UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

LA SEGURIDAD EN LOS CENTROS DE COMPUTO DE LOS INSTITUTOS TECNOLOGICOS

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A :

MARTIN F. ESTRADA OCAMPO

DIRECTOR DE TESIS:

ING. LUIS G CORDERO BORBOA

MEXICO, D. F. 1984.

C O N T E N I D O .

I N T R O D U C C I O N

I.- HISTORIA DE LOS INSTITUTOS TECNOLOGICOS.

II.- LOS CENTROS DE COMPUTO EN LOS INSTITUTOS TECNOLOGICOS

III.- ORGANIZACION DE LOS CENTROS DE COMPUTO.

IV.- LA SEGURIDAD DEL CENTRO DE COMPUTO.

V.- LA PROTECCION DE DATOS.

VI.- PREVENCION DE INCENDIOS.

C O N C L U S I O N E S .

BIBLIOGRAFIA.

I N T R O D U C C I O N

La p[illegible] Centro de Cómputo en lo referente al --- Hardware, Software, Equipos auxiliares y Edificios de diversos factores de riesgo tanto internos como externos cuya identificación, valoración y diseño de medidas de seguridad constituyen una labor muy compleja pero sumamente necesaria.

Por lo anteriormente expuesto, este trabajo presenta una serie de reglas y normas que considero deben observarse para el diseño de un sistema de seguridad simple; que a la vez servirá de base para el diseño de un sistema de protección más complejo, el cual deberá estar sujeto a una contínua actualización, para una correcta protección de los Equipos y sistemas de información que se manejan en el Centro de Cómputo.

El presente, se encuentra orientado, hacia los Centros de Cómputo de los Institutos Tecnológicos, buscando que en un momento determinado el Estudio sea llevado a la práctica.

En lo referente a su estructura este trabajo consta de --- seis capítulos, el primero trata de la Génesis del Sistema Nacional de Institutos Tecnológicos; el Segundo hace referencia a la ubicación de los Centros de Cómputo existentes en el Sistema de Institutos Tecnológicos.

El Tercer Capítulo trata sobre la Organización de un Cen--

tro de Cómputo aplicado en la Industria pequeña, la que podría ser utilizada para la Organización de los Centros de Cómputo de los Institutos Tecnológicos.

En los últimos tres Capítulos se hace referencia a diversas Normas y Reglas que deben observarse para el diseño de un sistema de seguridad base, para el mantenimiento y protección de Equipos y Sistemas de Información del Centro de Cómputo.

C A P I T U L O I

H I S T O R I A D E L O S I N S T I T U T O S T E C N O L O G I C O S .

El Desarrollo del Sistema Nacional de Institutos Tecnólogicos Regionales puede quedar limitado con la relativa facilidad de toda división Histórica, en cuatro etapas que son las siguientes:

1.- Primera Etapa que se le conoce como la de GENESIS del Sistema y comprende del año de 1948 a 1958,

2.- Segunda Etapa llamada de EXPANSION que inicia a mediados de 1959 y termina a inicios de 1976.

3.- Tercera Etapa o de TRANSICION que comprende de 1976 y finaliza a principios de 1977.

4.- Cuarta Etapa se empieza, la CONSOLIDACION del Sistema e inicia a partir de 1977.

La Etapa correspondiente a la Génesis; se inicia cuando se fundan los Institutos Tecnológicos Regionales de Durango y Chihuahua, a los que se les considera como los Pioneros del Sistema, fueron establecidos en 1948 como Dependencia Foráneas del Instituto Politécnico Nacional, quedando enmarcados en las corrientes Filosóficas de Educación Popular, para la capacitación de Material Humano, en calidad y cantidad suficiente, de acuerdo a las características de la Región donde se establecieran.

A finales de 1959, se fundaron siete Institutos los que --

atendieron preferentemente los Ciclos de Prevocacional, Vocacional, así como la impartición de cursos orientados a Programas de Capacitación para el Trabajo.

Su creación fué fundamentalmente como apoyo a la Política de Descentralización y Desconcentración de la Educacion Técnica; esto es, de ofrecer iguales oportunidades de Educación Tecnológica a jóvenes estudiantes de los demás Estados de la República, a la que solo tenían acceso los Alumnos del Instituto Politécnico Nacional.

En los albores de 1959, se da un gran impulso al desarrollo de Institutos Tecnológicos en los Estados, es cuando se inicia la etapa conocida como la EXPANSION.

Esto se origina como resultado de la Reestructuración de los Servicios Nacionales de Educación Tecnológica, cuando los Institutos Tecnológicos dejan de pertenecer al Instituto Politécnico Nacional para integrarse a la Dirección General de Enseñanzas Tecnológicas, Industriales y Comerciales, con Dependencia inmediata a la Subsecretaría de Educación Técnica Superior.

En el año de 1960, se configura la Enseñanza Superior, iniciándose la Carrera de Ingeniero Industrial que es la distintiva del Sistema.

Esto viene a dar apoyo para el posterior fortalecimiento -

de la Enseñanza Superior dentro de la Educación Tecnológica, a- la vez que segregaban el nivel medio básico y los Programas de Capacitación para el Trabajo.

La etapa del desarrollo Institucional y curricular donde - se fué precisando el concepto de Regionalización, y se fundamentaron las Reformas a los planes de estudio; se incrementaron -- los servicios externos, y se apoyó a la Industria, se desarro-- llan los primeros Programas de Inserción a la Región.

En la Década de los años 70, se contaba con 19 Institutos Tecnológicos Regionales mismos que pasaron a depender de la Dirección General de Educación Superior.

En el sexenio del entonces Presidente de la República Li-- cenciado Luis Echeverría Alvarez (1970-1976), fué cuando los -- Institutos Tecnológicos reciben un fuerte apoyo del Gobierno Federal para su expansión, al fundarse un total de 29 Tecnológi-- cos que sumados a los que funcionaban anteriormente, existen un total de 51 Tecnológicos distribuídos en toda la República. --- (Cuadro I. 1).

Al aplicarse la Reforma Educativa, en el año de 1971, los- Institutos Tecnológicos cimientan; los Planes de Estudio, que - son adaptados al Sistema para fortalecer con ello la imparti--- ción Escolar de los Ciclos Semestrales.

En el año de 1973, se establece el Sistema de Créditos y - una estructura curricular flexible a base de módulos interdisciplinarios, a la vez que se implementaban y validaban nuevas Técnicas de Enseñanza y de Metodologías, reduciéndose con esto la duración de las Carreras de Licenciatura.

Estas reformas propiciaron un incremento y diversificación de las carreras a nivel Técnico, que eran 12 en 1971, y las cuales aumentaron a 34, y las de nivel Superior se incrementaron - de 9 a 54.

En la Tercera Etapa el desarrollo de los Institutos se inicia a mediados de 1976, al establecer los siete Tecnológicos Regionales más recientes; se llega a la determinación que deberán de atender exclusivamente el nivel de Licenciatura.

Tal decisión, junto con el establecimiento en este mismo - año del Centro Interdisciplinario de Investigación y Docencia - en la Educación Técnica (CIIDET), y la iniciación de las Maestrías en los que posteriormente se les conocerían como Centros Regionales de Estudios de Graduados de Investigación Tecnológica (C.R.E.G.I.T.), promoviera la elevación del nivel Educativo, en el Sistema de Institutos Tecnológicos.

El C.I.I.D.E.T., es el Primer Centro de Especialización -- que se crea en el Sistema de Tecnológicos, y el cual es asociado al Instituto Tecnológico de Querétaro, y responde a la nece-

sidad de capacitar a los Profesionales, que desempeñan la docencia en la Licenciatura y Maestría y desarrollan a la vez, la investigación educativa en este Campo, a fín de crear las Tecnologías requeridas por los Institutos Tecnológicos; para una eficaz enseñanza en las áreas que les competen.

Por otra parte, el hecho de que en cada uno de los Estados de la República ya existían por lo menos un Instituto Tecnológico, contribuye a la conceptualización del conjunto de éstas Instituciones; como un Complejo Nacional de Educación Tecnológica Superior, unificando a través de sus objetivos y de su administración, se le ha reconocido con la denominación de Sistema Nacional de Institutos Tecnológicos (SNIT).

El Sistema ofrece educación de acuerdo a los requerimientos de desarrollo o incipiente Industrial que tengan los Estados en donde se establecen, es decir es un promotor de las Políticas Educativas del Gobierno Federal, Políticas que se desprenden del propósito de orientar la Educación para el desarrollo de México.

Esta es la razón, advertida en el periódo de Transición de planear la Educación Superior Tecnológica, en armonía con la Planeación Nacional; así como la de desarrollarla a efecto de fortalecer y estrechar la vinculación de los Institutos Tecnológicos con los Sectores Productivos de bienes y servicios y con la totalidad de Instituciones de Educación Superior, la preci--

sión de los objetivos fijados para los Institutos Tecnológicos, así como la reafirmación de sus modelos curriculares, le ha permitido estar acorde con los lineamientos que emanan de la Política Educativa, tanto a nivel Federal como Estatal.

En 1977, con la reorganización de la Secretaría de Educación Pública, se inicia la etapa de Consolidación al crearse la Dirección General de Institutos Tecnológicos (D.G.I.T.); dependencia creada para la Administración y desarrollo de todos los Institutos Tecnológicos, que existían en toda la República Mexicana.

Es así, como esta Dirección basada en los estudios antes realizados, efectúa una reorganización administrativa del Sistema la cual queda precisada en los organogramas de la Dirección General de Institutos Tecnológicos, así como los correspondientes manuales de operación.

La D.G.I.T., al seguir los lineamientos emanados de la acción Educativa del Sistema, al cumplir con las metas previstas en el Plan de Desarrollo (1977-1982), y respetando los planes Políticos particulares de cada uno de sus Institutos, inicia la creación de siete Centros de Estudios de Graduados e Investigación Tecnológica (C.R.E.G.I.T.), donde se sistematiza las Maestrías en Ciencias, diseñadas tanto para la especialización de los Profesores del Sistema como para la formación de los Técnicos altamente especializados que requiere el Desarrollo Regional.

Para lograr este objetivo, se ha tomado la estrategia de - polarizar deliberadamente recursos, a efecto de elevar los Institutos Tecnológicos más desarrollados, del sistema, a la categoría de Centros de Graduados, al impartirse en ellos Maestrías y Doctorados, para convertirlos en Instituciones especializadas en el Campo de la Tecnología, que se encuentran acordes con el desarrollo Regional donde se localicen en la República Mexicana.

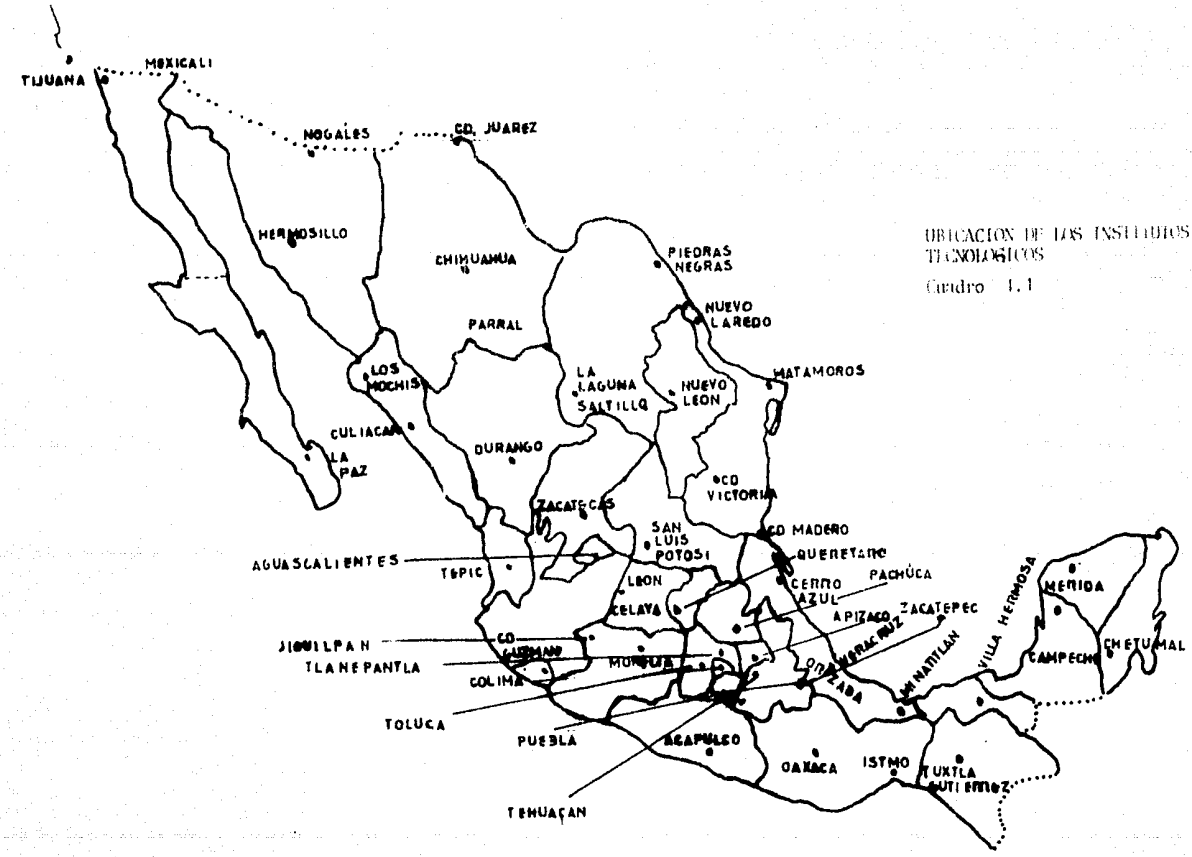
Con el propósito de regular y normar la asignación de Re-- cursos Humanos necesarios para la Administración y Servicios de los Institutos Tecnológicos, se han diseñado algunas matrices - de integración de las cuales han surgido varios Organigramas Tipos, que han servido como guía para conocer las necesidades de Recursos Humanos que tiene algún Instituto según los alumnos -- que atienda independientemente de las Carreras que imparta; en la época de la Expansión del Sistema, se diseñó una matríz orgánica tipo que consta de tres etapas cuadros I.2 (A, B, C, D,), cada una de las cuales consta de Tres Fases, siendo diferente - el número de alumnos para cada Fase y en cada Etapa.

Este es el Primer intento de la D.G.I.T., para que los Institutos Tecnológicos cuenten con una Organización adecuada que rija adecuadamente la administación que se ejerce en cada uno - de ellos.

Ante la necesidad fundamental de darle a los Tecnológicos una estructura Organizacional firme, se toma la desición de --- adaptar un manual de organización tipo, al cual deben atender -

todos los Institutos de acuerdo a su propio grado de desarrollo, esto se fundamenta en el conjunto de experiencias obtenidas por el ejercicio de las funciones realizadas en cuanto a Docencia, Investigación, Administración y Extensión circunscritas dentro de las Políticas del Sector Educativo a nivel de Sistema.

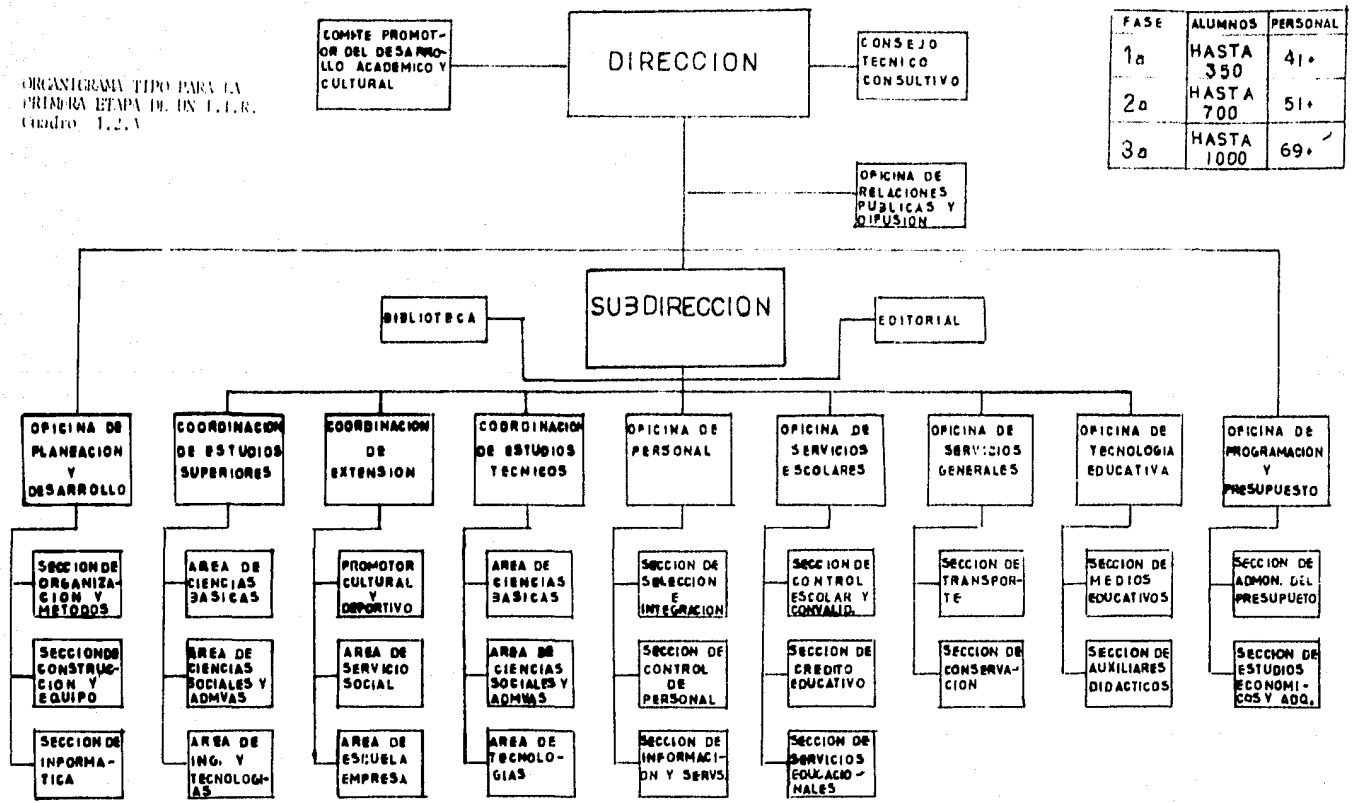
Por lo anterior, en el mes de Agosto de 1982, se establecieron Políticas generales, así como una matríz de integración orgánica, que servirá como apoyo para normar el crecimiento de la Institución Escolar con el propósito de que la Comunidad Estudiantil en sus Diversas Especialidades, logren su meta, de ser buenos Estudiantes y magníficos Profesionistas y contar con una área Administrativa excelente y eficáz que conformará la estructura más idónea de cada Tecnológico del País.



UBICACION DE LOS INSTITUTOS TECNOLOGICOS

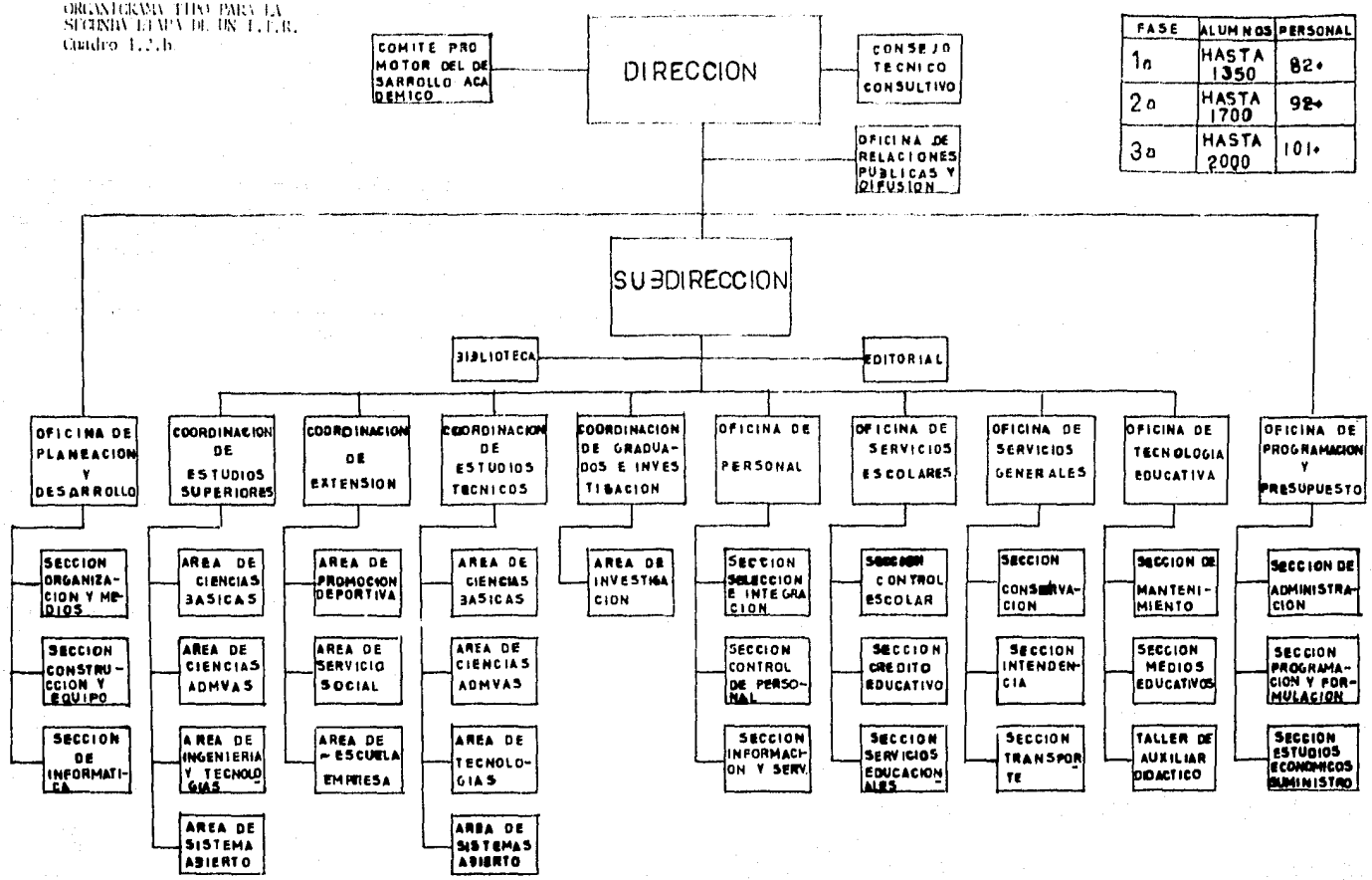
Cuadro 1.1

ORGANIGRAMA TIPO PARA LA PRIMERA ETAPA DE LOS I.T.E.R.
Cuadro I.2.V



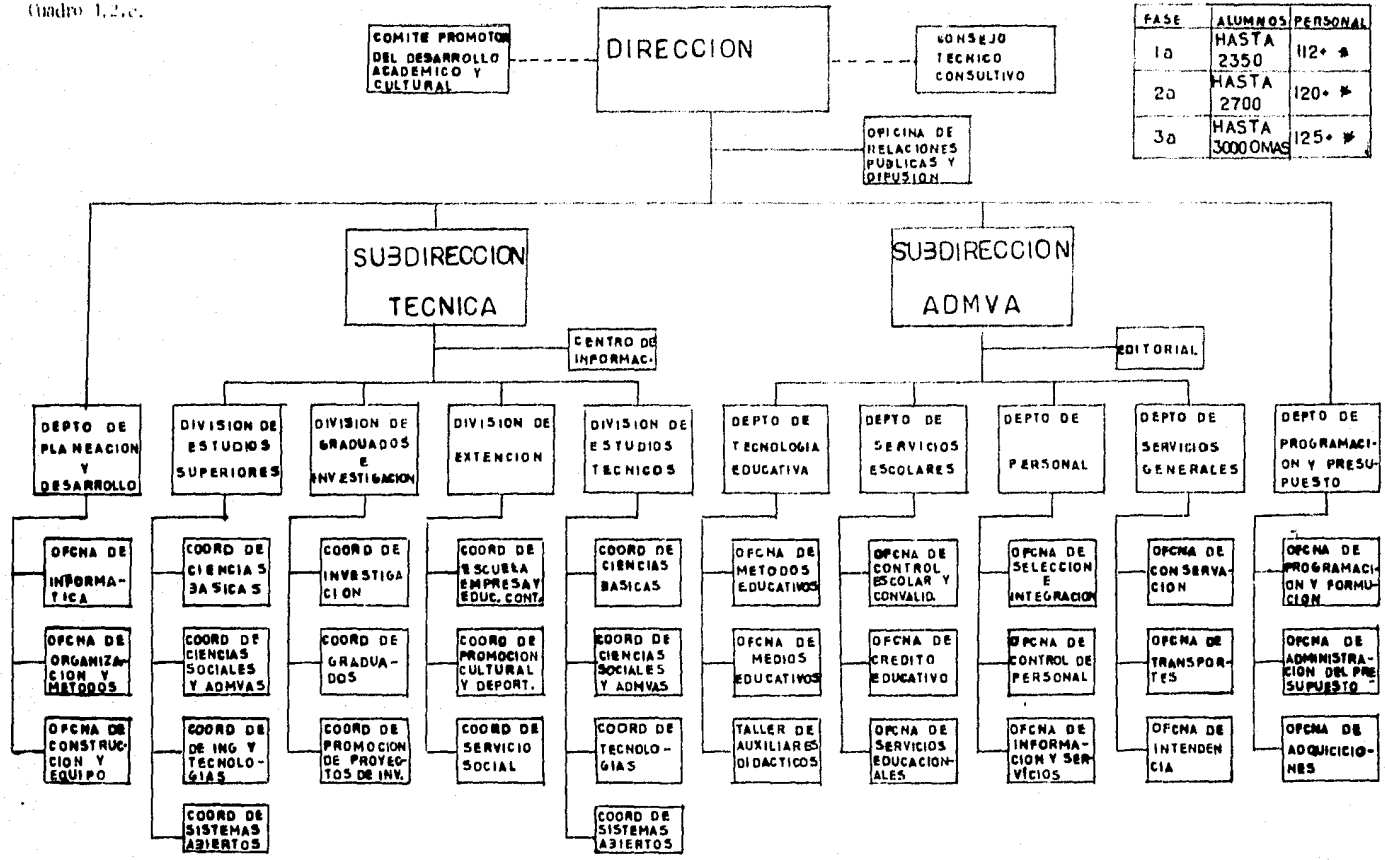
FASE	ALUMNOS	PERSONAL
1a	HASTA 350	41+
2a	HASTA 700	51+
3a	HASTA 1000	69+

ORGANIGRAMA TIPO PARA LA SEGUNDA ETAPA DE UN I.T.R.
Cuadro I.7.b



FASE	ALUMNOS	PERSONAL
1a	HASTA 1350	82+
2a	HASTA 1700	92+
3a	HASTA 2000	101+

ORGANIGRAMA TIPO PARA LA TERCERA ETAPA DE UN I.T.R.
Cuadro 1.2.c.



FASE	ALUMNOS	PERSONAL
1a	HASTA 2350	112+ *
2a	HASTA 2700	120+ *
3a	HASTA 3000 OMAS	125+ *

PUESTO	1 FASE HASTA 350	2 FASE HASTA 700	3 FASE HASTA 1000	1 FASE HASTA 1350	2 FASE HASTA 1700	1 FASE HASTA 2050	1 FASE HASTA 2350	2 FASE HASTA 2700	3 FASE 3000 O MAS
DIRECCION	DIRECTOR 1 SECRETARIA							1 SECRETARIA	
RELACIONES PUBLICAS			1 JEFE DE OFNA 1 SECRETARIA		1 ADJ DIFUSION				
PLANEACION	1 JEFE 1 ORG Y MET	1 CONSTRUCCION Y EQUIPO	1 SECRETARIA 1 ADJUNTO A ORGANIZACION Y METODOS	1 INFORMATICA			1 ADJ INFORMATICA	1 ADJ A CONST Y EQUIPO	
PROGRAMACION Y PRESUPUESTO	1 JEFE 1 EST. ECON Y SUM 1 ADMON DEL PRES	1 ADMON DEL PRESUPUESTO	1 SECRETARIA 1 ALMACEN	1 PROGRAMACION Y FORMULACION 1 ACTIVO FIJO		1 SECRETARIA 1 ADJ A EST ECON Y SUM		1 ADJ A PROG 1 ADJ A ADMON 1 ADJ A EST ECON	
SUBDIRECCION ADMINISTRATIVA	1 SUBDIRECTOR 4 SECRETARIAS 1 EDITORIAL	1 EDITORIAL	1 SECRETARIA	2 EDITORIAL		1 EDITORIAL		1 EDITORIAL	
SUDIRECCION TECNICA	2 BIBLIOTECA		2 BIBLIOTECA		1 BIBLIOTECA		1 SUBDIRECCION 1 SECRETARIA	BIBLIOTECA	
ESTUDIOS SUPERIORES	1 JEFE 1 CIENCIAS BASIC 1 TECNOLOGIAS	1 JEFE DE TALLER O LABORATORIO		1 JEFE DE TALLER O LABORATORIO	1 RESP DE AREAS 2 SECRETARIA	1 SISTEMAS ABIERTOS		1 SECRETARIA 1 ADJ SIST ABIERTOS RESP DE AREA	RESP DE AREAS ASESORES DE SISTEMAS ABIERTOS
ESTUDIOS TECNICOS		1 JEFE 1 CIENCIAS BASICAS 1 TALLER O LAB	1 CIENCIAS SOCIALES Y ADMVAS 1 SECRETARIA	1 JEFE DE TALLER O LABORATORIO		1 SISTEMAS ABIERTOS		SECRETARIAS 1 ADJ A SISTEMAS ABIERTOS RESP DE AREAS	RESP DE AREAS ASESORES DE SISTEMAS ABIERTOS
GRADUADOS E INVESTIGACION					1 JEFE 1 COORDINADOR DE INVESTIG. 1 SECRETARIA			ADJUNTO DE POSTGRADO INVESTIGADORES	ADJ INVESTIGACION INVESTIGADORES 1 PROM PROY INVMD
TECNOLOGIA EDUCATIVA	1 JEFE 1 ASESORIA EDUC 1 AUXILIAR DIDAC 1 INVESTIGADOR	1 ASESORES ACADEMICOS 1 DIBUJANTE	1 ADJUNTO A METODOS 1 SECRETARIA	1 DIBUJANTE 1 OR VOC Y PROF	1 AUDIOVISUAL	1 DIBUJANTE 1 ADJ A MEDIOS	1 AUDIOVISUAL ADJUNTO A METODOS	ADJUNTO A MEDIOS	
EXTENSION	1 JEFE 1 PROMOTOR DEP 1 PROMOTOR CULT		1 SECRETARIA 1 ESC EMPRESA 1 SERV SOCIAL			1 SECRETARIA	EDUCACION CONTINUA		
PERSONAL	1 JEFE 1 SELECC. E INT 2 AUX DE CONTROL		1 SECRETARIA 1 ADJUNTO A CONTROL ESC				AUX DE CONTROL		
SERVICIOS ESCOLARES	1 JEFE 1 CONTROL ESC 1 SERV MEDICOS		1 SECRETARIA 1 ADJ A CONT. ESC.	1 BECAS	1 ADJ A CONTROL ESCOLAR	1 CONT ESC Y CONVL	1 ADJ CONT ESC 1 ADJ FINANDE EST		
SERVICIOS GENERALES	1 JEFE 4 DE INTENDENCIA 1 DE ALMACEN 1 OPERADOR	1 JARDINERO 2 INTENDENCIA		2 MANT Y TRANS	1 JARDINERO 1 INTENDENCIA	INTENDENTES	INTENDENTES 1 TECNICO EN SEC 1 MANTENIMIENTO 1 OPERADOR	JARDINERO 1 INTENDENTE	INTENDENTE 1 MANTENIMIENTO 1 OPERADOR
NUMERO DE PERSONAS	41	10	18	13	10	9	11	8	9
		69			32			24	

CAPITULO II

LOS CENTROS DE COMPUTO EN LOS INSTITUTOS TECNOLOGICOS

Desde el inicio de nuestra era el hombre ha tenido la necesidad de ampliar cada vez más sus conocimientos los que a la -- postre han traído cambios muy significativos en su forma de vida, esto, lo podemos constatar con la Primera Revolución Industrial a mediados del Siglo XVIII donde se produce una masiva -- aparición de inventos como son: La fundición del coque, Máquinas Segadoras, Trilladoras y de Coser, Vehículos de Vapor que - se aplican al Ferrocarril como substitución de la Diligencia, y en el Barco de vapor que entra en el lugar del de velas, el telar mecánico con lazadera automático que desplaza a rueda y la rueca, así como el telar de Jacquard antecedente de la automatización, ya que empleaba un programa de tarjetas perforadas.

Es así,como van evolucionando cada vez más los conocimientos del hombre y vuelve a entrar a otra etapa importante para - su desarrollo como es la segunda Revolución Industrial que surge a fines del Siglo XIX y principios del XX, es en esta época cuando se introduce la energía eléctrica a todas y cada una de las actividades que desempeñó el hombre desde su casa habitación hasta en las Industrias donde labora, así como en el transporte que viene siendo un factor importante para la difusión de los conocimientos del hombre al tener la facilidad de intercambiarlos con otros Países.

La Tercera Revolución Industrial aparece en el año de 1950, y su desarrollo se genera en un tiempo relativamente corto, --- puesto que bastan diez años para lograr una evolución muy avan-

cada, y es en este lapso de tiempo cuando el hombre se introduce a la era atómica, a la utilización de los plásticos y al desarrollo de la informática.

Es precisamente ésta última la que da a la Tercera Revolución su connotación más específica, pues no es solo un avance en el conocimiento científico, es sobre todo la difusión que el hombre puede hacer de él mismo de tal manera que los anteriores conceptos de comunicación han sido desbordados en gran márgen con la inclusión de la informática, que permite combinar en mil formas distintas sus recursos en una red de comunicación por medio de una o varias Computadoras.

En la actualidad la Computadora interviene en casi todos los aspectos de la vida cotidiana del hombre, por medio de sus recibos telefónicos, Cheques, Multas, etc., pero estas aplicaciones son las más sencillas que éstas pueden desarrollar, por lo que el hombre común no puede enterarse de la importancia que representa la Computadora para el desarrollo del género humano y es por esta razón que se debe dar a los asesores de las Empresas, a los Administradores y Ejecutivo las bases científicas con las que puede aconsejar el uso de los datos y los Archivos.

La ciencia del tratamiento automático de la información representa una etapa decisiva en la historia del conocimiento, ya que mediante la Computadora el hombre puede conservar y guardar el pensamiento humano.

El conocimiento humano ya adquirido no hay que ir repasándolo cada vez que se presente un problema, basta hacerlo en forma simple y sistematizada, cuando se vuelva a presentar aquel, una simple llamada a lo ya establecido evitará una nueva elucubración mental.

Es obvio como la información puede ser accesible en forma más selectiva, debido a que ingentes volúmenes de ella estará a disposición de investigadores, científicos, técnicos y Profesionistas.

Así tenemos las posibles aplicaciones en Medicina que cada vez son más frecuentemente utilizadas, llegándose al extremo de acumular Bancos de datos Mundiales que pueden ser consultados por vía Satélite.

Una tercera tendencia, muy interesante para los Administradores de Empresas, es que estos logren tener mayor facilidad para la toma de soluciones con menores riesgos, mediante el Empleo de Información almacenada; e incluso se pretende que las decisiones estén prácticamente hechas por programas de Computadoras que utilizan la información contenida precisamente en los Bancos de datos, como casos típicos de decisiones preconformadas, se podría hablar de los programas de Computadoras para la producción, los inventarios y la distribución.

De éstos planteamientos podemos deducir que el conocimien-

to científico ha sido incrementado por el hombre en una forma - progresiva, y que todo Administrador de Empresas, y sobre todo el Profesionista tienen la necesidad del uso de instrumentos, - cada vez más necesarios en la vida moderna como lo son las Computadoras.

Actualmente en México la Computación se encuentra presente, en cada una de las actividades económicas y Sociales que se desarrollan en nuestro País, por lo que se hace patente que nuestros Centros de Enseñanza Superior cuenten con este tipo de herramientas, como es la Computadora para que con ello tener Profesionistas capacitados que desarrollen y apliquen la Computación en las ramas productivas del País.

La Universidad Nacional Autónoma de México (U.N.A.M.) es - la primera Universidad o Empresa Latinoamericana que adquiere - un sistema de procesamiento Electrónico de Datos, por el año de 1958.

Es así como la máxima Casa de Estudios del País va a la -- Vanguardia en el desarrollo de la Tecnología y en la aplicación de la misma para el desarrollo de las actividades económicas y docentes.

Entre los años de (1970-1971) la U.N.A.M., apoya la Reu--- nión de varias personas y Catedráticos que habían estudiado ramas de la ciencia muy poco conocidas en México como eran (Esta-

dística, Computación, Teoría de la Probabilidad, Ecuaciones Diferenciales).

Con este hecho se crea el primer Centro de Investigación - orientado a proporcionar servicios de Cómputo a la comunidad -- Universitaria y empezar a realizar investigación autónoma en -- las diversas disciplinas de lo que se llamaría Matemáticas aplicadas, es este el nombre que se le da al centro C.I.M.A.S.S., - (Centro de Investigación en Matemáticas aplicadas Sistemas y -- Servicios), el que posteriormente debido al gran desarrollo, y el beneficio que aportaba a la Institución se divide en una parte de investigación (C.I.M.A.S.) y en otra de servicios (Centro de Servicios de Cómputo), otros Centros que se formaron similares a éste fueron el Centro de Investigación y Estudios avanzados del Instituto Politécnico Nacional.

De esta forma los Centros de Enseñanza más importantes dentro del ámbito Nacional; se actualizan en una rama de la Tecnología muy importantes como es la Informática, lo que viene a -- apoyar la preparación de Recursos Humanos en esta área incipiente en nuestro País.

Por otra parte los Institutos Tecnológicos en virtud del - tipo de Profesionistas que preparan, y del avance de la ciencia y la Tecnología, se crea la necesidad que éstos cuenten con los servicios de procesamiento electrónico de datos, para poder enfrentar la necesidad que tienen los Estudiantes de estas Insti-

tuciones de contar con esta clase de servicios, para que con -- ello coadyuvar un mejor desarrollo de su Profesión al estar actualizado con el avance tecnológico actual.

Es por esta razón que en el año de 1977, se inicia la dotación de éstos equipos de Cómputo a los Institutos Tecnológicos acción que viene a satisfacer con ellos los requerimientos de - contar con este tipo de Tecnología, para con ello, atender las necesidades de las cuatro áreas sustantivas del Sistema de Tecnológicos como son: La Docencia, Investigación, Administración, y Extensión, lo que repercutirá en una elevación en el nivel -- Académico de éstas Instituciones.

Este equipo adquirido se orientó a 13 Institutos que pre-- sentaban una mayor necesidad de contar con este servicio quedando distribuídos de la siguiente manera:

Instituto Tecnológico con PDP 11/34: Aguascalientes, Celaya, Durango, Mérida, Nuevo Laredo y Veracruz. Con PDP 11/40, el Instituto Tecnológico de Tijuana, el de Culiacán con la HP 3000, y con la HP 2000 los Institutos de la Laguna, Morelia, Pachuca, Querétaro, San Luis Potosí.

En Octubre de 1979, la Dirección General de Institutos Tecnológicos presentó un estudio de viabilidad sobre la dotación - de equipo de Cómputo a los Institutos Tecnológicos que no contaban con este servicio. En este estudio se estructura un plan de

5 años, y se incluyen las especificaciones del equipo y el re-- sultado del concurso de proveedores al que se convocó.

El estudio de viabilidad fué aprobado por el Comité Coordinador de Servicios de Cómputo de la Secretaría de Educación Pública en Noviembre de 1979.

En Mayo de 1980, la Dirección General de Política Informática de la Secretaría de Programación y Presupuesto, emitió el Dictámen aprobatorio para el estudio, de los cuales se adquirieron once PDP 11/23 y una PDP 11/34.

Este programa de adquisición ha continuado en la medida de las posibilidades presupuestales, y a la fecha se cuenta con un total de 33 equipos instalados en diferentes Institutos Tecnológicos y de dos equipos instalados en la D.G.I.T., y el otro en el C.I.I.D.E.T.

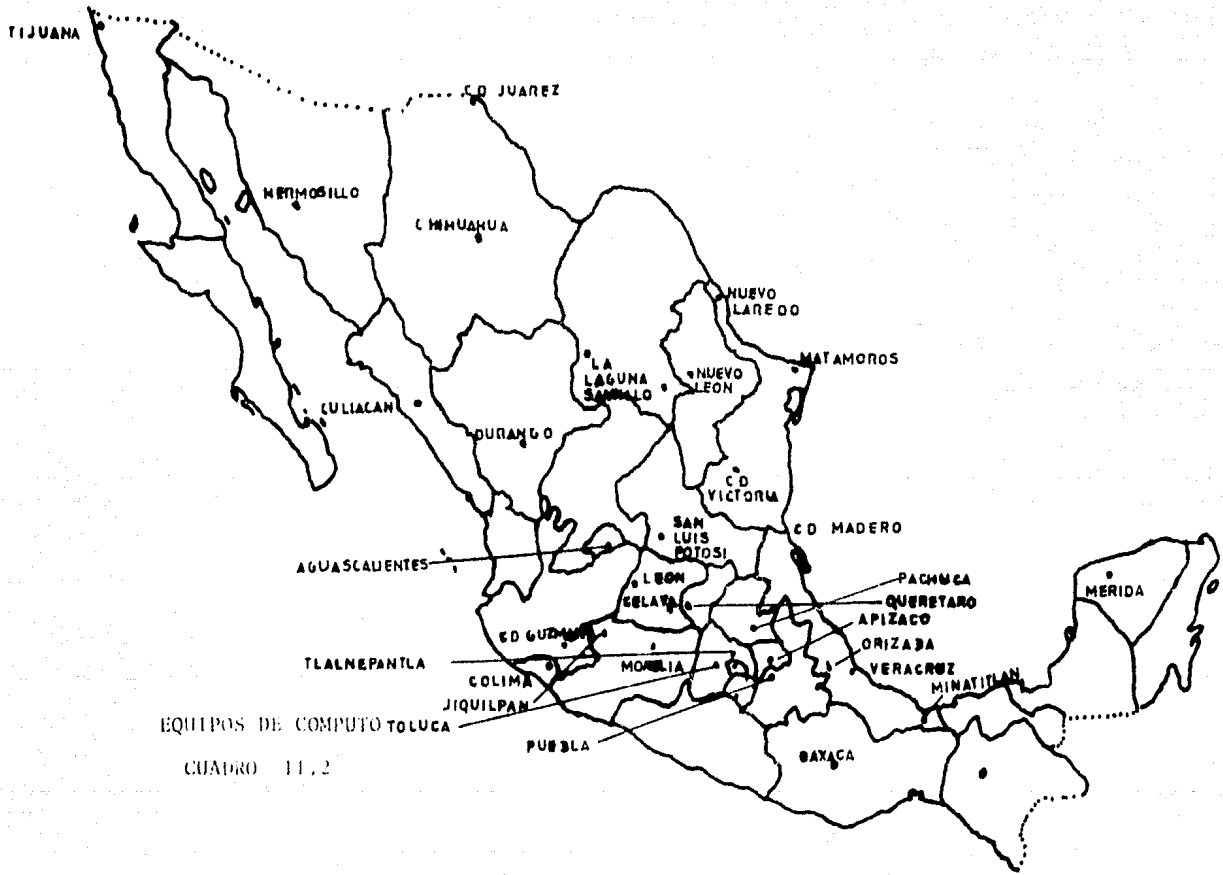
La distribución de equipos, de acuerdo con la marca y Modelo se encuentran localizadas como se muestra en el cuadro II.I

Así de los 52 Institutos que cuenta el sistema 33 se en--- cuentran equipados con Centros de Cómputo, 5 Tecnológicos tienen Microcomputadoras Multiusuario, lo que quiere decir que solo -- faltan de equipar 14 Institutos del total que tiene el sistema como se puede apreciar en el cuado II.2

PDP 11/23		PDP 11/34	HP - 2000
APIZACO	NUEVO LEON	AGUASCALIENTES	LA LAGUNA
CIUDAD GUZMAN	OAXACA	CELAYA	PACHUCA
CIUDAD VICTORIA	ORIZABA	CIUDAD MADERO	QUERETARO
COLIMA	PUEBLA	DURANGO	JIQUILPAN
CULIACAN	QUERETARO	MERIDA	TLALNEPANTLA
CHIHUAHUA	SALTILLO	NUEVO LAREDO	HP - 3000
HERMOSILLO	SAN LUIS POTOSI	VERACRUZ	CIUDAD JUAREZ
LEON	C.I.I.D.E.T.	PDP 11/40	MORELIA
MATAMOROS	D.G.I.T.	TIJUANA	CDC - 17
MINATITLAN			CHIHUAHUA

DISTRIBUCION DE EQUIPOS DE COMPUTO EN LOS INSTITUTOS TECNOLOGICOS.

CUADRO II.1



EQUIPOS DE COMPUTO

CUADRO II.2

CAPITULO III

ORGANIZACION DE LOS CENTROS DE COMPUTO

En la mayoría de las Organizaciones, el Personal de Datos se concentra en un grupo a que se les denomina: Departamento de Procesamiento de Datos, también recibe otros nombres como son: Centro de Procesamiento de Datos, Centro de Cómputo, Departamento de Informática.

Independientemente del Título que se les otorgue todos deben tener las mismas estructuras de su Organización aunque éstas difieran dependiendo del tipo de Empresa que se trate como son la pequeña, mediana o grande en los cuadros III.1, III.2, - III.3, se presentan organigramas estructurales para este tipo - de Empresas.

Estas estructuras organizacionales se dividen escencialmente en tres grupos operativos principales como son la operación, programación y sistemas, debido a que cada grupo realiza una -- función específica.

La responsabilidad primaria del grupo de operación es el - de llevar a cabo el procesamiento en la Computadora de cada trabajo, es decir maneja físicamente toda la información que entra en la Computadora y se encarga de enviar oportunamente la información hacia la Gerencia, así que las principales Funciones que realiza este grupo son:

1.- Preparación y limpieza de todo el Hardware usado en el

proceso de datos diarios.

2.- Mantenimiento de todas las bitácoras e informes de la Computadora.

3.- Manejo eficiente de todos los suministros y materiales requeridos en la Sala de Cómputo.

El grupo de Programación son los que proporcionan la programación que se va a ejecutar en la Computadora cuando esta se requiere, o modificar los programas existentes según sea necesario y se aseguran que todos los programas operen correctamente, es decir se encargan de dar el mantenimiento necesario, así como actualizar el Software que se maneja en el Centro de Procesamiento de Datos.

El grupo de Sistemas es el que se encarga de coordinar y supervisar el trabajo que realiza el Personal de Programación y Operación, puesto que son los encargados de que los datos se manejen en una forma correcta y eficiente a través de toda la organización en que laboran, también trabajan en el desarrollo de nuevos proyectos que les indique la Gerencia, así como el estudio para la implantación y puesta en marcha de nuevos sistemas de Cómputo que pretenda adquirir la Institución.

En toda organización es de vital importancia que cada miembro conozca el papel que desempeña dentro de la Organización --

para que con esto el flujo de la información o del procesamiento de datos se haga de una forma eficiente y se pueda disponer de la información en el momento preciso que se requiera para una toma de decisión.

A continuación se darán las funciones más importantes que deberán desempeñar el Personal que labora en el Departamento Informático estas funciones están tomadas de acuerdo a los Organigramas que aparecen en los cuadros III.1, III.2, III.3.

Director de Informática.

Responsabilidades Generales.

Es el responsable ante la Dirección General, del establecimiento y del funcionamiento del Sistema de Cómputo de manera que satisfaga las necesidades de información de la Institución a corto y largo plazo.

Es el asesor de la Dirección en cuanto a la utilización de las Computadoras y el Director Técnico Administrativo de todas las actividades del proceso de Datos.

Ayuda a la Dirección a determinar las necesidades en lo referente a la información necesaria para la Institución, para que pueda alcanzar sus objetivos y hacer frente a sus obligaciones, informa a la Dirección en lo concerniente al interés de la

utilización de las Computadoras para responder a sus necesidades en cuanto a sus posibilidades.

Responsable de los Estudios y la Programación.

Responsabilidades Generales:

Es el responsable ante el Director de Informática, de todas las funciones que tengan relación con los estudios y la programación.

Según la importancia de los proyectos o trabajos que se desarrollen dentro del Instituto, podrá supervisar los trabajos del Jefe de Ingenieros del Sistema.

Jefe de Proyectos.

Responsabilidades Generales:

Son los responsables ante el Director de Informática o ante el Jefe de Estudios y Programación, según el caso de la puesta en marcha del Proceso de Datos para los trabajos definidos en el plan de mecanización y de los cuales están encargados.

Así como establecer las consignas de puesta en práctica de los trabajos y dan formación, en su caso, al Personal de mantenimiento y de ejecución, una vez que la aplicación se encuentra

en el estado de Ejecución, ya no son consultados más que en los casos de modificaciones fundamentales.

Responsable de la Concepción de Aplicaciones.

Responsabilidades Generales:

Este empleo es intermedio entre el Jefe de Proyectos y del Analista, y responde a las necesidades de la responsabilidad derivada de la complejidad creciente de los trabajos mecanizados.

El Ingeniero de Aplicaciones trabaja:

Directamente a las órdenes del responsable de Estudios y Programación, en cuyo caso deberá tener las responsabilidades y las cualidades del Jefe de Proyecto, (pero a nivel menor).

Jefe de Grupo de Ingenieros de Aplicaciones:

Este puesto no existe generalmente más que en las instalaciones muy grandes, es un puesto escencialmente Jerárquico.

Asesor en Proceso de Datos o Ingeniero en Informática.

Responsabilidades Generales.

Es un puesto escencialmente Jerárquico, pero que no exige

conocimiento técnico muy completos y que únicamente puede trabajar con un Asesor en Proceso de Datos.

Coordinador de Servicio.

Responsabilidades Generales:

El Coordinador de servicio no forma parte del área de Proceso de Datos, está ligado Jerárquicamente y funcionalmente a su servicio, y trabaja en estrecho contacto con las personas encargadas de concebir y poner a punto la mecanización de Datos.

Analista.

Responsabilidades Generales:

Es el responsable de la concepción y de la puesta en marcha del expediente de análisis, en el cual deben figurar todos los elementos necesarios y suficientes para la escritura y buen funcionamiento del programa; que permitirá alcanzar los objetivos fijados por el Ingeniero de Aplicaciones o el Jefe de Proyectos.

Deberá verificar que el programa proporciona, los resultados deseados sin exceder el márgen de errores o de rechazos previamente definido, y preveer los procedimientos de control y de reanudación para obtener estos resultados, habrá de documentar el programa de tal manera que una tercera persona, pueda leer --

fácilmente el expediente de análisis, y asímismo, deberá comprobar que los documentos necesarios para la explotación estén completos y sean fácilmente comprensibles.

Programador de Aplicaciones.

Responsabilidades Generales.

Es el responsable de transformar el expediente de análisis, suministrado por el analista, de tal manera que pueda ser ejecutado por la Computadora, deberá comprobar que el programa, concebido de éste modo, alcanza efectivamente los objetivos previstos. Es responsable de su trabajo ante el Jefe de grupo de análisis y de programación, pero deberá trabajar estrechamente en colaboración con el analista encargado de la aplicación, a fín de que pueda estar seguro de que ha comprendido bien sus Directrices.

Programador de Sistemas.

Responsabilidades Generales:

Es el asesor de los programadores de aplicaciones, o de toda otra persona que tenga necesidad de estas informaciones en lo concerniente a las relaciones entre los programas y el sistema - operativo.

Es el responsable, en su caso de la programación de los módulos de programas, o de los programas que utilicen las posibilidades del sistema operativo en un mayor grado que lo hacen normalmente los lenguajes empleados es el encargado de la actualización y mantenimiento del sistema operativo.

Jefe de Grupo de Análisis y Programación.

Responsabilidades Generales:

Su función es el de definir y controlar el trabajo del grupo de análisis y programación, es además responsable, según el caso ante el Director de Informática o ante el Jefe de Estudios de Programación, de la Planificación y de la ejecución de los trabajos de análisis, de la programación, de las pruebas de los proyectos en curso de desarrollo y del mantenimiento de los programas en curso de explotación.

Explotación.

Responsabilidades Generales:

Es el responsable, ante el Director de Informática, de la ejecución de los trabajos previstos en el plan de mecanización del Instituto, puestos a punto por los grupos de concepción y de realización es un productor, cuya responsabilidad es semejante a la de cualquier otro responsable de producción.

Operador Jefe de Consola.

Responsabilidades Generales:

Es el responsable ante el Jefe de Equipo de la ejecución -- del trabajo diario, del Control y funcionamiento de la Computa-- dora, de las unidades periféricas y de todos los dispositivos -- conectados.

Operador.

Responsabilidades Generales:

Prepara las unidades periféricas, carga y descarga las unidades de cinta, disco, las lectoras y perforadoras de fichas, -- impresoras, bajo la Dirección de Operador de Jefe.

Bibliotecario.

Responsabilidades Generales:

Es el responsable ante el Jefe de Equipo de Almacenamiento y mantenimiento de todos los ficheros utilizados por el equipo, papel, fichas, de cintas, discos, hojas, etc.

Preparador de Trabajos.

Responsabilidades Generales:

Es el responsable de agrupar los elementos necesarios para la ejecución de un trabajo: documentos básicos, papel, fichas de cintas y discos, todo ello en función de la planificación del -- equipo.

Controlador de Trabajo.

Responsabilidades Generales:

Es el responsable de la supervisión y del control de los datos que entran en el equipo, de los trabajos que salen, y de las relaciones diarias con los servicios del usuario.

Las funciones definidas anteriormente corresponde a la Organización del Centro de Cómputo de la Gran Empresa.

Por lo que respecta al tipo de organización que es conve--- niente a los Institutos Tecnológicos para la organización de sus Centros de Cómputo es la que utiliza la pequeña Empresa y de la cual su Organigrama se muestra en el Cuadro III.2, en donde se - requieren un total de 8 personas las cuales tendrán asignadas -- las siguientes Funciones:

1.- Jefe de Servicios de Proceso de Datos.

Responsabilidades Generales:

Supervisará las actividades de Procesamiento de Datos den-- tro de la Institución, además brindará apoyo para la programa--- ción, operación, y desarrollo de los sistemas a automatizar.

Seleccionará la adquisición de Equipo para el Centro de Cómputo.

Aplicará técnicas que simplifiquen el análisis y diseño de sistemas.

1.1 Analista Programador Jefe.

Responsabilidades Generales:

Es el responsable de la concepción y puesta a punto de expedientes de análisis, en el cual deben figurar todos los elementos necesarios y suficientes para la Escritura y buen funcionamiento de los programas que permitan alcanzar los objetivos, fijados por el Jefe de Servicios de Procesos de Datos, con respecto al sistema a automatizar.

Deberá verificar que el programa proporcione los resultados deseados sin exceder el márgen de errores o de rechazo previamente definidos.

1.1.1. Analista Programador.

Responsabilidades Generales:

Bajo la Dirección del Jefe analista participará en el análisis de los sistemas a implantar, además solucionará los problemas que puedan generarse en la implantación del sistema.

1.1.1.1 Programador.

Responsabilidades Generales:

Es el responsable de transformar el expediente de análisis suministrado por el analista, de tal manera que pueda ser ejecutado por la Computadora. Deberá comprobar que el programa concebido de este modo alcanza efectivamente los objetivos previstos, es el responsable de su trabajo ante el analista Jefe, pero deberá trabajar en estrecha colaboración con el analista programador, a fin de estar seguro de que ha comprendido bien sus directrices con respecto al sistema a programar.

1.2 Operador Jefe de Consola.

Responsabilidades Generales:

Es el responsable del buen funcionamiento de la Computadora y equipo periférico que esté a su cargo.

1.2.1. Operador

Responsabilidades Generales:

Deberá preparar las unidades periféricas, cargar y descargar las unidades de cinta, disco, lectoras y perforadoras de fichas e impresoras bajo la Dirección del Operador Jefe.

I.2.1.1 Perforista.

Responsabilidades Generales:

Deberá capturar los datos de acuerdo con las instrucciones previstas por el Analista Jefe.

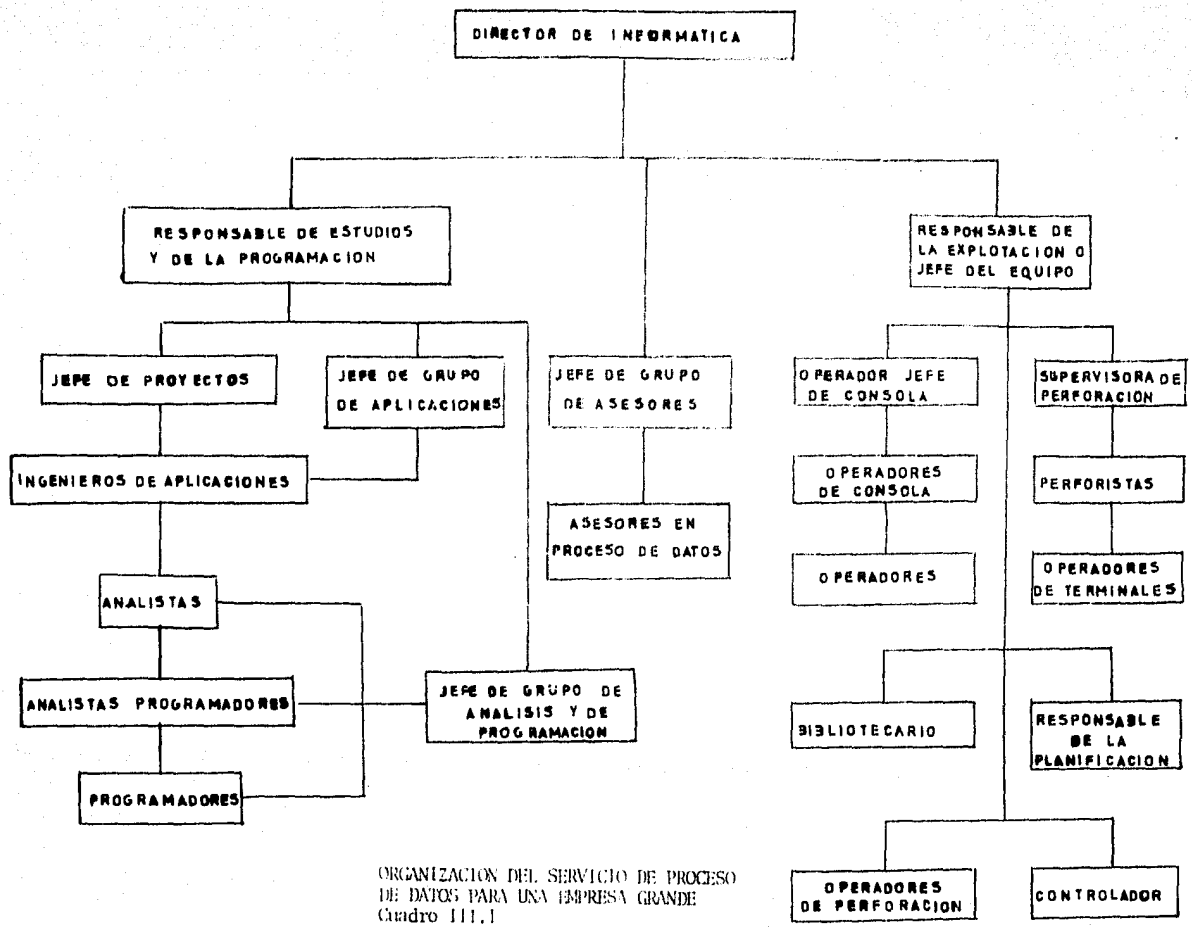
Detectará errores en la captura de datos y corregirlos posteriormente.

I.3 Preparación y Control.

Responsabilidades Generales:

Es el responsable de agrupar los elementos necesarios para la ejecución de un trabajo como son: Documentos básicos, papel,- fichas, cintas, discos y ficheros todos ellos en función de la - planificación del equipo.

Deberá asegurarse de que la secuencia de operaciones se ejecuta efectivamente diseñando una serie de controles para la llegada y ejecución de trabajos, documentos producidos, y para clasificar y archivar los materiales utilizados en el proceso.



ORGANIZACION DEL SERVICIO DE PROCESO DE DATOS PARA UNA EMPRESA GRANDE
Cuadro III.1

ESTRUCTURA ORGANICA
SERVICIO DE PROCESO DE DATOS PARA
UNA EMPRESA PEQUEÑA.

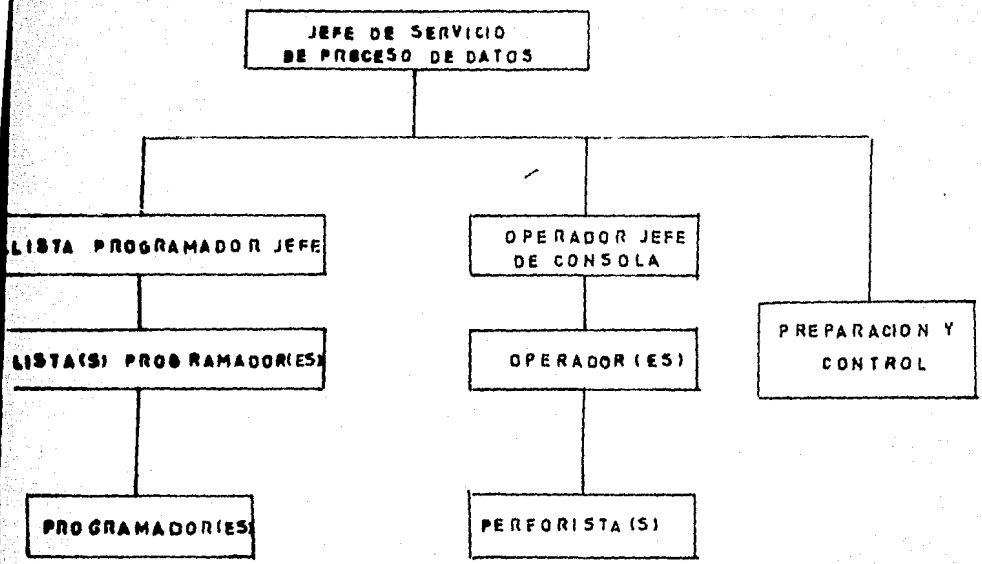
1 JEFE DEL SERVICIO DE PROCESO DE DATOS

1.1. ANALISTA PROGRAMADOR JEFE
1.1.1 ANALISTA PROGRAMADOR
1.1.1.1 PROGRAMADORES

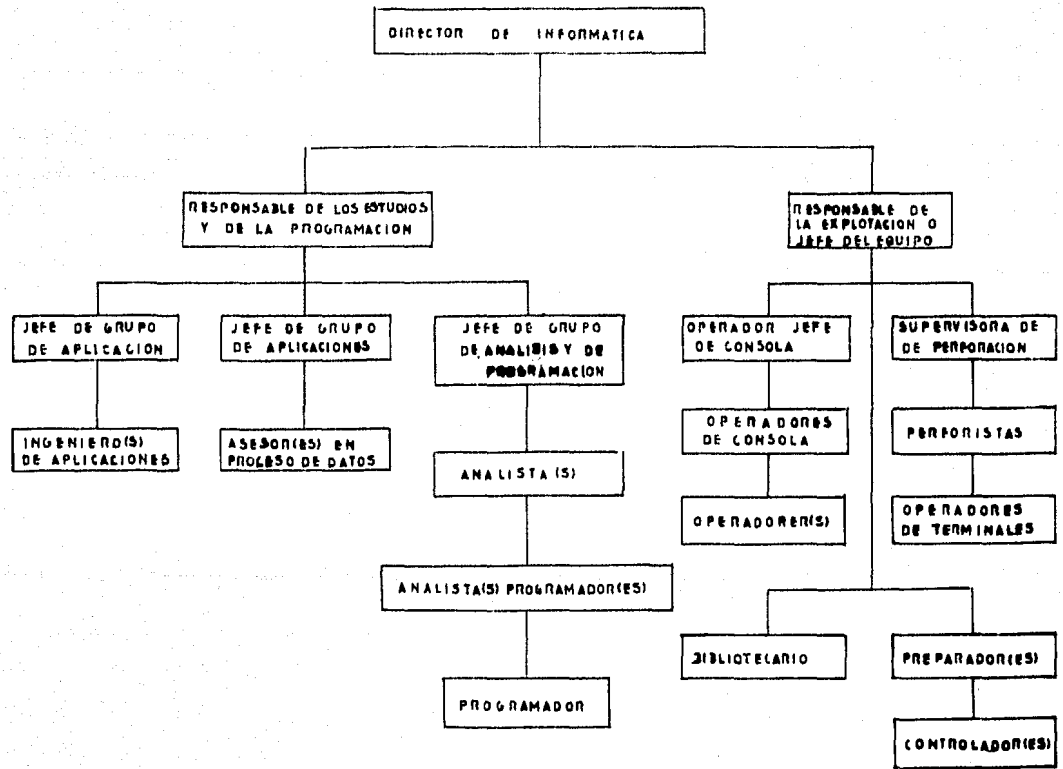
1.2 OPERADOR JEFE DE CONSOLA
1.2.1 OPERADORES
1.2.1.1 PERFORISTA

1.3 PREPARACION Y CONTROL

CUADRO III.2A



ORGANIZACION DEL SERVICIO DE PROCESO
DE DATOS PARA UNA EMPRESA PEQUEÑA
Cuadro III.2



ORGANIZACION DEL SERVICIO DE PROCESO DE DATOS
PARA UNA EMPRESA MEDIANA O GRANDE

CUADRO III.3

C A P I T U L O IV

L A S E G U R I D A D D E L C E N T R O D E C O M P U T O .

La primera etapa del diseño de cualquier sistema de seguridad debe tener como objetivo:

a).- Qué es lo que debe ser protegido.

b).- Porqué ha de ser protegido.

c).- Centro o Centros que han de protegerse.

d).- Cuáles son los niveles de riesgo aceptados.

e).- Valoración de los daños y el costo de la protección.

Han de considerarse todos los posibles factores generadores de riesgo, por improbables que parezcan, dado que el riesgo se define como el producto de la probabilidad del suceso (que puede ser baja) y los daños ocasionados por el mismo (que pueden ser muy altos).

Existen factores de riesgo tanto internos (anomalías en instalaciones del Centro, anomalías originadas por el Personal encargado de la explotación del mismo, accidentes fortuitos en el seno del mismo), como externos (catástrofes naturales, accidentes producidos en el entorno del Centro, acciones llevadas a cabo por el Personal ajeno al Centro), cuya identificación, valoración y diseño de medidas de seguridad adecuadas constituyen una labor muy compleja: máximo teniendo en cuenta que el sistema de seguridad debe de asegurar la protección del Centro.

A continuación trataremos las partes en donde se debe poner más atención para su protección.

1.- Edificio donde se alberga el Centro de Cómputo:

Es muy conveniente que un Centro de Cómputo se ubique en un edificio dedicado en exclusiva al mismo, aislado de otros, y --- construído en un recinto propio suficientemente amplio.

Otro aspecto que no se debe descuidar es la elección de la ubicación del Centro para que con esto reducir el riesgo de accidente.

En este sentido han de evitarse zonas con riesgos de inundaciones (proximidad a ríos, mar, etc.,) Zonas en donde existan -- instalaciones emisoras de radio Frecuencia de alta intensidad -- (por la interferencia que causa para el funcionamiento de la unidad central de proceso), productos inflamables o explosivos y zonas de tráfico intenso o de alta densidad de estacionamiento.

Por lo que respecta al Recinto constituye la primera de las tres barreras de seguridad aconsejables: Recinto, Edificio, Principal, y áreas internas reservadas, ha de estar dotado de un sistema de cierre accionado únicamente desde el interior, así como de una adecuada iluminación y de un adecuado sistema de drenaje.

En lo concerniente al Edificio principal donde se alberga el Centro de Cómputo, ha de ser Arquitectura sólida, disponiendo de Puertas y ventanas seguras, y prestando especial atención a - los conductos para salida de desperdicios, entrada de combusti--

ble, torres de aire acondicionado, montacargas, etc., es conveniente disponer de una sola puerta de acceso para el Personal y de otra más grande y pesada para entrada de equipo, cuyas condiciones de solidéz han de ser mayores; también es aconsejable dotar a las ventanas de cristales de seguridad y rejas.

Por lo que respecta a las áreas funcionales, el Local será estructurado en diferentes áreas a las que corresponderán distintos niveles de seguridad (de carácter físico o puramente organizativo). Entre las áreas funcionales a implantar cabe distinguir la recepción (personal de vigilancia y visitantes); la de desarrollo y organización (personal de análisis, programación, planificación, control y, eventualmente la dirección) que estará alejada de las Computadoras; la de explotación (personal de explotación y operación) contigua a la Sala de Computadoras y, finalmente, la Sala de Computadoras dotada de grandes medidas pasivas de seguridad: paredes, techos y suelo de alta resistencia Mecánica y revestidos de material incombustible; el techo deberá ser impermeable: los equipos de fuerza, aire acondicionado y grupo electrógeno se ubicarán en la Sala pero aislados del resto y además entre sí por paredes impermeables e incombustibles siendo para uso exclusivo de la Sala de Computadoras: La Biblioteca de soportes magnéticos se ubicará asímismo en esta Sala con las condiciones anteriores los servicios higiénicos y la Sala de reposo se ubicarán fuera de la Sala.

2.- Instalaciones Auxiliares.

Por lo que respecta al sistema de alimentación eléctrica es aconsejable tener un Banco de Baterías y la alimentación eléctrica proporcionada por la Comisión Federal de Electricidad e instalar equipos de Conmutación Automática entre las dos fuentes para que se pueda pasar de una a la otra sin interrupción en casos de emergencia. En el caso de que la operación de las Computadoras haya de ser contínua se recomienda utilizar un grupo electrógeno.

Al planear la instalación eléctrica habrá de procederse a tender circuitos independientes y aislados para la iluminación la ventilación y la alimentación de las Computadoras y periféricos, debiendo dotar a los elementos informáticos de cables de alimentación blindados y con una tierra electrónica de baja impedancia. Todos los cables deberán estar revestidos de material incombustible y habrá que proveer de sistemas automáticos de interrupción de suministro y aislamiento del área, en casos de emergencia.

En lo relativo al sistema de aire acondicionado para la Sala de Computadoras deberá estar ubicado en la propia Sala, convenientemente aislado, y ser independiente del sistema para el resto del Edificio tanto por condiciones de seguridad como por los distintos requisitos de la Sala de Computadoras y de los Locales donde se encuentra el Personal. El sistema seleccionado ha de cumplir las necesidades especiales de una Sala de Computadoras:

Alta capacidad de Refrigeración; impulsión a través del falso -- suelo; posibilidades de Refrigeración, calefacción humidifica--- ción y deshumidificación: alta capacidad de filtrado de aire: -- control automático; bajo nivel de ruido; alto grado de seguridad con redundancia de los circuitos críticos, que le permitan fun-- cionar todo el año sin interrupción.

Especial precaución hay que tener con la propagación del -- fuego a través de los conductos de aire acondicionado, para lo - cual es recomendable el uso de cortinillas cortafuegos en las bo cas de salida del aire accionadas automáticamente por el sistema de alarmas.

3.- Equipo del Centro de Cómputo.

Para garantizar una gran fiabilidad y disponibilidad del -- Centro es preciso seleccionar aquellos equipos que a nivel indi- vidual suministren un tiempo medio entre averías (MTBF) largo y un tiempo medio para reparación (MTTR) corto, así como proceder a una configuración de los mismos que se atenga a estos crite--- rios, aumentándolos incluso con relación a los valores de los -- elementos individuales.

Para ellos se ocurre a técnicas diversas como son: duplici- dad de elementos críticos (unidad central de proceso, subsistema de comunicaciones, unidades de control y/o de almacenamiento de memorias masivas etc.) que funcionen de modo interrumpido efec-

tuando todos las mismas operaciones (HOT-STANBY), o bien entran - únicamente en funcionamiento al producirse una avería (COLD-STANBY) utilización de conmutadores manuales o automáticos que permiten eliminar las unidades defectuosas y remplazarlas por otras en correcto estado, redundancia en la información (bits para el control y corrección de errores de paridad) y en los componentes -- (más unidades de disco y cinta de las estrictamente necesarias, más unidades de adaptación de líneas, etc), utilización de consolas de control para monitorización del sistema y reconfiguraciones del mismo en caso de fallas.

4 - Medios de Comunicación.

Existen procedimientos técnicos muy diversos para conseguir una gran fiabilidad en la transmisión de información como son duplicidad de circuitos utilizando trayectos físicos diferentes -- (rutas alternativas) e incluso medios de tecnología diferentes - (por ejemplo, un circuito va por cable y el duplicado va por radio), duplicidad de las unidades de conversión y adaptación de señales, utilización de conmutadoras manuales o automáticas que permitan asiganciones variables de circuitos a unidades y/o adaptadores de líneas, utilización de la red automática Conmutada telefónica como respaldo de los circuitos punto a punto en caso de fallo, utilización para la transmisión de redes públicas de ---- transmisión de datos, que garantizan una mayor fiabilidad que -- las redes privadas, dispositivos para la monotorización de las - líneas y determinación de las causas y lugar del fallo (bucles -

locales y/o remotos a nivel analógico y/o digital), comunicaciones de voz entre operadores.

5.- Control de Acceso al Centro.

Para que un sistema de seguridad sea efectivo se debe disponer de un adecuado sistema de control de acceso de Personal y materiales al Centro, así como de la circulación de los mismos una vez en el interior, para prevenir y detectar los posibles incidentes que por intrusión, robo, sabotaje, bandalismo y otros se podrían producir.

Habrá que distinguir básicamente entre los accesos a las instalaciones (Recintos, Edificios Principal, y áreas reservadas) y la circulación del Personal tanto del propio Centro (que habrá de identificarse para la entrada al mismo y cuya circulación deberá estar limitada a ciertas áreas) como el Personal ajeno perteneciente a Servicios externos del Centro (mantenimiento de la Computadora y mantenimiento del Edificio) y las visitas.

Para disminuir los niveles de riesgos ha de procederse a una Selección cuidadosa de los Suministradores de servicios externos (experiencia, estabilidad, etc.) y asegurar que el contrato incluya una relación detallada y específica de las labores a efectuar; especificando las responsabilidades de ambas partes, las garantías, debe tener la existencia de una cláusula razonable de cancelación y a que el incumplimiento obligue más bien a

compensaciones que a castigos.

El vigilar que se cumplan las reglas anteriores podemos confiar que el Centro de Cómputo estará trabajando en óptimas condiciones en lo que se refiere a la seguridad del Centro.

CAPITULO V

LA PROTECCION DE DATOS

Los datos son los testimonios de la información que tenemos acerca de un hecho, son el reflejo de las condiciones en que se encuentra una situación dada.

El Archivo es un conjunto de datos que tienen entre sí algo de común, es decir, que los datos poseen un criterio de pertenencia que les permite ser identificados como elementos o miembros del conjunto.

La unidad elemental de información en un Archivo se le denomina Registro.

Algunos Tipos de Archivos son los siguientes:

Programas en Lenguaje fuente.
Programas en imagen de memoria.
Programas en módulo objeto.
Archivos de Datos (Registros de Empleados de Inventarios de pedidos, una colección de lecturas de un experimento).

Directorios.
Trabajos de Usuarios.
Archivos de Contabilidad del sistema mismo.

Un Archivo reside en alguna parte, y durante su vida, en diferentes partes de la memoria.

Dada la importancia que representa un Archivo debido a la - información que éste maneja se debe garantizar la privacidad y - confidencialidad de ésta, la cual no deberá ser develada más que a la persona que se encuentre debidamente autorizada para hacer - uso de ésta.

Con el uso de recursos compartidos y los inevitables fallos (accidentales o deliberados) de cualquier sistema informático, - lleva a la necesidad de implantar medidas de seguridad que evi-- ten por un lado la interferencia entre los distintos usuarios y aseguren, por otro, una máxima fiabilidad disponibilidad y confi dencialidad del sistema.

En una Computadora dedicada, a trabajar para un solo usua--- rio, con un Sotfware ya probado y ofreciendo una fiabilidad ya -- completa, no habría ninguna necesidad de protección, la necesidad surge, precisamente, al no cumplirse alguna (o todas) de las con diciones anteriores.

Como se indicaba anteriormente la necesidad actual, por razo nes de economía y de interconectividad, es hacia el uso compartido de recursos (unidad central, memorias centrales, y masivas, - periféricos, etc.), y de datos (bases de datos, Bancos de datos, etc.) por diferentes aplicaciones y usuarios.

El problema se agrava si no se puede predecir de antemano -- cuales van a ser los datos utilizados por cada aplicación en un -

momento determinado, con lo cual resulta muy difícil exigir barreras de protección que impidan las interferencias indeseadas, y si además han de existir zonas comunes entre las diferentes aplicaciones y usuarios para intercambio de datos, lo cual impide el confinamiento total de cada aplicación mediante la técnica de "máquinas virtuales" (cada aplicación opera como si dispusiera realmente de un sistema informático dedicado).

Además se deben tener en cuenta las inevitables fallas del sistema (de Hardware o Software) y garantizar en la medida de lo posible que los fallos no corrompan y confudan los datos del sistema y minimizar las posibilidades de que el fallo cause una puesta en fuera de servicio del sistema).

Por ello son necesarias una pronta detección del fallo (mediante redundancia en los datos, las direcciones y los Descriptores), así como esquemas que impidan la propagación del mismo (minimización del volúmen de datos que se adquieran en cada acceso, minimización del número de re-arranques del sistema.

Actualmente existe una gran variedad de clases de protección que pueden ser utilizadas en un sistema informático como los que se enuncian a continuación:

1.- Autentificación el uso de un Computador requiere una comprobación previa de la autenticidad del usuario. Esto se suele hacer mediante el uso de palabra clave o contraseña (Pass word)

lo cual exige la protección física del fichero donde se almacenan las contraseñas, la autentificación del propio sistema de cara al usuario (para evitar que alguien simule el proceso de identificación y se haga con la contraseña de otro usuario).

2.- Prevención del uso no autorizado de datos. Se establecen controles de acceso que investiguen y comprueben sí un determinado sujeto (programa, proceso o usuario) tiene derecho a acceder a unos determinados objetos del sistema (segmentos de memoria, archivo, etc.) y la naturaleza de este acceso (lectura, escritura, borrado, prueba, etc.). Es necesario que el sistema informático sea físicamente seguro, pues sino no tendrían efectividad los controles de acceso.

3.- Prevención del flujo no autorizado de información en ciertos casos es necesario evitar que ciertos datos utilizados por un programa puedan ser reproducidos y lanzados al exterior (mediante un listado), lo cual lleva a establecer restricciones sobre lo que puede hacer con los datos.

4.- Prevención del uso no autorizado de programas. Pueden existir programas cuyo uso hay que restringir. Esto se consigue habitualmente separando físicamente, en la memoria, los programas de los datos.

5.- Prevención de prohibiciones indebidas de servicio, debe evitarse de cualquier usuario del sistema puede hacer que un de-

terminado servicio, el cual está autorizado, le sea denegado a - otro usuario. Estas prácticas fraudalentas puede realizarse mediante modificaciones de la lista de autorizaciones, uno indebido de los enclavamientos (interlocks), excesiva frecuencia en el uso de un determinado fichero, etc.

6.- Prevención de acceso a datos en tiempo indebidos, esto podría ocasionar, si no se evita, los abrazos mortales (deadlocks) en los cuales un usuario espera a liberar unos recursos, que son vitales para otro usuario, a que este otro usuario libere a su vez otros recursos que son vitales para el primer usuario.

En cualquier situación en que hayan de protegerse datos es necesario partir de ciertas hipótesis básicas relativas a qué clases de protección deben preveerse y en que grado. Así es necesario saber si vamos a confiar en la integridad de los medios de comunicación o, en caso contrario, acudir a técnicas de cifrado, hasta que grado se confía en la honradéz de los programadores del sistema, hasta que punto son fiables los compiladores y si debemos establecer comprobaciones periódicas de los mismos durante las ejecuciones de los programas; vamos a adoptar un sistema de protección total (no se pueden vulnerar las medidas de seguridad) o más bien adoptamos tácticas defensivas (las medidas de seguridad se van a vulnerar pero nos aseguramos de que hay constancia grabada de que ha ocurrido y de como ha sido) y proveemos alarmas y registros especiales para proceder a una labor

posterior de auditoría; vamos a aceptar las características de seguridad que dice tener el sistema o vamos a realizar algún tipo de pruebas de las mismas para comprobar su eficacia; no permitir los accesos indiscriminados a la Sala de Computadoras.

Cualquier responsable de la operación de un sistema informática deberá elaborar reglas básicas para la protección de datos.

Hay ciertas directrices generales que deben observarse en cualquier esquema de protección que se adopte, a fín de garantizar una protección eficáz:

1.- Simplicidad. Un diseño simple del esquema de protección implica una menor probabilidad de error, un costo y tiempo de ejecución, y una mayor facilidad de comprensión por parte del Personal de explotación del Centro.

2.- Completo. Cualquier operación factible debe ser comprobada y autorizada, lo cual implica que esta comprobación debe hacerse a nivel Hardware.

3.- Nivel de actuación lo más pequeño posible. Cada privilegio o autorización debe incluir tan pocas funciones y grados de acción como sea posible (por ejemplo, el tamaño de los segmentos protegidos debe ser igual y no mayor que el definido por el acuerdo de direccionamiento del sistema).

4.- Protección total en caso de falla del sistema. En caso de que falle el sistema de protección o no esté activado de manera explícita, el estado de reposo (default state) ha de ser la prohibición total de accesos de cualquier objeto y la necesidad de obtener permisos explícitos para cada operación.

5.- Concesión del número mínimo de privilegios Al operar cada programa y usuario del sistema utilizado el mínimo de privilegios necesarios para llevar a cabo la tarea que se está realizando en ese momento se limitan los daños que se producirían en caso de accidente o fallo y se reducen al mínimo las correcciones necesarias en caso de errores, lo cual lleva a una deseable modularización del sistema de protección.

6.- Uso compartido de recursos bajo control. Así, si dos aplicaciones pueden acceder al mismo segmento de datos y ambos pueden modificarlos, se establecerán enclavamiento para evitar accesos simultáneos.

7.- Tamaño mínimo del material común. De especial relevancia en el caso de memoria principal, para evitar que una subrutina defectuosa pueda dañar a todos los otros usuarios que la compartan.

8.- Encapsulación o confinamiento. Agrupar todas las operaciones que trabajan sobre una determinada área de datos en un solo programa.

9.- Separación de privilegios. Se establecerán múltiples condiciones distintas a satisfacer antes de conceder un acceso determinado, para así obtener una mayor probabilidad de que no se vulnerará el sistema de protección.

1 .- Sospecha mutua. Los programas deben de interactuar sobre la base de sospechar entre sí y del propio sistema operativo, a fin de evitar prácticas fraudalentas

11.- Posibilidad de efectuar cambios dinámicos y revocaciones en el sistema de protección. Para facilitar las altas y bajas en el sistema; la creación, modificación y eliminación de privilegios, etc.

12.- Confinamiento de los datos. Protección no solo del lugar donde se encuentran los datos, sino también del contenido prevención de que un programa que haya accedido a los datos pueda acceder a un canal de salida.

13.- Alto factor de rendimiento. Se define como el cociente entre los esfuerzos necesarios para vulnerar las medidas de protección y los recursos de que presumiblemente dispone el atacante. Así por ejemplo, las contraseñas y claves han de ser largas y sometidas a cambios frecuentes para evitar su posible descubrimiento por cálculos sistemáticos.

Algunas medidas prácticas para la protección de archivos de

datos son las que se enuncian a continuación.

1. Verificar consistencia de apuntadores: apuntadores de directorios deben dirigirse a otros directorios o a archivos propiamente dicho En estructuras bi-direccionales, ir hasta un extremo y luego regresarse. cuadro V.1

2.- Usar redundancia en la información. Por ejemplo en alguna lista de inventario de unidades, especificar que -- proceso tiene asignadas las unidades, según la clasificación que tengan dentro del archivo.

3.- Aplicación de cifras de control y dígitos verificado--- res. Esto es muy util para aislar partes alteradas.

4.- Series automáticas de respaldo de archivos. Se respal-- dan solamente aquellos archivos que han sido modifica-- dos.

5.- Vaciados periódicos de partes del sistema, selecciona-- dos en orden de peligro y cíclicamente.

6 - Vaciados totales, a intervalos más largos

Algunas de las técnicas utilizadas para la protección de datos son las que se expondrán a continuación:

Codificación de privilegios.

Consideremos el sistema informático compuesto de un conjunto de sujetos (entidades activas en el sistema y que se corresponden a usuarios, tareas y programas) y de otro conjunto de objetos (entidades pasivas correspondientes a ficheros, segmentos, cintas magnéticas, pilas de discos).

De forma general los objetos almacenan información y los sujetos la utilizan o procesan. Nuestro objetivo consiste en proteger esta información, o sea en controlar los modos en que los sujetos operan sobre los objetos.

Imaginemos que tomamos una fotografía del estado de protección del sistema y escribimos en una columna todos los nombres de los sujetos y en una fila todos los nombres de los objetos y, finalmente rellenamos las casillas de intersección con el grado de acceso que cada sujeto posee con un determinado objeto (lectura, escritura, etc.). Así obtendríamos una tabla de dos dimensiones llamada matríz de acceso, un ejemplo de la cual se muestra en el cuadro V.2.

De esto podemos observar que la matríz de acceso no es muy práctica puesto que la mayoría de las casillas están vacías (no se permite el acceso sujeto-objeto) y algunas filas o columnas se repiten mucho (varios sujetos gozan de acceso a un mismo objeto).

Si tomamos solamente las columnas de la matríz de acceso, - omitimos las casillas en blanco y rellenamos las otras con el - nombre de los sujetos correspondientes y su grado de acceso, tendremos una representación del esquema de protección más viable - para su implantación en la Computadora y que se denomina lista - de control de acceso (cuadro V.3).

A veces se agrupan varios sujetos juntos, que gozan de los mismos privilegios con respecto a un determinado objeto y se denominan clases. En el cuadro V.3 correspondería al objeto RACU - CODIGO, cuyo sujeto es cualquiera.

Si procediéramos a la inversa y tomáramos las filas de la - matríz de acceso, omitiéramos las casillas vacías y rellenáramos las otras con los nombres de los objetos correspondientes (cuadro V.4) junto con el grado de acceso obtendríamos otro posible esquema de protección basado en las denominadas capacidades. Todos los sujetos poseen un conjunto de capacidades que son asimilables a tarjetas no falsificables conteniendo permisos para acceder de determinado modo a determinados objetos.

Como representación del estado estático de protección de - una máquina, las capacidades y las listas de control de acceso - (LCA) son equivalentes. Sin embargo, desde el punto de vista de cambios dinámicos en el estado de protección, difieren considerablemente, dado que las capacidades se asocian con el sujeto y se almacenan en el espacio de Direcciones del mismo, mientras que -

las LCA se asocian con los nombres de los objetos y se incorporan habitualmente como parte de la estructura del Directorio del sistema de ficheros. Por lo tanto, los cambios del esquema de protección generados por el usuario son tratados más fácilmente por un sistema basado en capacidades, mientras que los cambios de esquema de protección que afectan a un objeto (por ejemplo), renovación de todos los accesos al mismo pueden ser fácilmente resueltos por un esquema LCA.

Se pueden combinar ambos esquemas reservando el esquema de capacidades para los cambios a corto plazo y el esquema LCA para contener los estados de protección que se prevean de largo plazo.

Protección de Memoria.

Constituye el nivel básico de protección de un sistema a partir del cual se pueden implantar otros esquemas más elaborados de protección de otros objetos, como el de las capacidades y el LCA descritos anteriormente. Queda claro que una vez protegido este objeto podremos pasar a otros objetos más abstractos como los ficheros o los flujos de entrada salida. Asímismo es evidente la íntima conexión entre la protección de memoria y el direccionamiento de la misma, de tal modo que el Hardware de la máquina pueda validar todas las referencias a la memoria al ser direccionada.

Los sistemas más primitivos (y también las primeras microcomputadoras) no disponían de ninguna protección y por lo tanto era inútil tratar la multiprogramación en éstas máquinas.

Avanzando en complejidad tenemos los sistemas con dos estados de protección (todo o nada). En el estado privilegiado se tiene acceso completo a toda la memoria y en el otro estado solo a la que se encuentra por debajo de un cierto límite. El sistema operativo se encontrará en aquella parte accesible tan solo en modo privilegiado y los usuarios compartirán todos la zona no privilegiada y no están protegidos entre ellos ni del sistema operativo. El cambio entre estados solo puede hacerse en el Estado privilegiado (cuadro V.5).

Avanzando más llegamos a un sistema de clases no jerarquizado donde existen varios estados de protección identificados por una clave entera. La Computadora opera en el estado indicando por el contenido del Registro de clave, la memoria se divide en Regiones, a cada una de las cuales se asigna una clave, y solo se puede acceder a aquellas Regiones cuya clave coincida con el Estado de la máquina. Escepcionalmente, el sistema operativo opera en el nivel 0 y si la máquina se encuentra en ese Estado, se puede escribir en toda la memoria (cuadro V.6).

Las limitaciones principales de este sistema son la imposibilidad de compartir una Región de memoria entre usuarios, el excesivo privilegio del sistema operativo y la ausencia de con-

trol sobre la lectura.

Un paso ulterior nos lleva a los sistemas basados en un Registro descriptor único donde se opera con direcciones relativas, en lugar de absolutas, efectuándose así una separación entre los esquemas de direccionamiento y de protección.

Se mantiene el modo de funcionamiento del estado privilegiado, pero las Direcciones generadas en los Estados no privilegiados se modifican mediante un argumento contenido en el Registro descriptor antes de convertirse en direcciones absolutas. Este - Registro descriptor no privilegiados) y un campo límite (que especifica la dirección máxima permisible para las zonas no privilegiadas). Así podemos ubicar la zona no privilegiada en cualquier posición de la memoria principal (cuadro V.7) y puede haber tantos posibles estados como se desee. Subsisten no obstante. las dificultades de compartir memoria entre usuarios y el Estado superprivilegiado del sistema operativo.

En los sistemas dotados de múltiples Registros descriptores, asequibles simultáneamente, los usuarios no privilegiados - especifican junto con la Dirección a que desean acceder el número del descriptor que van a utilizar, habiendo llegado así a la noción de segmento; una zona de memoria direccionada de modo continuo y accesible separadamente.

Ahora ya se puede conseguir, mediante el uso adecuado de los descriptores, múltiples, que varios usuarios compartan uno o varios segmentos de memoria, mientras que disponen también de su zona privada.

Los Registros descriptores pueden utilizarse asimismo para controlar el grado de acceso al segmento de memoria mediante la inclusión en los mismos bits que identifiquen estos accesos ... (cuadros V.8), consiguiente así la separación entre segmentos .. conteniendo programas (solo se permite lectura o ejecución) y .. los que contengan datos (solo se permite lectura o escritura).

Todavía persiste la dificultad de que los Registros descriptores solo pueden ser manipulados por el sistema operativo. Para subsanar este privilegio excesivo se pueden utilizar los esquemas anteriores de capacidades y LCA, permitiendo a ciertos sujetos el acceso a ciertos Registros descriptores para manipular su contenido. (operaciones de carga y almacenamiento)

Arquitecturas Jerarquizadas o en anillo.

Este tipo de Arquitectura trata de dividir el sistema en .. capas concéntricas cuyos privilegios van aumentando gradualmente hacia el interior, de tal modo que cada capa dispone de todos .. los privilegios de las capas más externas o periféricas además de otros suyos propios.

La Arquitectura en anillo constituye un esquema de protección jerarquizada donde existe un conjunto de Estados diferentes de protección, asignados cada uno a una de las capas o anillos (cuadro V.9). En el ejemplo hay 8 Estados siendo el 0 el más privilegiado y el 7 el menos. Tanto los segmentos claves y todos los programas como los de datos contienen clases y todos los programas y datos con la clave constituyen la capa n, de tal modo que los programas situados en la capa n, solo pueden acceder datos de la capa m si n es menor o igual que m. La identidad del programa que se esté ejecutando determina el Estado de protección de la máquina.

Este esquema de protección va superpuesto a otros esquemas basados en las capacidades o LCA y requiere para su soporte en el Hardware de la máquina que los Registros descriptores incluyan una clave para el segundo en cuestión o que se dispone de un Registro descriptor específico, para cada capa o anillo.

Arquitecturas no Jerarquizadas.

Dado que habitualmente los requerimientos del usuario de gozar de privilegios se encuentran muy localizados alrededor de un cierto programa o conjunto de programas, se introduce el concepto de dominios de protección para satisfacer esta demanda y reducir al mismo tiempo la disponibilidad de la mayoría de los privilegios asociados para acceder a segmentos de datos, ficheros, etc., de tal modo que los privilegios de un dominio son solo ase

quibles al usuario cuando está ejecutando un programa contenido en el dominio. Un programa de usuario constituye un caso especial de dominio y puede disponerse que los dominios del sistema no tengan acceso a otros segmentos del usuario más que a los permitidos explícitamente por él mismo. Se puede dividir un sistema en un gran número de pequeños dominios, con una interacción entre ellos tan pequeña como sea posible (cuadro V.10).

Incidencias del esquema de protección en la estructura del sistema informático. Debe quedar muy claro que las medidas de protección van a tener efectos en la estructura del Software del sistema así como en la Arquitectura física, siendo ésta la más acusada.

Así, si se adopta una estructura en anillo, el nivel gradual de complejidad creciente ha de ser inverso al nivel creciente de dependencia por lo que se refiere a distintos niveles de abstracción del sistema (cuadro V.11) de tal modo que el nivel más complejo (el programa de usuario) sea el menor de dependencia (está situado en la capa más externa) y el nivel más simple (la propia máquina) se encuentra en el Centro del anillo, dependiendo de todos los otros niveles Los problemas de protección pueden surgir del solape entre espacios de Direccionamiento.

En las estructuras basadas en capacidades, la posesión de una determinada capacidad por un sujeto no debe implicar ni de presuponer la posesión de cualquier otra capacidad y las especi

ficaciones relativas a la protección estarán separadas de los -- programas del sistema, para así permitir una Inspección más fá-- cil

Al efectuar la planificación y asignación de los diferentes recursos del sistema conviene, a efectos de protección, implan-- tar mecanismos que encaminen a los progrmas solamente hacia los datos que sean factibles de acceso correcto en lugar de dejarlos encaminarse a cualquier otro tipo de datos y atraparlos cuando - vulneren las normas de protección.

Esto es análogo a la diferencia de procedimientos que exis- te en evitar que los coches vayan por direcciones indebidas (se- máforos, prohibiciones, multas, etc.).

Hay que prestar asimismo atención al problema que puede dar se en la validación de datos que pasan a un programa en el senti do de que se están realmente utilizando, debido a que se pueden haber producido entre tanto otros accesos asincronos o que el he cho de verificarlos haya modificado su contenido. Para evitar es te problema se adopta el principio de que los datos pasados por un usuario al programa puedan ser tocados una sola vez; el proce dimiento de validación consistiría en copias primeramente los da tos de un área segura (perteneciente al programa solicitado), -- comprobar que cumplen las condiciones pertinentes y, en caso --- afirmativo, utilizarlos de la copia.

Para la comprobación del correcto funcionamiento del sistema de protección, habrá de distinguir primeramente tres aspectos: La lógica seguida en el sistema de protección, el modo como ésta lógica se ha implantado y la forma como ésta lógica se está utilizando en la práctica.

El último aspecto es muy importante, pues podría darse el caso de que los programas de aplicación no hicieran un uso correcto o no se aprovecharan del sistema de protección

- NOMBRE
- UBICACION
    - DISPOSITIVO
    - DIRECCION DENTRO DE LA UNIDAD
- ORGANIZACION
- LONGITUD
- TIPO
- PROPIETARIO (O CREADOR)
- USUARIOS AUTORIZADOS

IDENTIFICACION.

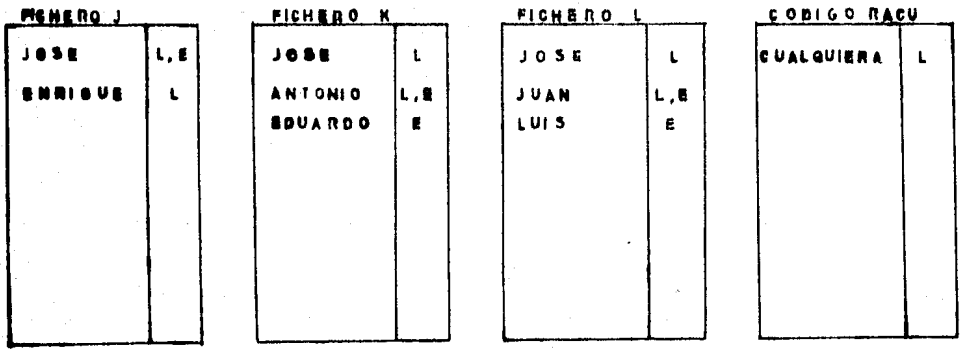
- ACCESOS AUTORIZADOS
    - LECTURA — TODO O PARTES
    - MODIFICA — DEL ARCHIVO
    - ESCRITURA
    - BORRA
- OTROS
    - CONTABILIDALES
    - NUMERO DE VERSION
    - ACTIVIDAD

DESCRIPTOR DE UN ARCHIVO CUADRO V.1

	FICHERO J	FICHERO K	FICHERO L	CODIGO RACU
JOSE	L E	L	L	L
ANTONIO		L E		L
JUAN			L E	L
EDUARDO		E		L
LUIS			E	L
ENRIQUE	L			L

L: EL SUJETO PUEDE LEER EL OBJETO
E: EL SUJETO PUEDE ESCRIBIR EN EL OBJETO

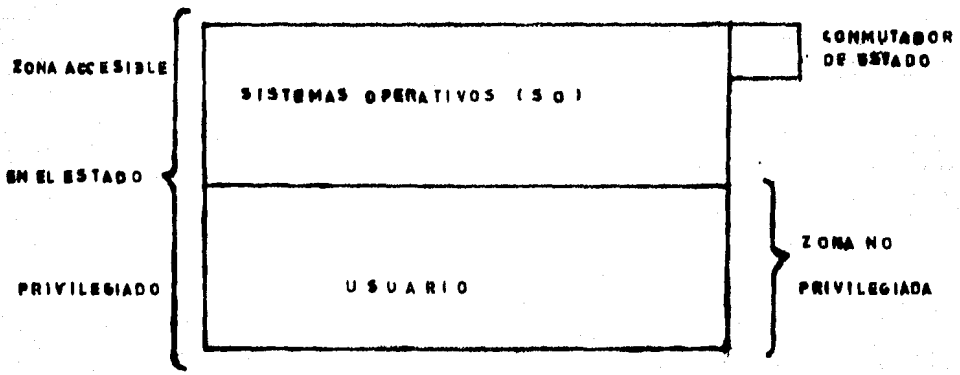
MATRIZ DE ACCESO
Cuadro V.2



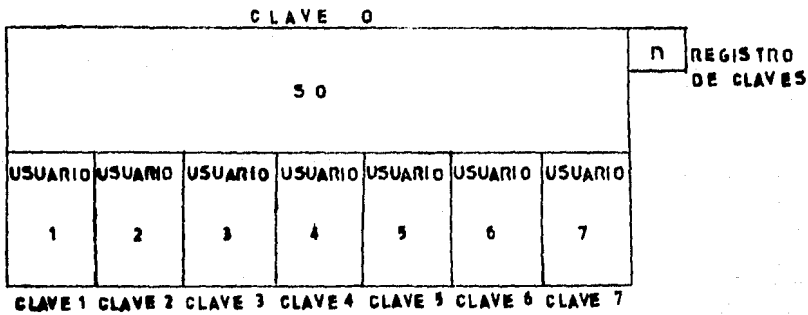
LISTAS DE CONTROL DE ACCESO
Cuadro V.3

JOSE	FICHERO J L E	FICHERO K L	FICHERO L L	CODIGO RACU L	
ANTONIO	FICHERO K L E	CODIGO RACU L			
JUAN	FICHERO L E	CODIGO RACU L			
EDUARDO	FICHERO K E	CODIGO RACU L			
LUIS	FICHERO L E	CODIGO RACU L			
ENRIQUE	FICHERO J L	CODIGO RACU L			

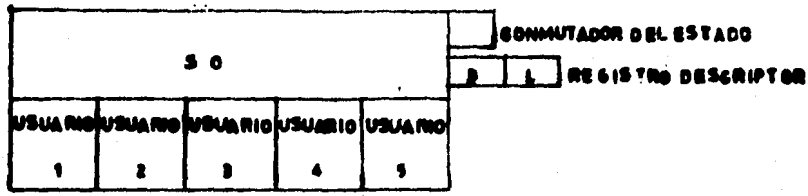
CAPACIDADES
Cuadro V.4

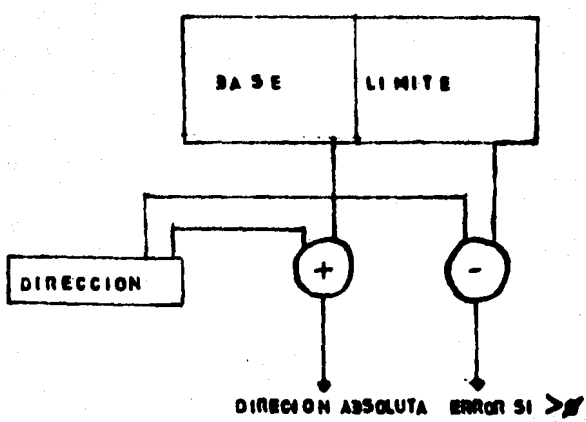


SISTEMA TODO O NADA
Cuadro V.5

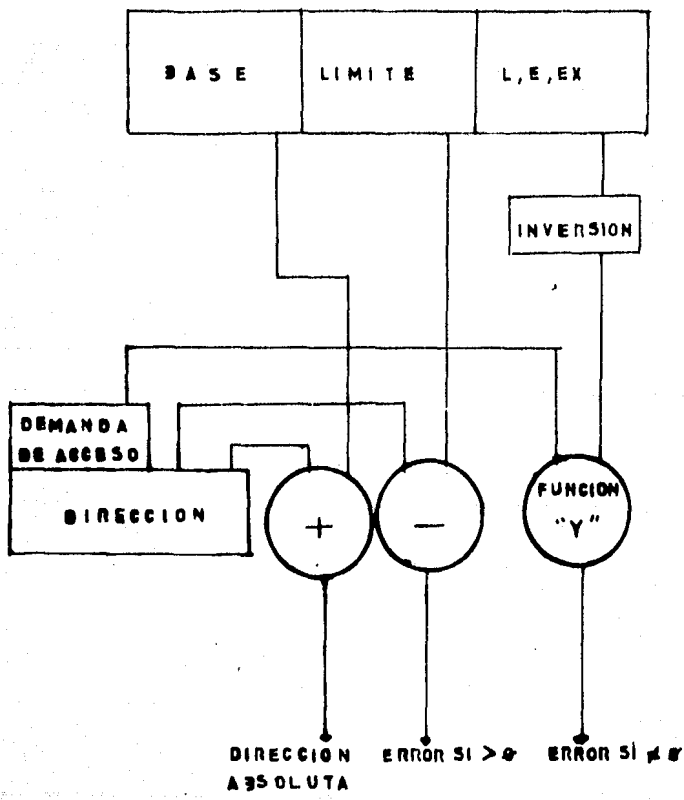


SISTEMA DE CLAVES NO JERARQUIZADAS
Cuadro V.6

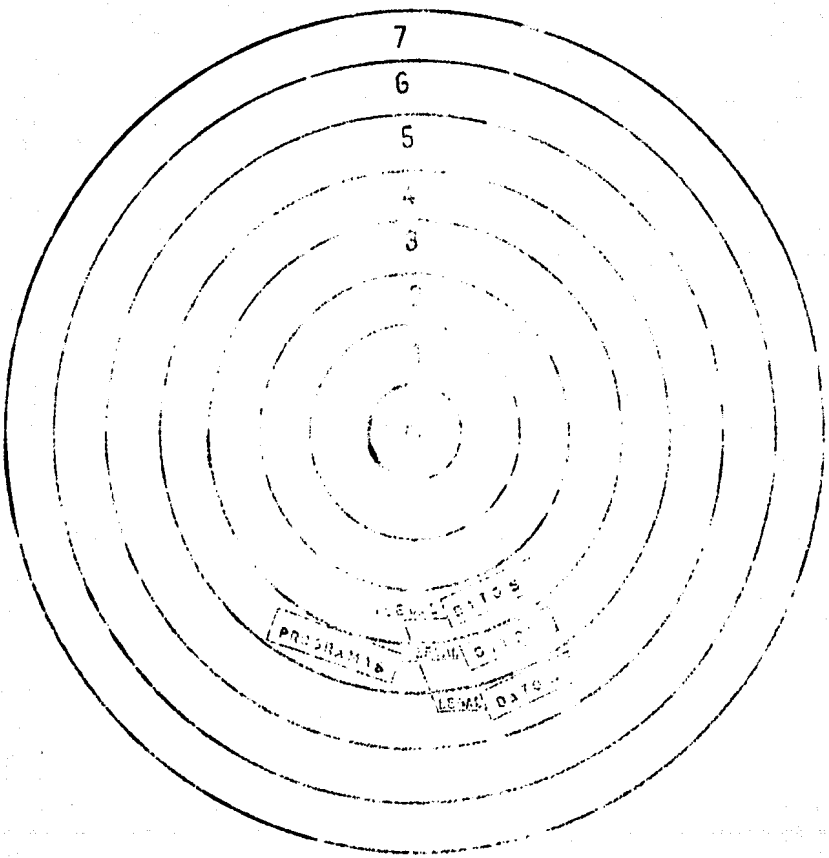




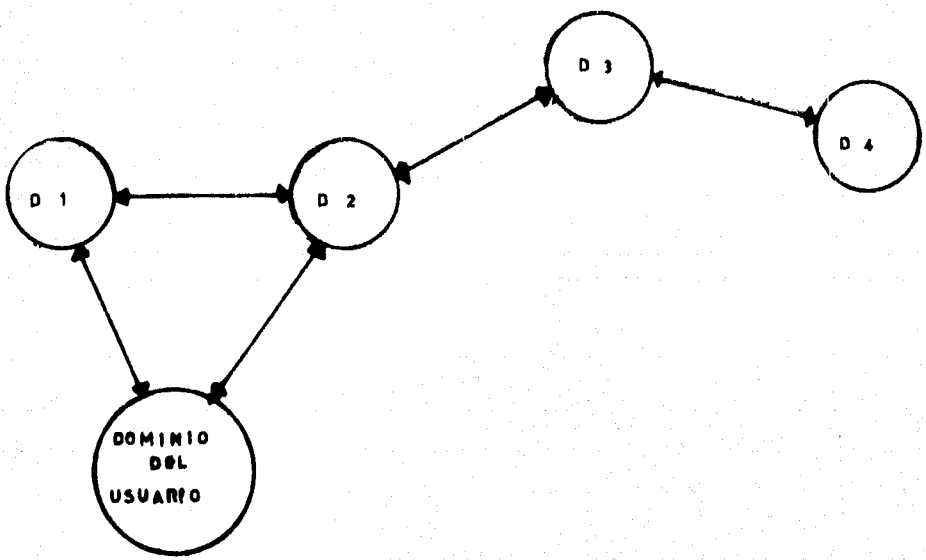
SISTEMA DE DESCRIPTOR UNICO
Cuadro V.7



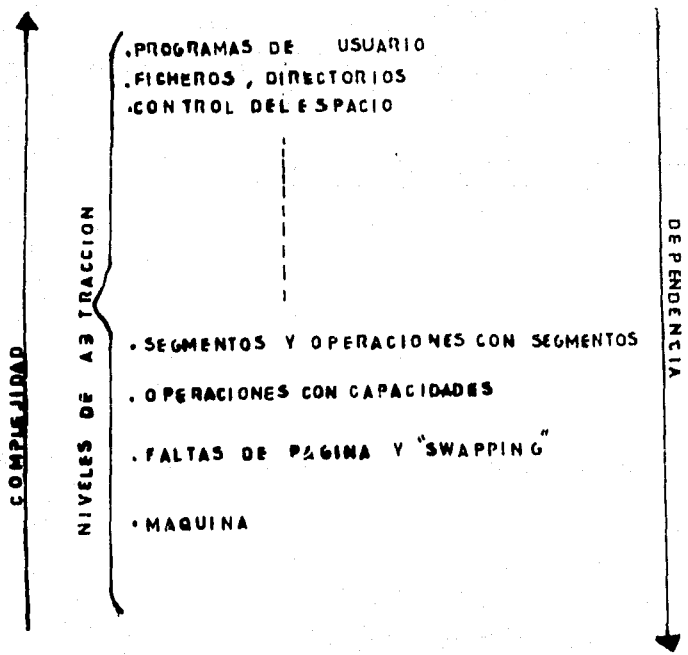
SISTEMA DESCRIPTOR CON CONTROLES DE ACCESO
Cuadro V.8



SISTEMA DE PROTECCION EN V-11
Cuadro V.9



DOMINIOS DISCRETOS DE PROTECCION
Cuadro V.10



CONSTRUCCION DE UN SISTEMA EN ANILLO
CON DEPENDENCIA UNIDIRECCIONAL ESTRICTA
Cuadro V. 11

C A P I T U L O V I

P R E V E N C I O N D E I N C E N D I O S .

Dado que el fuego es uno de los accidentes más frecuentes y de mayores consecuencias y que su probabilidad es mayor en la -- Sala de Computadoras, Almacenes y los Equipos de Aire Acondicionado, es imprendecible establecer una normativa detallada del manejo de materiales combustibles y de los equipos probables generadores del fuego, así como proceder a un diseño especial de la infraestructura de las instalaciones: paredes, suelos, ventanas, puertas, techos y revestimientos han de ser de material incombustible; división de las áreas importantes en compartimientos separados y resistentes a la propagación del fuego; prohibición de - fumar así como almacenamiento de papel usado y de material de papel en la Sala de Computadoras; Inspección periódica del cableado eléctrico; sistema de desconexión del suministro de fuerza y aire acondicionado; provisión de un sistema combinado de detección de incendios (por elevación de temperatura o por detección de gases de gases o humos) y de extinción de los mismos mediante utilización de gas carbónico (eficaz pero muy peligroso para el Personal y para los equipos, debido a un choque término elevado), agua pulverizada (requiere drenaje y puede producir cortocircuitos y daño a los equipos), espuma (eficaz pero difícil de eliminar) o halógenos (muy recomendables por ser eficaces no presentar peligros para las personas y no producir choques térmicos).

Detectores de humos.

Existen unos fenómenos determinados que preceden y acompañan al fuego; gases y vapores invisibles (aerosoles de combus---

tión) humos, visibles, llamas y brazas.

En la actualidad existen detectores capaces de reaccionar - ante cualquiera de los fenómenos señalados anteriormente y que - puedan clasificarse en dos grupos:

1.- Los que responden a los fenómenos que acompañan al in-- cendio.

Detectores térmicos (reaccionan ante variaciones de tempera tura).

Detectores de infrarrojos, ultravioletas (sensibles a las - llamas).

2.- Los que responden a los fenómenos que preceden al incen dio.

Detectores ópticos de humo (reaccionan ante los humos visi- bles).

Desde el punto de vista de seguridad, es evidente que siem- pre que sea posible, habrá que recurrir a aquellos detectores -- que respondan a las manifestaciones mínimas que preceden al fue- go, con el fin de conseguir una detección lo más rápida posible. Es por esta razón que el tema a que hago referencia se encuentra centrado en el segundo grupo.

Todos los detectores de este grupo se basan en el principio óptico según el cual, el humo que se interpone a un haz luminoso, o bien lo obscurece o bien lo refracta hacia una célula fotoeléctrica, activando la correspondiente señalización de alarma.

Los tipos de estos detectores son:

Detector puntual: Su funcionamiento consiste en la emisión de un haz de luz corto que es recogido por un receptor el obscurecimiento parcial que se produce en el rayo luminoso por el humo que se interpone entre el foco emisor de la luz y el receptor, basta para accionar la alarma cuando el obscurecimiento alcanza un valor crítico.

Otro tipo de detector óptico puntual, es el que funciona según el principio de refracción de la luz hacia una célula foto-- conductiva por la interposición de las partículas de humo. Este detector consta de una cámara, abierta a la atmósfera, con un foco de luz y una célula fotoconductiva, cuya posición impide que el haz que emite la fuente incida sobre ella. Cuando en el interior de la cámara se alcance una cantidad suficiente de partículas de humo, la luz se refracta e incide en la célula fotoconductiva, permitiendo que la célula active la señal de alarma.

Detector lineal: Su funcionamiento se basa en el Empleo de una fuente emisora y un receptor. Cuando el humo se interpone -- entre la fuente y la célula receptora, la cantidad de luz que --

llega a la fuente disminuye y activa la señal de alarma.

Como podemos ver, el inconveniente principal de los Detectores ópticos radica en la determinada cantidad de humo visible -- que necesitan para su activación.

Detectores iónicos: Su principio de funcionamiento se basa en la célula de detección que tiene como base el Empleo de una - fuente radioactiva. El elemento de acción es el aire ambiental - que por sus modificaciones químicas (naturaleza de los gases) o físicas (cambio molecular o de ionización). Actúa directamente - sobre la célula creando una modificación de estado eléctrico. La causa original de las transformaciones constitución de la atmósfera será, el principio de incendio (aerosoles de combustión).

Constitución elemental de una célula de detección. Bajo la acción de radiaciones emitidas de forma contínua por una substancia radioactiva, los gases se hacen conductores según el procedimiento siguiente: en el momento del paso de las radiaciones y -- principalmente de las partículas alfa a través de los gases, se producen en éstos iones gaseosos electrificados cargados positiva y negativamente. Si a éstos iones se les aplica con la ayuda de un campo eléctrico apropiado, un movimiento de conjunto al -- mismo tiempo que una velocidad determinada obtendremos en el gas una corriente eléctrica de intensidad medible. Si recubrimos la parte interior de un cilindro de hueco A (cuadro VI.I) de una --

sal radioactiva y si se establece un potencial acelerador entre el cilindro y un electrodo central B, un galvanómetro C nos demuestra que el circuito eléctrico se cierra, indicando así la aparición de una descarga lenta en el espacio interior del cilindro.

Se ha demostrado por medio de pruebas que el valor de la corriente medida varía en función del peso molecular de los gases, según las formas y enlaces moleculares de un mismo gas y según la intensidad del campo acelerador aplicado los resultados prácticos permiten considerar que cuando un cuerpo se encuentra en ignición, con o sin desprendimiento de humo, e incluso no produciendo más que débiles cantidades de calor, el estado físico de la atmósfera ambiente se modifica profundamente por ionización y por transformación de su composición gaseosa.

Los componentes de un equipo de detección de incendios deben cumplir las siguientes funciones:

A.- Detectar el Incendio. Esta detección se lleva a cabo mediante detectores iónicos que denotan la presencia de pequeñas cantidades de humo.

B.- Dan la alarma. Un impulso codificado es transmitido a la central de alarma de incendio por medio de un circuito de alarma controlado electrónicamente. El impulso es analizado y la alarma activada automáticamente, lo que permite no perder tiempo

para tomar las medidas de lucha contra incendios.

C.- Mandan a otras instalaciones. Puede también mandar automáticamente otras instalaciones para ayudar a combatir incendios o para mantener itinerarios de evacuación libres de humo. Puede mandar, por ejemplo, una instalación de surtidores (sprinklers), puertas, cortafuegos, puede abrir exutorios de humos, desconectar máquinas.

El sistema principal es conocido como Tarjeta Central y puede ser conectado a la red de 220 volts. la cual mediante la ayuda de un circuito de control electrónico es rectificada y estabilizada cumpliendo las siguientes funciones:

A).- Proporciona potencia a los circuitos de las diferentes tarjetas de línea conectadas a los detectores y pulsadores de alarma.

B).- Es la unidad de alimentación y carga de las baterías.

C).- Puede adicionalmente proporcionar potencia a los diversos equipos de protección contra fuegos, como por ejemplo, exutorios de humos, puertas, corta fuego, etc.

Siempre que la central esté conectada, se carga contínuamente la batería, de modo que dicha carga es verificada y monitorizada por una sección del sistema que detecta las posibles averí

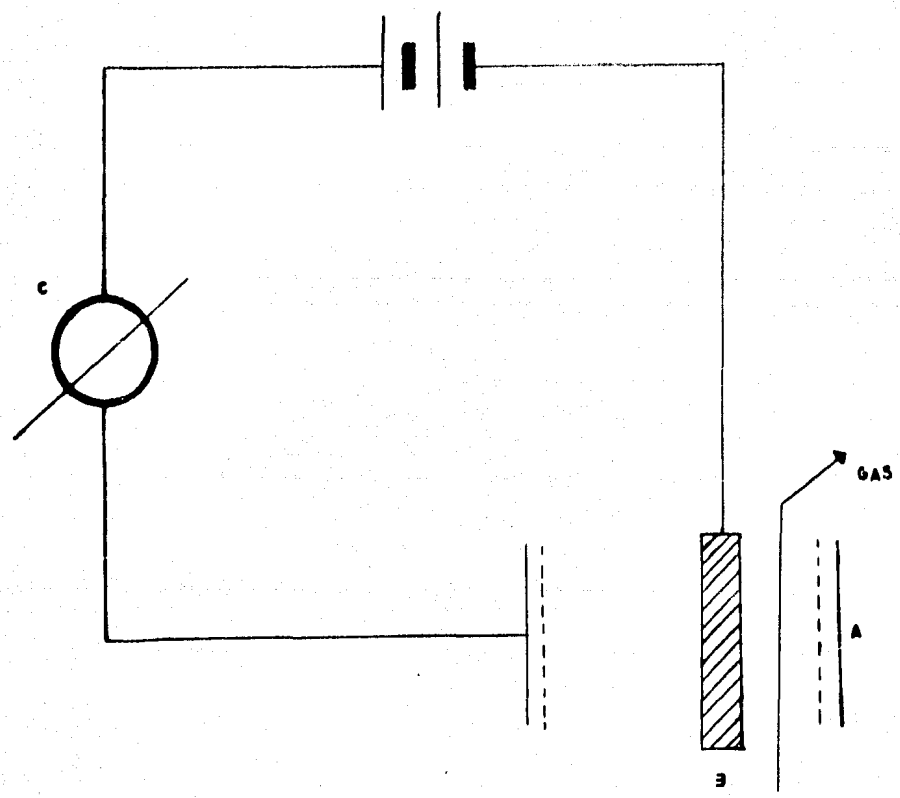
en la mencionada alimentación de corriente visualizándola mediante el Led correspondiente.

La tarjeta central recibe las señales de avería y/o alarma de dos tarjetas diferentes que son:

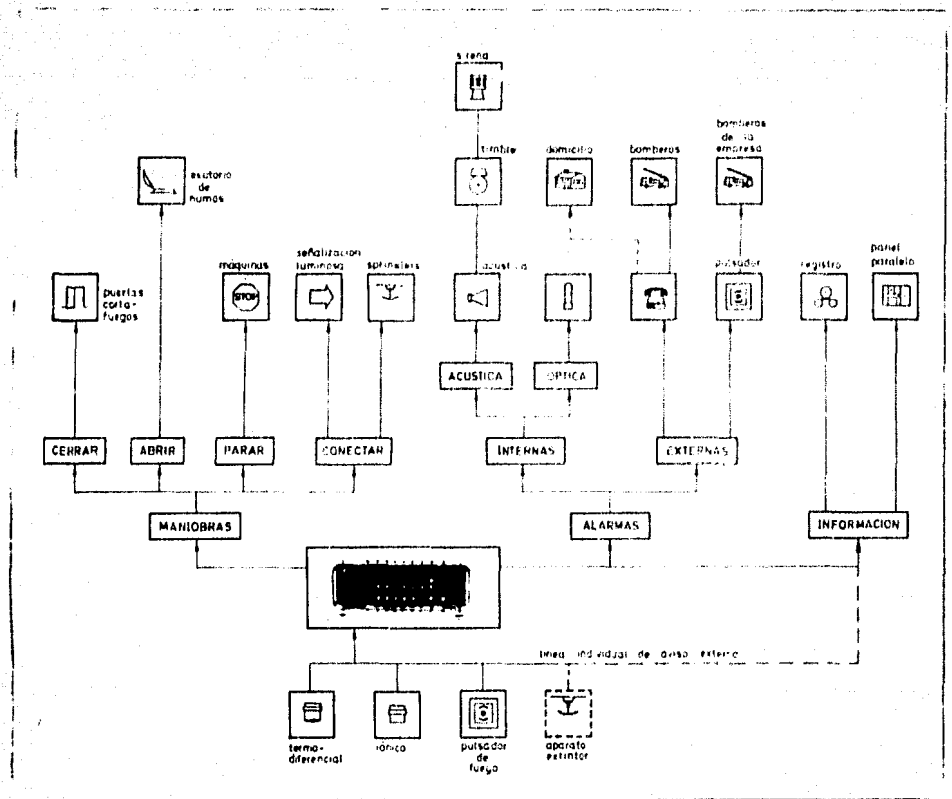
A).- Tarjeta de Verificación. A fín de conocer el Estado general de todo el sistema se incorporen este tipo de tarjetas mediante la cual se simulan situaciones de alarma y/o avería en cada una de las líneas de detección comprobando la respuesta de la central ante cada situación provocada. Para realizar esta función, la tarjeta de prueba dispone de un conmutador rotativo mediante el cual se selecciona la tarjeta de línea de detección en este tipo a verificar.

B).- Tarjeta de línea de detección. En este tipo de tarjetas se recibe la información de los detectores iónicos de humo, termodiferenciales y termomaximales, así como de pulsadores manuales de alarma.

Al recibir éstas señales se activan los equipos contra fuego a la vez que se visualiza mediante una led si se ha producido alarma en las líneas o averías en los circuitos tanto internos como externos, haciendo sonar un pequeño sumbador incorporado que avisa acústicamente al Personal que se encuentra en el Centro de Procesamiento de Datos.



ESQUEMA DE PRINCIPIO DEL
ELEMENTO DE DETECCION
Cuadro VI. 1



ESQUEMA DE FUNCIONES DE UN EQUIPO DE DETECCION DE INCENDIOS

CUADRO VI.2

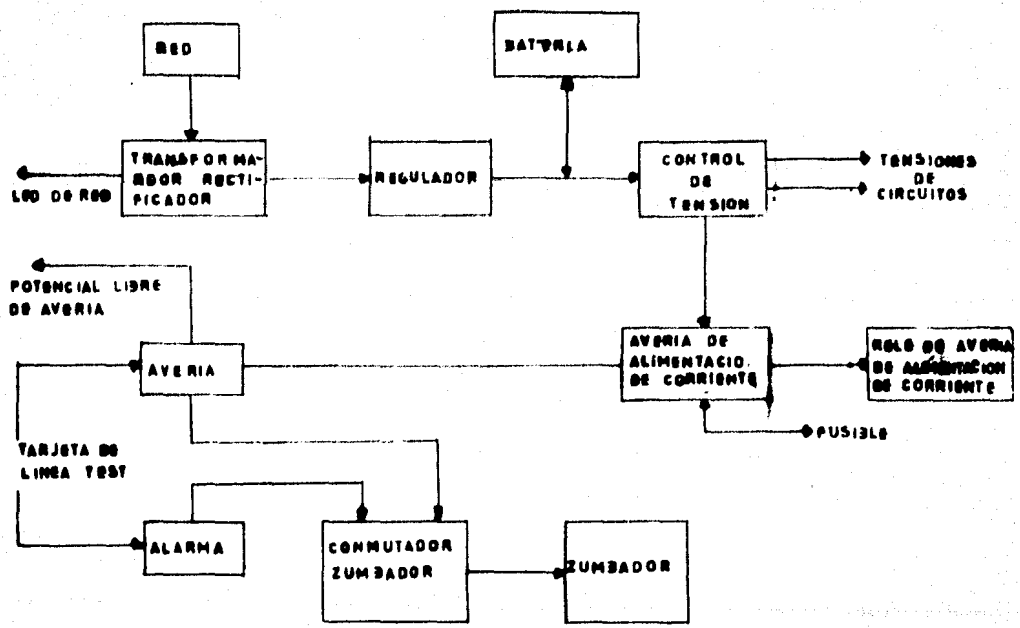
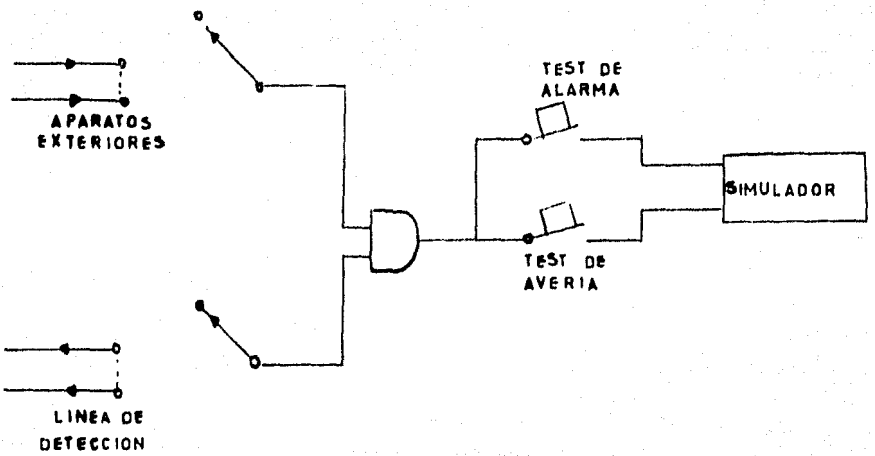


DIAGRAMA DE BLOQUES DE
LA TARJETA CENTRAL
Cuadro VI. 3



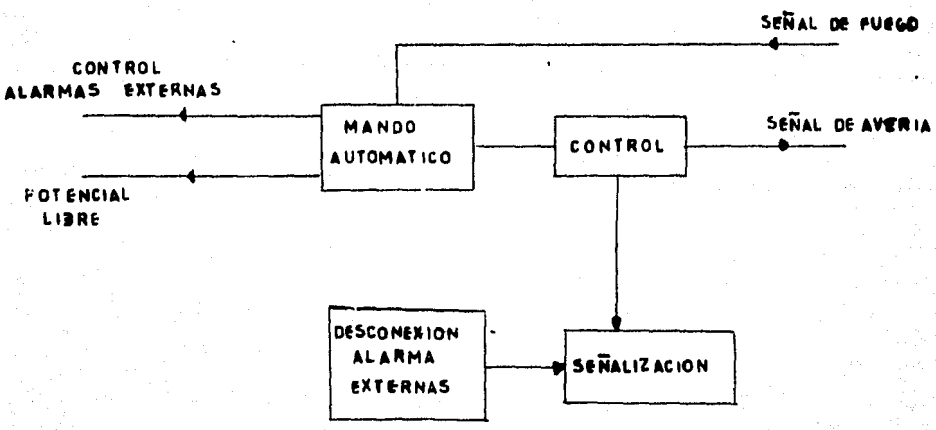


DIAGRAMA DE BLOQUES DE LA
TARJETA TEST
Cuadro VI. 4

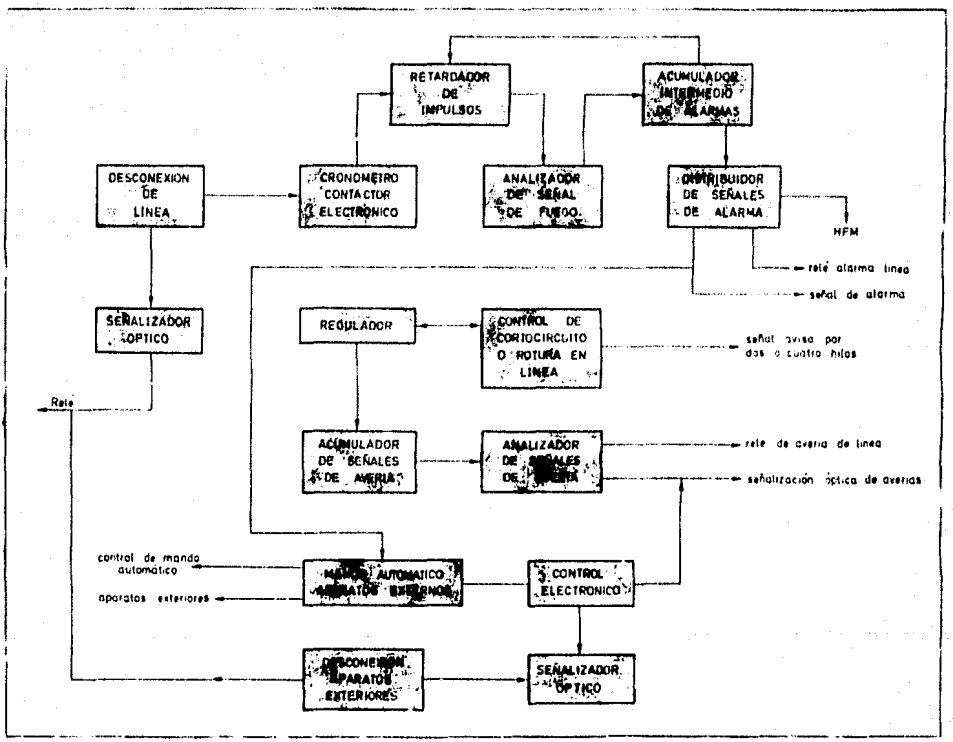


DIAGRAMA DE BLOQUES DE LA TARJETA DE LINEA

CUADRO VI.5

C O N C L U S I O N E S

La seguridad de la información y, en consecuencia, de los - equipos para el tratamiento de la misma (los equipos de Cómputo), así como de las instalaciones auxiliares y Edificio donde se ubica el Centro es una cuestión que llega a afectar a la Institución en lo referente a su administración e investigación que ésta realiza.

Desafortunadamente las Computadoras han sido y son instaladas todavía en sitios vulnerables, como son dentro de las Oficinas de un Departamento, y cuando se les construye un Edificio -- aparte tienen acceso tanto alumnos como Personas ajenas al Centro, que en un momento determinado pueden reconocer que este es el nervio central de la Institución, dado que normalmente maneja toda la información que se genera en ella, y que a menudo, es -- vulnerable a cualquier ataque, por no contar con un sistema de - seguridad eficáz.

Es por esta razón que el centro de Cómputo al no contar con un sistema de protección adecuado es vulnerable a agentes naturales y a múltiples ataques externos.

De entre los peligros naturales podemos señalar tanto al -- agua como al fuego, siendo este último probablemente, el más crítico, pudiendo afectar irreversiblemente tanto a los equipos como a los soportes de información, por lo contrario el agua por -

si sola no constituye un serio peligro y el calor por debajo - de 120 grados no es perjudicial, pero ambos elementos pueden -- causar serios problemas ya que las cintas magnéticas pueden ser destruídas por temperaturas de solo 54 grados cuando la humedad relativa es del 85 por ciento.

En lo referente a los ataques externos podemos señalar --- tres que son de suma importancia como son el Robo, Fraude y Sabotaje.

Las computadoras son posesiones muy valiosas de las empresas y estan expuestas al robo de la misma forma que lo están -- las piezas de almacen. Es frecuente que los operadores utilicen a la computadora para realizar trabajos privados a otras organizaciones y de ésta manera robar tiempo de máquinas.

Las tres principales áreas donde se produce el Fraude son:

1.- Manipulación de información de entrada, fácil de realizar y muy difícil de detectar, al ser de los métodos de validación de entrada simples y, en general conocidos por un gran número de personas en la Institución.

2.- Alteración o creación de Archivos de información. Se - alteran los datos directamente del Registro o se modifica algún programa para que realice la operación deseada.

3.- Transmisión ilegal. Interceptar o transferir información de teleproceso.

De los ataques externos el más temido por los Centros de Procesamiento de Datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel han encontrado que la protección contra el saboteador es el de los retos más duros; éste puede ser un Empleado o un sujeto ajeno a la propia Empresa.

Los imanes son herramientas muy recurridas; aunque las cintas estén almacenadas en el interior de su funda de protección, una ligera pasada y la información desaparece.

Cuando el equipo de Cómputo se encuentra a simple vista es, una invitación para el lanzamiento de bombas de fuego y otros proyectiles: suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado del falso suelo; líneas de comunicaciones y eléctricas pueden ser cortadas, en fin, un sinnúmero de daños pueden ocurrir si el Centro de Cómputo no está protegido debidamente.

Es por ésta razón que el problema de seguridad de la Computadora debe ser tratado como cualquier otro problema importante de la Institución. Los riesgos y peligros deben de ser identificados y evaluados, para conocer las posibles pérdidas y para que puedan ponerse en práctica los adecuados métodos de prevención.

En el presente trabajo se dan una serie de normas y reglas que se deben observar para la seguridad y protección del Hardware y Software así como de las instalaciones auxiliares y Edificio que ocupa el Centro de Cómputo.

Con esto pretendo que el Centro de Cómputo se le dé la importancia que merece, y a la vez contribuír en una mejora a la seguridad que éstos actualmente tienen.

B I B L I O G R A F I A .

DATA PROTECCION TECHNIQUES
INFOTECH INTERNATIONAL LTD
DICIEMBRE 1977

BASES PARA EL DISEÑO DEL SISTEMA DE SEGURIDAD DEL CENTRO.
SERVICIO TELEINFORMATICO DE GESTION
FEBRERO 1978

MUNDO ELECTRONICO
ROIXAREU EDITORES
DICIEMBRE 1981

INTRODUCCION AL PROCESAMIENTO DE DATOS
LAWRENCE S. ORILA
MO GRAW HILL
MAYO 1983

PROGRAMACION DE SISTEMAS
JONH J. DONOVAN
EL ATENEO

MANUAL DE ORGANIZACION
DIRECCION GENERAL DE INSTITUTOS TECNOLOGICOS
SEPTIEMBRE DE 1977

REUNION NACIONAL DE DIRECTORES DE LOS
INSTITUTOS TECNOLOGICOS
LEON, GUANAJUATO
MAYO 1983

APUNTES DEL CURSO DE ANALISIS Y DISEÑO DE SISTEMAS
I.B.M. DE MEXICO
MAYO 1977.