de fiabilidad de los datos de la instalación, dado que existe la posibilidad de que los datos se alteren de manera más o menos indiscriminada por personal informático.

Todo ello se debe a la falta de la figura del Administrador de las Bases de Datos, que asuma la responasabilidad sobre la integridad y privacidad de los datos del sistema.

No existen:

- planes de hardware y sotware a corto y largo plazo
- control de seguridad de las bases de datos y archivos
- monitorización de rendimientos y ajustes
- documentación sobre utilidades y procedimientos de Backup y Recover
- documentación de definición de bases de datos y archivos

4.2.3.- SEGURIDAD LÓGICA SOBRE LAS APLICACIONES

Existen usuarios que acceden al sistema compartiendo el código de identificación de usuario y la password de seguridad. Esto puede ocasionar riesgos al no quedar constancia de quién realiza unas funciones concretas, siendo generalmente personas con las mismas labores profesionales durante el mismo horario y turno de trabajo.

El código de identificación y la password deben ser personales y confidenciales, de manera que toda persona que acceda al sistema sea responsable único y directo de aquellas operaciones que quedan registradas con su código de usuario.

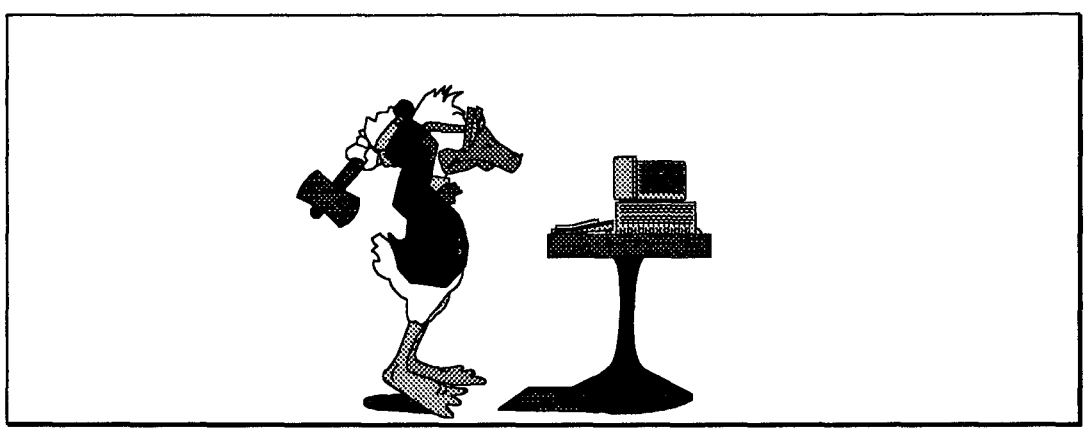
No existe separación de las máquinas de desarrollo, pruebas y explotación. Se han realizado estudios con vistas de efectuar una reestructuración del hardware existente, mediante una separación física, pero aún no se han abordado dichos cambios.

La carencia de esta medida, junto a la falta de otros controles puede llevar a facilitar el acceso de los programadores al entorno de explotación y sobre datos reales, o al acceso de operadores a librerías y programas de desarrollo, con el inherente riesgo que ello conlleva, sobre todo en este servicio que cuenta con personal externo. Además conlleva a que se procesen tareas no autorizadas o de manera no controlada, provocando una fuerte dependencia del personal de la consejería que accede a dichos entornos, y se está confiando demasiado en el personal externo que colabora en el desarrollo de ciertas aplicaciones. La situación actual es grave y no garantiza la integridad de los datos.

No se realiza control adecuado sobre los programas de explotación. No se realiza un labor de seguridad específica que pudiera consistir en detectar cualquier posible cambio no comunicado en los programas mediante el tamaño del mismo, o realizar con cierta frecuencia un recopiado de programas a partir de las copias de seguridad.

No existe ningún inventario de programas de explotación que incluya versión de programa, fecha y hora.

La carencia de un control exhaustivo de los programas de explotación puede dar lugar a procesamientos indebidos. Es evidente que en este servicio existe una restricción de tiempos muy fuerte, por tanto, la no detección de un cambio en un programa o un error inesperado, puede provocar retrasos irrecuperables, aumento en la carga de trabajo, por no mencionar la posibilidad de pérdida de programas, cambios de versiones, o modificaciones que alteren los resultados en gran medida.



4.3.- SEGURIDAD EN LAS TELECOMUNICACIONES

4.4.1.- SEGURIDAD FÍSICA

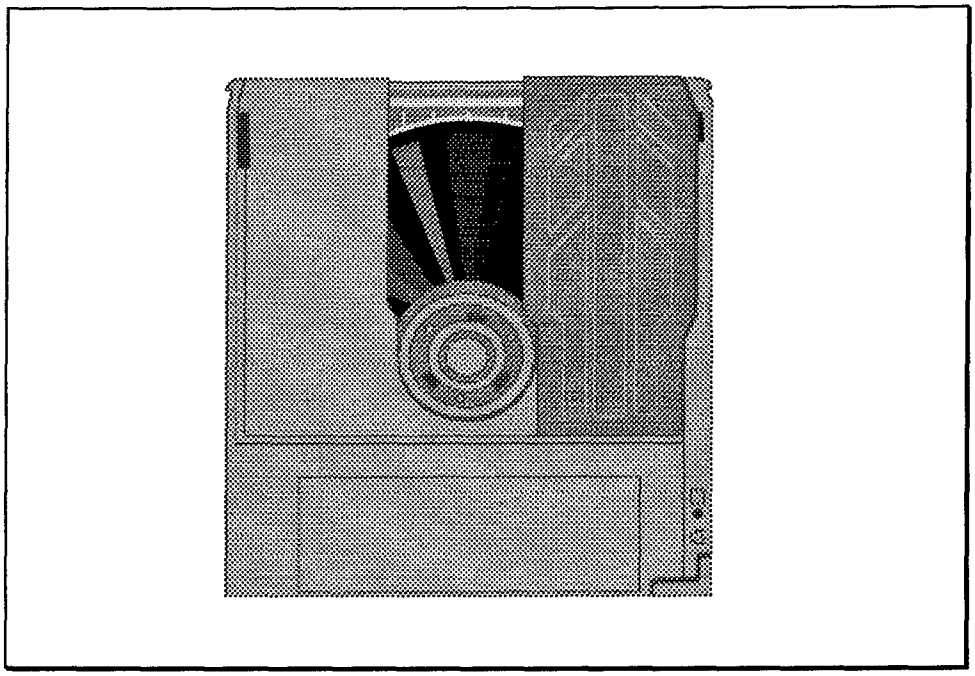
Los riesgos que plantea la situación actual de equipos, tanto en las instalaciones remotas de las provincias, como en el Centro de Procesos de Datos, son innumerables. Desde estar expuestos a contingencias naturales, como el fuego o la humedad, hasta ser robados en determinadas circunstancias, incluso quedar expuestos a la acción saboteadora, ocasionando el que no se puedas prestar el servicio adecuado, o dificultándolo en su totalidad.

Actualmente no existen medidas de seguridad normalizada para la ubicación de terminales y equipos en las provincias. Cuando se instalaron, se suministraron ciertas normas de seguridad, pero dado el gran aumento sufrido por la red en cuestión de equipos, se sabe a ciencia cierta que no se respetan en casi ningún caso, no existiendo medidas de seguridad adecuadas, ni siquiera fuera de horas, estando situados ciertos terminales en habitaciones que no poseen ni cerradores e incluso puertas.

Otras situaciones encontradas son:

- No se realizan controles de acceso a la zona donde se encuentran los equipos.
- No existe una planificación para evitar accidentes.
- Los diskettes se quedan sobre las mesas o dentro de cajones sin cerrar con llave.

- No existe control de ambientación en la zona donde se encuentran los equipos.



4.4.2.- SEGURIDAD LÓGICA DEL SISTEMA

En la red de SNA no existe un mecanismo para detectar los intentos de violación de accesos, o que deje constancia en el *log* de la red. El *Net Master* controla de manera bastante adecuada el acceso a la red, pero es factible que dicho control se salte desde un terminal remoto. Es decir, no se dispone de *loggin* de accesos a la red.

Esto supone un riesgo muy importante que se asume al no poder seguir la pista concreta a todo usuario que se conecta a la red, de modo que toda operación quede registrada. incluso en determinadas ocasiones, los controles impuestos por el software de acceso a la red pueden ser obviados.

La importancia radica tanto en seguir la pista de un usuario concreto, como en poder tomar acciones en consecuencia, en función de su actividad, así como para detectar posibles fallos en la conexión, o en la propia red, o bien de un control de tráfico y dimensionamiento apropiado, que puede afectar al tiempo de respuesta, y la calidad del servicio.

En cada provincia existe un ordenador que actúa como concentrador provincial, pero no existe un equipo de reserva del mismo para sustituirlo en un momento dado, y evitar que se interrumpa la comunicación. Tampoco existen rutas alternativas que se puedan utilizar como backup de líneas de comunicaciones en caso de interrupción del servicio por problemas de una de ellas.

Por tanto, la falta de elementos hardware supletorios de los ordenadores provinciales, así como de las alternativas dentro de las redes de comunicaciones de

la Consejería de Sanidad, puede ocasionar, y de hecho ocasiona, que con la relativa frecuencia no se pueda dar servicio, por incidencias frecuentes en las líneas y equipos, a los usuarios remotos.

Existen dos productos que realizan la gestión de los accesos lógicos, dependiendo del entorno al que el usuario está conectado.

- No se limita el número erróneo de intentos de conexión de un usuario final.
- No se desactiva una terminal después de un período de inactividad, ni se pide reconfirmación de código de usuario ni de password.
- No se obliga a cambiar la password cada cierto tiempo.

Para evitar la adivinación de la password mediante procedimientos de prueba de combinaciones manuales, o alternativas, se debe limitar el número de intentos fallidos, y además, obligar a que se cambie la password con frecuencia.

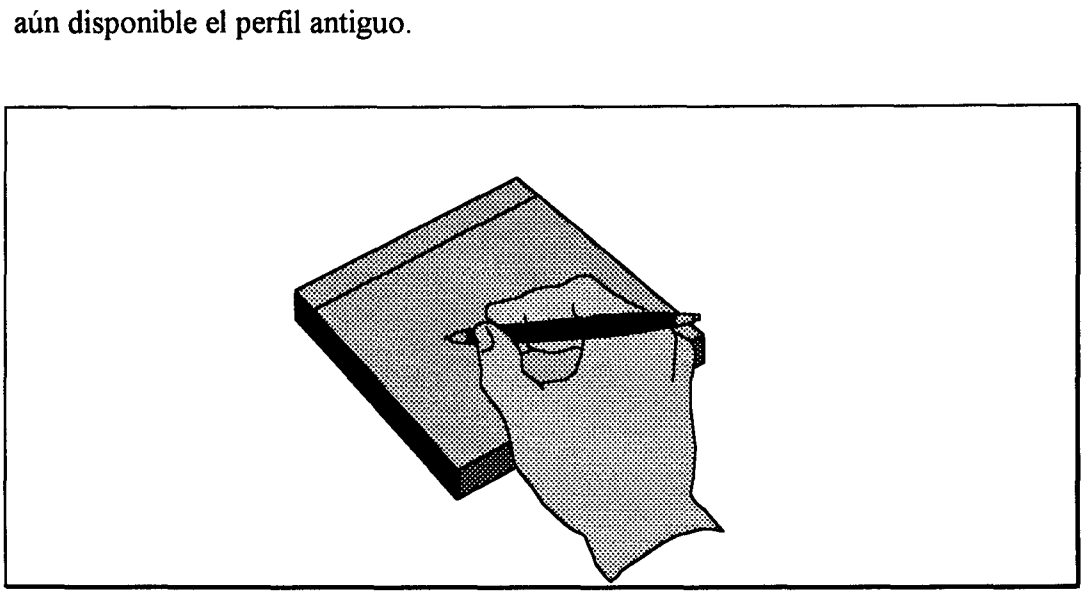
Por otro lado, debieran existir unos controles físicos de acceso a los terminales, de modo que reduzcan la posibilidad.

El riesgo ocasionado por la carencia de un control de acceso lógico de la red, posibilita múltiples acciones y daños incuantificables por su naturaleza.

El hecho de que no se cierre el teleproceso durante la noche, incrementa los riesgos existentes, como la mayor facilidad para accesos incontrolados desde las terminales de la red de comunicaciones.

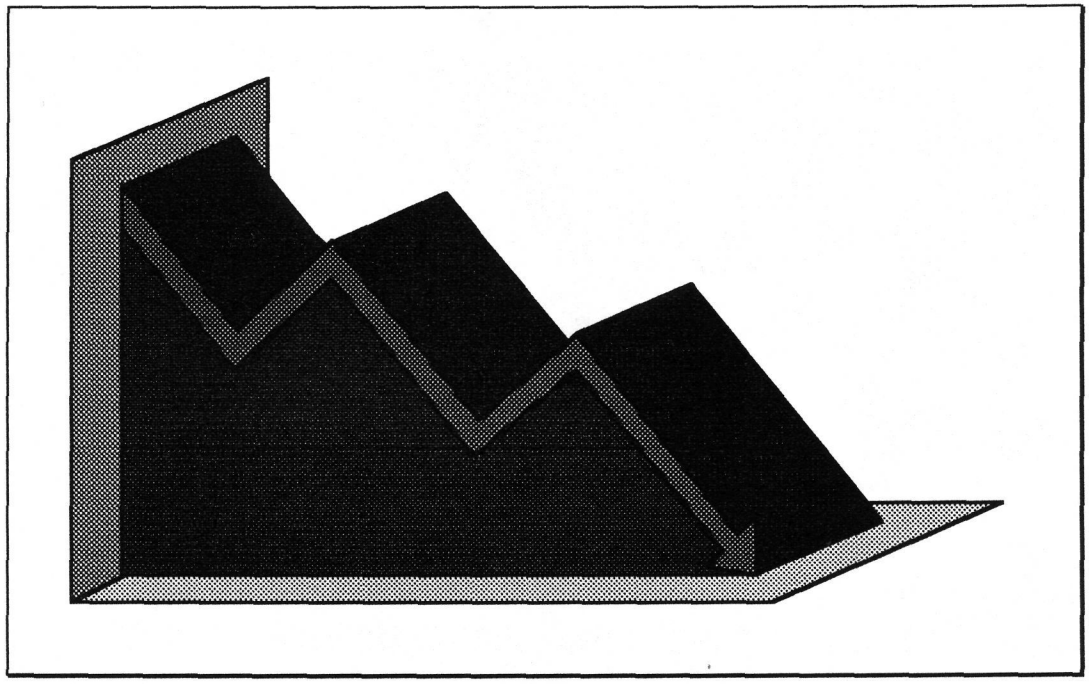
Si la debilidad de controles de acceso lógico y físico implica un riesgo importante, el mantener abierto el teleproceso durante toda la jornada, incrementa dicho riesgo en gran medida.

El procedimiento existente para informar de la baja de un usuario de la red de teleproceso, o su cambio de destino, se realiza mediante un comunicado oficial, que en la mayoría de los casos no se utiliza. Si un usuario cesa en su actividad y no es dado de baja en el sistema de gestión de la red de teleproceso, puede ocurrir que la disponibilidad de acceso de ese usuario sea utilizada con fines fraudulentos o delictivos. De igual forma, podría ocasionar problemas al no comunicarse un cambio de destino de un usuario, y no poder acceder con un nuevo perfil, estando aún disponible el perfil antiguo.



Se han detectado otras situaciones que se citan a continuación:

- No se realizan Estadísticas de tráfico de la red, para observar el rendimiento de las comunicaciones y contribuir al control del sistema.
- No se lleva un diario de operaciones que permitan realizar un seguimiento de los cambios ocurridos en la red.
- No existe una guía bien documentada de los comandos de conexión y desconexión del sistema.



4.3.3.- SEGURIDAD LÓGICA DE DATOS

En cada provincia existe un ordenador que actúa como concentrador provincial, pero no existe un equipo de reserva del mismo para sustituirlo en un momento dado, y evitar que se interrumpa la comunicación.

Los backups de los procesadores de comunicaciones no se realiza de un modo adecuado. Se hacen copias de seguridad de forma variable cada 3 ó 6 días, por duplicado y se almacenan en las propias librerías del sistema. Esto no garantiza la recuperación en cualquier caso, ya que las propias copias de seguridad residen en los discos del sistema, dentro de las librerías asignadas. Con ello, pueden estar sujetas a los mismos riesgos que el resto de la instalación, y quedar dañadas en circunstancias análogas, con lo que las copias de seguridad pierden toda su validez.

La carencia de documentación adecuada en los procedimientos de recuperación, y en general en toda la explotación del entorno IBM, provoca que exista una dependencia personal de aquellos miembros más experimentados de explotación, o incluso del personal del soporte técnico. Esto supone un riesgo grave en momentos con menos personal, turnos de noche o fines de semana.

Los procedimientos de recuperación existentes en el entorno IBM son los estándar de dicha firma más alguno que se ha desarrollado en el propio centro. Estos procedimientos fueron probados en el momento de su incorporación a las librerías del sistema, pero no se realiza unas pruebas periódicas de su funcionamiento. Para evitar que en el momento de necesitarlos no se disponga de

la versión adecuada y que funcione correctamente, se debe establecer un calendario de pruebas, que se adapta al propio de la explotación diaria.

Por otro lado, tras la utilización de uno de estos procedimientos de recuperación no se toman las medidas de precaución consistentes en chequear los ficheros implicados en el incidente, para verificar su estado. Pudiera ocurrir que, debido a la carencia de pruebas de los procedimientos, se produzcan incoherencias en los ficheros recuperados.

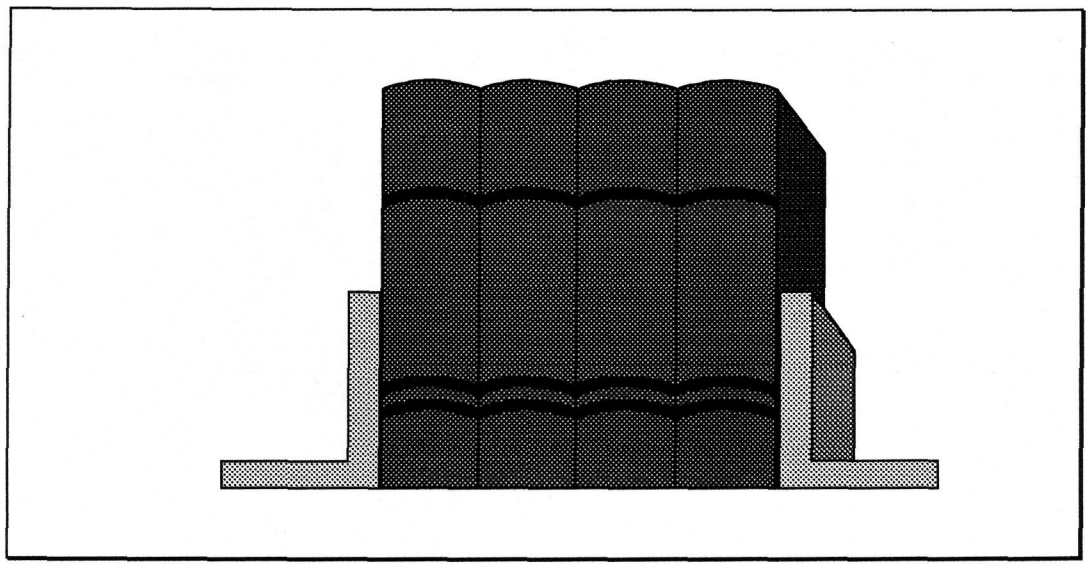
Por tanto, es un punto de gran interés, dado el riesgo que entraña.

Por otro lado, no se realizan procesos de *encriptación* de la información.

Toda información almacenada en un ordenador debe tener unas copias de seguridad que permitan la reconstrucción de una situación en el caso de que se produzca una contingencia. Esto no suele tenerse en cuenta en este servicio, en el sentido de la documentación anexa al ordenador, que debiera ser duplicada u guardada con las mismas normas de seguridad.

La pérdida de documentación en un caso de contingencia leve, sería de menor importancia que la pérdida de datos, pero no por ello, carece de importancia

La biblioteca de soportes magnéticos de la sala de ordenadores no posee las medidas de seguridad apropiadas. Los armarios situados en el sótano del edificio no tienen los mecanismos adecuados de protección contra fuego, humedad o robo. Únicamente los armarios ignifugos utilizados para alojar cintas se ciñen a un mínimo de condiciones que garanticen su contenido, pero son de poca capacidad.



Dentro del Centro de Procesos de Datos es de destacar la carencia de un plan de desastre que documente y garantice la continuidad del servicio de procesos de datos ante la ocurrencia de una contingencia de cualquier tipo.

Esta debilidad es perfectamente subsanable mediante el estudio, desarrollo e implantación de un adecuado plan de contingencias. Es demostrable que la improvisación en este terreno, aunque puede lograr la recuperación parcial del sistema, no es eficaz en modo alguno.

El hecho de que no exista un documento que, formal y sistemáticamente recoja el conjunto de medidas que deberían ser tomadas en el caso de la ocurrencia de contingencias en el Centro de Procesos de Datos, compromete de forma clara la continuidad de los servicios informáticos en caso de circunstancias desfavorables.

Por otra parte, las deficiencias señaladas en seguridad física, ponen aún más de manifiesto el riesgo que se está asumiendo.

4.3.4.- SEGURIDAD LÓGICA DE APLICACIONES

Existen una debilidad muy acentuada en la gestión de los accesos lógicos:

- No se limita el número erróneo de intentos de conexión de un usuario final.
- No se desactiva una terminal después de un período de inactividad, ni se pide reconfirmación de código de usuario ni de password.
- No se obliga a cambiar la password cada cierto tiempo.

Para evitar la adivinación de la password mediante procedimientos de prueba de combinaciones manuales, o alternativas, se debe limitar el número de intentos fallidos, y además, obligar a que se cambie la password con frecuencia.

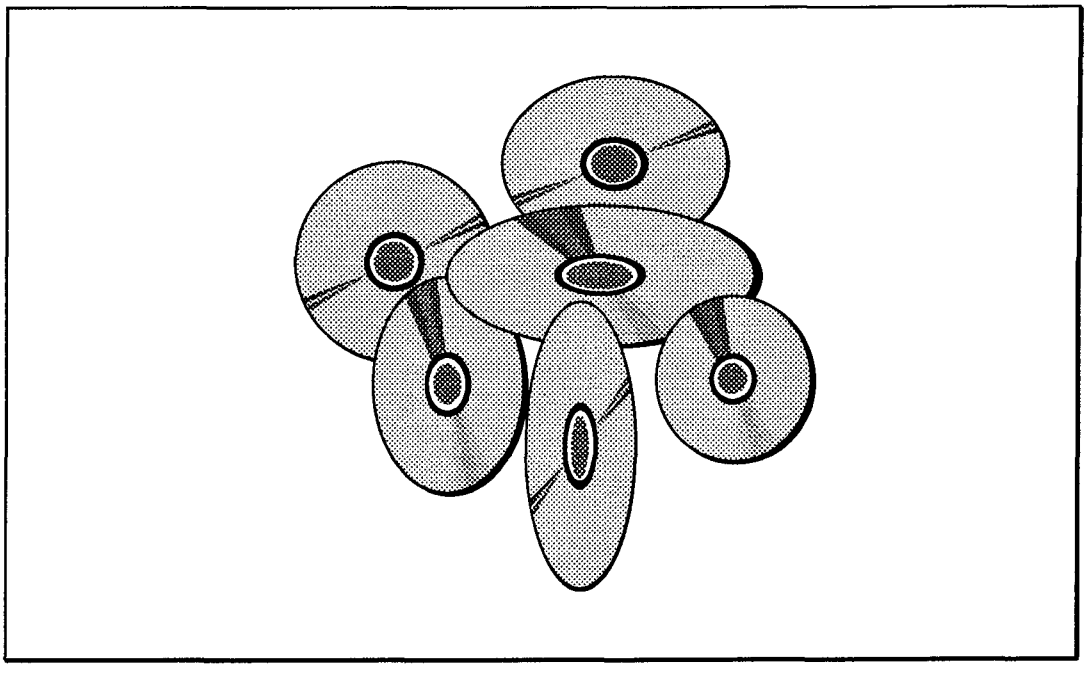
4.4.- CONTROL SOBRE LA EXPLOTACIÓN DEL SISTEMA

4.4.1.- SEGURIDAD FÍSICA DE SOPORTES MAGNÉTICOS

Se maneja un gran volumen de soportes diariamente, lo que provoca una gran cantidad de almacenamiento en ambos entornos. Los soportes magnéticos tienen un tiempo de vida limitado, y variable dependiendo en muchos casos de la utilización que se haga de ellos, y del lugar donde se almacenan. En la actualidad no se toma la medida de limpiar y verificar convenientemente las cintas que pudieran dar problemas.

El hecho de que no se reciclen las cintas debidamente, provoca un gran almacenamiento de soportes , siendo inútiles, Este es un gran riesgo, no tanto por la pérdida económica, sino por la facilidad de combustión de los soportes, lo que constituye un riesgo totalmente innecesario.

Las cintas no se encuentran numeradas sino con etiquetas que indican su contenido y el uso de los mismos. En ningún caso contienen la fecha de caducidad, o período de vigencia, de manera que se pueda controlar las cintas disponibles. De esta manera, se producen colapsos en cuestión de almacenamiento innecesario de información caduca, e incluso en algunos casos, de dudosa utilidad, al pertenecer a versiones de ordenadores anteriores, y actualmente en desuso.



También pudiera provocar el extravío de algún soporte, al no estar ubicado donde lógicamente le corresponda, y no existir un control adecuado de acceso a la biblioteca.

En el entorno IBM se posee un software bastante cómodo para la gestión de soportes magnéticos. Este producto es el llamado PCIN, y permite realizar consultas sobre el estado de un soporte determinado, relación de los disponibles, así como dar de alta o baja cintas concretas.

Es un recurso manejado indistintamente para preparación de trabajos y por los bibliotecarios, pero no existe ningún tipo de restricción para el resto de los usuarios del sistema.

Es por tanto, una valiosa herramienta para la labor de planificación y biblioteca, pero no se halla debidamente controlada. Esto es de suma gravedad, por la posibilidad de que un usuario malintencionado altere la información residente sobre las cintas o produzca alta y bajas indiscriminadas, con lo que ello supondría de problemático para la explotación.

La carencia de un inventario de soportes magnéticos puede ocasionar, como de hecho a ocurrido, la pérdida o extravío de cintas, o el borrado de información útil, así como el mantenimiento de copias de seguridad caducas.

De este modo, no es factible conocer de forma inmediata el número de cintas que se utilizan en explotación, la dedicación de dichos soportes, y la ubicación exacta de uno en particular.

Los técnicos que desempeñan labor de bibliotecarios son las únicas personas que acceden a los soportes magnéticos, sin embargo, cualquier persona del Centro de Procesos de Datos podría acceder libremente. Esto puede ocasionar el extravío, voluntario o no, de algún soporte en concreto o el deterioro del mismo, al no haber tomado las necesarias medidas de seguridad para su uso.

El riesgo es bastante alto, y de graves consecuencias, siendo aún más grave durante el turno de noche, al no existir bibliotecario y ser el propio operador quién realiza sus funciones.

4.4.2.- SEGURIDAD LÓGICA SOBRE EL SISTEMA

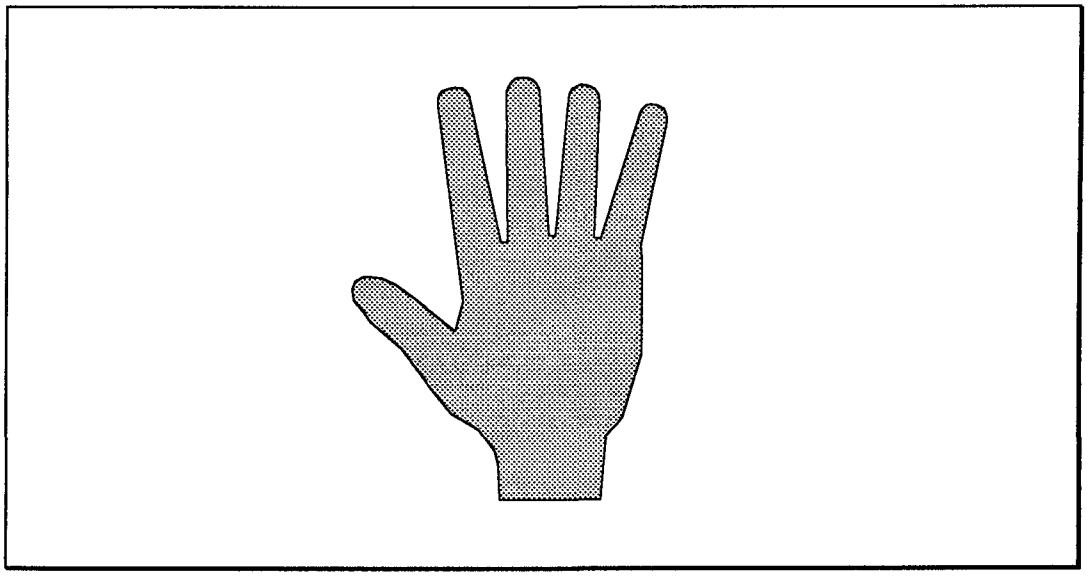
No existe una convención adoptada para la nomenclatura de los programas y los jobs, de manera que se puede crear un programa con libertad para nombrarlo. Esto puede ocasionar problemas al necesitarse de un diccionario de programas que indique su finalidad y la aplicación a la que pertenece, o bien crear una dependencia de la memoria de la persona que necesita utilizarlo, por no nombrar problemas de repetición de nombres en distintas librerías, para programas que no son idénticos.

El tiempo durante el cual se mantiene el *log* del sistema no guarda relación con la periodicidad de ciertos procesos, puesto que se retienen, en algunos casos, durante un espacio de tiempo muy inferior al que debiera, considerando que hay algunos procesos cuya perioricidad es mensual o incluso mayor.

Una debilidad que en sí misma no debería entrañar mayor importancia, lo constituye el hecho de que la fecha del sistema puede ser alterada con excesiva facilidad. Está alteración puede realizarse si la necesidad de que se detengan los procesos activos ni de que haya que arrancar el sistema completo. Esto podría ocasionar que ciertas referencias sobre el momento de ejecución de trabajos concretos, se vean afectados seriamente, acumulándose las consecuencias que de ellos puedan extraerse.

No existe un control sobre los cambios que se realizan en programas y jobs de explotación, de modo que prácticamente todo técnico con acceso a explotación, podría realizar ciertos cambios con absoluta libertad.

Por otro lado, al carecer de este control, aparece la posible diversidad sobre las versiones de los programas.



4.4.3.- SEGURIDAD LÓGICA SOBRE TAREAS DE EXPLOTACIÓN

La carencia de una planificación automática de las tareas de explotación informática, obliga a la continua presencia del operador para que introduzca parámetros o conteste mensajes. Esto lleva una carga suplementaria de trabajo para los operadores, lo que impide su dedicación a labores diferentes.

Existe una planificación se las tareas batch de explotación que se ejecutan diariamente, pero según se encuentra la seguridad lógica y la separación de entornos, cualquier usuario informático tiene libertad para ejecutar cualquier proceso de explotación. Esto resulta sumamente peligroso. Se podría alterar el normal funcionamiento del Servicio, al realizar fuera de plazo un proceso o incluso alterar los resultados introduciendo parámetros improcedentes.

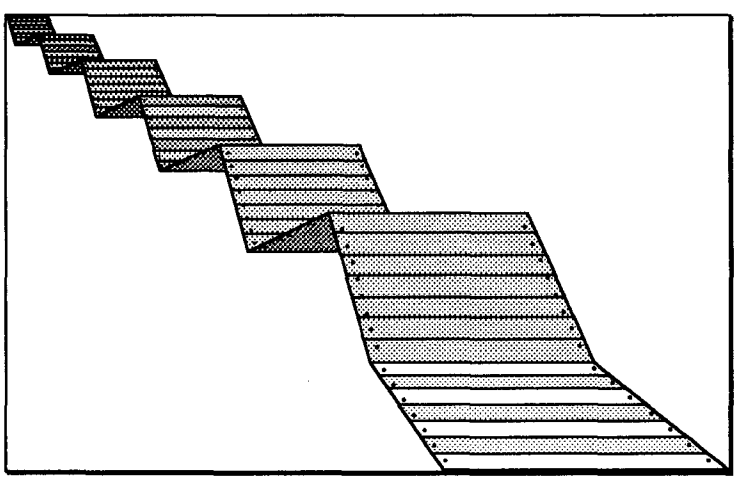
La carencia de un formulario adecuado al efecto, puede ocasionar problemas a la hora de exigir responsabilidades por la realización de un cierto trabajo. Cierta cantidad de trabajos son solicitados por teléfono, sin posterior respaldo documental, e incluso en aquellos casos en que se realiza mediante el documento oficial, éste no posee la firma o sello de la entidad solicitante.

La presencia de un libro de incidencias, para cada entorno, en la sala de ordenadores,, en el cual se refleje todo tipo de imprevistos acaecidos durante un turno laboral, junto con la información referente a su solución, hora que aconteció y causas que lo provocaron, es de vital importancia a la hora de realizar una labor preventiva de problemas en los procesos, así como establecer estadísticas. Sin embargo, este Servicio no realiza una documentación clara y concreta de todas aquellas incidencias que acontecen en los procesos realizados diariamente.

Actualmente, se obliga a que el personal de explotación dependa, en muchos casos, de su memoria para resolver problemas que saben que ocurren con determinada frecuencia.

De este modo, el riesgo asumido posibilita varias acciones de diferente naturaleza, lo que hace que el coste del mismo sea no cuantificable.

A pesar de realizarse comprobaciones por parte de los jefes de sala de los trabajos planificados, no se lleva a cabo una revisión exhaustiva del *log* de consola, de modo que se podrían detectar posibles duplicidades en el procesamiento o incluso omisiones no contrastadas. El *log* de consola es el registro real de la actividad del ordenador, en el que se puede encontrar información concerniente a procesos, ficheros y programas, así como loa fecha y la hora.



No existe una supervisión continua o directa del trabajo realizado por el personal de operación, de manera que hasta la fecha de la revisión, la única supervisión consistía en comprobar de un modo superficial, en la mayor parte de los casos, que se habían procesado los trabajos planificados, y como aportación de experiencia en caso de posibles incidencias.

Por otro lado, loe errores de hardware que ocurren sí se documentan, dado que se disponen de técnicos especialistas de las compañías correspondientes, los cuales elaboran los partes de actividad en caso de avería o mantenimiento.

No existe un control adecuado sobre la autorización y control del borrado de programas de explotación, de manera que cualquier operador, en ambos entornos, podría borrar un programa o partes de él con total impunidad. A pesar de ser concretos los técnicos con acceso a cada entorno, no se prohibe la realización de este hecho por el resto de personal.

La biblioteca de manuales de aplicaciones o de soporte técnico de cada una de las áreas que componen la instalación, se encuentran adecuadamente separadas unas de otras. Sin embargo, la correspondiente a explotación se encuentra en unos armarios convencionales que no pueden ser considerados como seguros. Se halla dentro de la sala de ordenadores, sin medida de protección específicas, con las deficiencias de la misma sobre el acceso del personal no autorizado.

Por tanto, la documentación de explotación no se halla ubicada en un lugar seguro, pudiendo ocasiona extravíos o pérdidas incontroladas, dado que el acceso a la sala no posee de las medidas de seguridad.

4.5.- CONTROL SOBRE EL DESARROLLO Y MANTENIMIENTO DE APLICACIONES

4.5.1.- ESTUDIOS DE VIABILIDAD

En el área de Desarrollo y Mantenimiento de aplicaciones no se realizan Estudios de Viabilidad ni Análisis de Costes y Beneficios de los nuevos proyectos que se abordan. En muchos casos, no se realiza ni petición formal por parte del usuario.

Esto puede ocasionar que algún proyectos concreto no se ajuste a lo esperado, por la existencia de problemas de recursos humanos, o que no se cumplan los plazos estimados.

Esto puede provocar un aumento de carga de trabajo para el personal vinculado al proyecto, e incluso retrasos en el mismo, así como en otros planificados, como secuenciales en el tiempo, o de menos prioridad, lo que puede redundar en un mal servicio al usuario, o en un servicio fuera de plazo, con la pérdida no cuantificable de horas/hombres y recursos, así como de imagen, tampoco cuantificables.

4.5.2.- CONTROL DE PROYECTOS

El control de proyectos se realiza de un modo informal, sin seguir una normativa o metodología común y de obligado cumplimiento por el personal del área de desarrollo.

Los riesgos que se producen con esta debilidad son grandes y con consecuencias negativas, tanto en el trabajo de las personas implicadas como en el servicio al usuario.

La existencia de un *diccionario de datos* completo y actualizado es una característica esencial de toda instalación informática que posea una base de datos

Actualmente, si por motivos externos a la normativa vigente, o por la gestión del servicio, hay que realizar modificaciones, o incluir elementos dentro de las bases de datos habría que realizar una búsqueda secuencial sobre los programas, para estudiar si procede modificarlos o no.

Esto supondría un coste levado de horas/hombre que no puede ser cuantificado.

No se realizan estudios de la idoneidad de adquirir productos software, ni de las necesidades a cubrir, así como de los costes que dicha incorporación acarrea. De modo que se puede llegar a provocar un gran desembolso económico, originado por la necesidad de un hardware específico para dicho producto hardware, dado que a menudo no se dispone de los recursos necesarios apropiados para el mismo.

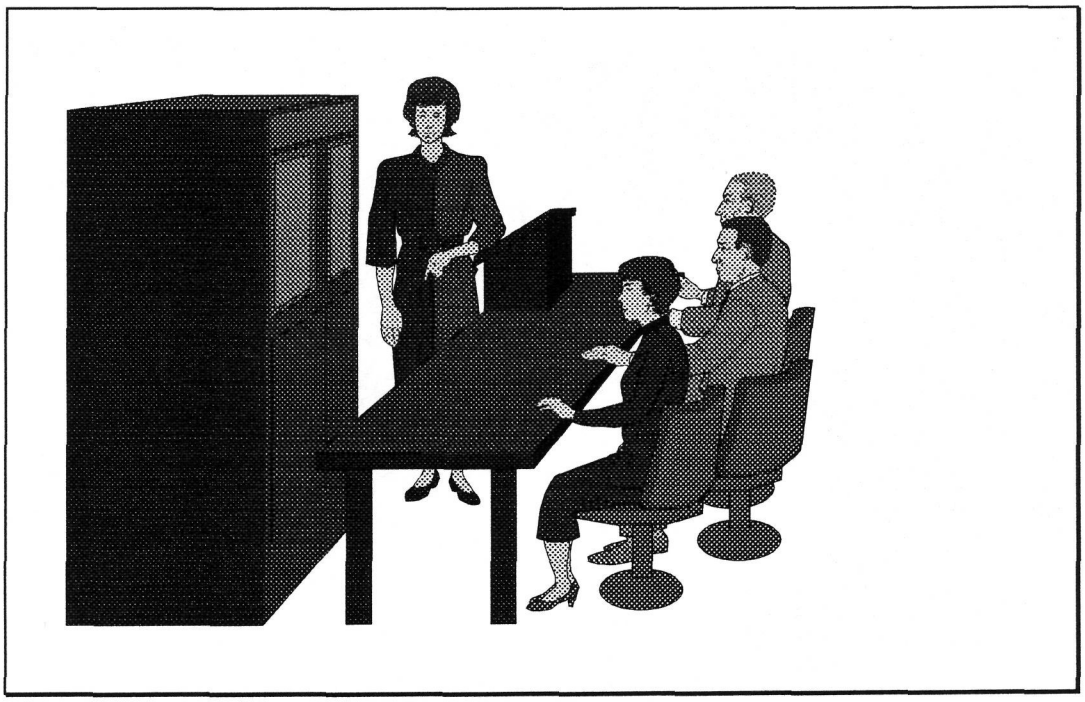
Tampoco se realizan análisis comparativo con otros productos del mercado, evaluando ventajas e inconvenientes, de cada una de las posibles alternativas antes de la decisión definitiva. Actualmente, se toma una decisión en base a breves conocimientos sobre el software en cuestión, y la limitada información procedente de correspondencia o propaganda.

No existe un procedimiento a seguir entre los servicios de BD y las áreas de desarrollo, pudiendo provocar retraso en plazos de ejecución con motivo de plazos ajustados o un calendario de trabajo muy apretado.

Las responsabilidades y labores de los administradores de las BD deben ser concretas y claras, y no deben estar en función de las necesidades puntuales de situaciones específicas. De no ser así, se viola el principio de segregación de funciones, tareas y responsabilidades, aumentándose el riesgo de accesos a áreas fuera de su responsabilidad, y disminuyéndose las garantías de seguridad que deben imperar en todo Centro de Procesos de Datos.

El riesgo ocasionado por falta de segregación de funciones incide en las posibilidades de accesos incontrolados a las BD, cuyo coste se define como no evaluable.

En este servicio, la labor de administración de la base de datos se encuentra repartida entre varias personas, una de las cuales ejerce de máximo responsable. En circunstancias puntuales, colaboran directamente con otros servicios como explotación y sistemas, realizando ciertas labores que son impropias de su perfil funcional.



4.5.3.- CONTROL DE DESARROLLO DE APLICACIONES

La situación actual muestra una falta de uniformidad en la aplicación de normativas y metodologías de desarrollo dentro de las diferentes aplicaciones realizadas por este Servicio. Esto puede provocar problemas de incompatibilidad de datos entre diferentes aplicaciones de varias áreas, que en la actualidad no aparecen pero en un futuro puede ser posible

Si bien todos los responsables de proyectos del Servicio de informática poseen sus propias metodologías para abordar tanto los análisis como las codificaciones, también es cierto que son diferentes.

Aunque se encuadren en diferentes sectores, no es adecuado que las normas sean diferentes, puesto que el ámbito de Desarrollo y Mantenimiento de aplicaciones debe ser considerado como un ente único, desde el punto de vista de la dirección del Servicio.

Existe una gran dependencia del Área de Desarrollo y Mantenimiento de las empresas de servicios subcontratadas por una carencia de recursos humanos. Sin embargo, resulta adecuado que sólo sea una empresa la que realice el soporte de los desarrollos subcontratados.

De cualquier forma, esto genera un riesgo, al poner en manos ajenas el desarrollo de aplicaciones que constituirán el esqueleto fundamental de la Consejería. Esto puede crear posteriores problemas de mantenimiento.

4.5.4.- CONTROL DE EXPLOTACIÓN DE APLICACIONES

No existe en la actualidad una normativa de gestión de paso a explotación de aplicaciones, módulos o nuevas versiones de programas.

Por otro lado, no existe en la actualidad un control de programas en explotación, ni un seguimiento de las últimas versiones de los mismos.

Las pruebas de las modificaciones de procesos de aplicaciones en explotación, se realiza de igual manera que en la fase de Desarrollo, sin contar con las posibles casuísticas de interrelación con otros procesos.

No existe una Base de Datos de pruebas para el control de calidad de los procesos antes de dar por finalizada la tarea correspondiente.

Por tanto, en muchos casos se utilizan copias de seguridad de la Base de Datos de explotación (datos reales), para la verificación del funcionamiento de los procesos realizados. Esto resulta una medida gravísima y con la cual se corre un riesgo muy peligroso, con la consiguiente pérdida de la confidencialidad y la integridad de los datos.

4.5.5.- CONTROL DE MANTENIMIENTO DE APLICACIONES

No existe en la actualidad ninguna normativa que gestione y racionalice las labores de los técnicos dentro del Área de Desarrollo y Mantenimiento.

En la actualidad se mantienen conversaciones telefónicas, e incluso se convocan reuniones de trabajo, haciendo constar de manera más o menos formal en un documento diseñado a su efecto, pero no se utiliza en todos los casos.

A pesar de ser buenas las relaciones existentes entre el usuario y el Área de Desarrollo y Mantenimiento, no se disculpa el hechos de carecer de una normativa que marque las directrices en la colaboración de ambos.

Esto podría ocasionar problemas en el diseño de aplicaciones, y en el funcionamiento de programas, provocando retrasos para nuevas codificaciones , falta de servicio al usuario, e incluso deterioro en las relaciones, al no aceptar responsabilidades cuando existan discrepancias entre lo realizado y lo que el usuario necesita.

Se originarían unos costes muy variables y no evaluables, dada la diversidad y naturaleza de los mismos.

No existe una normativa oficial y comúnmente aceptada, para realizar las pruebas de nuevos programas. Dependiendo de los casos, unos programas se prueban de forma somera por los técnicos, y se transfieren a explotación, y otros se prueban con juegos de ensayos completos y adecuados a cada circunstancia.

La carencia de una normativa para la realización de pruebas en programas provoca incidencias en el entorno de explotación. Esto se debe a errores en programas que no se adecuan a las especificaciones debidas, o bien producen errores de ejecución, cancelándose las cadenas en proceso, con el consiguiente retraso, tanto en explotación como en el mantenimiento del mismo.

En muchos casos, se utilizan copias de datos reales para realizar pruebas para cada programa o proceso. Esto produce problemas de confidencialidad, más aún cuando empresas de servicios colaboran en los desarrollos. El coste del riesgo es evidentemente invalorable.

4.6.- CONTROL SOBRE LA OFIMÁTICA Y LA MICROINFORMÁTICA

4.6.1.- NORMATIVA DE EQUIPOS

El área de microinformática es de reciente creación en este servicio, por lo que aún no tiene claramente definidas sus funciones y sus responsabilidades. Además no se conoce la cobertura de sus prestaciones, en el sentido de prestar servicio exclusivamente a la Secretaría General Técnica o además a todas sus Direcciones Generales.

La mayoría de las deficiencias y riesgos se deben en gran medida a la falta de definición concreta de funciones y responsabilidades.

Los riesgos que esto conlleva son claros, patentes y observables a simple vista. Entre ellos destaca la falta de procedimientos de seguridad y de backups, o normas a seguir en el caso del software de los ordenadores personales.

La inexistencia de un plan de contingencias para el Centro de Procesos de Datos es extrapolable al ámbito ofimático con las correspondientes consideraciones de entorno.

Es desaconsejable cualquier tipo de improvisación, por tanto, se asume un riesgo innecesario

4.6.2.- SEGURIDAD FÍSICA DE LOS EQUIPOS

No existe una normativa de seguridad acerca de los equipos ofimáticos y microordenadores. Una normativa que contemple desde las medidas a tomar por cada usuario al finalizar su actividad en el ordenador personal, hasta las correspondientes a la confidencialidad de la información manejada o incluso la seguridad de acceso físico a los diferentes elementos ofimáticos.

Esto provoca problemas dado que, en la mayoría de los casos, dichos elementos están situados en despachos con un control nulo de las personas que entran o salen. Incluso aquellos despachos personales, con material ofimático diverso, que no se cierran con llave al final de la jornada.

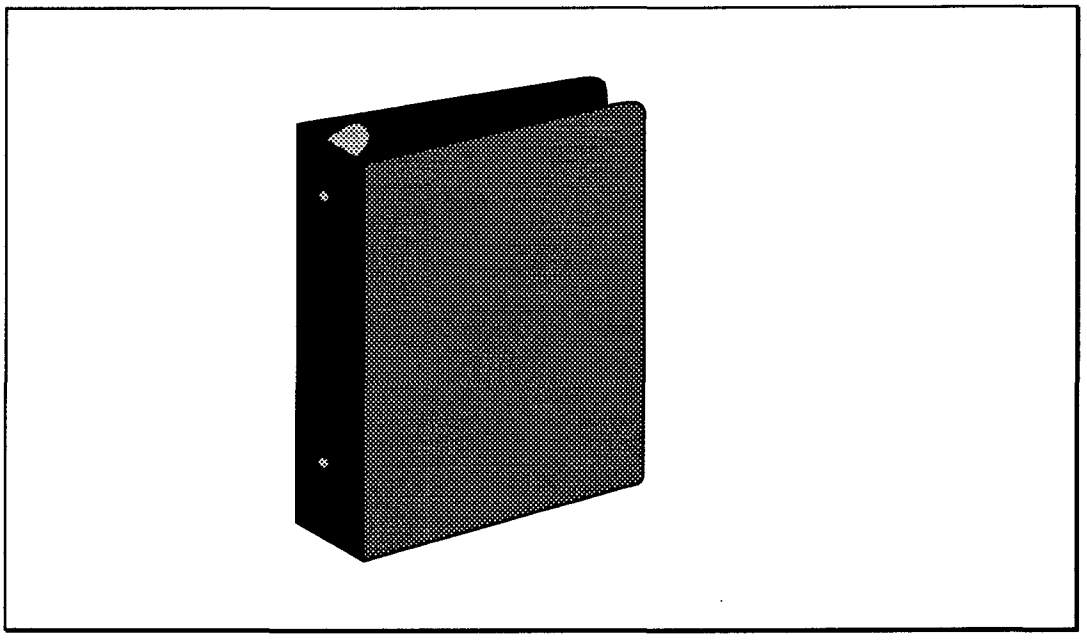
Además tampoco se toma la medida precautoria de desactivar lógicamente los ordenadores personales cuando el usuario se ausenta, o bien en el caso de que posea una llave de cerrar físicamente el ordenador.

Existen muchos productos software adquiridos sin la licencia adecuada, por trámites calificables, en algunos casos, como poco lícitos.

La existencia de copias de productos software sin la correspondiente licencia, y a través de los conductos oficiales de distribución, ha provocado una serie de inconvenientes considerables, como la aparición de **"virus informáticos"** en más de un ordenador. A pesar de que su acción aún no ha sido perjudicial, no se puede asegurar completamente el que continúe así.

Esto provoca además una carencia de documentación.

El hecho de no disponer de licencias oficiales de productos de software incide, además, en una carencia de documentación del producto. Esta documentación resulta ser un medio favorable para el usuario final.



4.6.3.- SEGURIDAD LÓGICA DE LA INFORMACIÓN

Una de las carencias más importantes es la carencia de una normativa sobre la obtención de copias de seguridad de los ordenadores personales y restantes equipos de ofimática. Tanto en lo referente a los paquetes de software de uso común como a las copias de seguridad de la información manejada, y su posterior almacenamiento fuera de línea.

Esta carencia ocasiona que pueda perderse información almacenada únicamente en los discos fijos de los ordenadores personales, y no poder recuperarse, con el trastorno que ello conllevaría.

Esto es de trascendental importancia, dado que no sólo se almacena información, en el concepto de datos procesables y elaborados, sino también informes y comunicados de vital importancia, al ser estos equipos utilizados frecuentemente por secretarías de dirección, e incluso por el propio personal directivo.

4.6.4.- MANTENIMIENTO DE EQUIPOS

La existencia de un parque de elementos hardware muy amplio y, a la vez heterogéneo, es totalmente desaconsejable por cualquier normativa, tanto de seguridad como de organización.

Esta heterogeneidad alcanza su mayor diversidad en el software de procesadores de texto, donde existe una completa variedad entre la mayoría de los ordenadores personales.

Esto ocasiona problemas a la hora de poder compartir un recurso concreto, o una información, sobretodo si se intentan conectar mediante redes locales o establecer estándares de uso.

No existen contratos de mantenimiento del parque de elementos ofimáticos, ni se realizan revisiones periódicas de dichos elementos, como práctica preventiva.

El único contrato existente es la garantía del equipo adquirido y proporcionada por el proveedor.

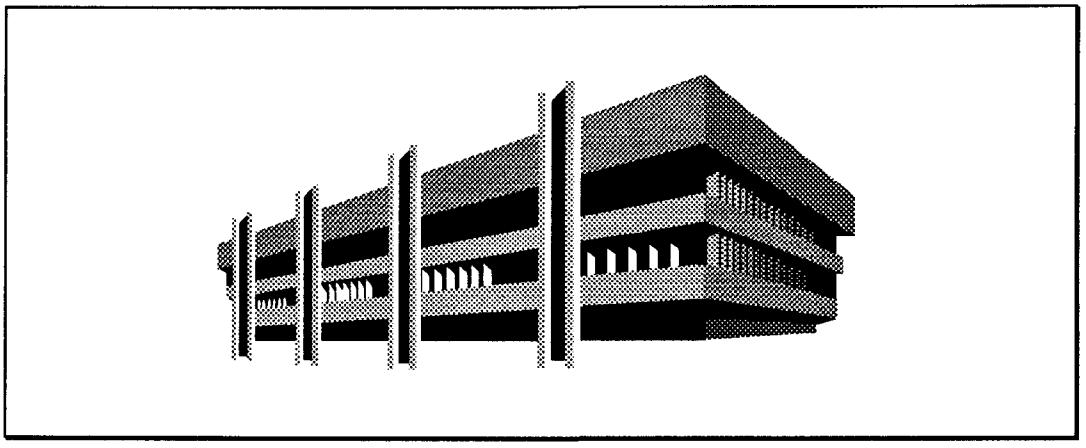
La carencia de contratos de mantenimiento y de unas revisiones preventivas periódicas están provocando excesivas intervenciones de los técnicos pertenecientes a las firmas suministradoras del servicio, siempre "a posteriori", con el consiguiente quebranto económico que conlleva las sucesivas facturas del servicio de mantenimiento.

5 - Mecanismos y Acciones correctoras

5.1.- SEGURIDAD FÍSICA

5.1.1.- UBICACIÓN DEL EDIFICIO

El edificio de la Consejería de Sanidad se encuentra ubicado en lugar no apropiado para oficinas, ni proceso de datos. Necesita grandes reestructuras, en lo que se refiere a su ubicación y las medidas de seguridad que la rodean.



Una posibilidad a tener en cuenta podría ser el situar todo el personal y el hardware que soporta el proceso informático, en un mismo centro de nueva construcción, con todas las medidas de seguridad necesarias.

Si esta medida fuera desestimada, debería reestructurarse el edificio, empezando por su recinto externo.

El recinto que rodea el edificio deberá estar perfectamente vallado, con cámaras de televisión que visualicen todos los puntos de la valla.

Las áreas de administración y las dedicadas al Servicio de Informática deberán estar debidamente diferenciadas.

Se trata de dar forma a un espacio dentro del cual puedan desarrollarse libremente y de forma rápida el ciclo de gestión burocrática y administrativa, sin retrasos inevitables que frenen la eficacia productiva.

No se recomienda proyectar el edificio en altura, debido a que se perderá diafanidad y extensión horizontal. Por tanto, se considera la característica de "edificios horizontales" como la construcción de edificio informático óptimo.

5.1.2.- **UBICACIÓN DEL C.P.D.**

El C.P.D. se encuentra situado en un edificio que se comparte con otros departamentos adscritos a la Secretaría General Técnica.. Necesita grandes reestructuras, en lo que se refiere a su situación y las medidas de seguridad que la rodean.

Una posibilidad a tener en cuenta sería cambiar la ubicación del C.P.D., si se estima la creación de un nuevo edificio que contemple todas las medidas de seguridad.

Otra posibilidad, sería trasladar todos los departamentos adscritos a la Secretaría General Técnica pero que no pertenecen al C.P.D. a otro edificio, quedando éste solo para el área de Informática. En este caso, se necesitaría una reestructuración del personal informático, para su adaptación a los nuevos despachos, así como de las medidas de seguridad que lo rodean.

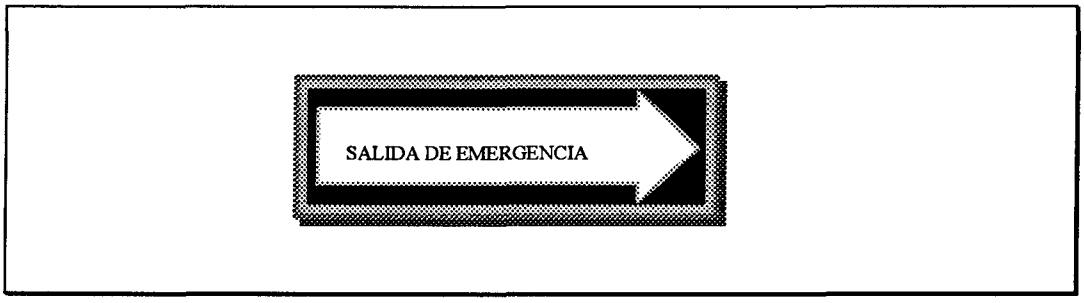
Una alternativa posible, ante la desestimación de las dos anteriores, sería la reestructuración del edificio existente, separando las áreas del C.P.D. y los departamentos restantes mediante unas puertas de seguridad (a las que sólo podrán acceder el personal autorizado) y el resto de las medidas de seguridad necesarias. Esto provocaría la reestructuración de la organización interna del resto de los departamentos, de modo que utilicen otro método de acceso a sus dependencias, sin necesidad de atravesar el C.P.D., acceso que existe actualmente, pero es de uso restringido para ciertos servicios.

Además sería necesario trasladar la máquina de café que existe actualmente en el pasillo común del C.P.D. y los accesos a otras oficinas. Este lugar suele ser un punto de encuentro a ciertas horas, para tomar café; personas de distintas áreas, que no sólo no están autorizadas al acceso al C.P.D., sino que además forman alboroto, y hablan a un volumen alto, lo que hace que no puedan trabajar los técnicos de sistemas que se encuentran en la sala contigua.

Por tanto, su traslado es urgente, y deberá ubicarse fuera de la puerta de seguridad del C.P.D..

5.1.3.- SALIDAS DE EMERGENCIA Y PLANES DE EVACUACIÓN

Deberá dotarse al edificio de las salidas de emergencia oportunas para facilitar la evacuación, además de colocar por todo el edificio, carteles orientativos, y croquis de evacuación, totalmente necesarios para que la misma se realice lo más rápidamente posible.



Asimismo, se nombrará un responsable de seguridad por planta y otro para todo el edificio, que en las evacuaciones deberá estar identificado. El responsable del edificio será el responsable de seguridad.

Los cursos formativos deben ser concretos, y los más breve posible, incluyendo la proyección de películas, charlas y facilitando la consulta o pregunta, por parte de cualquier persona, interno o externo. La asistencia a estos cursos deberá ser obligatoria.

En cuanto a la seguridad de las personas que normalmente trabajan en el edificio, deberán realizarse cursillos de mentalización y formación de todo el

personal, incluyendo proyecciones y transparencias. Todo ello complementado con las maniobras de simulación y de evacuación necesarias.

Deben establecerse procedimientos a seguir en todas las posibles situaciones planteables, en las que corra peligro la integridad física de las personas, como parte de un plan general de seguridad física en el que se defina un organigrama de responsables por zonas y edificios, y las normativas y procedimientos de actuación y simulacros.

Además, deben realizarse pruebas periódicas de ese plan, para evitar que las mismas medidas de seguridad no se olviden, y mentalizar al personal para cuando pueda surgir una situación real.

Este plan deberá ser impartidas anualmente, así como de un manual de normas o recomendaciones en caso de emergencia.

Estas pruebas serían de corta duración, unas 0,5 horas por personal al año.

Por otro lado, en los casos de fallos de energía eléctrica, se deberán instalar luces de emergencia alimentadas con baterías que iluminen el área de evacuación inmediatamente.

5.1.4.- SEGURIDAD EN EL ACCESO AL RECINTO

La conserjería del edificio deberá ser modificada en su actual estructura, para posibilitar la identificación de las personas dentro de la puerta y antes de su acceso definitivo. Por otro lado, las llaves de todas las dependencias que allí se guardan deberán estar bajo control del vigilante de seguridad en un armario totalmente cerrado, para evitar posibles sustracciones o pérdidas, dado el inadecuado control existente sobre ellas.

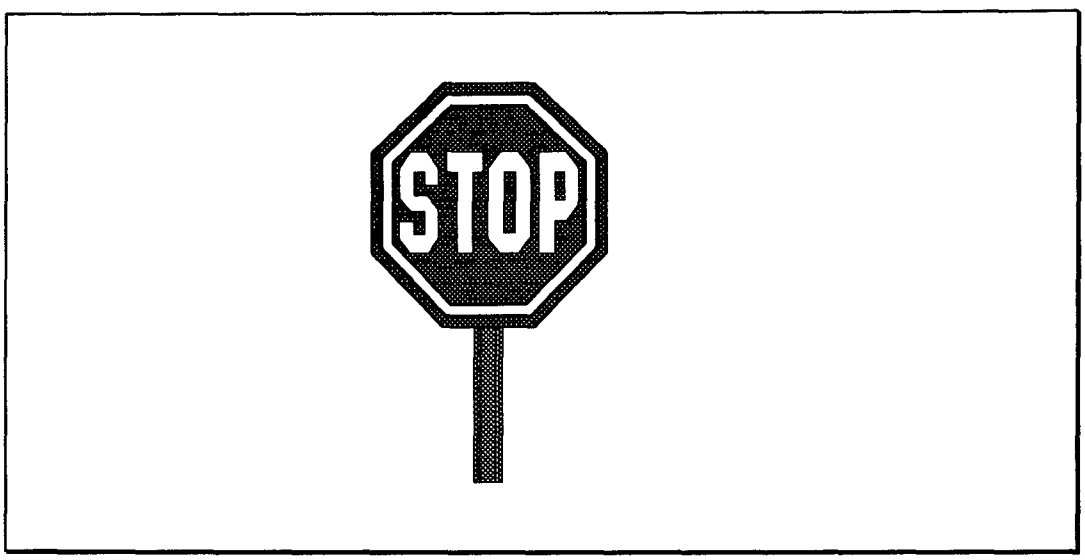
La puerta debería ser abierta y cerrada, de forma automática, desde la conserjería, y debe ser utilizada para retener al personal externo durante su identificación.

También debiera incluirse una cámara de circuito cerrado en la puerta de entrada, para la ayuda a la identificación.

En la barrera de entrada el recinto se procederá a una primera identificación y reconocimiento del vehículo, en caso de que se lleve, comunicando al vigilante que estará en la conserjería a la entrada del edificio, la presencia de personas y su identificación, para que allí se autentifique y se proceda al registro de los maletines y paquetes que portan.

Para la realización de este control de bultos podría utilizarse algún equipo de los existentes en el mercado, que no dañe el contenido de los soportes magnéticos y permita prevenir atentados; o bien permita establecer un procedimiento de claves para autentificar el envío

Debe realizarse una clasificación de todas las dependencias del edificio, para poder establecer las autorizaciones de acceso del personal, tanto funcionarios, laborales, colaboradores externos o visitantes. Dicha medida debe ir complementada con la debida autorización personal, previa identificación y asignación de una tarjeta que deberá llevarse en sitio visible.



La clasificación de las áreas restringidas irá acompañada, para una mayor eficiencia, por una clasificación de toda la información tratada y almacenada en la Consejería en función de su confidencialidad.

La identificación que se realiza en la entrada al recinto, debe ser comprobada y constatada en el parte de visitas en la entrada principal del edificio, donde se procederá a un registro de aquellos objetos que porte. Dicho registro se deberá

repetir a las salida del edificio, anotándose en el parte de visitas la hora de su salida.

Las restricciones de acceso a una persona cualquiera se le asignaría al identificarse como visitante, con lo que tendría un nivel de autorizaciones apropiadas para su cometido. Irá acompañada dicha medida, con la asignación de tarjetas de identificación, que deben llevarse en lugar visible.

Implantar la obligatoriedad de registrar los maletines y los bultos, tanto a la entrada como a la salida de las dependencias de la Consejería de Sanidad. Por otra parte, deberá entregarse una autorización escrita por el responsable de seguridad de cada edificio, para permitir la salida de material del mismo.

Esta medida de seguridad puede ir complementada con un etiquetaje estándar de los paquetes que entren y salgan, y deben ser obligatorias para todas las empresas que colaboren con la Consejería de Sanidad, anotándose en la recepción de cada edificio la entrada o salida, la referencia del paquete, así como el destinatario, o el emisor, comprobándose la autorización del envío.

La reestructuración del edificio sería una medida de bastante urgencia, dado el descontrol reinante en cuanto a los accesos a las diferentes dependencias, y en particular, a la sala de ordenadores. Por ello, debe abordarse una clasificación de todas las dependencias del mismo, estableciendo un nivel de acceso, que conllevaría unos niveles de autorizaciones, para todo el personal que acceda el edificio.

5.1.5.- SEGURIDAD EN EL ACCESO AL C.P.D.

Para adecuar el acceso de personas a la sala de ordenadores, habría primero que trasladar todos aquellos elementos que no deben residir en ella, y departamental la misma con diferentes accesos.

Ni la cintoteca, ni las impresoras deben estar situadas dentro de la sala, así como ningún despacho, como el de planificación o centro de control de la red.

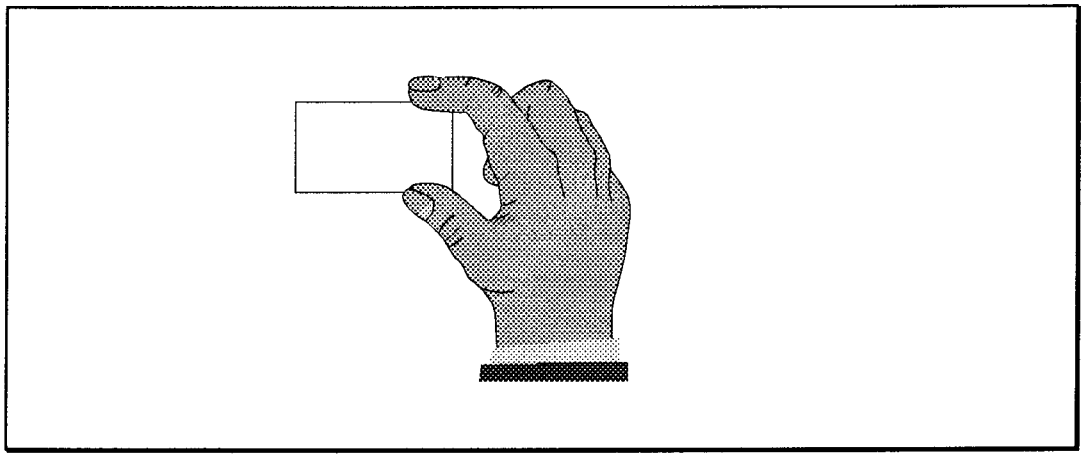
Se colocarán en una habitación separada, las consolas y los dispositivos de soporte magnético, como las unidades de cinta o cartucho. De esta manera, se evitaría la circulación de personal y se clasificarían los niveles de acceso, controlándose de forma más adecuada.

Las impresoras deben estar situadas en una habitación específica, con un control de acceso a personas autorizadas, que gestionarán el reparto o distribución de la información que se obtenga. De esta manera, cada persona que realice una petición sólo podrá acceder a los listados correspondientes, y nunca acceder a consultas de datos o listados de otras entidades o personas.

El ubicar las impresoras en otra sala dentro del propio edificio, puede ocasionar un coste nulo, salvo que conlleve el adecuar el nuevo recinto.

En cualquier caso, el acceso a la sala deberá estar controlado por un mecanismo automático mediante tarjetas magnéticas, con clave de acceso, con

posibilidad de incluir un teclado anexo, para mayor seguridad, o bien otro tipo de mecanismo de similares características.



Con las medidas de restricción de acceso definidas en cuanto al recinto a personas, se incluirá también una reforma en el acceso a la sala, en la cual se contemplará el separar en dependencias distintas todo el material ubicado en la actualidad en la propia sala. Cada una de estas dependencias poseerá su autorización y control de acceso propio.

Podría realizarse un esquema de las áreas de confidencialidad, como un conjunto de circuitos concéntricos en el que el núcleo, de mayor nivel de confidencialidad, estaría ocupado por la sala, y el resto de los anillos irían disminuyendo a medida que se alejan del centro.

5.1.6.- **SEGURIDAD DEL C.P.D.**

La situación actual, en cuanto a la protección del Centro de Procesos de Datos contra el fuego, es gravísima.

Debería abordarse una obra para sustituir el actual recubrimiento de la sala y del resto del edificio. Dicha obra debe contemplar todas las medidas de seguridad necesarias, como son el cerrado permanente de la sala, y la redistribución del equipo del edificio. Debe dotarse, a todas las dependencias, de los necesarios mecanismos de detección de incendio y extinción adecuados.

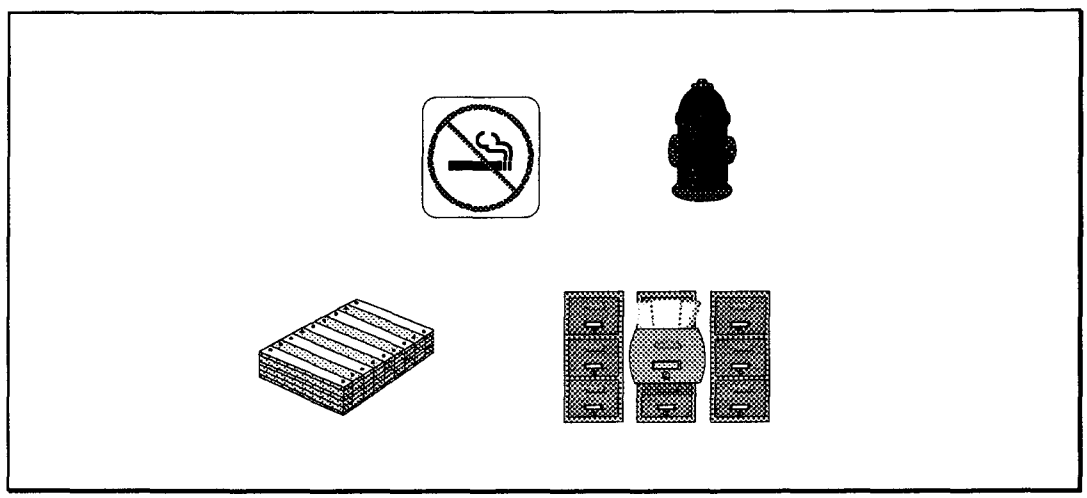
Los materiales que componen las paredes de la sala son combustibles, y facilitarían la propagación del fuego con bastante rapidez. Lo mismo ocurre con el resto de los despachos situados en la parte superior del edificio, que también facilitan la propagación del fuego, en caso de que éste aparezca.

Se recomienda que se aborde urgentemente una obra encaminada a recubrir convenientemente, con material antifuego toda la sala de ordenadores, cerrarla herméticamente, y hacer exhaustivo el recubrimiento antifuego al resto del edificio.

Deben situarse, en número adecuado los detectores de incendio suficientes para evitar la propagación del fuego, tanto en la sala de máquinas de aire acondicionado, como en la sala de las UPS's y baterías, y en las restantes salas del sótano, tales como el almacén de papel, y donde se ubica el almacenamiento masivo.

La central térmica produce vapor de agua para la sala de ordenadores, y calor para la calefacción. Esto produce inundaciones por lo que deben realizarse las obras adecuadas en el edificio, para evitar que ocurran contingencias no deseadas.

Debe establecerse la prohibición de fumar en la sala, y velar para que se cumpla.



La restricción debe extenderse a todas las dependencias de riesgo, como son los almacenes de papel, de material combustible, o las cintotecas en cualquiera de sus ubicaciones, así como la sala del sótano, que alberga la maquinaria de mantenimiento.

5.1.7.- SEGURIDAD DEL PERSONAL INFORMÁTICO

Debe implantares una política de seguridad que contemple:

- incompatibilidades familiares en puestos de trabajo directamente dependientes
- establecimiento de un procedimiento formal de denuncias e investigación
- solicitud de referencia personales, en los casos en que proceda, al realizar nuevas contrataciones, subcontratados o traslados
- en el caso de empresas, hacer un procedimiento de clasificación y homologación de las mismas
- identificación del personal permanentemente visible
- evaluaciones periódicas del rendimiento
- evaluaciones periódicas del trabajo desarrollado
- evaluaciones periódicas de la evolución profesional

La confidencialidad de la información con la que trabajan los técnicos en informática ha de garantizarse desde la creación de la misma, hasta su destrucción, pasando por el Centro de Procesos de Datos, las líneas de comunicación y el entorno del usuario final.

5.1.8.- SEGURIDAD DE LA INFORMACIÓN

Resulta urgente, desde el punto de vista del acceso al Sistema, establecer mecanismos de control de los intentos de entrada o acceso al Sistema, de tal forma que permita la conexión cuando un usuario lo solicite y pase el control correspondiente, rehaciendo el intento en aquellos casos en que la identificación del supuesto usuario no sea satisfactoria.

Uno de los mecanismos más usuales es la introducción de una Palabra Clave (PASSWORD) para la identificación del usuario. La fórmula más extendida es la de pedirle su nombre de usuario (USERNAME) y a continuación la palabra clave, tal que el mecanismo accede al archivo correspondiente para contrastar los datos recibidos y aceptar o rechazar el intento. Esta palabra clave se debe grabar en los archivos de administración del Sistema codificada o encriptada para que no sea fácilmente reconocible por cualquier persona.

Los intentos fallidos de acceso deberán de ser registrados por el Sistema, con el fin de que el Administrador del Sistema pueda estudiar cada cierto tiempo si se está o no intentando transgredir la seguridad del Sistema.

El Sistema deberá dotar al Administrador del Sistema, para que en cualquier momento, se pueda realizar un alta o una baja de un usuario, asignándole en el primer caso, ademas de un USERNAME, la correspondiente contraseña o PASSWORD inicial. Mientras que el USERNAME es público, la PASSWORD no lo es, siendo recomendable su cambio cada cierto tiempo.

Cuando es tecleada la PASSWORD en un terminal para su acceso al Sistema, no deberá aparecer en la pantalla como ocurre con el resto de los datos que se teclean, para así conservar el secreto de la misma.

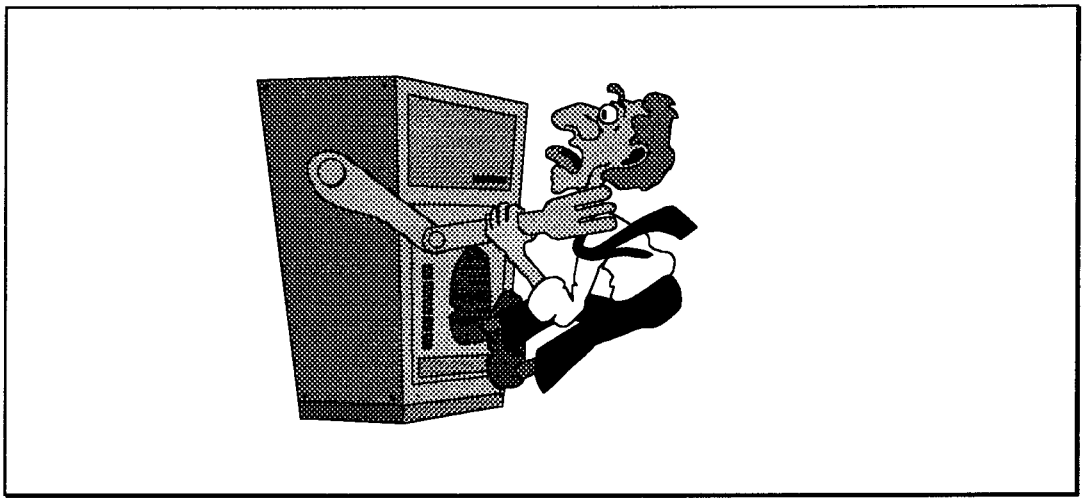
Al proceso de petición de entrada a un Sistema, contestación a las preguntas de identificación, contrastación de los datos recibidos y dar el correspondiente acceso, se denomina LOGIN. Así mismo al proceso de despedida del Sistema, se le denomina LOGOUT.

Por otro lado, deberá elaborarse, un organigrama alternativa, en el que todo puesto de responsabilidad específica tenga previsto una persona como suplente. Será la labor del Servicio de Informática, el comprobar que todas las áreas desempeñadas por una persona, puedan ser realizadas, en la mayoría de las circunstancias, por el suplente correspondiente.

Asímismo, debe tenerse en cuenta esta definición de puestos claves para la planificación del período vacacional.

La información manejada dentro del Servicio, posee diversos orígenes y es muy variado el tratamiento que de ella se hace. La clasificación de toda esa información beneficiaría de manera interna, al facilitar la creación de unos niveles de responsabilidad, y de acceso a la información. Igualmente, evitaría el acceso a información sensible por parte de personal externo o subcontratado.

No puede caer sobre un mismo estamento la labor de gestionar el sistema, con la peligrosidad inherente de esta labor, junto con la labor de seguridad y control de las tareas de los demás técnicos.



Por ello, debe crearse una oficina de seguridad, bajo la dependencia directa del Servicio de Informática, que entre las labores, coordinará la seguridad informática, con el establecimiento de perfiles de acceso adecuados, y la revisión periódica de los mismos.

5.2.- SEGURIDAD LÓGICA

5.2.1.- SEGURIDAD LÓGICA SOBRE EL SISTEMA

Todos los accesos a los recursos y datos de los ordenadores deben estar perfectamente controlados, de manera que ninguna persona pueda acceder a información o herramienta a las cuales no esté autorizado.

El método más comúnmente utilizado para ello es la implantación de un software de seguridad específico. Este software de seguridad fundamenta su efectividad en la confidencialidad de códigos de usuario, personales e intransferibles, y claves de acceso secretas, con grado máximo de confidencialidad.

Se debe asignar a cada usuario un perfil de acceso adecuado, en el que se establezcan claramente a qué ficheros puede acceder, y en qué modo, es decir, consulta, actualización, etc.

Los códigos de usuarios y passwords de acceso deben cumplir una serie de condicionantes:

- deben ser únicas para cada usuario
- no deben compartirse
- deben ser totalmente confidenciales
- no deben ser visualizadas por pantalla, ni figurar impresas en ningún listado
- deben ser de 6 a 8 dígitos

- no deben incluir el carácter blanco
- las passwords deben ser cambiadas periódicamente
- la nueva password no debe ser igual a ninguna de las diez últimas

De este modo, debe existir una mentalización de todo usuario sobre la confidencialidad de los códigos, y claves de acceso, para lo cual se deberían impartir cursos monográficos, dado el nivel actual existente en cuanto a esta conciencia.

Por otro lado, deben crearse los procedimientos adecuados para la comunicación de altas y bajas de usuarios al sistema, mediante la utilización de un impreso, que debidamente cumplimentado, y con la firma del Jefe del Servicio o del Área correspondiente, notifique oficialmente el cambio de su situación.

El software del sistema se puede considerar como responsabilidad de los técnicos del sistema operativo, y serán los únicos que podrán realizar cambios sobre los procedimientos o programas, bajo la supervisión del Jefe de Área

El entorno de explotación debe ser especialmente protegido, de manera que los programas, cadenas y jobs no puedan ser ejecutados por ningún técnico que no pertenezca a explotación.

En el caso del entorno de IBM, el software que gestiona los soportes magnéticos es el PCIN, que deberá dotarse de medidas de protección adecuadas, de modo que sólo pueda ser utilizados por los técnicos correspondientes.

Es necesaria la formalización mediante un impreso adecuado a tal efecto, cuando el usuario cause baja en la entidad o bien cambie de destino dentro de la Consejería de Sanidad. Lo que puede obligar a una modificación de las autorizaciones y derechos de acceso.

Este impreso deberá ser cumplimentado y enviado por el departamento correspondiente a los responsables de la administración del sistema de seguridad, con la debida antelación, para que se produzcan las modificaciones en el código de usuario en el mismo momento en que se produzca la modificación de su situación persónalo.

Dicho impreso debe incluir la fecha efectiva de baja, en los casos que procedan, y las características del nuevo perfil y su nuevo destino , en el caso de los modificaciones.

La necesidad de que en determinados momentos se consulte el fichero de password para visualizar la correspondiente a un usuario en concreto, no justifica la existencia del programa que lo posibilita.

Este programa debe eliminarse de la instalación, o bien ubicarse en zona de uso exclusivo del personal responsable de la administración de password, y de la gestión de perfiles de acceso,.

Se debe realizar una revisión formal de log del sistema, y de los diferentes loggin específicos con el fin de detectar posibles intentos de violación las autorizaciones establecidas, o el procedimiento indebido de determinados trabajos.

También puede servir para comprobar que se han realizado todas las tareas planificadas en un determinado período y que su finalización ha sido la adecuada.

La revisión debe realizarse en profundidad sobre un listado impreso, anotándose las consideraciones oportunas, y deberá quedar constancia de la persona que lo realiza, la fecha y la hora.

Una vez finalizada la revisión, y con las medidas adecuadas para solventar problemas, deberá guardarse como soporte documental durante el período de tiempo que se considere oportuno, teniendo en cuenta que el fichero de la instalación que lo contenga deberá estar incluido dentro del calendario de salvaguardas con la periodicidad oportuna.

Existe un procedimiento de colaboración con Desarrollo se realiza en términos adecuados, pero es necesario normalizar las relaciones existentes en la actualidad para instrumentar de un modo formal dicha colaboración.

Deberán incluirse en esta normativa los calendarios de reuniones previas, el oficializar los acuerdos a los que se lleguen, el realizar seguimiento de lo acordado, y los plazos a cumplir, y el delimitar claramente las responsabilidades de cada persona, entidad u organismo que participe en las mismas.

En cualquier instalación que posea el hardware suficiente, es recomendable realizar una reestructuración física de máquinas, de manera que todo trabajo de explotación se encuentre desvinculado y segregado de todo el correspondiente a desarrollo y pruebas.

Esta medida implica una serie de controles que aumentan en gran medida la seguridad de la instalación, siempre y cuando los recursos que se compartan para ambas máquinas, y la comunicación entre ambas, esté debidamente controlada.

Con ello, se conseguirá imponer una traba suplementaria a los posibles intentos de acceso de personal no autorizado, generando un coste incuantificables por la propia naturaleza de la medida.

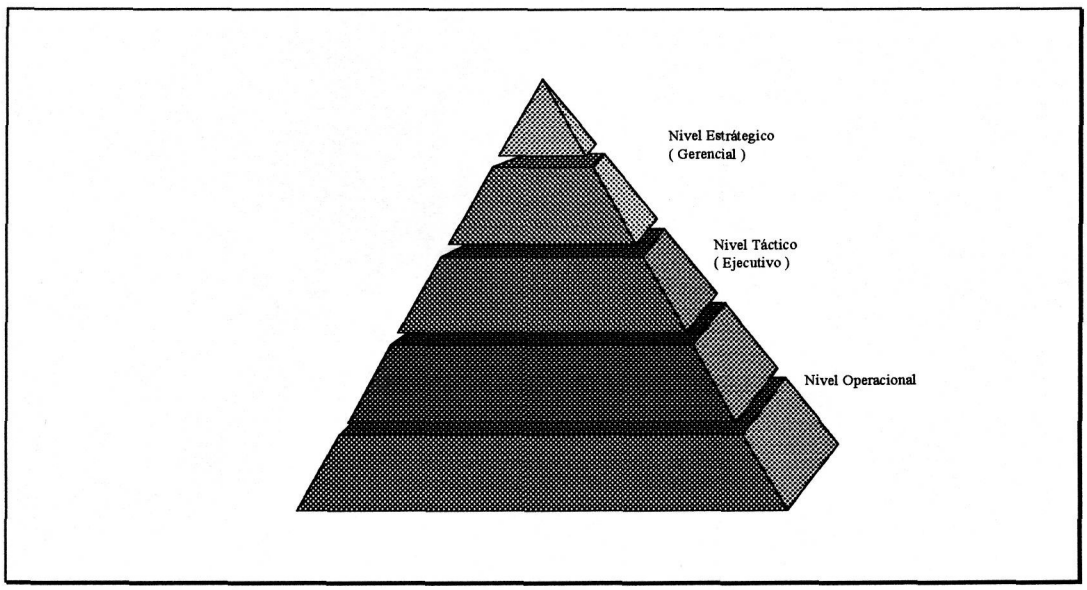
Para garantizar la completitud del software del sistema instalado, y realizar un control adecuado sobre las versiones y release que se implantan, se debe mantener un inventario de todos aquellos productos software que se encuentren activos en la instalación, incluyendo la versión, la fecha de incorporación y la persona que lo implantó.

Además dicho inventario deberá ser utilizado periódicamente para comprobar el estado de los diferentes módulos software de la instalación, y para poder detectar nuevas incorporaciones no autorizadas, o modificaciones incontroladas.

Otra medida preventiva contra posibles alteraciones no controladas del software del sistema, puede consistir en el recopiado de ciertos módulos software desde sus copias de seguridad, con la frecuencia o perioricidad que se considere oportuno, y dependiendo de la importancia del software en cuestión.

Debe implantarse un conjunto de restricciones, encaminado a limitar el uso de recursos software. Dicho conjunto de restricciones debería ser adaptable a cada

usuario, dependiendo de su ubicación dentro de la estructura organizativa y del cargo desempeñado.



Así pues, algunos usuarios tendrán acceso al software del sistema para por utilizar algunas de las herramientas, y a otros les estará prohibido por el nivel de autorizaciones. El copiado y el renombramiento, así como el borrado de módulos software, deben estar totalmente restringidos, de manera que sólo sea personal de sistemas quien pueda realizarlo, bajo los controles establecidos por los administradores de la seguridad.

Todas estas labores deberán estar incluídas dentro de la descripción del puesto de las personas que se responsabilizan de la seguridad lógica.

En todo centro informático de gran envergadura, como es el caso del Servicio de Informática estudiado, en el que existen áreas de trabajo dentro de cada entorno, que deben ser totalmente disjuntas, es d vital importancia el evitar que se puedan realizar trabajos restringidos desde terminales no pertenecientes al propio entorno físico donde se ubican las personas que lo realizan normalmente.

De esta manera, se consigue que cualquier acceso lógico no autorizado debe superar dos barreras importantes, una primera consistente en adivinar o identificar un código de usuario autorizado para realizar lo que se quiere, además de su password, o bien puentear los controles existentes mediante el conocimiento profundo del software en cuestión: y una segunda barrera que obligará a que la persona que va a realizar el acceso indebido, lo realice desde una sala al cual no debe tener acceso libremente.

Esta es una medida que tiene un componente informático del software utilizado para ello, y un componente organizativo del personal que accede a cada recinto de una instalación.

A esta medida puede incluirse la consistente en incluir horarios de trabajo a los códigos de usuario, como una medida más encaminada al control de accesos.

Los editores deben ser de uso exclusivo del personal de desarrollo, con las restricciones específicas a cada librería en concreto.

Todo el personal, que por las necesidades de su empleo, deba acceder ocasionalmente a los editores, deberá tener muy restringuido los recursos a los que pueda acceder con ellos.

Con ayuda del software de protección adecuado, se deben agrupar y clasificar las diferentes utilidades del sistema, de modo que a cada tipo de usuario se le asigne una autorización adecuada a la labor a realizar, y que tengan acceso exclusivo a aquellas utilidades que le correspondan.

Esta es una medida que puede ser complementaria a la restricción de acceso a recursos concretos, como pueden ser ficheros, librerías de explotación, programas de desarrollo, etc...

También se puede tomar la precaución consistente en mantener off-line todas las utilidades sensibles, y que merezcan atención especial, por lo peligroso de su uso, y que para utilizarse haya de realizarse una petición autorizada.

5.2.2.- SEGURIDAD LÓGICA SOBRE LOS DATOS

Los procedimientos de recuperación deben ser, dentro de lo posible, automáticos, de forma que se inicie y ejecute el proceso de recuperación con la intervención del operador reducida al mínimo imprescindible.

Los procedimientos de backup estarán incluidos al final de la cadenas de ejecución, para proceder de forma automática a la obtención de las correspondientes copias de seguridad. Por otro lado, existirán los planes periódicos de copias, semanal, mensual, trimestral, anual, todos ellos con los períodos de retención adecuados en cada caso.

Una vez que se haya procedido a una recuperación, se debe activar un proceso, bien estándar o bien desarrollado, que chequee el estado de todos los ficheros que se han visto de alguna manera involucrados en el incidente y su posterior recuperación, garantizando la disponibilidad de todos los datos o, en su defecto, indicando cuál de los ficheros debe ser recuperado desde una versión previa, o desde una copia de seguridad.

Por otro lado, debe tomarse la precaución de borrar totalmente un soporte magnético antes de regrabar o al reciclar, de modo que se garantice la inaccesibilidad a datos a personas que no estuvieran autorizadas a ellos.

Con vistas a garantizar la confidencialidad de la información, debe abordarse una clasificación de toda la información manejada dentro de la Consejería de

Sanidad, aunque es muy diversa, con orígenes muy diferentes, y con tratamientos muy variados de un tipo a otro.

Dicha clasificación en función de la confidencialidad propia de la información, beneficiaría internamente al Servicio de Informática, al facilitar la creación de unos niveles de responsabilidad, y de acceso a la información existente, y muy útil por la presencia de personal subcontratado, técnicos de ordenadores, seguridad, limpieza,.

Por otro lado, el transporte, distribución y la destrucción de la información, tanto en soporte magnético como en papel, debe quedar garantizada estableciendo procedimientos de obligado cumplimiento.

Resulta de gran interés el crear la figura de Administrador de la Base de Datos, como responsable de la autenticidad y validez de la información almacenada en las bases de datos, con unos procesos periódicos de comprobaciones y con las herramientas necesarias que le permitan navegar dentro de la estructura.

Deberán implantarse las debidas restricciones informáticas de acceso, correspondientes a una estructura jerárquica y funcional adecuada. No basta con que los organigramas jerárquicos de funciones existan, sino que debe de ser implantada la separación adecuada, con ayudas del software de control apropiado, del cual se dispone en ambos entornos informáticos.

Es de suma importancia el establecer un calendario que incluya todos los ficheros de ambos entornos, y que establezca una perioricidad adecuada a cada uno de los ficheros, para que, dependiendo los casos, se realicen pruebas sobre su contenido, con vista a garantizar la fiabilidad de la información.

Estas pruebas pueden realizarse sobre el total de los datos, mediante revisión de campos clave, o bien sobre nuestras estadísticas seleccionadas convenientemente, que asignen a dicha muestra cualidades propias de la población completa de registros.

El estado actual lleva a la necesidad de abordar una estructura funcional de todo el personal que accede a recursos informáticos en la Consejería de Sanidad.

En esta nueva estructura tendrán que diferenciarse claramente las personas que accederán y los recursos a los que tendrán acceso, dependiendo del perfil de usuario que se les asigne. Habrá que realizar, dentro de cada entorno informático, una separación del área a que corresponda cada usuario (desarrollo, explotación, sistemas) y loa labor que desempeñará o puesto que ocupará (operador, programador, analista, jefe de proyectos,..).

Una vez realizada esta estructura funcional, habrá que asignar las responsabilidades adecuadas a cada puesto y categoría, y llevarlo al plano informático.

Hoy en día, todo trabajo periódico y repetitivo, necesita de unas normas que sirvan de guía, y marquen las pautas a seguir, para que se consiga el máximo de eficacia.

La obtención de copias de seguridad, y en particular, las del software del sistema, posee una problemática muy específica, lo que hace todavía más necesaria la existencia de unas normas.

Dichas normas deben incluir la perioricidad adecuada, dependiendo de cada instalación, o de cada entorno, y el método de actuación en los casos de nuevas incorporaciones, indicando claramente la vigencia de las mismas, y el lugar de ubicación en caso de ser necesarias medidas especiales.

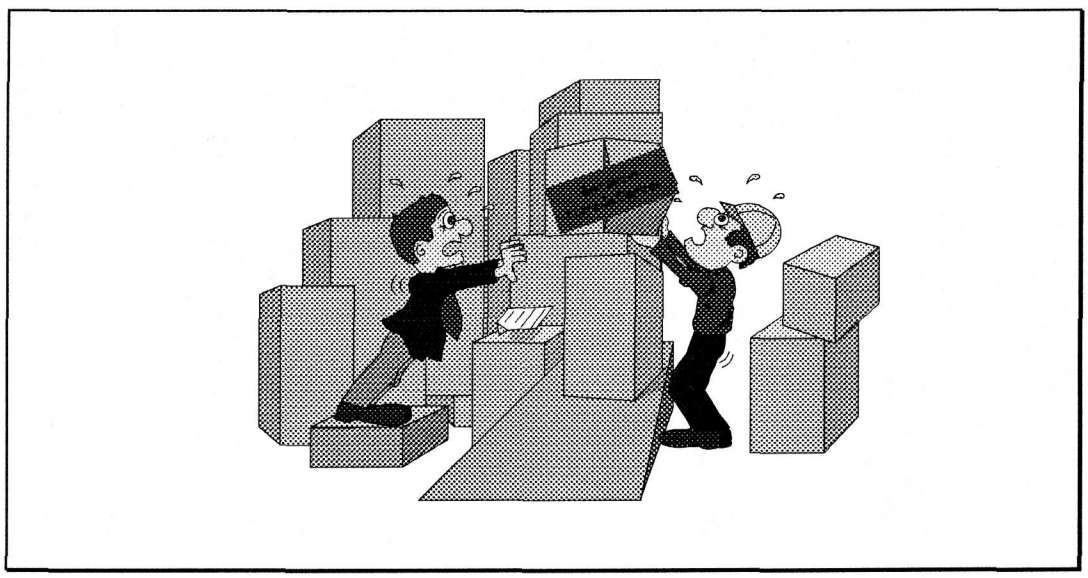
Es totalmente necesario que se establezca una separación orgánica y funcional entre el personal que realiza las labores de administración de la seguridad lógica de la instalación, y de los que realizan las labores de gestión técnica del sistema.

En este caso particular, y con la distribucción de áreas existente, los administradores de seguridad deben pertenecer a ambas áreas, es decir, a la de Desarrollo y Mantenimiento, y a la de Sistemas y Explotación; aunque lo ideal no sería esto.

Por otro lado, se recomienda realizar las siguientes actuaciones en un plazo de tiempo corto, para evitar posibles errores agravados:

- inventariar los ficheros existentes

- inventariar las cesiones de datos que se realizan, tantos cesionarios como cedentes.



- comprobar que los datos contenidos en los ficheros satisfacen las necesidades legítimas para los que fueron obtenidos, son adecuados, pertinentes y no excesivos.
- adaptar los ficheros a las comprobaciones, si fuera necesario

5.2.3.- SEGURIDAD LÓGICA SOBRE LAS APLICACIONES

El acceso al sistema de los usuarios informáticos, debe ser adecuadamente controlada por una sistema de códigos de usuario y password que restrinjan y autoricen los accesos.

Las password son uno de los elementos más importantes de la confidencialidad, y por eso debe existir una normativa que formalice tanto la codificación, como el mantenimiento de las mismas.

Entre otras características debe reunir las siguientes:

- ser única para cada usuario
- no deben compartirse
- deben ser totalmente secretas
- no deben ser visualizadas en ningún caso
- deben ser de 6 u 8 dígitos
- no deben tener el carácter blanco

Además habría que añadir el cambio periódico obligatorio para todos los usuarios.

Los software de seguridad que se poseen pueden proporcionar información completa sobre la actuación de usuarios concretos, así como de los intentos fallidos en su conexión, y controlar el número de ellos; por tanto, únicamente se recomienda su utilización, para poder obtener provecho con la información registrada.

Toda esta información puede quedar reflejada en *log* específicos para realizar un seguimiento mas o menos exhaustivo.

El seguimiento de los intentos fallidos en la conexión debe llevar a una investigación de las causas, y tomar las medidas oportunas, informando sobre aquellos casos que se consideren destacables.

Los sistemas operativos vigentes en la actualidad en el Centro de Procesos de Datos, y los paquetes de seguridad adquiridos por la Consejería de Sanidad posibilitan la restricción a nivel fichero de los controles de acceso lógico.

Dado que el software contratado aún no ha sido debidamente extendido a toda la instalación, es de máxima urgencia que así se haga y se estructuren debidamente los posibles usuarios, de modo que puedan ser agrupados por categorías o grupos de autorización.

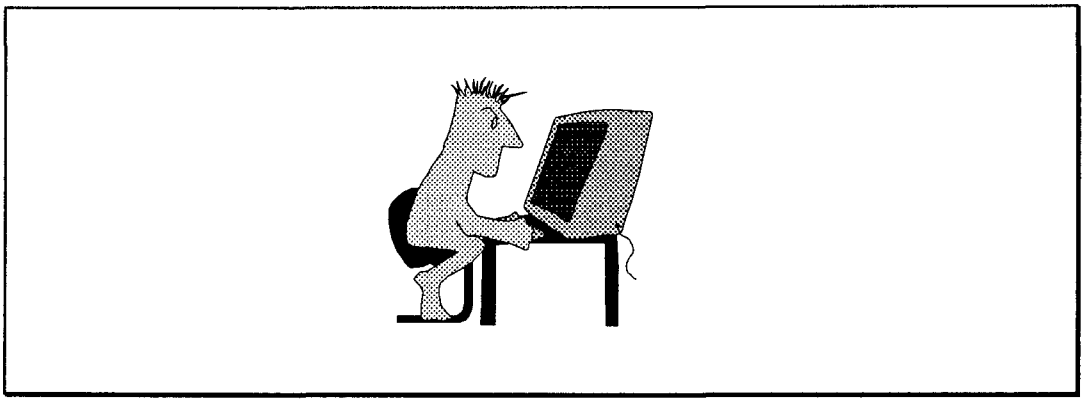
Todo ello facilitará el control de los datos de instalación, dotando de una fiabilidad a la información residente en ficheros.

Algunas de las medidas a tomar pueden ser el control periódico del tamaño de los programas, o que con relativa frecuencia, pero de una manera periódica, se proceda a recopiar programas partiendo de las copias de seguridad.

También se puede realizar un control estricto sobre la copia de seguridad para detectar si éste ha sido o no alterado, o comprobando la fecha de las versiones que se están utilizando para la búsqueda de posibles divergencias, o mantener un

inventario completo de programas que incluya la versión, hora y fecha de cada uno de los existentes en la instalación.

Toda modificación al software del sistema, independientemente de su envergadura e importancia, deberá ser formalmente autorizada por el jefe de área correspondiente, mediante una firma en un documento impreso, en el que se detalle brevemente la naturaleza del cambio a realizar, y de su necesidad, así como, la fecha esperada de posible incorporación definitiva de dicha modificación a la librería del software.



De este modo, además de garantizar la autorización de todos los cambios que se realicen, se podrá mantener un inventario de módulos software, con la fecha de incorporación, versión y estado en que se encuentra.

Se evitan así posibles problemas originados por la dependencia personal de quien realice los cambios de una manera efectiva, y de su memoria para diversas precisiones, o matices de la modificación.

5.3.- SEGURIDAD EN LAS TELECOMUNICACIONES

5.3.1.- SEGURIDAD FÍSICA

Deberán adoptarse las medidas de seguridad adecuadas en la ubicación de terminales en centros remotos, con la supervisión de personal responsable, y situándolos en despachos de acceso restringido.

Las terminales de usuario deberán estar en despachos que posean puertas con cerraduras, de manera que cuando el operador terminalista se ausenta, se pueda cerrar con llave la puerta de acceso. Además, aunque sea una medida más bien de seguridad lógica, si el terminal posee una llave, proceder a quitarla y guardarla en un lugar adecuado.

Por otro lado, el hardware de comunicaciones y de control de la red, debe ser contemplado como parte del de la sala y, por lo tanto, ser aislado convenientemente en una sala específica, con las autorizaciones de acceso necesarias para el personal de dichas áreas de telecomunicaciones.

Las medidas de seguridad con respecto al equipo central ubicado en el Centro de Procesos de Datos pueden extrapolarse al equipo de telecomunicaciones, por tratarse de una parte integrante de dicho centro, y estar ubicado dentro de la propia sala de ordenadores.

5.3.2.- SEGURIDAD LÓGICA DEL SISTEMA

Se recomienda designar un administrador de las Telecomunicaciones que asumirá la responsabilidad plena de la Gestión las comunicaciones: Existen tres áreas principales:

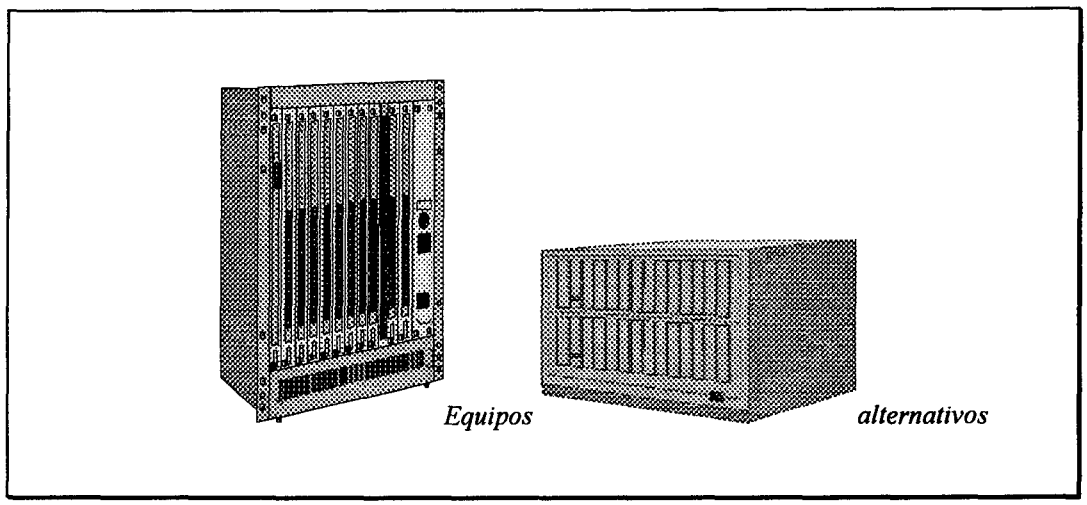
- *Seguridad* : Deberá asignar las contraseñas a los usuarios, el establecimiento de grupos de ellos y creación de informes acerca de la utilización real de las comunicaciones. Esta última tarea es esencial, porque los supervisores han de poder identificar a las personas que hayan venido accediendo a un directorio.

- *Rendimiento* : Puesto que los usuarios nuevos u ocasionales pueden experimentar dificultades con funciones de rutina, como la entrada (LOGIN), los supervisores, deberán de ayudarles estableciendo unos sencillos procedimientos o "rutinas" a seguir.

  Por otro lado, se podrá observar el rendimiento de las comunicaciones en las estadísticas de tráfico de la red, de modo que podrá contribuir al control del Sistema y al logro del máximo rendimiento.

Los administradores necesitarán llevar diarios de operaciones que faciliten la localización y el seguimiento de todos los cambios ocurridos en la red. Este libro o diario de operaciones debe guardarse bajo llave cuando no se esté utilizando.

Otro punto a tener en cuenta dentro de la seguridad de las telecomunicaciones, debe ser la disponibilidad de Hardware de reserva. Es conveniente disponer de recursos secundarios, ya que en caso de una avería, el Sistema puede volver a ponerse en marcha, una vez reemplazado el dispositivo defectuoso, de tal manera que no se vea afectado el servicio prestado al usuario.



Uno de los puntos más importantes de un buen sistema es su documentación; cuanto mejor sea la documentación, más fácil será instalar y mantener el Sistema.

La documentación debe de ser una descripción completa de la Red, incluyendo las estaciones, los periféricos, los cables y otros dispositivos. La documentación del Administrador, deberá contener toda la información necesaria para mantener la Red. Habrá de incluir las guías de operación de todo el equipo, los códigos y mensajes de error del Sistema, las guías de localización de problemas, etc.

Una buena documentación deberá incluir ejercicios, prácticas e instrucciones paso a paso de todas las situaciones, además de una ayuda relativa al contexto con información resumida que le sirva al operador para salir de una situación determinada sin tener que recurrir a los manuales.

Además, la información de los manuales, ha de ser fácil de localizar, bien sea por medio de un índice de contenido o por cualquier otro método. Las instrucciones de conexión y desconexión del Sistema y los comandos más importantes, deberán resumirse en una guía de referencia.

Debe plantearse la incorporación de un registro completo de las conexiones a la red, o bien completar de forma adecuada la información que suministran los *log* del software instalado.

Se debe adecuar la forma de conexión, de manera que los controles actuales no puedan ser saltados por los usuarios, junto con el correcto conjunto de perfiles de usuario de identificación personal.

El *log* por ambas redes deberá ser revisado exhaustivamente, para descubrir accesos indebidos, o tomar las medidas adecuadas a casos concretos, así como tener un control directo de la calidad del servicio.

El establecimiento de líneas de backup en la red de telecomunicación, instrumento mediante rutas alternativas entre nodos provinciales, es una necesidad urgente, que está contemplando en los planes del Servicio de Informática.

Deben agilizarse los trámites para que se lleven a buen fin las gestiones encaminadas a la adecuación y modernización de la actual red de teleproceso.

Se deberán adoptar las medidas oportunas para evitar todo tipo de incidencias en las terminales remotos de la red sean comunicadas telefónicamente al área de control de red, mediante la formación adecuada de usuarios, y el establecimiento de un procedimiento formal a seguir en cada caso.

Como medida de seguridad, y al menos mientras no se adopten controles adecuados de acceso a la red, sería recomendable el que diariamente, y finalizado el horario normal establecido para el teleproceso, se cierre durante la noche.

Otra posibilidad, dependiendo de las características propias de la red, sería abrir o cerrar determinadas líneas de la red durante ciertos turnos laborables, de manera que se tenga controladas las líneas de teleproceso abiertas, por expresa solicitud del usuario, durante horarios no habituales.

Se recomienda el uso del procedimiento existente, dado que su validez ha sido contrastada, y sea el único para tramitar y gestionar las bajas y cambios de destino de usuarios a través de la red de comunicaciones.

Otro punto a tener en cuenta dentro de la seguridad de las telecomunicaciones, es la disponibilidad de líneas y equipos alternativos, que puedan suplir la falta de uno de los equipos o líneas en un momento determinado, sin que por ello se vea afectado el servicio prestado al usuario.

5.3.3.- SEGURIDAD LÓGICA DE DATOS

Se recomienda el desarrollo de un programa cuidadosamente planeado para las Copias de Seguridad (Backup) de la Red, que deberá adecuarse a las necesidades de la instalación. Deberán realizarse diariamente, pero en la mayoría de los Sistemas de Software exige el backup sólo de aquellos archivos que hayan sufrido modificaciones desde el último backup (mediante la hora de dichos archivos). Estos se deberán realizar sobre soporte magnético, almacenándose en dependencias alejadas del Sistema y en armarios protegidos.

Deberían existir dos alojamientos adecuados para albergar el backup, uno dentro del propio edificio del Servicio de Informática, y otro externo. Ambos deberán tener protección adecuada contra el fuego, humedad, descargas eléctricas y acceso restringido, para evitar robos o pérdidas inintencionadas.

Además deberá dotarse al transporte de los soportes magnéticos de las medidas de seguridad adecuadas para garantizar la integridad y la completitud de la información que se envía.

La documentación del Administrador, deberá contener toda la información necesaria de las rutinas y procedimientos de recuperación para que puedan ser consultados en cualquier momento por el personal de explotación que lo necesite.

Se debe mantener una documentación completa y actualizada de todos los procesos de explotación, y en particular, de los de recuperación, sin que por ello se supriman comentarios aclaratorios en los propios jobs.

Es por lo tanto, absolutamente necesario el tomar consciencia de la importancia de poseer una documentación clara de todas las rutinas y procedimientos de recuperación que puedan ser consultados en cualquier momento por el personal de explotación que lo necesite. Deberá crearse una normativa al respecto.

Toda la documentación generada por la actividad del proceso informático como son los manuales, cuadernos de carga, especificaciones de jobs, etc, deberán ser copiados y almacenados con la misma medida de seguridad que el resto de los backup.

Por otro lado, para evitar el acceso a los datos durante la transmisión, lo que ocasionaría problemas de fiabilidad y de confidencialidad de la información, es recomendable la utilización de procedimientos de encriptación de la información. Este sistema de seguridad codifica todos los caracteres de un fichero, es decir, los cambia empleando un determinado algoritmo, de forma que no se pueda entender.

La mayoría de los sistemas de encriptación emplean una clave que consta de una clave de acceso o de números aleatorios, que se usa como base para codificar y decodificar los datos. Al pasar por una serie de transformaciones quedan irreconocibles. La instalación de un sistema de codificación se puede realizar mediante Hardware especial de codificación conectado a las lineas de comunicación, o Software implantado en cada estación.

De concienciarse al usuario final de la confidencialidad de los datos que maneja y debiera hacerse participe de la problemática que pudiera acarrear su transmisión a órganos no deseables.

En base a los siguientes factores se podrá estimar la necesidad de implantar un sistema de encriptación de datos:

- El grado de importancia de la información : cuanto más valiosa, más necesario será su encriptación.

- El coste : el Software de codificación no es muy caro, pero necesita mucha memoria y tiempo para encriptarla. Por el contrario, el Hardware de codificación es bastante caro.

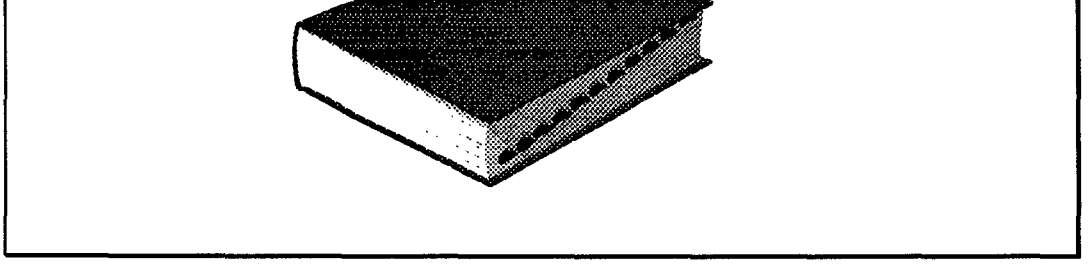
- El tiempo : el Software de codificación suele ser bastante lento, lo que reduciría el rendimiento de las comunicaciones. Siempre es posible utilizar Hardware de comunicación, que es varias veces más rápido que el Software.

Por otro lado se encuentra la fiabilidad de la transmisión de los datos, que juega un papel activo en todo el proceso. Los medios de transmisión influyen introduciendo un elemento importante del proceso de comunicación : el ruido, que es el conjunto de todas las interferencias, de cualquier clase, que van a deteriorar la calidad de una transmisión, llegando hasta el extremo de generar errores que la dificulten o incluso la impidan.

Se recomienda que el Servicio de Informática aborde la confección de un Plan de Contingencias que permita garantizar al máximo la continuidad de la actividad informática.

La Consejería de Sanidad se beneficiaría altamente al contar con un Plan de Contingencias, en el que se contemplase soluciones alternativas probadas para cualquier problema que pudiera surgir con la relación al proceso de datos.

Por otra parte, la existencia de un centro alternativo, en el cual, aún en modo restringido, se puede continuar la actividad informática, es la pieza clave de cualquier plan de contingencias. Se deberán abordar los análisis y estudios adecuados, con el fin de concertar un acuerdo formal con un centro de proceso de datos alternativo.



5.3.4.- SEGURIDAD LÓGICA DE APLICACIONES

El Sistema, en el momento de la conexión del usuario, tras su identificación asigna el perfil correspondiente a dicho usuario, deberá garantizar el acceso de las personas previamente definidas.

Deberá estructurarse el actual control de acceso lógico, para evitar que se puedan saltar controles. Es totalmente necesario que todas las aplicaciones necesiten de PASSWORD de acceso para todos los usuarios, que se realice un seguimiento sobre los códigos identificativos y las password de usuario.

Deben implantarse controles no existentes en la actualidad, que eviten la adivinación de password, como son:

- la limitación de intentos fallidos
- la desconexión por inactividad
- la reconfirmación de código y *password* después de un período largo de trabajo
- cambio frecuente de *passwords*, obligando a que la nueva password sea diferente a las cinco últimas

Deben documentarse completamente los procedimientos y normas a seguir en la gestión y administración de *password* y *códigos* de identificación.

5.4.- CONTROL SOBRE LA EXPLOTACIÓN DEL SISTEMA

5.4.1.- SEGURIDAD FÍSICA DE SOPORTES MAGNÉTICOS

La inmensa cantidad de información procesada en el Centro de Proceso de Datos implica la existencia de gran número de soportes magnéticos para almacenarla convenientemente.

La información es el bien más importante que posee la entidad, y por ello necesita de unas medidas de seguridad específicas.

Sería necesario cambiar la ubicación de la actual biblioteca de soportes magnéticos, de manera que sólo estuviesen en la sala, aquellos que están dispuestos para ser usados en un momento dado.

El almacenamiento de soportes magnéticos debe ser adecuado, en un lugar que reúna las condiciones de control precisas para los soportes magnéticos, tales como humedad, temperatura, y las medidas de seguridad adecuadas para evitar pérdidas o robos. Debe tenerse en cuenta que toda la información que se maneja en la Consejería de Sanidad es altamente confidencial.

En la sala de ordenadores la Biblioteca de cintas, no se encuentra en un lugar debido, puesto que está abierta a la circulación de personas, y no existe protección.

Las cintas deben estar en una sala específica para soportes magnéticos, separada de la que contiene los ordenadores, y las únicas personas que deben acceder a dicha sala, serán los que realicen la labor de bibliotecarios, con lo cual se consigue que el acceso este controlado.

Los soportes magnéticos deben poseer una etiqueta externa numérica o alfanumérica, que permita clasificarla y referenciarla adecuadamente, sin que por ello se suprima una adhesiva que indique el contenido.

Las cintas deberá ser clasificadas en base a esa etiqueta externa, y deberán ser solicitadas referenciándola por la misma.

Además, dentro del edificio deberá existirán lugar donde se guarden las copias de seguridad llamadas "internas". Este lugar deberá estar protegido contra incendios, mediante armarios ingnífugos, detectores y extintores automáticos, también contra las posibles inundaciones, con el correspondiente hermetismo, y alejado de fuentes de energía que eléctricamente pueda alterar o invalidar la información, de acceso exclusivo a bibliotecarios.

En determinadas circunstancias, y dependiendo de la estructura del edificio y volumen de procesos, podría coincidir esta última sala con la biblioteca de cintas general.

La existencia de un gestor automático de soportes magnéticos facilita, en gran medida, la labor el bibliotecario para mantener un inventario actualizado de soportes, donde conste si está o no disponible, y en su caso de no ser así, el

contenido y la vigencia del mismo. Este software puede adquirirse a una firma externa, pero podría también desarrollarse a medida según las necesidades del servicio.

Este gestor automático de soportes magnéticos debe ser de uso exclusivo del personal de la biblioteca y de los preparadores, o planificadores de tareas de explotación.

Todos los ficheros almacenados en soporte magnético, cinta o cartucho, que se conserven como seguridad, deben poseer etiquetas de cabecera, que el propio software pueda comprobar en el caso de que exista un error de los operadores al montar un soporte no adecuado.

Podría plantearse la adquisición de una máquina para la limpieza y verificación de cintas magnéticas, de manera que todas aquellas que no sean de utilidad, se destruyan o se envíen fuera para su destrucción, eliminando los peligros que ocasionan.

Debe realizarse una comprobación de todas aquellas cintas que contienen datos antiguos, para certificar su utilidad y proceder a reutilizarla o destruirla.

El inventario de soportes magnéticos debe ser controlado de forma automática por los bibliotecarios, realizándose las altas, bajas y modificaciones en tiempo real, cuando se comunique la utilización o liberación de una cinta. Con este inventario se evitarán problemas de pérdida de soportes o almacenamiento de información no útil.

5.4.2.- SEGURIDAD LÓGICA SOBRE EL SISTEMA

En una instalación de Procesos de Datos de cualquier envergadura es fundamental que todos los procesos de explotación estén bien documentados, tanto documentación en papel sobre manuales manejables, como en comentarios que autodocumenten los procesos y faciliten su consulta diaria.

En particular, los procedimientos de explotación, por su naturaleza, deben tener una documentación muy clara y completa. La importancia de estos procedimientos no radica tanto en la perioricidad de su utilización como en la propia función que realizan.

Deberá establecerse un calendario dentro de los procesos de explotación diaria, en el que se contemple las pruebas de los procedimientos, de manera que se pueda garantizar su funcionamiento en el caso de que fuera necesario.

Este calendario deberá elaborarse para posteriormente incorporarse al los planes de explotación.

Deberá existir una copia de seguridad de toda la documentación generada en esta área. Esto resulta de gran ayuda, evitando pérdidas irrecuperables, recurrir a fuentes originarias para recuperar manuales, además de la pérdida innecesaria de tiempo.

Por otro lado, debería llevarse un libro o cuaderno de incidencias, a modo de diario de problemas, en el que se reflejen todas las incidencias acaecidas, la hora y

la fecha, la causa que la motivó (en caso de conocerse), las acciones correctoras y los efectos ocasionados por dicha incidencia, dejando constancia de si se solventó o no, y en que fase de resolución se halla, para documentar a la persona que lo consulte.

Este libro deberá ser consultado por el Jefe del Sala de cada turno, y formará antes de que se proceda al relevo por el turno siguiente.

Será de responsabilidad directa del Jefe de Explotación, o de la persona en quien se delegue, el mantener una biblioteca de documentación de todas las aplicaciones y programas existentes en el ámbito de explotación, y exigir que junto con el traspaso de un módulo nuevo o modificado a explotación, se envíe la documentación correspondiente. De esta forma, se garantizará la actualización de la documentación de las aplicaciones en explotación.

En circunstancias muy puntuales, se procede a alterar la hora y la fecha del sistema, sin que se vea reflejado en los procesos activos. No es recomendable que se utilice de forma habitual, y mucho menos que esté disponible a personas no autorizadas, ya que se alterarían las referencias existentes al momento en que se realizaron ciertas actividades y dificultaría la investigación encaminada a buscar causas u orígenes de problemas.

5.4.3.- SEGURIDAD LÓGICA SOBRE TAREAS DE EXPLOTACIÓN

La planificación de los trabajos en procesos *batch* es una de la labores más importantes del entorno de explotación, y por lo tanto, de las más peligrosas. Por ser una labor tediosa y repetitiva, se tiende a realizarlas con productos software específicos. Deberá incorporarse una planificador automático, de manera que disminuya la carga actual de trabajo de los técnicos de explotación. Deberá realizarse la adquisición de un producto software adecuado o, en su defecto, desarrollar uno que se adapte a la instalación y que cubra las necesidades actuales.

La planificación deberá conllevar la comprobación a posteriori de la realización de todos los trabajos planificados, y de su correcta planificación, por parte de los técnicos que realicen la labor de supervisión. Para ello, es de gran utilidad la revisión exhaustiva del *log* de actividad, donde queda constancia de aquellos trabajos procesados, y si han finalizado correctamente, además se puede comprobar si se ha repetido indebidamente algún proceso. Es por ello que el log debe tener un período de retención alto, de manera que en cualquier momento se pueda acudir a él para localizar una situación concreta, o la causa de un error manifestado con cierto retraso.

Aunque las tareas planificadas suponen la mayor parte de la carga de explotación, existen las solicitudes de trabajos que no figuran en dicha planificación. Deberá existir un procedimiento y unas normas de obligatorio cumplimiento. Dicho procedimiento deberá instrumentalizarse con un documenta adecuado, para que el usuario deje constancia por escrito de la solicitud, de la

fecha, de la firma autorizada y una breve descripción del proceso a realizar. Toda solicitud que no se ciña a lo establecido, deberá ser rechazada en explotación.

Por otro lado, deberá existir una supervisión directa y un seguimiento de toda labor que realicen los operadores, ya que están utilizando datos reales, de forma que no pueden lanzar cadenas o trabajos impunemente, salvo los planificados o solicitados.

Deberán existir unos técnicos en el área de explotación cuya misión específica sea la recepción de aplicaciones, programas y procesos del área de desarrollo. Serán, por lo tanto, los responsables de mantener un inventario completo de los programas en explotación, siendo estos técnicos los únicos con acceso a modificaciones o borrado de módulos de explotación.

Dependiendo del volumen de trabajo, estos técnicos estarán dedicados a esta labor de manera exclusiva o no, repartiendo su tiempo con otras tareas de explotación.

Para solicitar la incorporación de una nueva versión de una aplicación o programa, deberá existir un documento desde el área de desarrollo, especificando el módulo, la librería, descripción, fecha y firma del solicitante, adjuntando las pruebas realizadas.

Deberá crearse una normativa para la codificación de nombres, tanto de programas como de jobs, que los identifiquen claramente y les asigne una aplicación sin necesidad de recurrir a diccionarios o documentación anexa.

Deberá llevarse un libro de incidencias, en el cual, el operador refleje todo tipo de incidencias y las causas que las provocaron, así como las acciones correctoras en cada caso. De esta forma, además de un registro adecuado de los hechos acontecidos, se poseerá un manual al cual recurrir en caso de que se presenten situaciones repetidas, Posteriormente, pueden realizarse estudio en base a las incidencias y elaborar estadísticas concretas.

A continuación se exponen las tareas que se recomienda seguir:

- *planificación de la carga diaria*: consiste en la determinación, preparación y adecuación de los procesos diarios, de los trabajos a ejecutar. Para esta tarea el planificador/preparador se apoya en la información contenida en el manual de explotación.
- *manipulación de discos, cintas o cartuchos*: Por un lado, el planificador define y prepara, desde el día anterior, los soportes físicos a manipular, y por otra, los operadores manipulan en el momento de ejecución de las cadenas, dichos soportes. Para ello, ambos deben tener conocimiento de los flujos de los procesos, así como de las vigencia de las distintas versiones de los ficheros, información contenida en los documentos de descripción de procesos y ficheros.
- *desencadenamiento de procesos*: esta tarea consiste en el lanzamiento de los distintos trabajos, de acuerdo con la planificación elaborada previamente.
- *tareas de recuperación y reinicio del sistema:* durante las ejecuciones de los trabajos puede existir incidencias que obliguen a tomar determinadas acciones por parte del personal de operación, a dichas incidencias

corresponden unos procedimientos de recuperación y rearranque que estarán plasmados en la correspondiente documentación del sistema.

- *procedimientos de emergencia:* en la explotación de sistemas pueden darse situaciones en las que, debido a causas externas al sistema, no se disponga de la funcionalidad completa. En este tipo de situaciones los procedimientos de emergencia contemplan los pasos que deben ser dados si el sistema va a estar indisponible total o parcialmente por un tiempo.
- *comprobación de ejecuciones*: mediante esta tarea el personal de explotación verifica la correcta ejecución de los trabajos procesados. Los puntos de control necesarios deberán estar documentados.
- *control de entrega de informes*: sirviéndose de la documentación del sistema preparada a tal efecto, el planificador realiza las comprobaciones pertinentes para asegurar la correcta edición y distribución de todos los informes previstos.
- *mantenimiento de históricos y copias de seguridad*: mediante esta tarea el personal de explotación asegura la correcta realización de las copias de seguridad, así como la elaboración de históricos, de acuerdos con los requerimientos del sistema, descritos en la documentación del mismo.

5.5.- CONTROL SOBRE EL DESARROLLO Y MANTENIMIENTO DE APLICACIONES

5.5.1.- ESTUDIOS DE VIABILIDAD

Desde el primer momento en que se concibe el abordar un nuevo proyecto de desarrollo, debe procederse a seguir los procedimientos que marcan todos los desarrollos de sistemas.

Lo primero a tener en cuenta, es la realización de un estudio formal de viabilidad, que contemple en detalle todas las circunstancias que rodean a la concepción, desarrollo e implantación del proyecto, ya sean favorables o desfavorables, ponderándolos adecuadamente. Asimismo, se debe realizar un análisis de costes y beneficios que incidirán durante la realización completa del proyecto, obteniéndose información para poder decidir la conveniencia o no de abordar el desarrollo, y en qué términos.

Por tanto, en el área de Desarrollo de aplicaciones deben realizarse estudios de viabilidad, análisis de costes y beneficios, previos a abordar cualquier proyecto.

Dichos estudios deben establecer las necesidades de recursos humanos e informáticos, e incluirse dentro de los planes del área correspondiente, con la prioridad adecuada a su urgencia.

En todo estudio se produce una investigación preliminar compuesta por tres aspectos fundamentales:

- *Aspecto Técnico*: Determinar si se dispone de equipo de trabajo y de tecnología para realizarlo
- *Aspecto Económico:* Determinar los costes y los beneficios del nuevo sistema.
- *Aspecto Operacional:* Determinar la utilidad del sistema por los usuarios, y la factibilidad del proyecto.

El aspecto fundamental es comprender todas las facetas del sistema que se encuentra bajo estudio. En definitiva, es necesario que se determinen los requerimientos del nuevo sistema. Para ello, se debe realizar una investigación para obtener información, que muchas veces requiere el estudio de documentos y la visión de condiciones reales en la actividad diaria.

Conforme se reúnen los detalles, se deben estudiar los datos sobre requerimientos con la finalidad de identificar las características que ha de tener el nuevo sistema.

El estudio de viabilidad debe realizarlo un equipo de técnicos que sean expertos en procesos de análisis y diseño de sistemas.

Entre los resultados de los estudios realizados, resultan proyectos no factibles y proyectos viables. Estos últimos, en función de las prioridades, pueden atenderse inmediatamente o incorporarse a los planes ya planificados, decidiendo el orden en que debiera llevarse a cabo.

Por otra parte, y dentro del entorno de desarrollo, se recomienda que, en aquellas circunstancias en que se plantee la posibilidad de adquirir un producto software a una de las empresas que suministran paquetes a clientes, se realice un estudio completo de las posibilidades que ofrece el mercado. Se deberá elegir una serie de productos que se ciñan a las necesidades manifestadas. De estos posibles candidatos a ser adquiridos, se realizará un estudio comparativo, y en detalle, de manera que una vez finalizado este estudio, se pueda establecer una clasificación de dichos productos antes de decidirse a incorporar uno en concreto. A continuación, se deberá solicitar la demostración de los productos que más se adapten a las necesidades, y de todo ello, deducir cuál puede ser el más idóneo para el caso concreto que se propone.

Por tanto, se recomienda que en futuras adquisiciones se analicen las características propias de los productos que puedan cubrir las necesidades planteadas, dando importancia a la posibilidad de que dichas necesidades puedan ser ampliadas, y estén cubiertas, dentro de lo posible, por el software que lo requiera.

Debe realizarse además un estudio comparativo entre los posibles candidatos, con un análisis coste/beneficio adecuado.

5.5.2.- CONTROL DE PROYECTOS

Para la supervisión del proyecto abordado y control de gastos y plazos, debe seguirse un procedimiento de control de trabajos que debe ser uniformemente aplicado a todos los trabajos del Área de Desarrollo y Mantenimiento. Este procedimiento marcará de forma muy concreta, los límites de cada una de las fases de desarrollo, los fines y plazos a cumplir en cada una de ellas, y la persona o personas responsables de que se cumpla.

Dependiendo de la envergadura del proyecto se realizarán controles periódicos, ya sean diarios o semanales, de los tiempos empleados y los fines conseguidos en los períodos de tiempo consumidos.

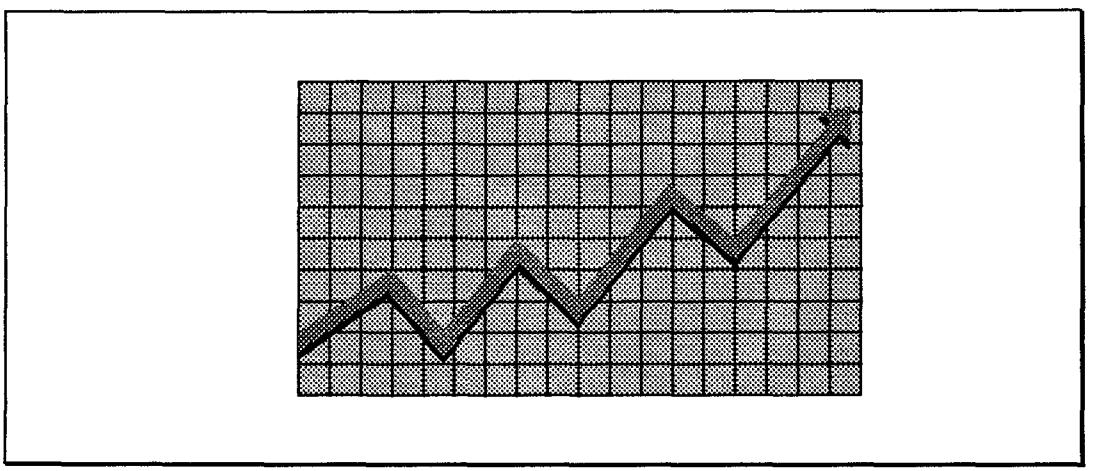
De esta manera, y realizando un control muy exhaustivo de la situación en cada momento, podrán irse corrigiendo las desviaciones o inconvenientes que se produzcan puntualmente, sin esperar al final donde la desviación puede ser considerable, y los inconvenientes pudieran haber causado problemas dificilmente resolubles. Si el problema se detectase demasiado tarde, podría obligar a replantear el desarrollo desde un punto concreto, con la carga accesoria de trabajo que ello ocasionaría. Todo ello incidiría negativamente en el análisis realizado y, por lo tanto, en los plazos a cumplir.

Por tanto, el control y seguimiento de proyectos es fundamental, y debe realizarse de forma continua, en todos los proyectos del Área de Desarrollo y Mantenimiento.

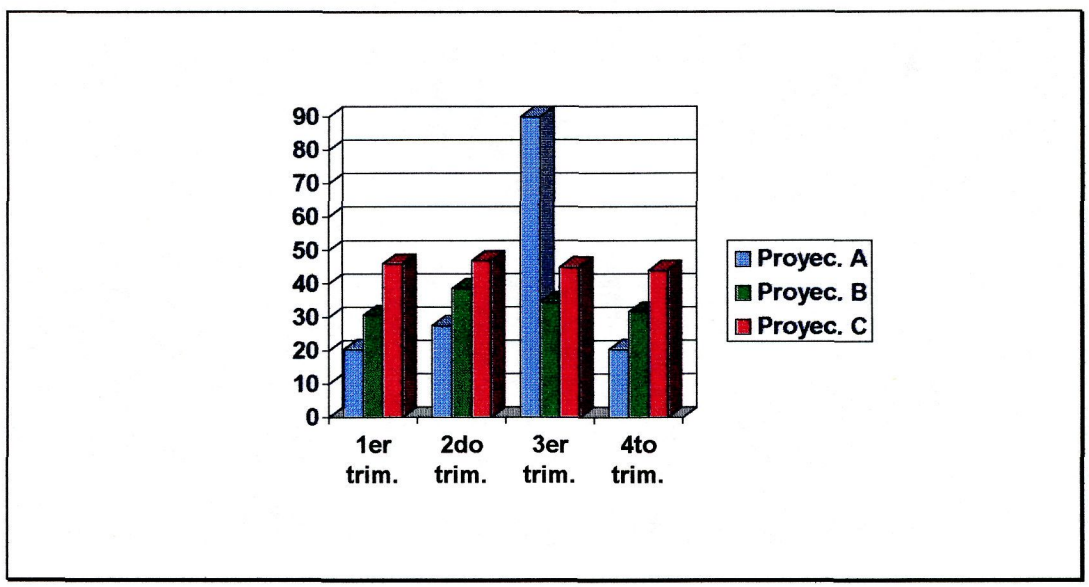
Uno de los aspectos más dificiles del proyecto es la estimación de los tiempos necesarios para el desarrollo de un sistema. Su precisión dependerá de la habilidad, conocimiento y experiencia del técnico encargado de dicha función. Otros aspectos que determinan la estimación del tiempo son la complejidad del mismo y las interrupciones no relacionadas con el proyecto que recaen directamente con el técnico que lo lleva a cabo.

Por tanto, deberá realizarse una planificación de proyectos y de técnicos responsables de los mismos, teniendo en cuenta el control de otros proyectos ya desarrollados, pero de responsabilidad de los técnicos ocupados actualmente.

A pesar de que el método que ofrece un enfoque más concreto a la estimación es el *método estándar*, en el que se identifican y cuantifican individualmente los factores que afectan más drásticamente al tiempo de desarrollo del sistema, el más utilizado en el Área de Desarrollo y Mantenimiento es el *método intuitivo*, basado en la estimación de tiempos en función de la experiencia. Este resulta ser más rápido y conveniente para la obtención de una estimación; aunque ésta .dependerá siempre del técnico que la realice.



Deberá incorporarse una herramienta CASE para el control de los proyectos que se desarrollan en el Área de Desarrollo y Mantenimiento, además se recomienda la utilización de uno de los métodos existentes para planificar el tiempo, por ejemplo el Diagrama de Barras, que resulta ser el más sencillo.



5.5.3.- CONTROL DE DESARROLLO DE APLICACIONES

La adopción de una metodología común para todo el desarrollo plantea varios beneficios:

- la mejora en la calidad del producto informático y en el volumen del desarrollo, al proponer esquemas de análisis muy dinámicos y polivalentes para diferentes áreas

- la mejora en la documentación general de las aplicaciones y en la capacidad de dicha documentación de ser puesta al día, al tiempo que sufren modificaciones los programas que la componen, simplificando igualmente esta tarea y asegurando que las actualizaciones en la documentación son llevadas a cabo

- una evolución mayor y más dinámica de los usuarios en las distintas fases del desarrollo

Este enfoque de beneficio múltiple informática/usuario hace altamente recomendable el unificar dichos criterios metodológicos, ya que se debe considerar único el ámbito de desarrollo de aplicaciones.

Deberá estudiarse la posibilidad de plantear la necesidad de la colaboración directa de los usuarios en el desarrollo de sus aplicaciones, cuando se crea

oportuno. De esta manera, los usuarios desempeñarán funciones de responsabilidad y los técnicos desarrollarán el proyecto en la línea adecuada.

Debe implantarse la utilización del método del *ciclo de vida para desarrollo de sistemas* que incluye las actividades de:

1- Estudio de Viabilidad

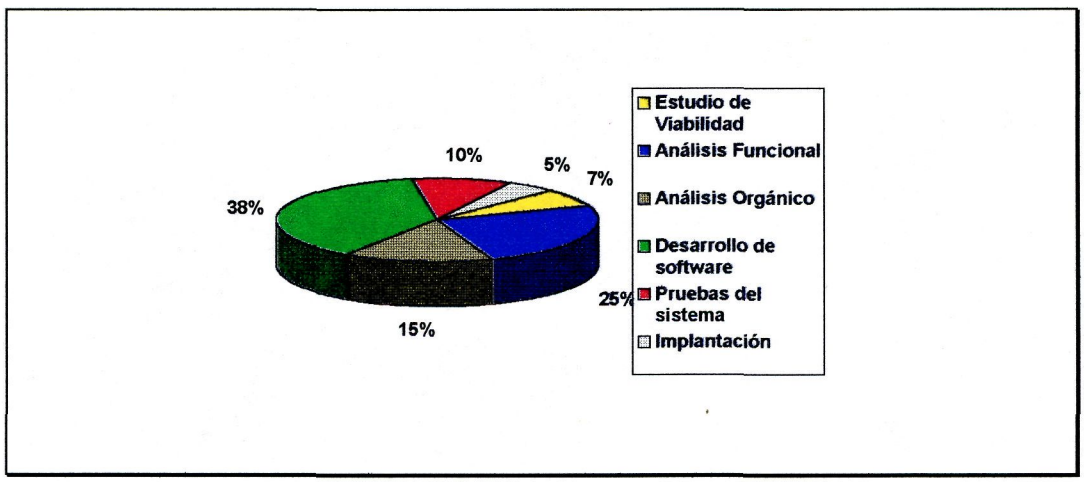
2- Análisis Funcional

3- Análisis Orgánico

4- Desarrollo de software

5- Pruebas del sistema

6- Implantación



En cada una de las etapas del diseño del nuevo sistema se deberán seguir las normas que se desarrollaran por el Área de Desarrollo y Mantenimiento, y que todos los técnicos deberán seguirlas forzosamente.

Dentro de este departamento en donde la información que se maneja es masiva, y su trascendencia sobre el tiempo necesario para la realización de algunas actividades es vital, la existencia de un *diccionario de datos* es fundamental.

El Diccionario de Datos que se utiliza en este C.P.D., es el llamado PREDICT, producto de Software A.G., que permite realizar el almacenamiento clasificado de datos que se necesita, pero que actualmente no se utiliza en toda su amplitud, dejando a un lado, por ejemplo, las Referencias Cruzadas, indispensable para la relación entre los datos y su posterior búsqueda de forma rápida y flexible.

Por tanto, se recomienda la utilización del diccionario de datos existente, pero en todos sus apartados, para poder considerar sus resultados.

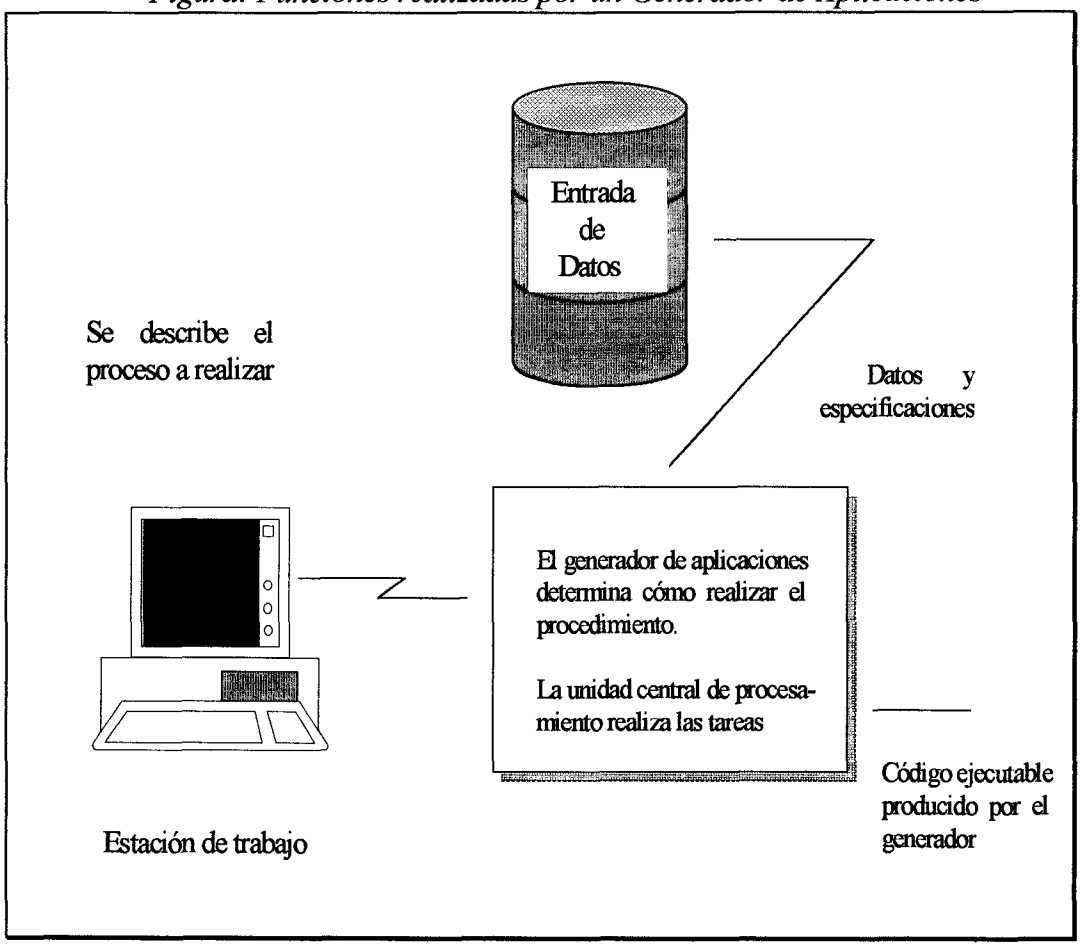
Debe tenerse en cuenta que, en muchas ocasiones, dentro del área a informatizar, todas las actividades se encuentran relacionadas y resulta difícil determinar el orden para efectuarlas. Por tanto, las diversas partes del proyecto pueden encontrarse al mismo tiempo en distintas fases de desarrollo.

Además, puede estudiarse la posibilidad de utilizar Generadores de Aplicaciones, para la realización de ciertos proyectos que sean de menor envergadura, acortando así el tiempo de su desarrollo. Estos generadores proporcionan las condiciones para desarrollar aplicaciones y aportan el código fuente de la misma.

Por otro lado, los generadores de aplicaciones disminuyen el tiempo de desarrollo de un programa, además aseguran una estructura estándar y consistente

para el programa, disminuyendo la concurrencia de algunos errores, con lo cual mejoran la calidad.

Figura: Funciones realizadas por un Generador de Aplicaciones

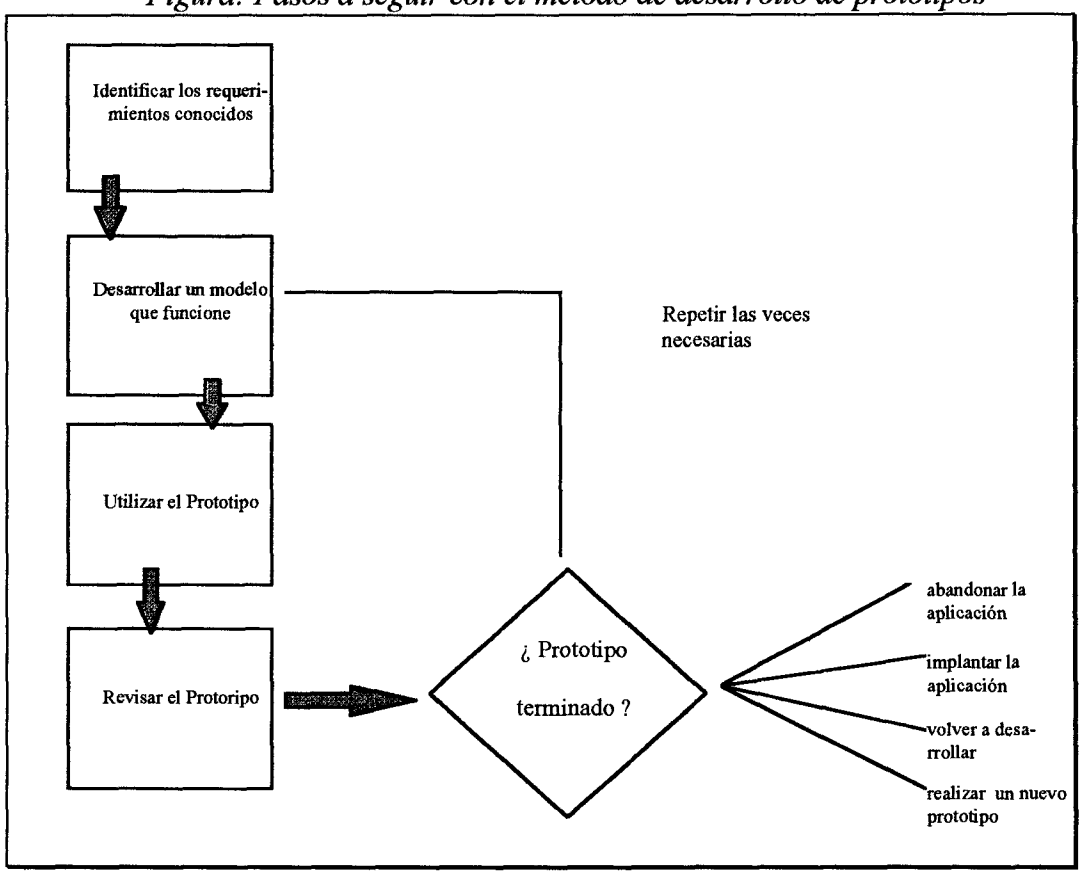


Por otro lado, una manera efectiva para asegurar que las necesidades de los usuarios son los requerimientos encontrados, se recomienda la utilización de *prototipos* al final de cada una de las etapas, para incrementar el nivel de productividad en el desarrollo de sistemas.

Las razones para el uso de prototipos son el resultado directo de la necesidad de desarrollar sistemas de información son rapidez, eficiencia y eficacia, como son el aumento en la productividad, el redesarrollo planificado y el entusiasmo de los usuarios con los prototipos.

Los usuarios pueden señalar con mayor facilidad las características que le agradan o desagradan en un sistema que funciona que en un papel o en un gráfico.

Figura: Pasos a seguir con el método de desarrollo de prototipos



5.5.4.- CONTROL DE EXPLOTACIÓN DE APLICACIONES

Al terminar un nuevo sistema y estar listo para el paso a explotación, es necesario llevar a cabo una serie de tareas, tales como verificar que el nuevo sistema está operativa, eliminar el antiguo, formar a los usuarios, desarrollar el manual de mantenimiento, instalar el sistema en explotación, comprobar el perfil de los usuarios finales que tendrán acceso al mismo, dar de alta los privilegios al nuevo sistema,...

Para el paso a explotación deberá presentarse la siguiente documentación:

- *Inventario de Ficheros:* consiste en una relación de los ficheros que utiliza el sistema, incluyendo una breve descripción del contenido funcional de los mismos.
- *Descripción de Ficheros*: para cada fichero existe un documento en el que se detallan las características del mismo.
- *Inventario de Programas*: consiste en una relación de todos los programas del sistema, con un breve descripción del objetivo de los mismos.
- *Descripción de Programas*: consiste en una información detallada de los objetivos de cada programa, incluyendo el flujo del proceso correspondiente, con los ficheros utilizados y los informes emitidos,..
- *Inventario de Pantallas*: consiste en una relación de todas las pantallas de la aplicación, en el cual se incluye la identificación funcional de las mismas.

- *Descripción de Pantallas*: para cada pantalla de la aplicación se facilita una información que comprende la representación gráfica de la misma.
- *Inventario de Informes*: consiste en una relación de todos los informes emitidos por la aplicación, incluyendo número de copias, destinatarios y perioricidad.
- *Descripción de Informes*: para cada informe existe un documento, que consiste en la representación gráfica del mismo, así como las indicaciones necesarias para su verificación y control.
- *Inventario de Tablas*: consiste en una relación de todas las tablas que contienen datos a utilizar como parámetros de la aplicación.
- *Descripción de Tablas*: para cada tabla se editará un documento con los valores específicos correspondientes a cada parámetro.

Se recomienda que se disminuyan las responsabilidades del personal externo perteneciente a la empresa de servicios en el entorno de explotación hasta llegar a anularlo completamente. Estas tareas deberían ser desempeñadas por personal propio, evitándose los problemas de seguridad, de dependencia externa y otros.

Por otro lado, se deberán mejorar las condiciones de seguridad con respecto al personal externo, en los términos de organización, normativas y procedimientos, y en general, dándoles un tratamiento especial.

Sería aconsejable realizar un control sobre el personal externo de la empresa de servicios que realiza tareas en el entorno de explotación, de modo que se realice un seguimiento de las mismas para garantizar en todo momento la información disponible.

5.5.5.- CONTROL DE MANTENIMIENTO DE APLICACIONES

Debe considerarse la adopción de una normativa que, oficial y comúnmente aceptada por el Área de Desarrollo y Mantenimiento, marque las pautas a seguir en la prueba de programas o aplicaciones.

La adopción de esta norma eliminará los problemas existentes en este ámbito, como son errores de programas en explotación por haberse probado deficientemente, o la utilización de datos reales para las pruebas, con la pérdida de confidencialidad que ello ocasiona.

Esta norma contemplará la creación de modelos completos de ensayo que, para cada programa, estudien todas las posibilidades existentes. Se realizarán a medida de la aplicación, y debido a sus características propias, deberían ser guardados como parte integrante de la documentación.

Los programas deberán ser probados individualmente una primera vez, y luego dentro del marco total de la aplicación, para la comprobación del interface entre dichos programas. Todo ello, previo su traspaso a explotación.

Se recomienda, en cuanto a las pruebas de calidad, que se contemplen cuatro niveles:

- *Prueba:* Ejecutar un programa con la intención de hallar errores
- *Verificación*: Ejecutar un programa en un simulacro para detectar errores
- *Validación*: Uso del software en una ambiente no simulado
- *Certificación*: Garantía del correcto funcionamiento

Las estrategias de prueba se refieren a las pruebas de la lógica del programa y las pruebas de las especificaciones del proceso. En cuanto a los niveles de prueba se deberán realizar pruebas parciales, de carga máxima, de almacenamiento, de procedimientos, y del tiempo de ejecución.

Se recomienda la creación de una librería de prueba con datos desarrollados para realizar las pruebas de la totalidad de un sistema, que por otro lado, deberá conservarse durante toda la vida del sistema, ya que para el mantenimiento posterior también sería de gran utilidad.

Los datos de salida deben de sufrir un proceso de conciliación con los de entrada, no sólo a nivel de trámites generales, sino también a datos concretos, incluso si estos proceden de cálculos. Para ello, podrán realizarse comprobaciones muestrales sobre elementos convenientemente extraídos de la población total.

En el caso de que se produzcan errores, o no corresponda su funcionamiento con el especificado, deberá procederse a una recodificación. Todo estos pasos deben de estar documentados con firmas antes del paso a explotación.

De todo esto, se desprende que debe existir una intensa colaboración entre los departamentos u organismos usuarios y el Área de Desarrollo y Mantenimiento. Esta permanente colaboración debe normalizarse mediante unos procedimientos formalmente establecidos, que determinen responsabilidades y marquen pautas de realización.

Esta colaboración entre usuarios y desarrollo debe empezar en la fase de diseño conceptual y esquemas directores del proyecto, donde ambas partes firmarán los puntos acordados y los plazos a cumplir, fijándose las necesarias reuniones posteriores para que, una vez elaborado el Análisis Funcional, sea conjuntamente discutido, aprobado y firmado. Desde ese momento empieza la fase de elaboración de cuadernos de carga, que darán origen al Análisis Orgánico y su correspondiente codificación.

La colaboración y respaldo de los desarrollos que se aborden, que comienza desde la fase de concepción del diseño preliminar, debe continuar en la fase de análisis, y finalizar en la de pruebas. En todas ellas debe estar implicado directamente el usuario, firmando aquello que se vaya acordando, incluyendo las pruebas.

Una vez finalizada esta fase, existirá una prueba global y conjunta, hecha por el usuario y por el equipo de desarrollo. Una vez realizada, y comprobado que se ciñe a lo descrito, será aprobada y firmada por las dos partes, guardándose el juego de ensayos utilizado, como soporte documental de la aplicación, incluyendo los resultados obtenidos.

De esta forma, se evitarán posibles problemas que surjan a raíz de retrasos en al implantación, o por la no formalización en un documento de las necesidades previamente manifestadas por el usuario.

Toda instalación informática medianamente grande, debe contar con unos trámites de colaboración debidamente reglamentados, obteniéndose con ello un beneficio para ambos interlocutores.

Por otra parte, en cuanto al mantenimiento de programas de aplicaciones en explotación, deberán conservarse las normas referentes al desarrollo de las mismas, además de llevar un control especial para el posterior paso a explotación de la nueva versión del programa, documentando las modificaciones y adjuntando las pruebas realizadas.

Se recomienda que se disminuyan las responsabilidades del personal externo perteneciente a la empresa de servicios de un modo paulativo, incorporando personal propio en la plantilla y proporcionando nuevos desarrollo a los primeros. De esta forma, se controlaría un poco la dependencia que existe actualmente hacia ellos.

Por otro lado, se deberán mejorar las condiciones de seguridad con respecto al personal externo, en los términos de organización, normativas y procedimientos, y en general, dándoles un tratamiento especial.

Sería aconsejable realizar un control sobre el personal externo de la empresa de servicios, de modo que se realice un seguimiento de las tareas que desarrollan, exigiendo un plan de actuación a corto y medio plazo. Además se deberían solicitar unos partes de control que fueran más detallados que los actuales, y un desvío de los proyectos encomendados, con las causas que lo han motivado.

5.6.- CONTROL SOBRE LA OFIMÁTICA Y LA MICROINFORMÁTICA

5.6.1.- NORMATIVA DE EQUIPOS

Es prioritario el crear la definición de la plataforma que se ha de implantar, de los objetivos a corto, medio y largo plazo, funciones específicas y responsabilidades concretas.

Se debe hacer hincapié sobre el apartado de responsabilidades, en el cual debe quedar definido qué organismos y entidades dependen del Área de Microinformática, qué equipos son de responsabilidad departamental y cuáles no.

Deberá crearse toda una normativa sobre procedimientos propios del área, y velar por el cumplimiento de dichos procedimientos, siendo el Área de Microinformática el supervisor de toda la información, a nivel conceptual, que se almacene y produzca en ordenadores personales.

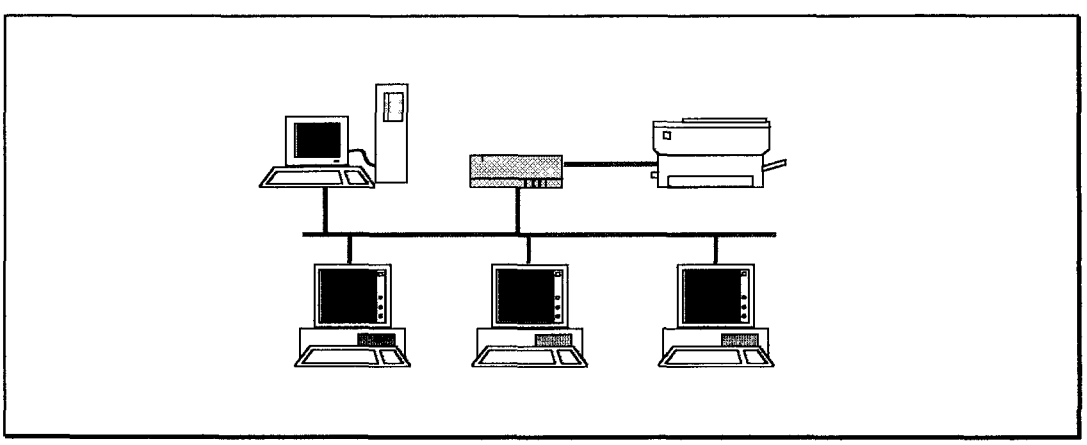
Se recomienda la elaboración del Plan de Contingencias, que de manera formal estudie todo tipo de situaciones planteadas, y medidas de emergencia que debieran tomarse en cada paso para subsanar, en lo posible, los desastres ocasionados por la ocurrencia de la contingencia. En el mismo, deben involucrarse las aplicaciones ofimáticas de alto riesgo en la continuidad operativa.

Mediante cursos de formación se debería crear la mentalización del personal usuario de los sistemas ofimáticos, cumplimentándose con una definición de estándares, los cuales deberán difundirse posteriormente, de manera que se motive al usuario.

Al ser un servicio que englobará los mismos problemas que un clásico centro de proceso de datos, aunque de reducido tamaño, y matizadas características, se plantearán necesidades a cubrir desde un punto de vista de formalismo.

Entre las necesidades a cubrir deben destacarse las siguientes:

- el acceso físico a todos los elementos ofimáticos y su ubicación dentro de oficinas poco adecuadas
- el acceso lógico a ordenadores personales
- normas de confidencialidad de la información
- normas sobre recursos compartidos
- responsabilidad sobre el software
- responsabilidad sobre el material



5.6.2.- SEGURIDAD FÍSICA DE LOS EQUIPOS

Dotar de medidas y normas de seguridad a una instalación informática siempre es difícil, dado que el concepto de seguridad en la informática, data de poco tiempo atrás, y la mayoría de los centros llevan funcionando bastante tiempo, con lo que subyace un problema de comodidad y conservadurismo del estado vigente.

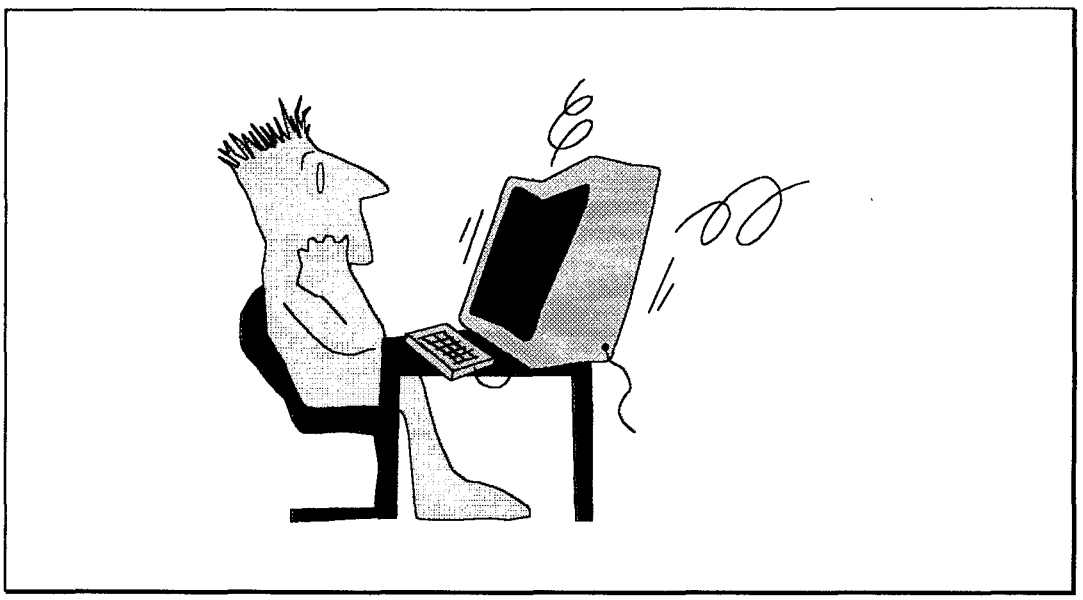
Es por esto que, dado que se esta empezando a concebir la idea de un Área de Microinformática como gestor y responsable de la ofimática en la Consejería de Sanidad, éste puede ser el momento oportuno para ir creando la adecuada mentalidad y responsabilidad en todo el personal involucrado, y simultáneamente ir diseñando normas de seguridad y procedimientos de obligatorio cumplimiento.

Deberán estar contemplados:

- acceso físico a los elementos ofimáticos
- normas de confidencialidad de información
- responsabilidades sobre el material y sobre el software

Se recomienda iniciar un proceso, aprovechando la homogeneidad de productos software, para reemplazar todo paquete existente en la actualidad y adquirido a través de conductos no apropiados, por software adecuado, y con la consabida licencia legal. Se borrarán de modo paulatino, todos los productos así obtenidos, y todos los ficheros que sea posible, para evitar la presencia de virus residentes en ellos, y otras reclamaciones legales que pudieran existir.

Se debe dedicar especial atención a la utilización de productos software adquiridos en los concesionarios oficiales y a través de los trámites legales, de manera que posean la licencia de uso legal de todo producto que exista en la Consejería de Sanidad. Para ello, y ya que existen elementos software que no cumplen estas normas, debe procederse a una supresión o reemplazamiento del software existente por copias legales, evitándose el contagio de *virus informáticos*, así como de otro tipo de problemas, mediante un proceso de borrado paulatino.



5.6.3.- SEGURIDAD LÓGICA DE LA INFORMACIÓN

Es una de las normativas más urgentes de elaboración y de implantación por la importancia inherente de la información que se maneja.

Dicha normativa deberá contemplar tanto las copias de seguridad del software utilizado, como la de la información obtenida o proporcionada fijándose plazos de realización y períodos de vigencia.

Se estudiará la posibilidad de clasifica la información en diferentes niveles de confidencialidad, con las medidas de seguridad propias de cada uno, y la prohibición de que aquella información de más alto nivel de confidencialidad figure en el disco fijo de cualquier ordenador personal.

Por tanto, es urgente elaborar una normativa, dentro del entorno ofimático, sobre las copias de seguridad, dado que la importancia de y confidencialidad de la información así lo precisa. Esta normativa contemplará la obtención de copias de seguridad del software utilizado, de los datos procesados, y de la información obtenida, fijándose un calendario para las mismas, variable según la actividad, y un período de vigencia de cada copia.

Esta normativa además contemplará la ubicación, en lugar seguro, de una copia de seguridad de la totalidad del backup, que será renovada periódicamente. Esta medida puede ser completada con un adecuado estudio sobre los niveles de confidencialidad de la información, de manera que ninguna información con el más

alto nivel, se almacene en el disco fijo de ningún ordenador personal; y una definición de las aplicaciones de alto riesgo en equipos ofimáticos.

5.6.4.- **MANTENIMIENTO DE EQUIPOS**

Teniendo en cuenta la gran cantidad de elementos ofimáticos y la diversidad de los mismos, así como la difusión que están teniendo en el mercado actual, lo que va a provocar la paulativa incorporación de nuevos equipos y productos, se hace necesaria una homogeneización de todo recurso, más aún si tiende a una gestión centralizada desde el Área de Microinformática.

Se recomienda, se tienda a la uniformidad de equipos y productos, tanto de las nuevas adquisiciones como del parque actual existente.

Se recomienda que, dentro de lo posible, a todo nuevo elemento que se incorpore al parque ofimático se le adjunte un contrato de mantenimiento por parte del distribuidor; así como estudiar la posibilidad de realizar contratos de mantenimiento, que incluyan revisiones preventivas para los equipos existentes en la actualidad.

6 - Propuesta de Mejoras del Sistema

6.1.- COMUNICACIONES

Debido a la reciente formación de esta área dentro del C.P.D.se ha visto como la más necesitada de mejoras, por ello se hace más incidencia en la misma.

Se presentan las especificaciones que se consideran para el diseño de una infraestructura de voz, datos y centralización de corriente. Se pretende unificar el diseño de una infraestructura que cumpla con todas las espectativas de la integración, reducción de costes, multifuncionalidad y desarrollo propio de los edificios llamados "inteligentes", con la consiguiente mejora y aprovechamiento de los medios disponibles, que se traducirán a un mejor servicio.

• *Subsistema de cableado horizontal:*

Contempla todos los elementos que se encuentran entre las rosetas y los repartidores de planta (cables) y deberá cumplir:

- las canalizaciones de voz y datos deberán ser independientes a las del tendido eléctrico

- el tendido horizontal desde los armarios repartidores de cada planta será en configuración en estrella.

• *Subsistema de cableado vertical:*

La interconexión entre planta constará de un backbone multipar de cobre con funciones diversas, cables multipar para servicio telefónico y fibra óptica entre los armarios repartidores, para el servicio de datos.

El backbone vertical de cobre estará compuesto por mangueras de pares trenzados FTP y se utilizarán como medio auxiliar para los servicios entre plantas, que no puedan realizarse por fibra. También, como sistema de respaldo en caso de fallo en los subsistemas de transmisión por fibra óptica.

El servicio de telefonía se realizará mediante cables multipares para telefonía, en cantidad suficiente para dar servicio a las extensiones previstas.

El tendido de fibre se realizará con tecnología multimodo.

Estos tres tendidos, se canalizarán por los patinillos interiores de comunicación entre plantas del edificio.

• *Subsistema de Administración de cableado.*

De este subsistema forman parte los armarios repetidores de cableado horizontal y vertical, módulos de conexión, path cords, fuentes de energía eléctrica, etiquetado y presentación de los ponectores, así como la conexión con la centralita de telefónica.

Existirá un cuadro de distribución de cableado por planta. En el caso que, por problemas de espacio, se necesiten múltiples cuadros por planta, estos estarán juntos fisicamente e interconectados de manera que no disminuyan las prestaciones de operación y mantenimiento con ellos.

Toda la conectividad presentada en los cuadros de distribución de cableado, se realizará con conectores RJ-49 y RJ-45 (excepto las correspondientes a fibra óptica).

En cada armario, los servidores de cableado dentro del cuadro de distribución sean identificables.

Se incluíran las batería de enchufes, con sus protecciones correspondientes, precisas para dar servicio a todas las necesidades de energía de los equipos.

Cada regsiro dispondrá de los siguientes servicios mínimos, que serán fácilmente distinguibles:

- 2 tomas para servicio de voz y datos con conector RJ-49
- 2 enchufes de corriente de red directa con toma de tierra
- 2 enchufes de corriente de UPS con toma de tierra

magnetotérmicos de protección

- *HARDWARE Y SOFTWARE DE RED*

Este apartado se compone de los equipos concentradores de cableado, equipos de internetworking, software de gestión de red, que irán empotrados en los armarios distribuidores de cableado, y los adaptadores de red para los ordenadores necesarios para la puesta en explotación de los puntos de red existentes.

En cada armario existirá un concentrador, bien moduldor o stand alone, según las necesidades. Los puestos de cada concentrador serán RJ-49.

En el caso de existir portadores de fibra, en el armario principal deberá incluirse un módulo de puertas de FO con interfaces ST para la exploración de los portadores de fibra. Así mismo, deberán contemplarse los transceptores de fibra para los armarios secundarios.

El sistema de gestión de red deberá dar solución a las necesidades de gestión de fallos, funcionamiento, configuración, seguridad y administración. Cumplirá el estándar SNMP.

Las tarjetas adptadoras de red deberán cumplir las siguientes especificaciones:

- interface de red IEEE 802.3, 10 BaseT, CSMA/CD 10Mbps
- bus ISA de 16 bits
- salidas AUI y par trenzado RJ-49
- latiguillos de 3 mt con conectores RJ-49
- software de diagnóstico y drivers

- *Centralización de corriente y unidad de alimentación ininterrumpida*

Cada puesto dispondrá de tomas de corriente directa y tomas de corriente filtrada a través de un equipo UPS.

Los canalizadores deberán ser independientes de los correspondientes a su voz y datos.

En el caso de existir zonas de distribución extensas, cada planta tendrá su cuadro eléctrico de alimentación con:

- entrada al cuadro será trifásica
- cada una de las salidas monofásicas
- magnetotérmico y diferencial para el cuadro eléctrico
- se incluirán pilotos de señalización para la entrada y para las salidas

El sistema UPS alimentará a los siguientes elementos:

- cada uno de los puestos de trabajo
- centralita telefónica y sus subsistemas
- hardware de red
- equipos de comunicaciones

Deberá tener las siguentes características:

- alimentación trifásica o monofásica según la potencia requerida
- sistema de alarma y diagnóstico

- en el caso de existir un grupo electrógeno de alimentación, se deberá solucionar su conexión a el sistema UPS y su cuadro de maniobra deberá dimensionarse para dar servicio eficaz al sistema informático.

- *Subsistema de Tierra*

Deberá cumplir las especificaciones del Reglamento Electrotécnico de Baja Tensión para instalaciones de tipo informático. En todo caso deberá ser inferior a 3 ohmios.

Deberà existir un sumidero para el mantenimiento constante de la calidad de dicha Tierra.

- *Subsistema de seguridad*

Los sistemas de aire acondidionado serán independientes del general del edificio. Se tendrá en cuenta las condiciones de humedad y ventilación óptimas en la sala. La temperatura para las máquinas de la sala en ningún caso será menor de 20 grados centígrados.

En el caso de existir un equipo UPS de alta potencia, en la sala destinada a dicho equipo existirtá un sistema de ventilación auxiliar de seguridad.

- botella extintor de gas halón en las salas destinadas a equipos informáticos
- alumbrado e indicadores de emergencia según normativa vigente
- cuadros de alarmas por incendio o exceso de temperatura

6.2.- SOFTWARE

Para el buen funcionamiento del *Hardware Central* se recomienda la contratación de las siguientes licencias:

- **PSF, OGL/370, PPFA/370 y GGDM**. Productos que permiten la definición de recursos, formularios, overlays y gráficos en la impresora de lata velocidad IBM 3825.

- **Informes de Rendimientos**. Obtiene estadísticas en cada sesión sobre accesos a discos, consumo de CPU,...

- **ISPF V3.** Este programa permite la creación de pantallas basadas en menús de pantalla completa. Es un instrumento básico para el desarrollo de aplicaciones de Sistemas.

- **ISPF/PDF**: Herramienta de desarrollo de aplicaiones que permite realizar llamadas al sistema desde la programación ISPF.

Para un buen desarrollo de los Proyectos encomendados se debería realizar la adquisición de los siguientes productos:

- **Herramienta de Control de Proyectos**: Destinado no sólo a los gestores de proyectos profesionales sino también al analista de la aplicación, de modo que le permita realizar seguimiento de sus tareas.

Por ejemplo: **Microsoft Project 4.0**

- **Herramienta para el desarrollo de aplicaciones del tipo cliente/servidor**: Se hace necesario la utilización de estos productos de programación orientada a objetos para dar soluciones rápidas a temas de ámbito depertamental.

Por ejemplo: **VisualAge** de IBM

- **Herramienta para realizar prototipos de aplicaciones previo el desarrollo**: Es útil para la optimización de aplicaciones en menos tiempo y con el visto beuno del usuario final.

Por ejemplo: **ProtoView**

6.3.- RECURSOS HUMANOS

El equipo de trabajo es fundamental es una estructura de las características de la que se está exaiminando. Los técnicos que trabajan en el C.P.D. son insuficientes para realizar las labores que se dictan.

Por ello, y con la experiencia en la materia en cuestión, se ha llegado a la siguiente propuesta de ampliación de plantilla, a corto plazo, que debería realizarse lo antes posible dada la envergadura de las áreas afectadas.

2 Analistas

1 Gestor de la Base de Datos

2 Programadores Senior

1 Auxiliar administrativo

1 Programador de Sistemas

1 Operador de Sistemas

1 Técnico soporte a usuarios

7 - Balance Comparativo, Grado de Ejecución y Presupuesto

7.1.- DEFINICIÓN DE PRIORIDADES

Se presentan los balances comparativos de las debilidades encontradas y los riesgos asumidos, frente a las acciones correctoras, con una valoración de recomendaciones.

Se muestran a continuación unos baremos que se utilizarán para indicar tanto el *Nivel de Riesgo* como la *Dificultad de Implantación*:

- **A** Alto
- **M** Medio
- **B** Bajo

A continuación, se indica el orden que indicará el *Grado de Ejecución* recomendado:

- **1** Máxima De acción inmediata
- **2** Media Hasta dos años
- **3** Mínima Hasta cuatro años

7.2.- ESQUEMAS COMPARATIVOS

7.2.1. - SEGURIDAD FÍSICA

Debilidades encontradas	Nivel de Riesgo	Acción Correctora	Grado de Ejecución	Dificultad de Implantación
4.1.1- Ubicación del Edificio	A	5.1.1.	1	M
4.1.2- Ubicación del C.P.D.	A	5.1.2.	1	M
4.1.3- Salidas de Emergencia y Planes de Evacuación	M	5.1.3.	2	M
4.1.4- Seguridad en el acceso al Recinto	A	5.1.4.	1	B
4.1.5- Seguridad en el acceso al C.P.D.	A	5.1.5.	1	B
4.1.6- Seguridad del C.P.D.	A	5.1.6.	1	M
4.1.7- Seguridad del Personal Informático	B	5.1.7.	3	B
4.1.8- Seguridad de la Información	A	5.1.8.	2	M

7.2.2. - SEGURIDAD LÓGICA

Debilidades encontradas	Nivel de Riesgo	Acción Correctora	Grado de Ejecución	Dificultad de Implantación
4.2.1- Seguridad Lógica sobre el Sistema	A	5.2.1.	1	M
4.2.2- Seguridad Lógica sobre los Datos	A	5.2.2.	1	M
4.2.3- Seguridad Lógica sobre las Aplicaciones	M	5.2.3.	2	B

7.2.3. - SEGURIDAD EN LAS TELECOMUNICACIONES

Debilidades encontradas	Nivel de Riesgo	Acción Correctora	Grado de Ejecución	Dificultad de Implantación
4.3.1- Seguridad Física	B	5.3.1.	2	M
4.3.2- Seguridad Lógica del Sistema	A	5.3.2.	1	M
4.3.3- Seguridad Lógica de Datos	A	5.3.3.	1	M
4.3.4- Seguridad Lógica de Aplicaciones	M	5.3.4.	2	B

7.2.4. - SEGURIDAD SOBRE LA EXPLOTACIÓN DEL SISTEMA

Debilidades encontradas	Nivel de Riesgo	Acción Correctora	Grado de Ejecución	Dificultad de Implantación
4.4.1- Seguridad Física de Soportes Magnéticos	A	5.4.1.	2	M/A
4.4.2- Seguridad Lógica sobre el Sistema	M	5.4.2.	2	M
4.4.3- Seguridad Lógica sobre Tareas de Explotación	A	5.4.3.	1	B

7.2.5. - CONTROL SOBRE EL DESARROLLO Y MANTENIMIENTO DE APLICACIONES

Debilidades encontradas	Nivel de Riesgo	Acción Correctora	Grado de Ejecución	Dificultad de Implantación
4.5.1- Estudios de Viabilidad	M	5.5.1.	2	M
4.5.2- Control de Proyectos	M	5.5.2.	2	B
4.5.3- Control de Desarrollo de Aplicaciones	B	5.5.3.	2	M
4.5.4- Control de Explotación de Aplicaciones	M	5.5.4.	2	M
4.5.5- Control de Mantenimiento de Aplicaciones	M	5.5.5.	2	M

7.2.6. - CONTROL SOBRE LA OFIMÁTICA Y LA MICROINFORMÁTICA

Debilidades encontradas	Nivel de Riesgo	Acción Correctora	Grado de Ejecución	Dificultad de Implantación
4.6.1- Normativa de Equipos	M	5.6.1.	2	M
4.6.2- Seguridad Física de los Equipos	A	5.6.2.	1	M
4.6.3- Seguridad Lógica de la Información	A	5.6.3.	1	M
4.6.4- Mantenimiento de Equipos	B	5.6.4.	3	B

7.3.- PRESUPUESTO DE LA MEJORA

Concepto	Presupuesto
Seguridad Física :	
- Reubicación de las dependencias y del Personal adscrito	NO CUANTIFICABLE
- Instalación de 2 Puertas de Seguridad con tarjeta	2.600.000
- Contratación de un Auxiliar Administrativo responsable de la documentación que se tramita en el Servicio	1.900.000
Seguridad Lógica :	
- Contratación del Producto ISPF V3	545.370
- Contratación del Producto ISPF / PDF	575.350
- Ampliación de la capacidad de Disco del Ordenador Central (2 GB)	4.500.000
- Contratación de un Administrador de las Bases de Datos	4.600.000
- Creación de una Base de Datos de Prueba por Personal Interno (dependerá de capacidad del Disco)	SIN COSTO ALGUNO
Seguridad en las Telecomunicaciones :	
- Contratación de Producto de Seguridad y Administración de Redes	1.400.000
- Contratación de un Programador de Sistemas	3.500.000

Concepto	Presupuesto
Control sobre la explotación del Sistema :	
- Contratación de Producto PSF, OGL/370, PPFA/370 y GGDM	550.390
- Contratación de Producto de Informes de Rendimientos	445.280
- Contratación de 1 Técnico de Soporte a Usuarios (Las Palmas)	3.200.000
- Contratación de 1 Operador de Sistemas (Las Palmas)	2.100.000
Control sobre el Desarrollo y Mantenimiento de Aplicaciones :	
- Contratación de Herramienta de Control de Proyectos	75.000
- Contratación de Herramienta para el Desarrollo Aplicaciones de tipo Cliente/Servidor	291.000
- Contratación de Herramienta para el Desarrollo Aplicaciones de tipo Cliente/Servidor para Redes	584.000
- Contratación de Herramienta para Prototipos de Aplicaciones	37.500
- Contratación de 2 Analistas de Aplicaciones	8.500.000
- Contratación de 2 Programadores de Aplicaciones Senior	6.400.000
Control sobre la Ofimática y la Microinformática :	
- Contratación de 20 Licencias de B.D. Access	900.000
- Contratación de 190 Ampliaciones de Memoria de PC's (2 MB)	3.800.000
- Realización de Cursos de Formación a todos los usuarios	4.150.000
- Implantación de Normativa sobre uso de Ordenadors Personales (desarrollado por personal interno)	SIN COSTO ALGUNO

Bibliografía

- INSTALACIONES DE SALAS INFORMÁTICAS
  Paraninfo S.A.
  Carlos A. Soriano Calvo / Fernando Navarro García

- SISTEMAS DE EXPLOTACIÓN DE COMPUTADORES
  Paraninfo S.A.
  Crocus

- TELEMÁTICA Y ORDENADORES
  Grupo Editorial Jackson
  G. Saccardi

- ANÁLISIS Y DISEÑO DE SISTEMAS DE INFORMACIÓN
  Editorial Mc. Graw Hill
  James A. Senn

- SISTEMAS DE INFORMACIÓN PARA LA ADMINISTRACIÓN
  Grupo Editorial Iberoamérica
  James A. Senn

- SISTEMAS OPERATIVOS
  Editorial Mc Graw Hill
  J. A. Pérez / E. Alcalde / J. Morera

- TELEINFORMÁTICA
  Editorial Mc. Graw Hill
  Rafael Ale / Fernando Cuellar

- REDES DE ÁREA LOCAL
  Editorial Anaya Multimedial
  Stan Schatt