Universidad Nacional de Ingeniería

FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

"Seguridad y Plan de Contingencia en Centros de Informática"

Informe de Ingeniería

Para Optar el Título Profesional de :

INGENIERO DE SISTEMAS

Carmen Rosa Peña Enciso

Lima - Perú
1995

AGRADECIMIENTO.

A mis asesores,

en gratitud a los profesores

de mi Alma Màter la

Universidad Nacional de Ingeniería

y los que en forma desinteresada

y patriótica me han

apoyado en la elaboración

del presente trabajo; con

el que colaboro en el

desarrollo de la Ciencia

de la Informática.

INDICE

CAPITULO III

SEGURIDAD DE LA INFORMACION

CAPITULO IV

CONFIDENCIALIDAD DE LA INFORMACION EN LOS SISTEMAS DISTRIBUIDOS

CAPITULO V

CONTROLES DE DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACION

CAPITULO VI

OCURRENCIA DE DESASTRES

CAPITULO VII

VIRUS INFORMATICO

CAPITULO VIII

PLAN DE CONTINGENCIA

OFICINA DE SISTEMAS - 1993

SEDAPAL

PROYECTO DEL PLAN DE CONTINGENCIA

DESARROLLO DEL PROYECTO

INTRODUCCION

En los actuales momentos, en el Perú, diversas Instituciones cuentan con sofisticados Centros de Informática, que han permitido modernizar el trabajo y el producto obtenido, mejora en cantidad y calidad cada vez más creciente.

La seguridad como obligación compartida es fundamental, ya que los riesgos internos y externos atentan contra la vigencia institucional, impidiendo la continuidad y cumplimiento de las labores.

Dentro del contexto enunciado presento el trabajo de ingeniería **SEGURIDAD Y PLAN DE CONTINGENCIA EN CENTROS DE INFORMATICA**, producto de **seis años de servicio** en la Unidad de Producción, de la Oficina de Sistemas del Servicio de Agua Potable y Alcantarillado de Lima - SEDAPAL.

El propósito del trabajo, es contribuir a formar conciencia cívica en las instituciones en general y en SEDAPAL en particular para que cuenten con **Plan de Contingencia**, que permitan trabajar con tranquilidad y seguridad.

El trabajo consta de ocho capítulos:

En el primer capítulo se expone la necesidad de formular un **plan de contingencia** como objetivo eje el que lleva a enunciar la hipótesis de que un Plan de Contingencia asegura la operatividad de los sistemas de informática. Ambos planteamientos es el resultado del análisis de siniestros que destruyeron equipos e informaciones almacenados en los registros de los centros de informática a nivel mundial.

A continuación se expone la organización funcional de SEDAPAL, cuyo fin es brindar servicio de agua potable y alcantarillado a las provincias de Lima y Callao. Dentro de la organización, la Unidad de Producción procesa, mantiene y conserva la información de las unidades orgánicas de la Empresa, a través del centro de cómputo.

Luego se da a conocer las **técnicas y medidas de seguridad** que protegen las nuevas tecnologías de hardware, software y comunicaciones como núcleo de los centros de informática.

La **ocurrencia de los terremotos** se analizan como la causa que más daño provoca a los sistemas informáticos, ya que el suelo peruano se encuentra en el cinturón de fuego del Pacífico Sur. De igual manera recibe la acción directa de la placa de Nazca que se desplaza debajo de la placa continental y por

consiguiente genera continuos sismos.

El capítulo de **virus informático** merece especial atención por los graves problemas que afectan a los centros de informática ocasionando pérdidas materiales y horas hombre.

En el último capítulo se informa el **Plan de Contingencia de SEDAPAL**, que fue elaborado por los integrantes de la Oficina de Sistemas y que tiene dos años de vigencia. En la segunda parte del capítulo en mención y con la experiencia ganada presento un proyecto alternativo al primero, en base a visitas, entrevistas y encuestas aplicados a seis grupos de instituciones equipadas con centros de cómputo en la ciudad de Lima. En la mayoría de las Instituciones encuestadas trabajan Ingenieros de Sistemas, egresados de la Universidad Nacional de Ingeniería.

Finalmente subrayo que este trabajo constituye un paso más al desafiante reto de los investigadores de la ciencia de la informática, los que han de corregir errores y agregar omisiones, para que en un futuro cercano el **PLAN DE CONTINGENCIA**, sea el valuarte de seguridad de los Centros de Informática.

Carmen Rosa Peña Enciso.

CAPITULO I

GENERALIDADES

1. ANTECEDENTES

El 24 de Marzo de 1980 se dió a conocer en la revista COMPUTERWORLD un siniestro de incendio que destruyó los equipos sofisticados de cómputo y toda la documentación e información almacenada en los registros de la Corporación General Computer Services; localizada en Huntsville, Estado de Alabama de los Estados Unidos de Norteamérica.

A pesar de las pérdidas sufridas la corporación logró cumplir su compromiso con sus clientes gracias a que existían casi todos los programas softwares cerca de Birmingham gracias a que un vendedor de procesamiento remoto había instalado un sistema de respaldo con todos los datos que la corporación había perdido en el siniestro.

El presidente de la corporación frente a los problemas de reinstalación y reconstrucción del

sistema de comunicaciones declaró: **Cualquier cosa que pueda fallar, fallará.**

En el Perú en diversas ciudades vienen ocurriendo siniestros. Dos casos se relacionan con el tema: **El incendio de Hogar S.A.** (20 Julio 1990) y el **sospechoso fuego del Banco Minero** (1991).

El relato dado por Alberto Villa, subgerente de Sistemas de Hogar S.A., se publicó en la revista PC 2000 POPULAR COMPUTER. En síntesis dice: "La información del día y de los días anteriores. Todo ello estaba en cintas de backup (copias de respaldo) listas para ser llevado a un lugar seguro...". [1]

La noche del 20 de julio de 1990 un gran incendio acabó con las mercaderías y el centro de cómputo de la tienda principal Hogar S.A. en San Isidro. Termina su informe dando recomendaciones para prevenir contingencias.

Entonces **¿Cómo una cinta backup salvó a HOGAR?**. Un trabajador de dicha empresa por casualidad llevó la cinta de backup, y con ella se reconstruyó la información completa de Hogar S.A.

El caso del Banco Minero, **sospechoso fuego**, se informa: "En lo que se refiere al Banco Minero, la ausencia de la documentación que identifica a los

[1] PERIODISTAS: Revista, PC 2000, Popular Computer, Julio 1990.

deudores aparentemente desapareció por completo durante el misterioso incendio que devoró parte de sus antiguas oficinas en 1991". [2]

"El 12 de octubre de 1985, el New York Times publicó un artículo sobre un hombre que había cargado, por teleproceso, un programa desde un sistema informático de tablón de anuncios en Long Island. El programa se llamaba EGABTR y estaba supuestamente diseñado para aumentar notablemente la prestación de cualquier compatible con IBM con tarjeta gráfica EGA. En vez de ello, mientras distraía al usuario con una presentación en pantalla, el programa borró de forma sistemática todos los archivos del disco duro. Para empeorar las cosas, el programa terminó lanzando en la pantalla de la desventurada víctima la frase **Arf! Arf! Got You**". [3]

"Otra de las causas de pérdida de datos son los terremotos ocasionales. Tras el terremoto del año pasado en Los Angeles, muchos expertos esperaban encontrar sistemas principales tendidos **patas arriba** en salas informáticas demolidas. No fue así. Los daños más importantes se produjeron en PC, que quedaron

---

[2] DIAZ, MIGUEL: La República, 10 Octubre 1995, p. 45.

[3] LEVIN, RICHARD B.: Virus Informáticos, Mc Graw-Hill Interamericana de España, S.A., 1991, p. xxi.

destruidas o abandonadas en edificios destrozados en los que no se podía entrar.

Cuando la tierra empieza a temblar, la unidad de cinta de su PC de tipo medio no va a pararla, decía refiriéndose a la seguridad de la empresa Larson de IBM. En el reciente terremoto de California del Sur, muchos usuarios perdieron el acceso a sus PC y copias de seguridad. Una de las personas que está de acuerdo con esta conclusión es Scott Cumbie, experimentado administrador de almacenamientos desde hace 11 años en Providan Corp. y miembro del Storage Management Steering Commitee del grupo de usuarios SHARE que está estudiando los problemas de gestión de almacenamiento que las empresas van a encontrar en el futuro." [4]

Los problemas descritos nos muestran la enorme importancia de la seguridad de la información por cuanto los sistemas de información mecanizados de toda empresa se han convertido en el centro nervioso de todo el negocio.

El presente trabajo trata fundamentalmente sobre este tema de capital importancia que debe tenerse en cuenta en la elaboración de un **Plan de Contingencia.**

---

[4] MORRISON, DAVID: Practicando el Almacenamiento Seguro, Software Quarterly, Invierno 1994/1995, p. 37,38.

2. OBJETIVOS GENERALES

Analizando la repercusión de los siniestros; sea incendios, sismos y vandalismos; que destruyen todo centro de informática se plantea los siguientes objetivos generales:

2.1 Formular un **Plan de Contingencia** que asegure la continuidad operativa de los Centros de Informática.

2.2 Capacitar al personal profesional y técnico que laboren en los centros de cómputo de las empresas para conseguir una alta producción y productividad.

2.3 Lograr que las computadoras y materiales a usarse en los sistemas de seguridad informática sean el producto de la más alta calidad científica y técnicas modernas.

2.4 Construir ambientes adecuados donde se instalen los centros de cómputo acorde con los adelantos de la ingeniería civil y los requerimientos de los sistemas de informática.

3. HIPÓTESIS

El planteamiento de los objetivos lleva a enunciar las siguientes hipótesis:

3.1 Los **planes de contingencia** aseguran la operatividad de los sistemas de informática.

3.2 Todo programa debe contar con un sistema de respaldo que permita el funcionamiento del trabajo sin interrupciones.

3.3 El personal que labore en los sistemas de informática debe estar integrado por profesionales y técnicos calificados y confiables.

3.4 Las computadoras y materiales a usarse en los sistemas de informática deben estar de acuerdo con el avance de la ciencia y técnicas modernas.

4. METODOS, TECNICAS Y PROCEDIMIENTOS

El trabajo se desarrolla dentro del contexto social y económico, por tanto se aplicarán los métodos analítico y sintético.

Los métodos permitirán analizar los sistemas de

seguridad de los centros de cómputo, al personal, equipos y materiales. De igual manera los problemas y posibles soluciones para asegurar el trabajo de las empresas.

En el proceso de desarrollo de la tesis se analizará la bibliografía adecuada en trabajo de gabinete y mediante visitas y entrevistas se conocerán los problemas in situ a fin de plantear las posibles soluciones en cada caso.

5. ALCANCES

El propósito de este trabajo, es brindar información técnica necesaria para la preparación de **planes de contingencia** para los centros de informática, que brinden una respuesta efectiva en el manejo masivo de activos después de una catástrofe.

En base a la estructura existente del sistema de cómputo de cada empresa en el país, el presente trabajo trata de analizar los fundamentos que permitan la preparación y coordinación de planes de contingencia adecuados a la infraestructura de cómputo a fin de manejar de manera inmediata y adecuada las necesidades que surjan en casos de amenazas naturales y humanas desde el punto de información más simple hasta los centros de información más complejas.

CAPITULO II

SERVICIO DE AGUA POTABLE Y ALCANTARILLADO DE LIMA - SEDAPAL

ORGANIZACION Y FUNCIONES

1. GENERALIDADES

El agua es vida, es la expresión del hombre del campo y la ciudad; por cuya razón los analistas en recursos naturales han estudiado y planificado el uso racional del agua.

El Congreso del Perú a través de las diversas Constituciones Políticas ha legislado y definido que el agua como recurso natural es "patrimonio de la Nación. El Estado es soberano en su aprovechamiento. Por Ley orgánica se fija las condiciones de su utilización y de su otorgamiento a particulares. La concesión otorga a su titular un derecho real, sujeto

a dicha norma legal". [5]

Actualmente los pueblos del Perú, esperan con preocupación la nueva Ley General de Aguas ya que se enmarca dentro del proceso de privatización como política del gobierno de turno reflejo de la expansión del Capitalismo en el Tercer Mundo.

2. LA POBLACION DE LIMA Y CALLAO

Antes de la invasión española los grupos humanos autóctonos asentados en las llanuras del Rímac, Chillón y Lurín utilizaron las aguas de manantiales y de los ríos de dichos valles con técnicas hidráulicas muy avanzadas para esa época los que han sido destruídos por la expansión urbana cada vez más creciente.

Desde la fundación de la ciudad de Lima en 1535 hasta el presente se han multiplicado diversos problemas, así tenemos: la explosión demográfica, ocupación indiscriminada de las áreas agrícolas, contaminación del suelo, agua y atmósfera; los que a su vez han generado otros problemas en cadena cada vez más graves.

El agua corriente del río Rímac que se usaba para consumo humano en los albores de la colonia, muy pronto se contaminó y las autoridades se vieron obligadas

[5] CONSTITUCION POLITICA DEL PERU 1993: TITULO III DEL REGIMEN ECONOMICO CAPITULO II DEL AMBIENTE Y LOS RECURSOS NATURALES, Artículo 66, p.22-23.

a captar el agua de los manantiales y puquiales de la Atarjea.

Con el tiempo el sistema de conducción del agua quedó obsoleto y para superar este nuevo problema se creó la primera Empresa de Agua de Lima.

Posteriormente se denominó Empresa de Saneamiento de Lima, que integraba la Dirección General de Obras Sanitarias del Ministerio de Vivienda hasta que por Decreto Legislativo Nº 150 el 12 de Junio de 1981 se transforma en Servicio de Agua Potable y Alcantarillado de Lima - SEDAPAL y así funciona hasta el presente.

3. ENTORNO EMPRESARIAL DEL SERVICIO DE AGUA POTABLE Y ALCANTARILLADO DE LIMA - SEDAPAL

3.1 NATURALEZA

El presente trabajo ha sido aplicado a una Empresa de propiedad del Estado, de Derecho Público Interno, Sector Presidencia, con autonomía técnica, administrativa, económica y financiera. Sus servicios son de necesidad y utilidad públicas, y de interés social.

3.2 MISION - OBJETO

Brindar servicios de Agua Potable y Alcantarillado (captación/extracción, aducción/

conducción, tratamiento, almacenamiento y distribución de agua; y recolección, tratamiento y disposición de desagües).

3.3 OBJETIVOS

- Brindar un mejor servicio a la colectividad, en cantidad, calidad y oportunidad.
- Acercar (desconcentrar) progresivamente sus servicios al cliente.
- Simplificar, desburocratizar y hacer más austera su administración.
- Asumir criterios y mecanismos de flexibilidad estructural y funcional, que hagan posible una dinámica gestión institucional

3.4 RESPONSABILIDAD - FUNCION GENERAL

- Ejecutar la política del Sector en la operación, mantenimiento, control y desarrollo de los servicios, con funciones específicas en los aspectos de normatividad, programación, planeamiento, elaboración de proyectos, financiación, ejecución de obras, asesoría y asistencia técnica.

3.5 JURISDICCION GEOGRAFICA

- Provincias de Lima y Callao.

AMBITO GEOGRAFICO DE SEDAPAL

1,994

SERVICIO DE AGUA POTABLE :

AREA SERVIDA : 33,152 Hás.
LONG. DE LA RED : 7,121 Kms.

PROV. HUARAL
PROV. CANTA
PROV. HUAROCHIRI
CARABAYLLO
RIO CHILLON
ANCON
LURIGANCHO
CHACLACAYO
CIENEGUILLA
SAN JUAN DE LURIGANCHO
RIO RIMAC
PUENTE PIEDRA
COMAS
ATE
SANTA ANITA
LA MOLINA
VENTANILLA
LOS OLIVOS
INDEPENDENCIA
EL AGUSTINO
RIMAC
SAN LUIS
VILLA MARIA DEL TRIUNFO
RIO LURIN
LURIN
SAN MARTIN DE PORRES
LA VICTORIA
SAN BORJA
CERCADO
PACHACAMAC
CALLAO
SAN JUAN MIRAFLORES
VILLA EL SALVADOR
SANTIAGO DE SURCO
CHORRILLOS
PTA. HERMOSA
PTA. NEGRA
N. M.

OCEANO PACIFICO

Servicio de Agua Potable y Alcantarillado de Lima

SEDAPAL

3.6 ESTRUCTURA ORGANIZATIVA

ORGANOS DE DIRECCION

JUNTA EMPRESARIAL

DIRECTORIO

GERENCIA GENERAL

ORGANO DE CONTROL

OFICINA DE AUDITORIA INTERNA

ORGANOS DE APOYO

OFICINA COMERCIAL

- Unidad de Desarrollo Comercial
- Unidad de Facturación y Cobranzas

OFICINA DE SISTEMAS

- Unidad de Diseño de Sistemas
- Unidad de Producción
- Unidad de Información Gerencial

OFICINA DE RELACIONES PUBLICAS

OFICINA DE SECRETARIA GENERAL

OFICINA GENERAL ADMINISTRATIVA FINANCIERA

OFICINA DE LOGISTICA

Unidad de Abastecimientos

Unidad de Servicios Generales

Unidad de Seguridad Integral

OFICINA DE RECURSOS HUMANOS

Unidad de Personal

Unidad de Relaciones Laborales

OFICINA FINANCIERA

Unidad de Tesorería

Unidad de Contabilidad

Unidad de Presupuesto

OFICINA GENERAL DE PROYECTOS Y OBRAS

Equipo de Proyectos

Equipo de Obras I

Equipo de Obras II

ORGANOS DE ASESORAMIENTO

OFICINA DE ASESORIA JURIDICA

OFICINA GENERAL DE DESARROLLO

Equipo de Plan Maestro

Equipo de Plan Empresarial

ORGANOS DE LINEA DESCONCENTRADOS - PRODUCCION

GERENCIA DE PLANTA

Unidad de Protección de Instalaciones

División de Operación de Planta

División de Mantenimiento de Planta

GERENCIA DE AGUAS SUBTERRANEAS

Unidad de Control Operacional

División de Mantenimiento de Pozos

División de Mantenimiento de Equipos

GERENCIA DE REDES PRIMARIAS Y DISPOSICION FINAL

Unidad de Control Operacional y Catastro

Unidad de Evaluación de Calidad

División de Distribución Primaria

División de Recolección y Disposición Final

ORGANOS DE LINEA DESCONCENTRADOS - ZONALES

GERENCIA ZONAL NORTE

Centro de Servicios "Puente Piedra"

Unidad Administrativa

Unidad Técnica

División de Operación y Mantenimiento

División Comercial

GERENCIA ZONAL SUR

Unidad Administrativa

Unidad Técnica

División de Operación y Mantenimiento

División Comercial

GERENCIA ZONAL ESTE

Centro de Servicios "San Juan de Lurigancho"

Centro de Servicios "La Molina"

Unidad Administrativa

Unidad Técnica

División de Operación y Mantenimiento

División Comercial

GERENCIA ZONAL OESTE

Unidad Administrativa

Unidad Técnica

División de Operación y Mantenimiento

División Comercial

GERENCIA ZONAL CENTRO

Unidad Administrativa

Unidad Técnica

División de Operación y Mantenimiento

División Comercial

GERENCIA ZONAL CALLAO

Unidad Administrativa

Unidad Técnica

División de Operación y Mantenimiento

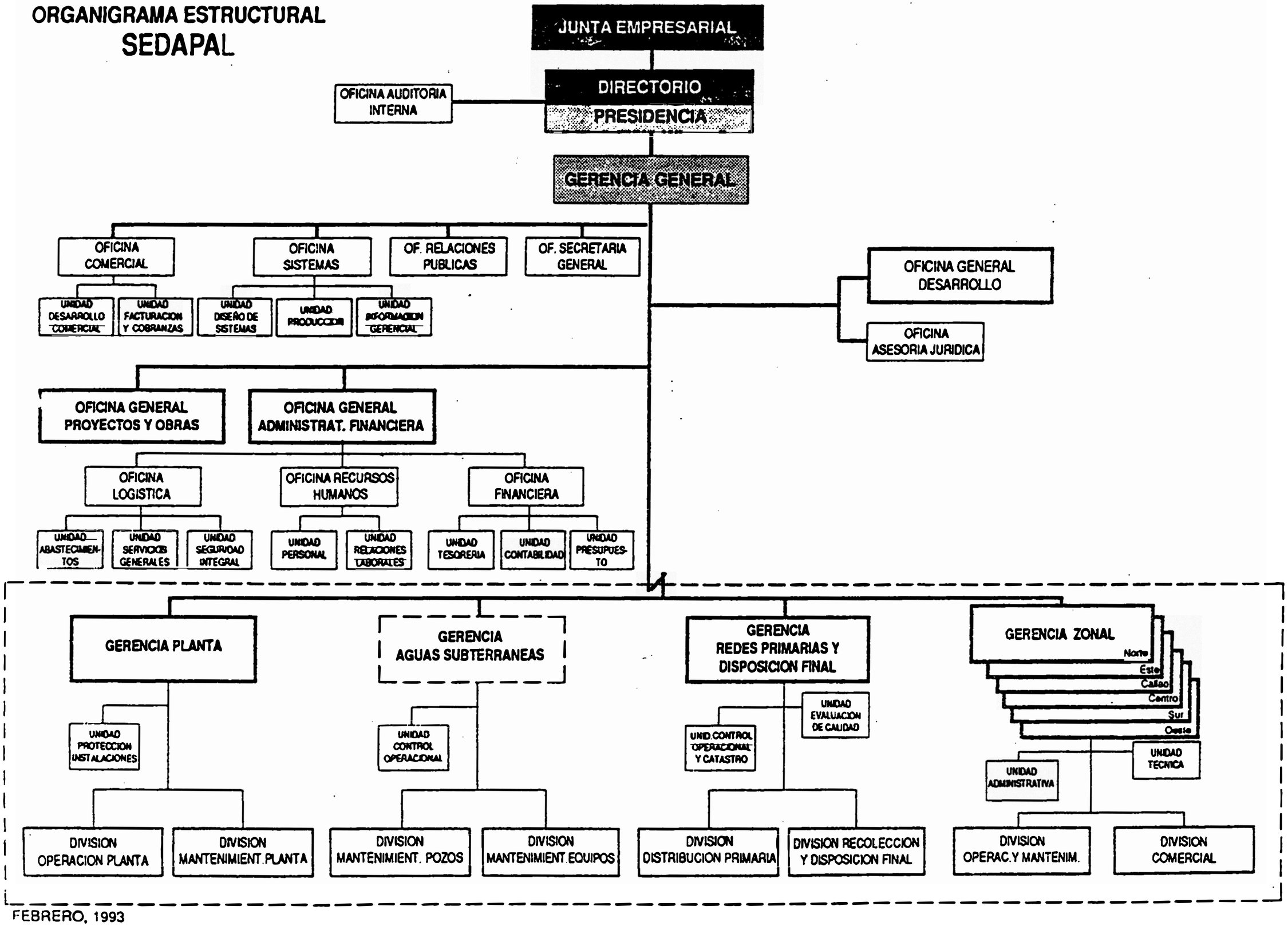
División Comercial

3.7 FUNCIONES GENERALES COMUNES DE LAS UNIDADES ORGANICAS

Además de las propias, las Unidades Orgánicas tienen la responsabilidad de las siguientes funciones:

- Formular, proponer, implantar y evaluar las políticas, normas, planes y programas comprendidos en el ámbito de su competencia, así como controlar su ejecución.
- Cumplir y hacer cumplir las disposiciones legales y normativas vigentes, con rela-ción a sus actividades.
- Suministrar la información y documentación procesada, de acuerdo a la normatividad y sistemas establecidos.
- Conducir las acciones comprendidas en el Sistema de Información Institucional, en el ámbito de su competencia.
- Desempeñar las demás funciones que, en el ámbito de su competencia,le sean asignadas

ORGANIGRAMA ESTRUCTURAL
SEDAPAL



FEBRERO, 1993

4. ORGANIZACION Y FUNCIONES GENERALES ORGANO DE APOYO:

OFICINA DE SISTEMAS

4.1 FINALIDAD

Establecer la Organización y Funciones Generales de la Oficina de Sistemas, así como las funciones de las Unidades Orgánicas que la conforman.

4.2 OBJETIVO GENERAL

Coadyuvar en el desarrollo de la gestión y toma de decisión Institucional, a través del diseño integrado de los Sistemas, el procesamiento actualizado de información así como de la producción y suministro de la información y Estadística Gerencial.

4.3 FUNCIONES GENERALES

- Formular, proponer, implantar y evaluar las políticas, normas, planes y programas comprendidos en el ámbito de su competencia, así como controlar su ejecución.
- Planificar, conducir, controlar y evaluar el diseño, desarrollo, implementación y mantenimiento de los Sistemas Organizativos e Informáticos, y de la normatividad correspondiente.

- Planificar, conducir y controlar el equipamiento, operatividad y mantenimiento de los medios de computación, dispositivos auxiliares e información procesada.
- Planificar, conducir y evaluar la identificación de las necesidades y la estructuración, desarrollo, ejecución e integración de los Sistemas Institucionales.
- Conducir las acciones de regulación y control de la asignación y utilización de equipos de microcomputación, programas productos, aplicaciones informáticas y dispositivos auxiliares.
- Conducir, controlar y proporcionar la Información Estadística y Gerencial y la Memoria Anual.
- Cumplir y hacer cumplir las disposiciones legales y normativas vigentes, con rela-ción a las actividades de la Oficina.
- Suministrar la información y documentación procesada en la Oficina, de acuerdo a la normatividad y sistemas establecidos.
- Conducir las acciones comprendidas en el Sistema de Información Institucional, en el ámbito de su competencia.

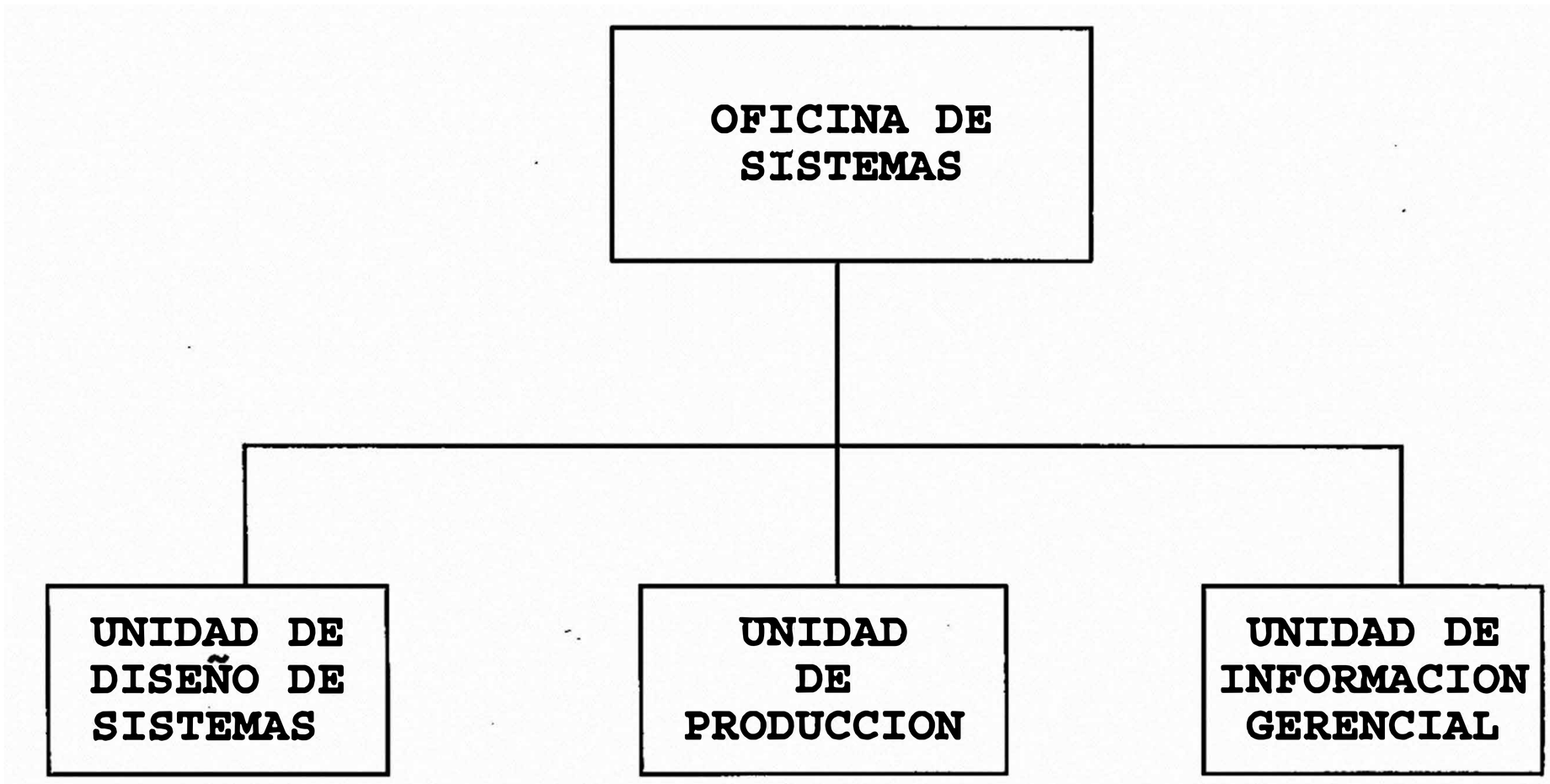
- Desempeñar las demás funciones que, en el ámbito de su competencia, le sean asigna-das por la Gerencia General.

4.4 ESTRUCTURA ORGANICA

La Estructura Orgánica de la Oficina está configurada por las siguientes Unidades Orgánicas:

- Unidad de Diseño de Sistemas
- Unidad de Producción
- Unidad de Información Gerencial

4.5 ORGANIGRAMA ESTRUCTURAL



4.6 LINEA DE DEPENDENCIA

La Oficina de Sistemas depende directamen-te de la Gerencia General.

4.7 LINEAS DE COORDINACION INTERNA

La Oficina de Sistemas mantiene coordinación interna con todas las Unidades Orgánicas.

4.8 LINEAS DE COORDINACION EXTERNA

La Oficina de Sistemas mantiene coordinación externa con el Instituto Nacional de Estadística e Informática (INEI), Instituto Nacional de Administración Pública (INAP), Proveedores de Servicios de Computación y las demás Instituciones y Entidades Externa que, por la Naturaleza de sus funciones, le son afines y/o necesarias.

5. ORGANIZACION Y FUNCIONES GENERALES :

UNIDAD DE DISEÑO DE SISTEMAS

5.1 OBJETIVO

Garantizar el nivel deseado de soporte y asistencia técnica en los asuntos relacionados con el diseño y desarrollo de la normatividad administrativa de los sistemas integrales de informática institucional.

5.2 FUNCIONES GENERALES

- Formular, proponer, implantar y evaluar las políticas, normas, planes y programas com-

prendidos en el ámbito de su competencia, así como controlar su ejecución.

- Formular y proponer el diseño y desarrollo de los Sistemas Integrales Informáticos de la Empresa.
- Desarrollar las acciones de racionalización administrativa de los procesos y procedimientos informáticos.
- Formular y mantener actualizadas las normas de gestión informática.
- Determinar, dar soporte y ejecutar las acciones de diseño, programación, implementación y mantenimiento de los sistemas y/o aplicaciones informáticas.
- Cumplir y hacer cumplir las disposiciones legales y normativas vigentes, con relación a las actividades de la Unidad.
- Suministrar la información y documentación procesada en la Unidad, de acuerdo a la normatividad y sistemas establecidos.
- Conducir las acciones comprendidas en el Sistema de Información Institucional, en el ámbito de su competencia.
- Desempeñar las demás funciones que, en el ámbito de su competencia, le sean asignadas por la Oficina de Sistemas.

5.3 ESTRUCTURA ORGANICA

La Unidad de Diseño de Sistemas no cuenta con Unidades Orgánicas dependientes.

5.4 LINEA DE DEPENDENCIA

La Unidad de Diseño de Sistemas depende directamente de la Oficina de Sistemas.

5.5 LINEA DE COORDINACION INTERNA

La Unidad de Diseño de Sistemas mantiene coordinación interna con todas las Unidades Orgánicas.

5.6 LINEA DE COORDINACION EXTERNA

La Unidad de Diseño de Sistemas mantiene coordinación externa, a través de la Oficina de Sistemas, con las Instituciones y Entidades Externas que, por la naturaleza de sus funciones, le son afines y/o necesarias.

6. ORGANIZACION Y FUNCIONES GENERALES :

UNIDAD DE PRODUCCION

6.1 OBJETIVO

Lograr la atención eficaz y oportuna de los requerimientos de procesamiento, mantenimiento y

conservación de información de las Unidades Orgánicas de la Empresa, a través del equipo de cómputo central.

6.2 FUNCIONES GENERALES

- Formular, proponer, implantar y evaluar las políticas, normas, planes y programas comprendidos en el ámbito de su competencia, así como controlar su ejecución.
- Desarrollar las acciones de elaboración del calendario de producción, atención oportuna de requerimientos, evaluación de la documentación y preparación de datos, a nivel del equipo central de cómputo.
- Efectuar las acciones de operación del equipo central de cómputo, así como de la obtención de información y de copias de respaldo.
- Desarrollar las acciones de seguridad y conservación de los archivos de información en medios magnéticos, así como de los materiales y suministros requeridos en la producción.
- Desarrollar las acciones de control y evaluación del uso y mantenimiento del equipo central de cómputo y periféricos.

- Cumplir y hacer cumplir las disposiciones legales y normativas vigentes, con relación a las actividades de la Unidad.
- Suministrar la información y documentación procesada en la Unidad, de acuerdo a la normatividad y sistemas establecidos.
- Conducir las acciones comprendidas en el Sistema de Información Institucional, en el ámbito de su competencia.
- Desempeñar las demás funciones que en el ámbito de su competencia, le sean asignadas por la Oficina de Sistemas.

6.3 ESTRUCTURA ORGANICA

La Unidad de Producción no cuenta con Unidades Orgánicas dependientes.

6.4 LINEA DE DEPENDENCIA

La Unidad de Producción depende directamente de la Oficina de Sistemas.

6.5 LINEA DE COORDINACION INTERNA

La Unidad de Producción mantiene coordinación interna con todas las Unidades Orgánicas usuarias.

6.6 LINEA DE COORDINACION EXTERNA

La Unidad de Producción mantiene coordinación externa, a través de la Oficina de Sistemas, con las Entidades e Instituciones Externas que, por la naturaleza de sus funciones, le son afines y/o necesarias.

7. ORGANIZACION Y FUNCIONES GENERALES :

UNIDAD DE INFORMACION GERENCIAL

7.1 OBJETIVO

Garantizar la correcta estructuración, integración, contenido y calidad del Sistema de Información Estadística y Gerencial, en sus niveles estratégico, táctico y operativo.

7.2 FUNCIONES GENERALES

- Formular, proponer, implantar y evaluar las políticas, normas, planes y programas comprendidos en el ámbito de su competencia, así como controlar su ejecución.
- Formular y proponer el Sistema de Información Estadística y Gerencial, así como controlar su implementación.
- Mantener actualizadas las normas, metodologías y estrategias de desarrollo del

Sistema de Información Estadística y Gerencial, así como evaluar su aplicación.

- Desarrollar las acciones de soporte a las Unidades Orgánicas para la determinación de sus necesidades de información y estudio de soluciones.
- Consolidar y formular la información Estadística y Gerencial y la Memoria Anual de la Empresa.
- Proporcionar asistencia técnica a las Unidades Orgánicas en la generación y uso de la Información Estadística y Gerencial.
- Cumplir y hacer cumplir las disposiciones legales y normativas vigentes, con relación a las actividades de la Unidad.
- Suministrar la información y documentación procesada en la Unidad, de acuerdo a la normatividad y sistemas establecidos.
- Conducir las acciones comprendidas en el Sistema de Información Institucional, en el ámbito de su competencia.
- Desempeñar las demás funciones que en el ámbito de su competencia, le sean asignadas por la Oficina de Sistemas.

7.3 ESTRUCTURA ORGANICA

La Unidad de Información Gerencial no cuenta con Unidades Orgánicas dependientes.

7.4 LINEA DE DEPENDENCIA

La Unidad de Información Gerencial depende directamente de la Oficina de Sistemas.

7.5 LINEA DE COORDINACION INTERNA

La Unidad de Información Gerencial mantiene coordinación interna con todas las Unidades Orgánicas.

7.6 LINEA DE COORDINACION EXTERNA

La Unidad de Información Gerencial mantiene coordinación externa, a través de la Oficina de Sistemas, con las Instituciones y Entidades Externas que, por la naturaleza de sus funciones, le son afines y/o necesarias.

CAPITULO III

SEGURIDAD DE LA INFORMACION

1. INTRODUCCION

En toda empresa, la seguridad de la información constituye el eje de su existencia; con la que se establece salvaguardas técnicas, procedimientos, programas de seguridad y planes de contingencia para la protección de los datos en relación con accesos y/o alteraciones no autorizadas.

El desarrollo acelerado de nuevas tecnologías de hardware, software y comunicaciones; hacen que la información sea más difícil de proteger. Para contrarrestar este riesgo también se han desarrollado nuevas técnicas y medidas de seguridad que las que se aplicaba cuando apareció la informática.

En entornos distribuidos hay mayor accesibilidad a los datos; incrementando la dificultad de programas de seguridad. Se ha reducido la eficacia del control centralizado de la organización y para contrarrestar

este peligro, es necesario adoptar medidas precautorias precisas y eficaces amparadas en normas legales del Estado.

2. CONCEPTOS PRELIMINARES

2.1 PRIVACIA

En las empresas que manejan sistemas de información, el derecho a la privacía constituye un tema legal y ético. Entonces preguntamos ¿Hasta qué punto el derecho a la privacía entra en conflicto con otros derechos?.

Los bancos de datos tienen derecho a la privacía; pero también la sociedad tiene la necesidad y el derecho de tener ciertos tipos de información que contribuyan al bienestar general, de lo contrario los datos demográficos y los niveles de ingreso de la población no se podrían aplicar en los programas de política nacional del gobierno. Un aspecto importante es, entonces, conocer el balance entre los derechos individuales y los costos de proteger y guardar los registros.

2.2 SEGURIDAD Y FRAUDE

En el diseño de un programa de sistemas, se debe contar con precauciones para evitar todo

posible fraude, para lo cual es necesario la presencia de programadores independientes que trabajen en las partes críticas del sistema y también deben intervenir muchos usuarios.

La presencia de una sola persona es inconveniente, ya que al aprovecharse del cargo único realizaría cambios sensibles para beneficiarse directamente en detrimento de la empresa.

La seguridad en los sistemas de informática tiene relación con el concepto de privacía. Mientras la privacía se caracteriza por su sensibilidad, **la seguridad es determinante para el éxito del sistema**, por tanto se debe de trabajar con un archivo de respaldo que almacene los datos en localidades físicamente separadas. Por ejemplo: la sede central en el Cercado de Lima y el respaldo del centro de informática en un lugar lejano geográficamente.

2.3 RESPONSABILIDAD

Es la cualidad que caracteriza al personal que labora en los centros de informática, desde el más alto nivel hasta los operadores y usuarios que han de asegurar el normal funcionamiento de los centros de informática.

Cuando falla un sistema de computadora no hay forma de señalar responsables, ya que el factor humano es limitado.

3. CONSIDERACIONES LEGALES

La modernidad implica el mayor uso de los ordenadores por las entidades públicas y empresas particulares, las que necesitan mayor contingente de profesionales y técnicos. Este incremento de personal es preocupante a la privacía. Unido el factor humano al mayor interés por los datos de los centros de computación, la seguridad está siendo legislada ya que se ha convertido en política del Estado.

"Con el fin de proteger la intimidad de las personas, el Congreso de los Estados Unidos, aprobó la ley de Informaciones Confidenciales de 1971, que establecía normas muy estrictas para las agencias de información.

Tres años después, el Congreso aprobó una ley sobre la intimidad, aplicable a las oficinas de Administración y a sus concesionarios. En 1978, la Oficina de Administración y Presupuestos envió una circular a los directores de las dos partes, para establecer los requisitos de seguridad de los sistemas automáticos de información. Este tipo de legislación,

en consonancia con el mayor interés público en la protección de la intimidad individual, ha contribuido a crear un estado de atención creciente hacia los problemas planteados por la seguridad de los ordenadores y de los datos mecanizados." [6]

En el Perú, la Constitución Política de 1993, en el TITULO I, DE LA PERSONA Y DE LA SOCIEDAD, CAPITULO I DERECHOS FUNDAMENTALES DE LA PERSONA, artículo 2° inciso 5, acápite segundo dice:

"El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refiere al caso investigado.", el inciso 6 dice:

"A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar." [7]

El 30 de marzo de 1995, por RESOLUCION JEFATURAL N° 090-95-INEI Aprueban recomendaciones técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración

[6] DALAL, JAGDISH R.: Gestión de Proceso de Datos, Ediciones Arcadia, S.A., España, 1984, p. 190.

[7] CONSTITUCION POLITICA DEL PERU 1993: p. 10.

pública.

De igual manera, en la misma fecha se aprobó y publicó la Directiva Nº 008-95-INEI/SJI, sobre "RECOMENDACIONES TECNICAS PARA LA PROTECCION DE LOS EQUIPOS Y MEDIOS DE PROCESAMIENTO DE LA INFORMACION EN LA ADMINISTRACION PUBLICA". [8]

4. ORGANIZACION Y SEGURIDAD

La organización de los sistemas informáticos se da en atención a los programas a emplearse, para lo cual se elaborará un **Plan de Contingencias**, que describa los riesgos potenciales y los correctivos a fin de superar los problemas que impiden el normal funcionamiento de la seguridad.

La seguridad para ser eficaz debe ser compartida y comprendida por todo el personal que laboran en la empresa.

La **Figura Nº1** muestra las **Funciones de organización de la seguridad informática**, posible de ser adaptado a un programa de seguridad de centros informáticos.

[8] EL PERUANO: Normas Legales, INEI, 01 Abril 1995, p. 130917 - 130919.

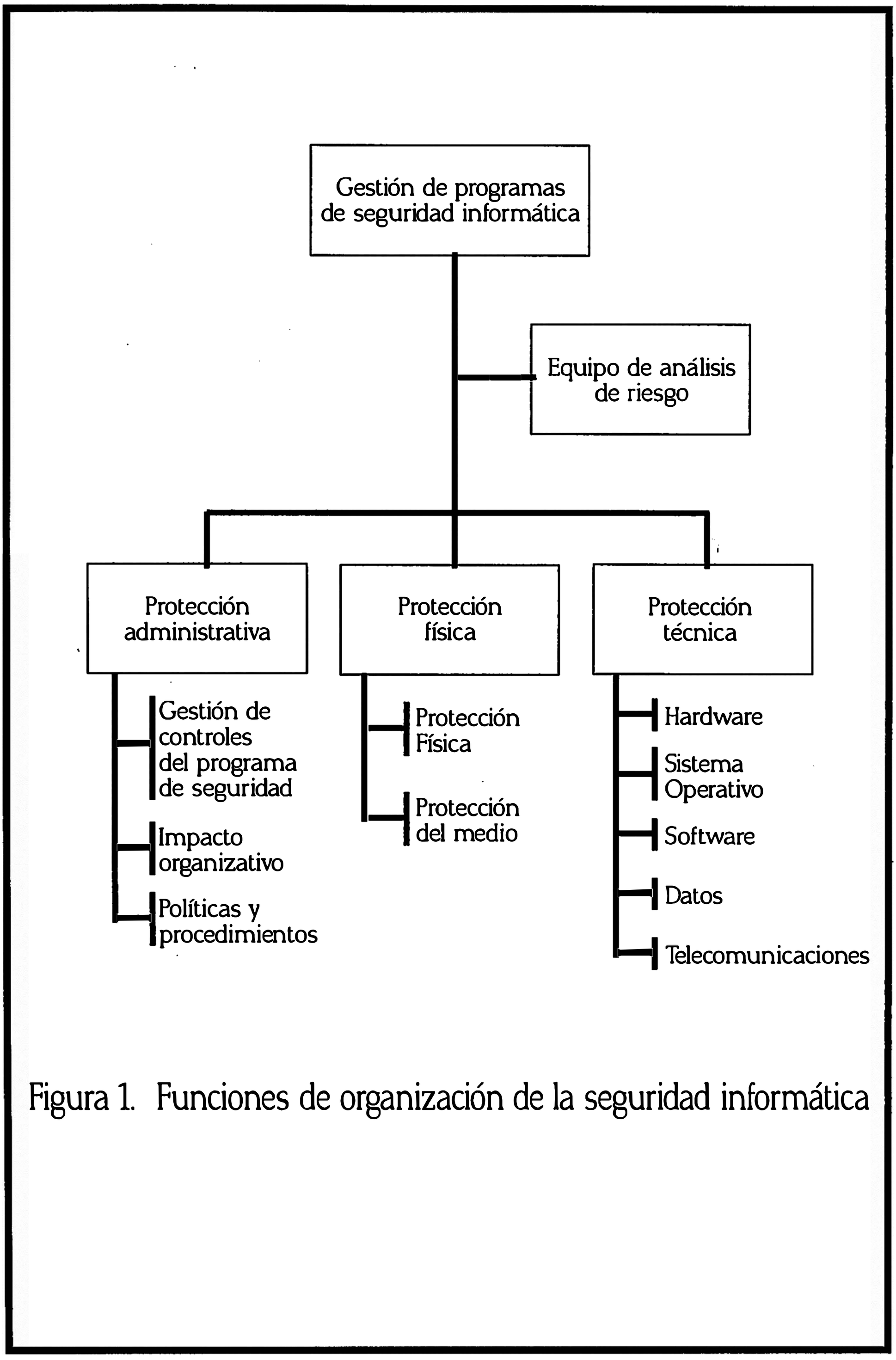


Figura 1. Funciones de organización de la seguridad informática

5. SEGURIDAD FISICA

Las medidas de seguridad intentan reducir las interrupciones del servicio, las pérdidas de activos y los accesos no autorizados al equipo. El acceso no autorizado a la información puede afectar también al servicio porque reduce la confianza en la seguridad de la información. Evidentemente a menos que el equipo de Proceso de Datos parezca estar físicamente seguro, cualquier intento de proteger los sistemas y los datos será inútil. Por lo tanto, la seguridad física es el primer aspecto que debe ser considerado al elaborar el programa de seguridad, que integra el **Plan de Contingencia.**

5.1 AMENAZAS A LA SEGURIDAD FISICA

Las amenazas pueden provenir de factores naturales y humanos; las cuales pueden destruir o bien simplemente alterar erróneamente el funcionamiento del sistema. Los factores naturales son, generalmente, imprevisibles y sus efectos pueden ser de largo alcance. Si no se adoptan previsiones para estos casos y no se ejecuta un plan de recuperación de desastres, estos factores pueden producir siniestros que hundan la organización. La destrucción por causas humanas, del equipo o de los datos es más fácil

de evitar; estos daños pueden ser originados por muchos motivos, desde el sabotaje, hasta los errores no intencionados.

Un programa de seguridad física debe considerar los riesgos potenciales debidas al entorno y al hombre y preveer medidas de seguridad contra ellos tal como lo muestra la **Figura N°2 Amenazas y medidas de seguridad.**

Amenazas	Medidas de Seguridad												
	a	b	c	d	e	f	g	h	i	j	k	l	m
Debidas al entorno													
Fuego	X	X	X	X	X		X					X	X
Tormentas	X	X		X	X		X					X	
Terremotos	X	X		X	X		X					X	
Inundación	X	X		X	X		X					X	
Fallos de Energía			X	X		X							
Fallo aire acondic				X		X							
Debidas al hombre													
Daños malintenc.	X	X	X	X	X	X		X	X	X			X
Fraude								X		X	X	X	X
Malversación								X		X	X	X	X
Robo			X		X			X	X	X	X	X	X
Uso no aut recurs.			X		X			X	X	X	X	X	X
Sabotaje/Espionaje			X	X	X			X		X	X	X	X
Daños fortuitos				X							X	X	X

CLAVES:

a. Diseño de edificio
b. Construc. edificio
c. Colocación de dispositivos detección
d. Identif. prueb. equipo backup
e. Sistema aviso bomberos policia
f. Backup de energía
g. Previsiones metereológ.
h. Control de acceso al sistema
i. Ventanas y puertas a seguir
j. Programa selección personal
k. Adhesión a auditorias, medios de registro y proced. control.
l. Estand y proc. documentados
m. Formación y entren. personal.

Figura 2. Amenazas y medidas de seguridad

5.2 ANALISIS DE LA FIGURA N°2 AMENAZAS Y MEDIDAS DE SEGURIDAD

Las amenazas debidas al entorno (en forma horizontal) :

- El fuego afecta a ocho medidas de seguridad.
- Los terremotos, tormentas e inundaciones afecta a seis medidas de seguridad.
- Las fallas de energía afecta a tres medidas de seguridad.
- Las fallas de aire acondicionado afecta a dos medidas de seguridad.

Las amenazas debidas al hombre (en forma horizontal):

- Los daños mal intencionados afecta a diez medidas de seguridad.
- Las amenazas de robo, uso no autorizado de recursos afecta a ocho medidas de seguridad.
- Las amenazas de fraude y malversación afecta a cinco medidas de seguridad.
- Los daños fortuitos afecta a cuatro medidas de seguridad.

6. ANALISIS DE RIESGOS

Para realizar un programa de seguridad eficaz, es necesario fijar la probabilidad de ocurrencia de cada posible siniestro y determinar el costo de implantación de las medidas preventivas.

La probabilidad del siniestro es muy importante, pero frecuentemente olvidado.

A pesar de que el análisis de riesgos precisa la ejecución de cálculos matemáticos, la intuición también puede jugar un papel muy importante.

Para efectuar estudios objetivos de alternativas, sin embargo, hay que cuantificar el mayor número de factores posibles.

La **Figura N°3 Metodología de análisis de riesgo,** describe los pasos necesarios que hay que dar para llevar a cabo un análisis de riesgos.

En resumen se debe establecer un equipo permanente de análisis de riesgos compuestos por representantes de la dirección de DP, de seguridad, departamentos usuarios claves (o clientes) y del departamento financiero.

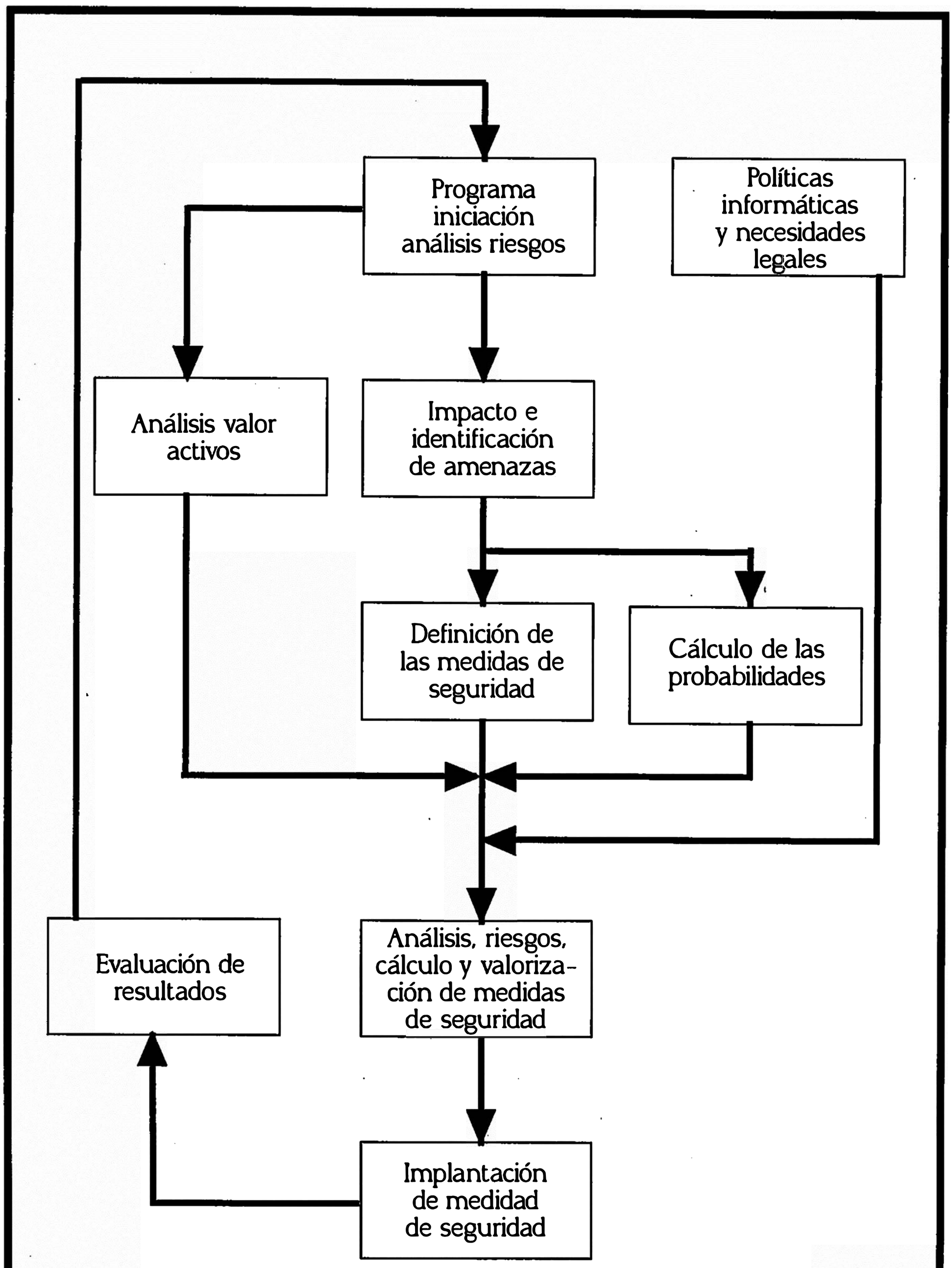


Figura 3. Metodología de análisis del riesgo

7. PLAN DE CONTINGENCIA

Es un sistema de seguridad construido rigurosamente, en la que la empresa se vea en la necesidad de abandonar el centro de proceso de datos y acudir a otra instalación que sirva como backup para continuar brindando el apoyo informático para la toma de decisiones.

La interrupción del servicio puede ocurrir debido al fuego, inundación, terremoto, falla de corriente eléctrica, huelgas; que pueda durar desde un día hasta semanas.

Una planificación adecuada y cuidadosa permitirá reducir las pérdidas en que se incurra por un desastre de algún tipo, pero lamentablemente, muchos **planes de contingencia** han resultado ser insuficientes.

Un plan completo puede ayudar en gran medida a hacerse cargo con éxito de tales interrupciones.

Se debe de considerar como mínimo lo siguiente:

- Procedimiento de notificación de la emergencia.
- Lista de organización para una contingencia.
- Identificación de los recursos afectados.
- Lista de los recursos disponibles.
- Procedimientos y normas escritas.

La importancia de tener **planes actualizados de contingencias** nunca será suficiente. Aunque estos planes pareciera no ser necesarios nunca ya que son parte esencial de la gestión del proceso de datos.

CAPITULO IV

CONFIDENCIALIDAD DE LA INFORMACION EN LOS SISTEMAS DISTRIBUIDOS

1. CONFIDENCIALIDAD, SECRETO, SEGURIDAD

La confidencialidad es el secreto y seguridad de los sistemas distribuidos del centro de cómputo.

En los sistemas distribuidos la confidencialidad de la información, incluye las materias de secreto y seguridad. Las diferencias y relaciones entre estas tres áreas deben ser perfectamente entendidas:

- El secreto de la información es responsabilidad de un sólo individuo.
- La confidencialidad es compartida por otra persona.
- La seguridad son medidas que resguardan la confidencialidad de la información.

1.1 OBJETIVOS

Desde que en 1970 aparece el concepto de datos como recurso de una empresa, se ha hecho hincapié en la gestión eficaz de este recurso y se logra mediante los siguientes objetivos:

- Lograr una mayor fiabilidad.
- Contar con mayor disponibilidad de recursos.
- Mejorar los tiempos de respuesta.
- Contribuir a un mejor control de los datos en los puntos de operación.

Cuando se alcanzan estos objetivos, el recurso datos contribuye a la buena marcha de la organización.

El proceso de datos distribuido implica la descentralización del procesamiento; lo que, a su vez, exige la descentralización del recurso datos. Por tanto, las necesidades para proteger la confidencialidad de los datos en un ámbito distribuido son más complejas.

1.2 CONTROL

El control como medida de protección en los sistemas informáticos mal interpretado puede, significar un retraso en el desarrollo de los proyectos, pero el término control desde un punto de vista positivo contribuye al éxito de los

proyectos que se desarrollan en los sistemas informáticos.

En cualquier caso, el control es necesario para asegurar la confidencialidad de la información en un ámbito distribuido.

1.3 TIPOS DE INFORMACION QUE DEBEN SER PROTEGIDOS

En un plan de seguridad dada la experiencia adquirida en atención a la confidencialidad, es el planificador el encargado de asegurar los datos referentes a:

- Información sobre empleados.
- Información sobre clientes.
- Información financiera.
- Clasificación sobre suministradores.
- Diseño de productos futuros.
- Estrategia de mercado.
- Técnicas de investigación.
- Información académica.
- Experiencia profesional.
- Póliza de seguros.
- Lista de socios.
- Lista de accionistas.
- Claves de seguridad.
- Correo electrónico.

Cuando la información se ve comprometida, suele ser difícil cuantificar los efectos adversos. Esta situación puede dar como resultado una baja moral de los empleados, la pérdida de la ventaja competitiva en el anuncio de un producto o en la penetración en un mercado, la falta de satisfacción en los clientes, pleitos, etc. La violación de la confidencialidad originada por la falta de controles adecuados puede tener también serios efectos en el departamento de proceso de datos.

2. ORGANIZACION Y CONTROLES

A medida que van surgiendo las aplicaciones de proceso de datos distribuido, deben analizarse las necesidades planteadas por la confidencialidad.

Los planificadores deben decidir cual es la información que debe ser protegida. Sólo después de que este aspecto haya sido analizado en profundidad, el personal encargado del desarrollo debe realizar las sugerencias respectivas de como proteger la información.

2.1 ¿QUE HAY QUE PROTEGER?

De acuerdo al tipo de negocio y los objetivos de la empresa, se analizará los datos que son procesados por las aplicaciones diferenciando niveles de confidencialidad.

El análisis enfoca la información desde la captura de datos hasta el proceso y distribución de la información, las funciones de mantenimiento y consulta también debe ser consideradas. El mantenimiento se realiza a menudo por un menor número de usuarios que las consultas.

Los usuarios deben de poseer una formación adecuada para el manejo de distintos tipos de información. A continuación se menciona una lista probable de información a proteger:

- Los datos para la confección de la nómina.
- El diseño de nuevos productos.
- La información financiera.
- El correo electrónico.
- Investigación y fallos de productos, etc.

2.2 CAMBIOS ORGANIZATIVOS

Para crear un ámbito de proceso distribuido con un buen prestigio en lo que se refiere a la confidencialidad, la empresa debe realizar primero cambios que definan las responsabilidades

en materia de seguridad y establezcan controles prácticos que sean comprendidos y aceptados.

Es esencial que dichos controles sean aceptados corporativamente. Si los ejecutivos, el personal de desarrollo del proceso de datos distribuido y los usuarios finales no cooperan con el mantenimiento de la confidencialidad, se darán muchos retrasos innecesarios en el proceso de datos distribuido, y la calidad del producto final reflejará probablemente esta falta de cooperación.

2.3 LA OFICINA DE SEGURIDAD

El primer paso organizativo es el establecimiento de una oficina de seguridad de proceso de datos distribuido, la cual proporcionará las políticas administrativas, los estándares, guías de comportamiento y procedimientos para los controles requeridos. La oficina debe también aportar servicios de seguridad durante la realización de los controles.

El personal de la oficina de seguridad del proceso de datos distribuido debe ser cuidadosamente seleccionado. Contar con el respeto y la confianza de la organización a la

que está encargado de proteger. También conocer lo suficiente sobre el proceso de datos distribuido para evitar ser abrumado con restricciones técnicas que pueden ser solamente excusas. Pocas personas cumplen estos requisitos.

Las personas seleccionadas para la oficina de seguridad deberán mantenerse firmes y cuándo pueden llegar a un cierto compromiso. La rigidez extrema en la seguridad, impedirá el crecimiento del proceso distribuido y también una persona débil puede anular la razón de ser de la Oficina de seguridad. Ambos casos, el cargo es consultivo y algunas veces resultará impopular, especialmente si la oficina de seguridad no está apoyada por los niveles superiores de dirección y no es comprendida por los jefes de operaciones.

El personal de la oficina de seguridad debe ser capaz de evaluar las necesidades de la empresa y traducirlas a consideraciones técnicas dentro del proceso de datos distribuido.

2.4 AUDITORIAS DE PROCESO DE DATOS

La auditoría que interviene en el proceso de datos debe trabajar estrechamente con la oficina de seguridad y controlar mejor la efectividad de la confidencialidad.

El trabajo de auditoría debe ser permanente para comprobar que las medidas correctivas propuestas, superen los problemas y satisfagan las necesidades de la organización del sistema.

2.5 DESARROLLO DE CONTROLES

El control para la confidencialidad en las informaciones se da en la fase de definición de los requerimientos, que contempla:

- Necesidades de los usuarios.
- Selección del suministrador y
- Cálculo de beneficio de la inversión.

Tanto la selección del suministrador como el beneficio a obtener de la inversión se verán afectados por la necesidad de confidencialidad de la información. Si el hardware y el software del proceso distribuido se seleccionan antes de que se discutan los aspectos de la confidencialidad, es posible que el equipo no satisfaga las necesidades de confidencialidad.

Para el éxito del control en la confidencialidad, el personal de seguridad debe trabajar junto con los usuarios para determinar qué información debe ser protegida. Una vez que se han especificado las necesidades de confidencialidad, el personal de desarrollo del

proceso de datos distribuido será el responsable de la puesta en práctica de cualquier control necesario.

3. ALTERNATIVAS DE CONTROL

El tipo de control elegido depende de las necesidades de los usuarios. Para facilitar la confidencialidad pueden utilizarse los siguientes controles:

- Controles físicos.
- Identificación de los usuarios, passwords (palabras clave) y perfiles de seguridad.
- Fragmentación de la información.
- Encriptación.

3.1 CONTROLES FISICOS

Los controles físicos se aplican al acceso físico al hardware del proceso distribuido. En el nivel más simple, puede instalarse una cámara de T.V. en la sala del terminal. El video obtenido puede ser supervisado a intervalos previamente especificados.

La sala del terminal, puede ser físicamente asegurada mediante guardias. También se pueden utilizar sistemas de reconocimiento automático si

la necesidad lo requiere; por ejemplo, lectores de banda magnética, lectores de huellas dactilares, sistemas de reconocimiento de la voz.

En todos los casos de controles físicos se considera el coste de las alternativas propuestas y que justifiquen la inversión en atención a la confidencialidad de los sistemas distribuidos de la empresa.

3.2 IDENTIFICACION DE USUARIOS, PASSWORDS Y PERFILES DE SEGURIDAD

Estos tres controles deben ser integrados en una estructura triangular como lo muestra la **Figura N°4 Estructura triangular de control**.

Si la dirección, los usuarios y el ordenador se ven como los ángulos de un triángulo, el sistema de autorización para el usuario puede ser visto como los lados del triángulo.

La puesta en práctica o integración del control del usuario requiere tres elementos. El más importante es la identificación del usuario. Una identificación de usuario es única para cada persona dentro de la población restringida que puede tener acceso a un sistema. El segundo es el password, que difiere de lo que es una identificación está adjudicada a un recurso.

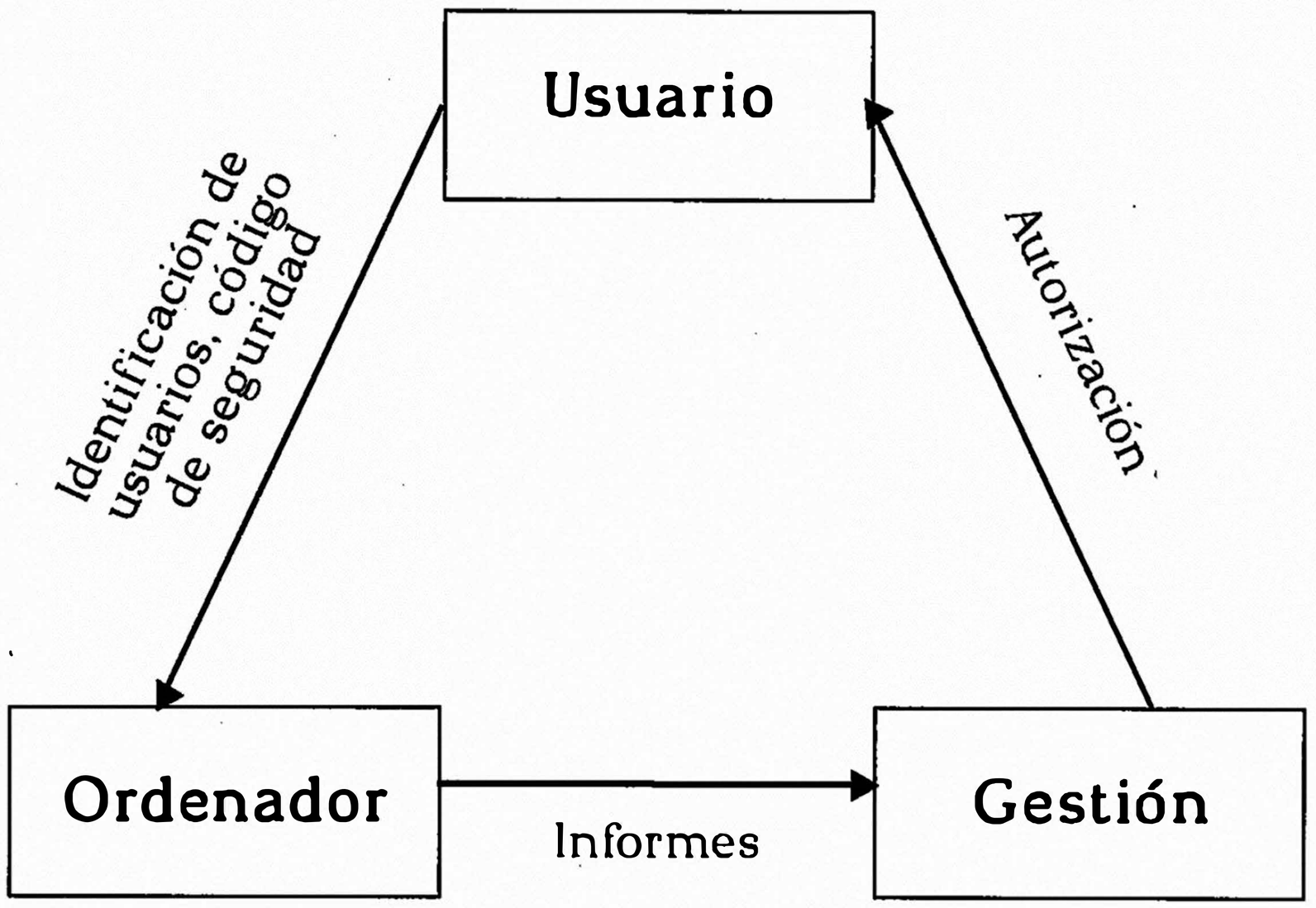


Figura 4. Estructura triangular de Control

La identificación autoriza a los usuarios en función **de quienes son**, mientras que un password lo hace en función **de lo que saben**.

El tercer elemento requerido para ligar la identificación del usuario y el password es el perfil de seguridad, que está orientado bien al recurso o bien al usuario y correlaciona los recursos con los usuarios. Una identificación carece de sentido a no ser que esté facultada para hacer algo; un recurso asegurado mediante un password es inútil a no ser que alguien lo conozca. Sin embargo, si el esquema de autorización al usuario comienza con el perfil, el sistema de ordenador tiene una definición que incorpora identificación y acceso.

La identificación y el password se combinan para formar un código de seguridad, proporcionando una cadena de caracteres que sirva para ambos propósitos.

3.3 FRAGMENTACION DE LA INFORMACION

La fragmentación de la información es una estrategia de diseño que puede utilizarse conjuntamente con otras alternativas de control. Al crearse subconjuntos de información se minimizan las violaciones de la confidencialidad.

La fragmentación no proporciona una protección óptima, pero reduce el coste de control. Ofrece también otros beneficios: en algunas arquitecturas de proceso distribuido, la fragmentación de los datos puede mejorar el rendimiento, simplificar la recuperación, facilitar el backup y permitir una mayor flexibilidad para una futura distribución de la información.

3.4 ENCRIPTACION DE LA INFORMACION

La encriptación como método más efectivo y que conserva la información, es la conversión de un mensaje (un texto normal) en un formato aparentemente carente de significado (un texto cifrado) mediante un algoritmo.

Los procesos de encriptación y desencriptación están controlados por una clave. Hasta ahora, la justificación de los costes de encriptación de los datos ha resultado difícil. El rápido descenso de los costes del hardware están cambiando favorablemente este cuadro; sin embargo, el manejo de la clave para la encriptación suele precisar el establecimiento del personal de seguridad o de un aumento del mismo, compensando así la reducción en los costes del hardware.

Si las condiciones de la empresa exigen la utilización de un sistema de encriptación, antes de poner en marcha dicho sistema debe realizarse un estudio y una planificación cuidadosa. La alternativa de la encriptación seleccionada puede afectar a la arquitectura del sistema y del hardware elegida para la red de proceso distribuido.

4. DESCUIDOS MAS COMUNES EN RELACION CON LA CONFIDENCIALIDAD

Los controles sobre la confidencialidad deben desarrollarse como parte de la metodología del desarrollo de la aplicación. Sin embargo, puede producirse descuidos comunes durante el desarrollo y después de la puesta en marcha.

4.1 DESCUIDOS EN EL DESARROLLO

Uno de los errores o descuidos más frecuentes cometidos durante el desarrollo tienen lugar en la conversión o traspaso de la información. Las nuevas aplicaciones del proceso de datos distribuido necesitan con frecuencia información procedente de archivos ya existentes.

Durante la puesta en funcionamiento del proceso de datos distribuido, los datos de producción deben ser traspasados o convertidos desde los viejos sistemas. Al realizar este trabajo, la información, que será confidencial una vez que el sistema sea operativo, suele estar descuidadamente al descubierto.

Por ejemplo, los archivos de trabajos temporales se crean y utilizan durante un período de tiempo que va desde unas pocas horas a muchas semanas. Los listados que contienen la información confidencial suelen estar impresos, de manera que el usuario y los analistas del proceso de datos distribuido puedan revisarlas para evaluar su precisión. Los archivos de conversión de información rara vez tienen protección alguna. Después de la puesta en marcha ni siquiera se considera la destrucción de estos archivos ni de los informes escritos.

Para asegurar la información deben tomarse dos medidas:

- Primero, el acceso a la documentación de los sistemas debe estar protegida con objeto de impedir un acceso no autorizado.
- Segundo, las violaciones originadas por errores inadvertidos deben ser eliminadas o

minimizadas impidiendo los controles adecuados a la documentación y a las modificaciones del sistema.

Supervisando adecuadamente las modificaciones, los problemas que plantea la confidencialidad pueden ser identificados antes de la puesta en marcha del sistema.

4.2 DESCUIDOS DESPUES DE LA PUESTA EN FUNCIONAMIENTO

Una vez que se ha implementado el proceso distribuido, se debe tener presente la implementación de procedimientos que permitan asegurar un normal funcionamiento del sistema:

- **PROCEDIMIENTOS DE RECUPERACION DEL SISTEMA**

  Se diseñará e implementará planes de contingencia, definiendo pruebas periódi-cas para todo nivel.

- **RECUPERACION DESPUES DE LOS SINIESTROS**

  Deberá existir una adecuada distribución física del hardware y la información almacenada en medios magnéticos o en papel los que reducirán los efectos de los siniestros.

- **MODIFICACIONES DE PROGRAMAS**

  Las modificacione y/o alteraciones a programas debe estar protegido con niveles

de acceso, dichos programas deberán ser almacenados en librerías privadas.

- **TRANSPORTE MEDIANTE RECADEROS**

  El transporte de la información debe estar asegurado y garantizado por servicios de recaderos de buena reputación. También se considerará el uso de contenedores con cerraduras y/o sellos, registrando las horas de salida/llegada así como la supervisión de los tiempos normales de entrega.

- **PERSONAL DE MANTENIMIENTO**

  El personal de mantenimiento del hardware debe estar registrado, en la organización, verificando las maletas de herramientas, así como el registro de las horas de visita.

- **REVISION DE LOS SISTEMAS**

  Durante el desarrollo de un nuevo proceso de datos distribuido, la participación de los usuarios y el personal de auditoría cumplen un papel fundamental estableciendo procedimientos adecuados dentro de la instalación, en los que se debe de considerar lo siguiente:

  - ¿Se siguen actualmente estos procedimientos?
  - ¿Son los adecuados?

- ¿Son demasiados restrictivos?
- ¿Están dentro de las estimaciones de costes establecidos?

Las respuestas a estas preguntas pueden llevar a tomar decisiones que precisen de normas adicionales de dirección, de una nueva formación, de cambios de procedimientos o de sistemas, etc. La revisión también mejorará las comunicaciones y proporcionará apreciaciones útiles para el futuro desarrollo del proceso de datos distribuido.

5. CONSIDERACIONES SOBRE LA SEGURIDAD EN RELACION CON LOS USUARIOS

Otro punto crítico en la puesta en funcionamiento de los sistemas de proceso de datos distribuido es la seguridad del usuario. Los cuales plantean diversas amenazas a la seguridad:

- La no separación de trabajos en el ámbito del usuario invita a una potencial violación de la seguridad.
- Puede existir una atmósfera informal de trabajo en las instalaciones remotas, impidiendo así que se siga una estricta disciplina en la seguridad.

- Desde el departamento central de seguridad hay que comunicar de alguna manera a la instalación local los procedimientos sobre seguridad y palabras claves. El proceso de comunicación está sujeto a menudo a algún tipo de infracción en las medidas de seguridad.
- La necesidad que tienen las instalaciones locales de comunicarse con la instalación central y/o con las instalaciones locales en formatos legibles por las máquinas puede hacer que en una determinada instalación local sea posible encontrar palabras claves de otras instalaciones distantes. Como resultado, una infracción de la seguridad en una instalación dada puede comprometer a toda una red.
- Las pólizas de seguro que compensen a la corporación en caso de violación de la seguridad pueden ser más difíciles de obtener, o más caras, debido a la diversa naturaleza de las instalaciones remotas.
- Una de las medidas de la seguridad que con mayor probabilidad se infringe en las instalaciones locales es la del relativo aislamiento del proceso de datos, debido a la gran cantidad de personas que entran en contacto con los sistemas de proceso de datos. Debido a que en estos

ámbitos los empleados realizan a menudo diversas funciones, pueden seleccionarse posibles empleados por razones distintas de su capacidad para utilizar correctamente el sistema ubicado en la instalación local.

Una buena seguridad puede conseguirse de varias maneras:

- Para las instalaciones remotas deben redactarse unas buenas políticas y procedimientos sobre seguridad, aun cuando el personal de esas instalaciones remotas pueda desviarse de los mismos.
- Debe hacerse responsable de la seguridad no solamente al personal relacionado con el proceso de datos, sino también al director (usuario) de la instalación.
- Deben realizarse planes para la seguridad de todas las transacciones en especial: datos, voz y/o correo entre las distintas instala-ciones.
- Deben establecerse los niveles directivos, duración y presupuestos necesarios para realizar las auditorías de las instalaciones remotas. Una auditoría requiere normalmente un mínimo de dos visitas anuales a una instalación remota.
- La seguridad de los archivos de backup de las instalaciones remotas deben ser considerada tan

cuidadosamente como si se tratara de la seguridad de los principales ficheros de producción.

- Deben tomarse en consideración las alternativas tecnológicamente avanzadas en materias de palabras claves. Por ejemplo: tarjetas de identificación magnéticas especialmente codificadas, identificación de la voz, chips de memoria de sólo lectura codificados y dispositivos para reconocimiento de huellas dactilares; son algunos de los elementos que han llegado a ser tenidos en cuenta para aplicaciones concretas.

- Al evaluar alternativas técnicamente avanzadas, los responsables de la seguridad no deben pasar por alto soluciones tan simples como el cerrar físicamente los terminales mediante una llave o el impedir de una manera electrónica y de modo remoto el acceso a la red conmutada de un sistema dado.

- Los planes para las eventualidades que se puedan producir deben estar suficientemente detallados para ser utilizados cuando aquéllas se produzcan. Sin embargo, estos planes también deben ser contemplados como un riesgo para la seguridad muy a menudo, constituyen una información sobre la seguridad que de otra manera estaría restringida.

- Debe ser tomado en consideración el personal que atiende y repara el sistema en las instalaciones remotas. Este personal puede tener acceso a la información de seguridad que afecta a una instalación remota dada, así como a otras instalaciones de la red.
- Los directores siempre deben ser conscientes del coste relativo y del valor de la seguridad. Este equilibrio entre coste y valor debe ser cuidadosamente sopesado, especialmente en aquellas instalaciones donde el acceso es solamente posible a los ficheros locales. Unas medidas excesivas de seguridad son costosas e influyen negativamente sobre la utilización del sistema y eventualmente crean riesgos para la seguridad en forma de cínicos usuarios del mismo.

6. PROCEDIMIENTOS DE AUDITORIA

Para ayudar al personal de auditoría en sus trabajos, frecuentemente se piden extractos de información para los auditores. Estos extractos aumentan los costes operativos y de desarrollo, y deben, por tanto, estar justificados por un análisis de las necesidades de la empresa.

La realización de auditorías periódicas de conformidad para informaciones críticas resulta una solución para la confidencialidad más económica, que satisfacerá las necesidades de muchas aplicaciones. Esta función de auditoría puede ejecutarse de una manera aleatoria y tiene, pues, algunas ventajas sobre la obtención de extractos para la auditoría realizados durante el tiempo de operación. Sin embargo, este tipo de protección tiene propiedades terapéuticas donde los problemas se identifican y luego son corregidos.

Las auditorías de conformidad deben utilizarse como un único elemento de protección solamente en sistemas en los que pueda tolerarse algunas transgresión en lo que a la confidencialidad se refiere.

6.1 EL NUEVO PAPEL PARA LOS AUDITORES

El advenimiento de las computadoras impulsó una nueva orientación de la tradicional auditoría y se inicia una nueva era en el aprendizaje de principios de los sistemas de computación y se equipan para manejar eficazmente, las operaciones por computación.

Para establecer una labor efectiva de los auditores se debe cumplir los siguientes objetivos:

- Desarrollar nuevas técnicas de auditoría computarizada y que se incluyera, cuando fuera posible, dentro del sistema.
- Desarrollar requisitos y técnicas de control y enfatizar en el equipo de diseño de sistemas la necesidad de contar con un sistema de control apropiado.
- Redoblar la eficacia del sistema de control mientras esté en proceso de diseño.
- Evaluar las demás áreas tales como la prueba y conversión del sistema, en los que los controles son esenciales.

El nuevo enfoque de la Auditoría del PED se denominó **AUDITORIA previa a la conversión** y proporcionó a la gerencia un control de evaluación independiente del control para los futuros sistemas de computación.

En un enfoque como el de la auditoría previa a la conversión, la gerencia está llamada a mediar entre los sistemas diseñados y los puntos de vista de las auditorías. Si existe una diferencia de opinión en una cuestión de control, a la gerencia le corresponde escuchar ambos puntos de vista y tomar una decisión sopesando el costo de los controles contra el nivel de riesgo involucrado.

6.2 ¿COMO HACER QUE EL SISTEMA SEA VERIFICABLE?

La responsabilidad del auditor es asegurar que los sistemas de computación sean verificables cuando se vuelven operativos. Debería estar continuamente alerta sobre los posibles efectos que tendrá el nuevo sistema propuesto en los controles interno y, por consiguiente, debería desarrollar requisitos de auditoría.

El auditor de PED debería intentar utilizar al máximo la tecnología de la computación como un instrumento para la auditoría. Debería tratar de que en los sistemas de computación se incluyera técnicas y rutina de auditoría siempre que sea viable y económico hacerlo. De este modo, gran parte del trabajo de auditoría se puede realizar como un producto derivado de la operación normal con un poco o ningún costo extra.

6.3 PRUEBA DE LA MINIMA COMPAÑIA

La prueba de la Mínima Compañía, es un método muy conocido por los auditores. Se caracteriza por ser más sofisticado y consiste en trazar transacciones ficticias de prueba a través de sus sistema de computación, al mismo tiempo que se pasan datos reales, sin afectar los registros o salidas reales. En otras palabras, es

un pequeño subsistema del sistema normal. Un conjunto separado de salidas, incluyendo informes y estadísticas, se produce para la mini-compañía. Esto sólo asegura que el material de prueba no interfiere con cualquier otra salida relacionada con la compañía real, sino que además permite al auditor revisar que las estadísticas e informes esté preparados correctamente.

Los auditores utilizarán la mini-compañía para revisiones periódicas del sistema y un grupo de control de calidad puede emplear la capacidades de la prueba continua con mayor ventaja al cumplir sus responsabilidades diarias de control de calidad de la producción del sistema.

6.4 OTRAS TECNICAS DE AUDITORIA

Además de la mini-compañía, se pueden desarrollar otros programas especiales de auditoría. En pocas palabras, he aquí programas especiales que pueden ser utilizados por el auditor tanto dentro como fuera de la línea:

- **COMPARACION**

  Une dos archivos duplicados contenidos en cinta magnética, tarjetas o discos; determina si son idénticos e identifica los

registros que difieren, este tipo de programas ha sido utilizado en el sistema Bell para verificar las tablas de clasificación de las llamadas de larga distancia.

En un caso, los archivos de cintas que contenían tablas de aproximadamente 35,000 puntos de clasificación se compararon en casi diez minutos usando una computadora de la segunda generación. Las ventajas del programa de comparación son su habilidad para realizar una verificación del 100% e identificar para el auditor cualquier excepción que necesita una revisión más detallada.

- **MUESTREO**

  Coloca al azar las muestras de registros en un archivo.

- **RECOPILACION**

  Revisa los cálculos matemáticos realizados por la computadora, tales como la suma o resta de campos relacionados de datos por una constante. Este tipo de programa es especialmente útil para la verificación de la aplicación apropiada de fórmulas en las operaciones de computación.

Por ejemplo, si las deducciones del seguro colectivo de los empleados se desarrollan en un sistema de nóminas multiplicando el salario anual por una tasa fija, el programa de recopilación puede hacer estos cálculos independientemente de los programas ordinarios. El programa de comparación aquí descrito puede entonces utilizarse para determinar si los resultados del programa de recopilación y las operaciones normales de nómina concuerdan.

CAPITULO V

CONTROLES DE DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACION

1. CONTROL DE FACILIDADES FISICAS

Los equipos en las instalaciones del computador tienen un valor, que va desde unos pocos miles hasta varios millones de dólares según el tamaño de la instalación. El equipo se concentra en un área pequeña y fácilmente puede ser dañado. En una conmoción civil o tumulto, una facilidad de computación centralizada es obviamente un objetivo de destrucción. La cinta y los paquetes de discos magnéticos tienen en sí mismo un valor modesto, pero los datos que ellos contienen un alto valor para la organización. En muchos casos, los datos en las cintas y discos son valiosos también para la gente de afuera por ejemplo: lista de posibles compradores, lista de empleados y lista de correos.

Debido al riesgo de daño a partir del acceso no autorizado y la pérdida potencial por robo o por destrucción de los archivos de datos, programas, procedimientos, etc.; el acceso a las facilidades del computador generalmente es restringido. Los controles organizacionales para la seguridad y protección incluyen la división de las responsabilidades, de tal manera que una persona no tenga el control completo sobre el procesamiento de una aplicación, las revisiones de auditoría interna y externas, el acceso restringido de los operadores a la documentación del programa y a los archivos de datos y de programas. Este último control se ejercita por medio del uso de un bibliotecario que sigue la pista a los archivos y los hace disponibles solamente al personal autorizado. El acceso al software puede ser controlado por el bibliotecario y el software de control de la biblioteca.

Con sistemas distribuidos, es más difícil el proveer seguridad física alrededor de cada instalación. Sin embargo, cada lugar representa una inversión más pequeña en hardware que un sitio centralizado. Las provisiones de disponibilidad de un sistema distribuido deberán incluir los procedimientos de autorización para conmutar el procesamiento a localidades alternas en caso de que un sitio local no

esté funcionando. La capacidad para continuar procesando en todos los sitios excepto el que no esté funcionando es llamada protección de **falla suave** y es una ventaja importante de un sistema distribuido sobre el procesamiento centralizado, donde si el computador se **cae** todo el procesamiento cesa.

La protección de las facilidades físicas también incluyen protección contra fuego e inundación y bóvedas a prueba de fuego. Los procedimientos de seguridad deben ser complementados con un seguro contra pérdidas de equipo, software y datos. Una cuidadosa selección de los empleados además de asegurar su fidelidad es útil para protegerse contra la deshonestidad de éstos.

En el caso de los pequeños computadores o terminales localizados en las áreas del usuario, deberá haber todavía algunas restricciones y controles sobre el acceso a los equipos, al software y a los archivos de datos.

2. CONTROLES DE ACCESO A TERMINALES

En sistemas que utilizan procesamiento en línea y redes de comunicaciones, debe haber la protección contra un acceso ilegal. Los terminales representan acceso a las capacidades de procesamiento del

computador y a los datos almacenados; por tanto, deberían haber controles sobre la entrada al dispositivo en sí mismo; varias llaves para prevenir la disponibilidad del acceso físico no autorizado y el control por palabra de **pase** para autorización con anterioridad a su uso. El control de palabra de **pase** se incluye en las características del sistema operativo del computador o en su software de seguridad especial. El control usualmente consta de una o más palabras de **pase** para el acceso que el usuario debe suministrar correctamente antes de accesar los programas y los datos del sistema. La protección por palabra de pase también se puede colocar en archivos individuales y en clases de registros, de tal manera que solamente los usuarios que la conozcan pueden llegar a él o actualizar los registros en ese archivo o porción de la base de datos.

3. RESPALDO Y RECUPERACION

El sistema de computación puede ser simple o complejo, lo importante son las previsiones de recuperación frente al fuego, desastre natural, daños malicioso, o accidente que destruya equipos, software o datos. Adicionalmente a esos desastres importantes, debe haber procedimientos para recuperarse de errores

o fallas al seguir procedimientos correctos. El enfoque general para la recuperación es el respaldo mediante la creación de copias de los archivos. Se establecen procedimientos para recrear el estado de procesamiento actual usando la copia de respaldo y todas las transacciones hechas con posterioridad al último respaldo. Por ejemplo, si un error destruye un registro en un archivo, los procedimientos de respaldo permiten restaurar una versión anterior del archivo y repetir el procesamiento. Ejemplo de provisiones respaldo y recuperación son:

- Copias de respaldo de los datos y del software almacenadas fuera de las instalaciones.
- Arreglo de sitios y facilidades de respaldo y suministro de respaldo de formularios y otros elementos.
- Plan de respaldo y recuperación.

Con un microcomputador, el respaldo es menos complejo pero deberá también ser realizado. Los casettes o diskettes con datos han de ser copiados cada noche o con otra frecuencia apropiada. Las copias de respaldo deben almacenarse en una localidad segura.

CAPITULO VI

OCURRENCIA DE DESASTRES

1. CONCEPTO

Los desastres son eventos o sucesos que ocurren en forma repentina e inesperada causando graves daños materiales en diversas zonas geográficas de la tierra.

Las causas son geológicas, climáticas y el hombre mismo que mal usa las ciencias y técnicas en su afán de imponer políticas socio-económicas.

2. CLASES DE DESASTRES

Por su origen los desastres son: naturales y humanos.

2.1 DESASTRES NATURALES

Son de origen geológico y climático. Entre ellos tenemos:

- Terremotos.
- Erupciones volcánicas.

- Remoción en masa.
- Tsunamis.
- Huracanes, ciclones y tifones.
- Inundaciones.
- Sequías.
- Incendios.
- Plagas.

2.2 DESASTRES HUMANOS

Son provocadas por el hombre. Entre ellos tenemos:

- Guerras.
- Explosiones.
- Sabotaje.
- Espionaje.
- Incendios.
- Daños mal intensionados (causas psicológicas, venganza, celo en el trabajo).
- Fraude.
- Robo.
- Malversación.
- Daños fortuitos.

3. TERREMOTOS

3.1 CONCEPTO

Son súbitos movimientos terrestres producidos generalmente por el desplazamiento de las rocas a lo largo de las fallas que se encuentran en actividad, por la formación de fallas como producto de fuerzas horizontales y verticales de la corteza terrestre. Estos sismos se denominan terremotos tectónicos. El tercer tipo de terremotos se producen por las explosiones volcánicas.

3.2 CARACTERISTICAS DE UN TERREMOTO

Un terremoto tiene tres sacudidas: Sacudidas preliminares, sacudida principal y sacudidas posteriores comúnmente llamadas réplicas.

Los terremotos tectónicos se originan a diversas profundidades y se denominan:

- **TERREMOTOS NORMALES**

  Se dan de 0 a 50 Km. de profundidad.

- **TERREMOTOS INTERMEDIOS**

  Se dan de 50 a 250 Km. de profundidad.

- **TERREMOTOS PROFUNDOS**

  Se dan de 250 a 750 Km. de profundidad.

Los terremotos volcánicos debido a explosiones gaseosas o a la formación o inyección de magma en las fracturas de las rocas son poco

profundas. Las ondas sísmicas no excede de un centenar de Km2; aunque la intensidad cerca al volcán es elevado.

3.3 FOCO, EPICENTRO Y ONDAS SISMICAS DE UN TERREMOTO

- **FOCO O HIPOCENTRO**

  Es el punto donde se origina el sismo y se localizan a diversas profundidades de la corteza terrestre.

- **EPICENTRO**

  Es el punto en la superficie terrestre que se encuentra verticalmente encima del foco o hipocentro donde se origina el sismo.

- **ONDAS SISMICAS**

  Son las vibraciones de la corteza terrestre que se propagan en forma de ondas a partir del foco de un terremoto. Las ondas son de tres clases:

  Onda Preliminar P.-

  Son las vibraciones preliminares y son rápidas.

  Onda Secundaria S.-

  Son vibraciones lentas.

  Ondas Largas L.-

  Limitadas a la corteza terrestre son muy lentas.

3.4 LOS SISMOGRAFOS Y LAS ONDAS SISMICAS

La intensidad de las ondas sísmicas que perturban una región determinada, son registradas por los sismógrafos para lo cual se utiliza una escala arbitraria de 12 grados que se detalla a continuación.

ESCALA DE MEDICION DE LOS SISMOS [9]

ESCALA DE RICHTER Magnitud (Escala abierta) GRADOS	ESCALA DE MERCALLI Intensidad (modificada) GRADOS	
2	I-II	Tan sólo registrado en el sismógrafo
3	III	Se siente en el interior de las casas.
4	IV-V	Casi todo el mundo lo siente. Ligero daño material.
5	VI-VII	Todos lo sienten. Corren fuera de las casas. Daño menor a moderado.
6	VII-VIII	Todo el mundo corre fuera de las casas. Daño de moderado a intenso.
7	IX-X	Gran daño y muertes.
8	X-XII	Destrucción total Cataclismo.

[9] EL PERUANO: Escalas de Medición de los Sismos, Instituto Nacional de Defensa Civil, Día Internacional para la Reducción de los Desastres Naturales DIRDN 1990-2000, 11 Octubre 1995, p. 11.

3.5 EFECTOS DE LOS TERREMOTOS

Los terremotos provocan perturbaciones de la corteza terrestre, de las masas de agua, destrucción de las obras del hombre y pérdida de vidas humanas. Analizando tenemos:

- Cerca al lugar de origen se producen largas ondas superficiales sobre el terreno y están sujetos a cambiantes ondulaciones. Estas ondas tienen 30 cm. de alto y 10 mt. de longitud de onda.

  La rapidez de la elevación y depresión de la onda da la impresión de que el suelo está ondulado "como el mar agitado por una tempestad".

- Las ondas abren grietas en las crestas y se cierran al pasar la onda y luego se convierten en depresión. En las carreteras se abren zanjas y grietas, los carriles de los ferrocarriles son doblados y retorcidos, los puentes se derrumban, los edificios se tambalean y hunden.

- El efecto de las vibraciones verticales es tan fuerte que provocan el desprendimiento de rocas y tierras de las laderas de los valles, los aludes se precipitan de los nevados (Ejemplo: siniestro del 31 de mayo

1970 Departamento de Ancash), las aguas subterráneas sufren grandes perturbaciones y salen a la superficie bajo la forma de potentes chorros.

- Los terremotos submarinos son seguidos por olas sísmicas marinas de gran velocidad que avanza al continente los que reciben el nombre de tsunamis altamente destructores.
- Los grandes edificios y viviendas se derrumban, los conductores de gas se rompen y provocan incendios incontrolables.
- Los servicios de agua, desague, electricidad, teléfono, transporte, mercado y hospitales son alterados o destruidos provocando sed, desesperación, enfermedades (epidemias) y como secuela el saqueo y robo.
- Frente a tal desastre la pérdida de vidas humanas es espantoso y cuantificando económicamente las pérdidas materiales y humanas son incalculables.

3.6 TERREMOTOS: DEPARTAMENTO DE LIMA, ULTIMOS 50 AÑOS

En el Departamento de Lima en los últimos 50 años han ocurrido cinco sismos de gran intensidad.

El 24 de Mayo de 1940 de 8.2 grados, 18 de Febrero de 1957 de 6.7 grados, 17 de Octubre de 1966 de 7.5 grados, 5 de Enero de 1974 de 6.6 grados y 3 de Octubre de 1974 de 7.5 grados en la Escala modificada de Mercalli. Todos ellos provocaron graves daños. A continuación se da a conocer el siniestro de 1970 en el Departamento de Ancash, con fuertes repercusiones en el Departamento de Lima.

3.7 SINIESTRO 31 DE MAYO 1970 : DEPARTAMENTO DE ANCASH-PERU

Parámetros Epicentrales del Terremoto:

Localización	:	Valle del Santa, Costa Central Norte del Perú
Hora	:	15 horas 23 minutos 28
segundos Latitud Sur	:	9 grados 18 minutos
Longitud Oeste	:	78 grados 83 minutos
Profundidad del foco	:	52 Km.
Magnitud	:	7.8 a 8 grados escala modificada de Mercalli

Intensidad:

- 8 grados en la escala de Mercalli en sedimentos aluviales y arcillosos marinos entre 8 grados a 11 grados Latitud Sur.
- 9 grados en la escala de Mercalli en sedimentos poco consolidados entre Casma y Chimbote. En este sector las vibraciones verticales fueron fuertes.
- 7 grados en la escala de Mercalli, Valle del río Santa, movimiento vertical menos pronunciado.

Daños en el Valle del Santa:

- Destrucción en gran escala del centro antiguo de Huaraz.
- Las viviendas de la margen derecha del río Quihay no sufrierón daños los muros y tejados permanecieron intactos.
- Derrumbes de rocas en las pendientes de la Cordillera Negra, deslizamientos de los bordes de las terrazas fluviales.

Causas:

- Se originó por el movimiento de la placa oceánica hacía y debajo de la placa continental.

Consecuencias del Sismo:

- 54,000 muertos y 150,000 heridos (informe del 25 de junio de 1970).
- Daños materiales del orden del presupuesto nacional.
- Produjo el alud aluvión del Huascarán.
- Represamiento del río Santa y aluvión (sector de Yungay).
- Destrucción de la línea férrea de Chimbote a Huallanca y destrucción de los medios de comunicación.
- Emigración de la población.
- Destrucción de las cuidades de Chimbote y Casma.
- Terremoto más destructor del Continente.
- Desaparición de la cuidad de Yungay como consecuencia del alud-aluvión.
- Hundimiento del suelo en amplios sectores de Chimbote y Huaraz.
- Después de 12' del terremoto el mareógrafo de Chimbote registra una subida del mar de 30 cm. y luego un descenso también de 30 cm. una amplitud de onda de 1 m.; fenómeno típico de maremoto. El mareógrafo del Callao también registró el mismo fenómeno marino.

4. ERUPCIONES VOLCANICAS

Son expulsiones violentas de magma y gas de los volcanes debido a la presión de gases y producen terremotos de diversa intensidad, derrame de lavas a altas temperaturas y ceniza volcánica. Estos fenómenos son continentales y submarinos.

Las erupciones volcánicas submarinas generan los tsunamis peligrosos para la actividad del hombre en las regiones costeras.

El suelo peruano, al formar parte del Cinturón de Fuego del Pacífico se encuentra en peligro permanente de sufrir desastres por erupciones volcánicas.

5. TSUNAMIS

Son las olas marinas de flujo y reflujo que adquieren gran velocidad de efectos desbastadores en las regiones costeras producidas por terremotos y erupciones volcánicas submarinas.

A nivel mundial un tsunamis catastróficos se produjo en Lisboa en 1755. El mar se retiró para luego volver con olas de 12 m. de altura y a gran velocidad destruyendo ciudades, provocando ruina y desolación.

6. REMOCION EN MASA

Es el desplazamiento de materiales de roca y suelo pendiente abajo por acción de los terremotos o por la saturación del suelo por lluvias fuertes y permanentes.

Los movimientos de remoción son caídas rápidas, hundimientos y deslizamientos. En todos los casos favorece la pendiente del terreno y el agua. Según su naturaleza se denominan: aludes, avalanchas, huaycos y aluviones. Estos fenómenos se originan por las vibraciones de las ondas sísmicas de los terremotos, tal como ocurrió con el terremoto del 31 de mayo de l970 en el Callejón de Huaylas y los desastres de huaycos de marzo de 1987 en Chosica, por fuertes lluvias en la estación de verano.

7. INFORMES Y ANALISIS ESTADISTICOS DE GRANDES TERREMOTOS

7.1 CANTIDAD DE GRANDES TERREMOTOS POR DEPARTAMENTOS EN EL PERU (1582-1964) [10]

Nro.	Departamento	Cantidad de Sismos
1	Tumbes	2
2	Piura	1
3	Lambayeque	1
4	La Libertad	8
5	Ancash	6
6	Lima	18
7	Ica	8
8	Arequipa	18
9	Moquegua	3
10	Tacna	3
11	Cajamarca	2
12	Amazonas	2
13	San Martín	3
14	Huánuco	2
15	Pasco	5
16	Junín	1
17	Ayacucho	2
18	Apurimac	1
19	Huancavelica	0
20	Cuzco	5
21	Puno	1
22	Loreto	0
23	Ucayali	0
24	Madre de Dios	0

---

[10] SILGADO FERRO, Enrique: Historia de los Sismos más notables ocurridos en el Perú, Instituto de Geología y Minería, Boletín N°3, Lima-Perú, 1978.

7.2 GRANDES TERREMOTOS EN EL DEPARTAMENTO DE LIMA (1586-1964) [11]

Nro.	Fecha	Región afectada	Magnitud
1 -	09.07.1586	Costa-Lima	8.1
2 -	13.11.1655	Isla San Lorenzo	7.4
3 -	20.10.1687	Costa S. Lima	8.2
4 -	28.10.1746	Costa N. Lima	8.4
5 -	07.12.1806	Frente Pto.Callao	...
6 -	11.03.1926	Lima	...
7 -	20.01.1932	Lima	6.75
8 -	24.05.1940	Lima	8.00
9 -	03.08.1952	Lima	...
10 -	15.02.1953	Lima	...
11 -	21.04.1954	Mala-Lima	...
12 -	09.02.1955	Cañete	...
13 -	18.02.1957	Sayan	6.75
14 -	28.01.1901	Mala-Cañete	5.00
15 -	17.11.1966	Norte-Lima	7.5
16 -	28.09.1968	Mala-Pisco	6.3
17 -	05.01.1975	Huarochiri	6.6
18 -	03.10.1974	Lima-Sur	7.5

7.3 ANALISIS

Analizando la relación de los grandes terremotos tenemos:

- Los departamentos donde han ocurrido el mayor número de terremotos son Lima y Arequipa con 18 grandes sismos.
- Los Departamentos de La Libertad e Ica con 8 terremotos.

---

[11] SILGADO FERRO, Enrique: Historia de los Sismos más notables ocurridos en el Perú, Instituto de Geología y Minería, Boletín N°3, Lima-Perú, 1978.

- Los departamentos de Ancash con 6, Pasco y Cuzco con 5 terremotos.
- Los departamentos de Moquegua, Tacna, San Martín con 3 terremotos.
- Los departamentos de Tumbes, Cajamarca,, Amazonas, Huánuco, Ayacucho, con 2 terremotos.
- Los departamentos de Piura, Lambayeque, Junín, Apurimac, y Puno con un terremoto.
- Los departamentos donde no han ocurrido grandes terremotos son: Huancavelica, Loreto, Ucayali y Madre de Dios.

8. RELIEVE SUBMARINO DE LAS FOSAS FRENTE AL PERU

8.1 LAS FOSAS

En la parte este del Oceano Pacífico existe una inmensa depresión o surco cuya profundidad varía de 5,000 a 8,000 mt., se extiende desde 5 a 35 grados Latitud Sur. Esta depresión presenta una discontinuidad a la latitud de Nazca por una elevación submarina llamada **lomada o placa de Nazca,** que divide la depresión en dos sectores. El sector norte fosa de Lima y el sector sur fosa de Arica o Atacama. Según lo muestra la **Figura N°5 Relieve Submarino de la Fosas frente al Perú.**

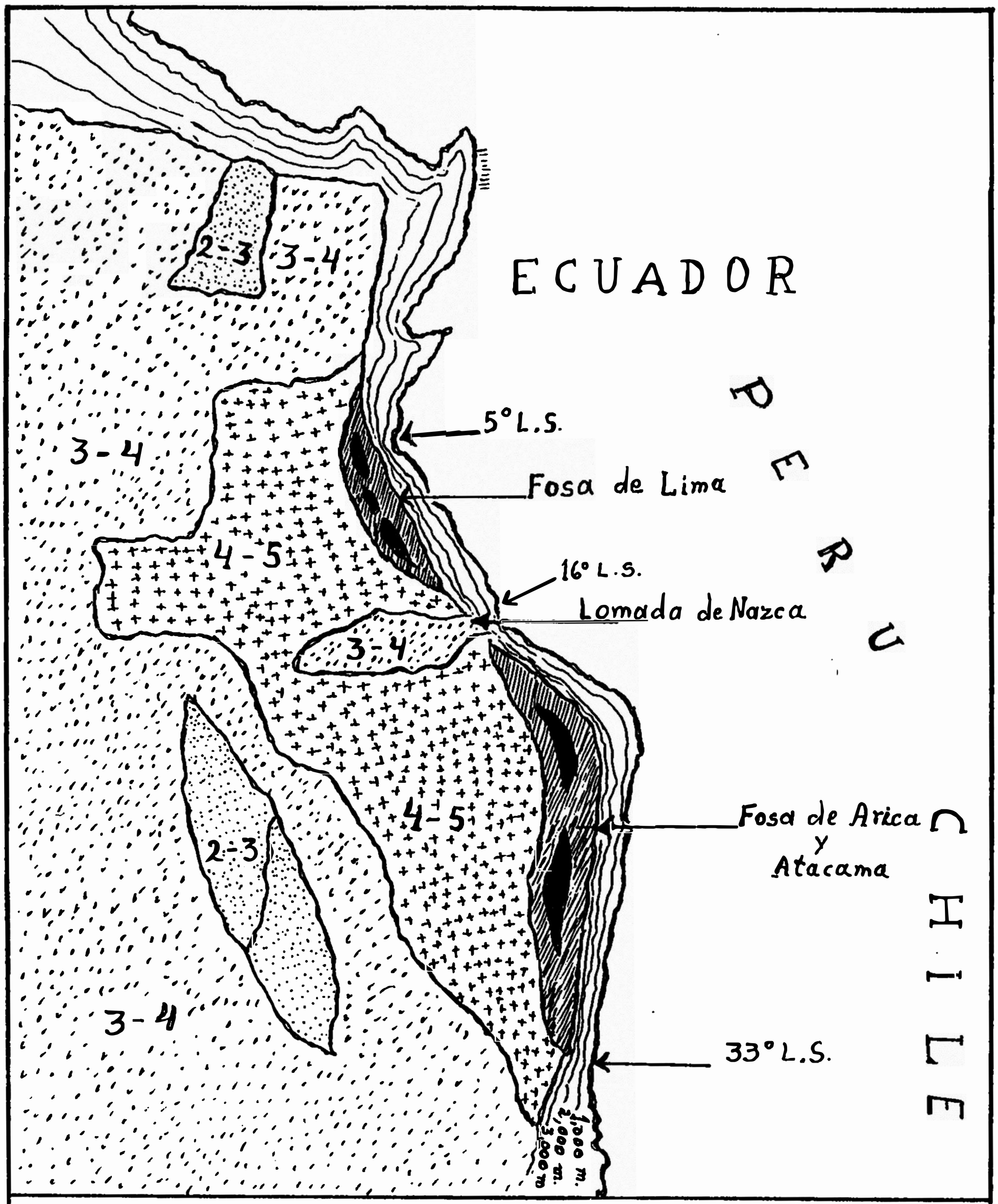


Fig. 5 Relieve Submarino de las Fosas frente al Perú

Símbolos	Profundidad en miles de m.
	2,000 a 3,000
	3,000 a 4,000
	4,000 a 5,000
	5,000 a 6,000

8.2 FOSA DE LIMA

Se extiende frente a la Costa peruana entre Punta Aguja y Punta de Paracas. Tiene una longitud de 1,200 Km., un ancho entre 30 y 40 Km. y una profundidad máxima superior a los 6,000 mt.

Su lado Oriental está formado por la placa continental (suelo peruano) y el lado occidental esta constituido por la pendiente oriental de la placa submarina.

Esta fosa es considerada como elemento dinámico generador de sismos y sus principales profundidades son:

Frente a Paracas	-	5,020 mt.
Frente a Cerro Azul	-	5,200 mt.
Frente al Callao	-	6,200 mt.
Frenta a Ancón	-	6,147 mt.
Frente a Huacho	-	6,047 mt.
Frente a Chimbote	-	6,263 mt.
Frente a Salaverry	-	6,003 mt.
Frente a Sechura	-	5,710 mt.

Al norte de Sechura existen dos fosas de 5,000 mt. y más al norte las profundidades disminuyen y frente a Ecuador la profundidad es de 3,000 mt.

8.3 FOSA DE ARICA O ATACAMA

Se extiende desde los 16 grados 30 segundos Latitud Sur (Ocoña), hasta los 35 grados Latitud Sur (Antofagasta) frente a Chile. Tiene una longitud aproximada de 2,000 Km. y su ancho varía entre 40 y 50 Km.

Presenta dos direcciones: Una de sur a norte frente a Chile desde los 35 grados Latitud Sur hasta los 19 grados Latitud Sur y la otra dirección de Sur-Sur Este al Norte-Noroeste desde los 19 grados Latitud Sur a los 16 grados 30 minutos Latitud Sur.

Esta fosa también es elemento dinámico generador de sismos y sus principales profundidades son:

- Frente a Chile (fosa de Atacama) en Antofagasta al Sur 7,918 mt. y al norte 8000 mt.
- Frente al Perú (fosa de Arica) a 26 grados Latitud Sur - 7,668 m. y 25 grados latitud Sur a 25 grados Latitud Sur 7,627 mt.

8.4 PLACA O LOMADA DE NAZCA

Según el Dr. Revelle (francés) a partir de la latitud de Nazca y con un ancho de 260 Km. y una longitud de 5,600 Km. viene desde el fondo

oceánico una gran cresta submarina que asciende desde el mar hacia la costa y chocar con la placa continental (suelo peruano) unos 3,000 m. de profundidad. Este relieve submarino recibe el nombre de placa o lomada de Nazca.

Esta placa divide el gran surco o fosa oceánica del Pacífico Oriental en la fosa de Lima al Norte y la fosa de Atacama al Sur.

Según las investigaciones del Dr. Revelle considera que la cresta submarina nos indica la existencia de un fuerte levantamiento del fondo del Pacífico Oriental.

En el flanco oriental del continente sudamericano, la placa de Nazca se mueve aproximadamente a 10 cm/año contra la placa continental que los hace a 4 cm/año en sentido contrario. La placa de Nazca (oceánica) se introduce por debajo de la placa continental hasta ser absorbida por el manto. Este movimiento produce la acumulación de energía en algunas zonas, que se resisten a los desplazamientos de las placas. Posteriormente, esta energía se libera en forma de actividad sísmica o valcánica. Según lo muestran la **Figura N°6 Configuración del contacto Placa de Nazca - Placa Continental y la Figura N°7 Corte Geológico Placa de Nazca y Placa Continental.**

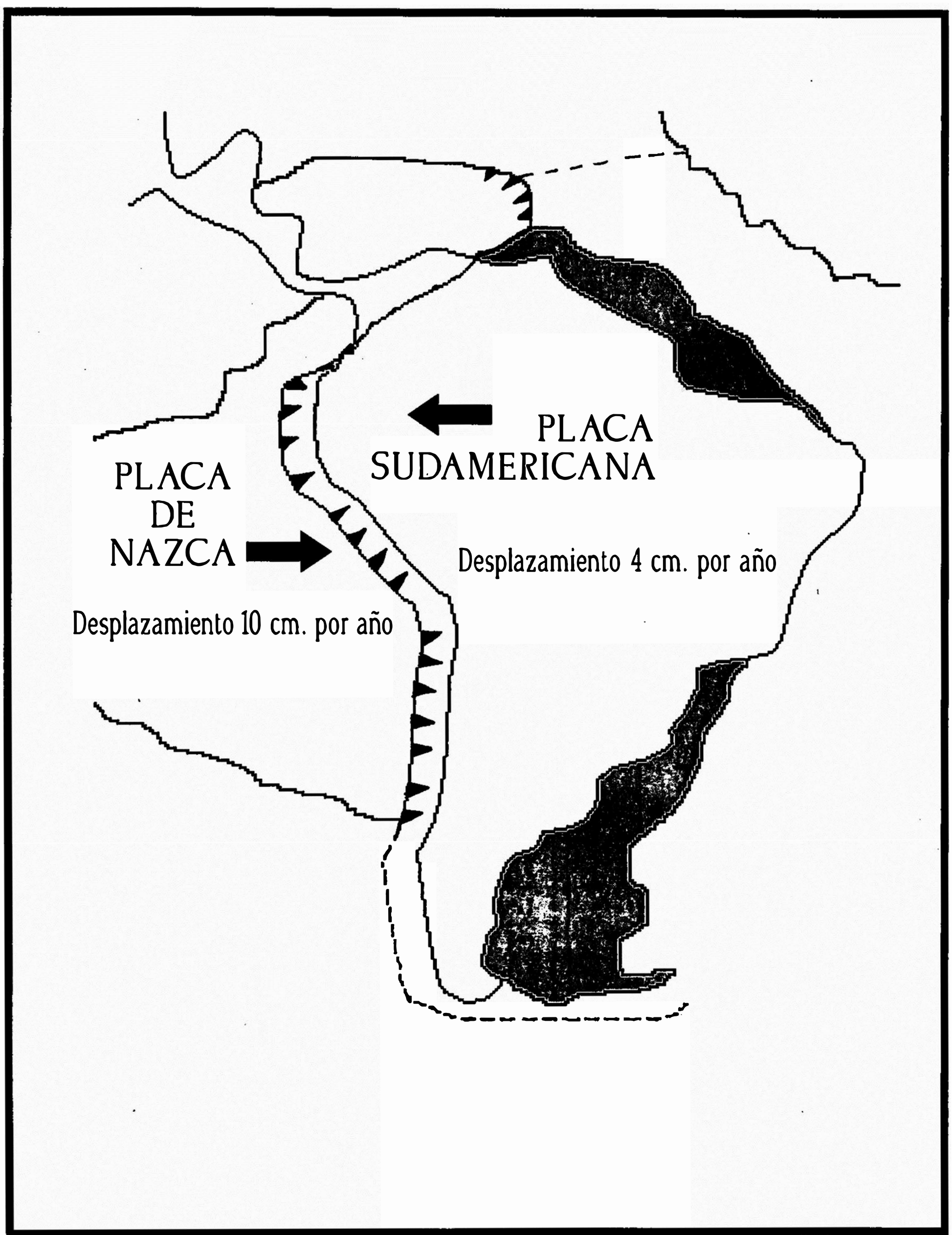


Fig. 6.

Configuración del contacto Placa de Nazca - Placa Continental

Hernando Tavera: La Tierra, Tectónica y Sismicidad - Inst. Geofísico del Perú 1993

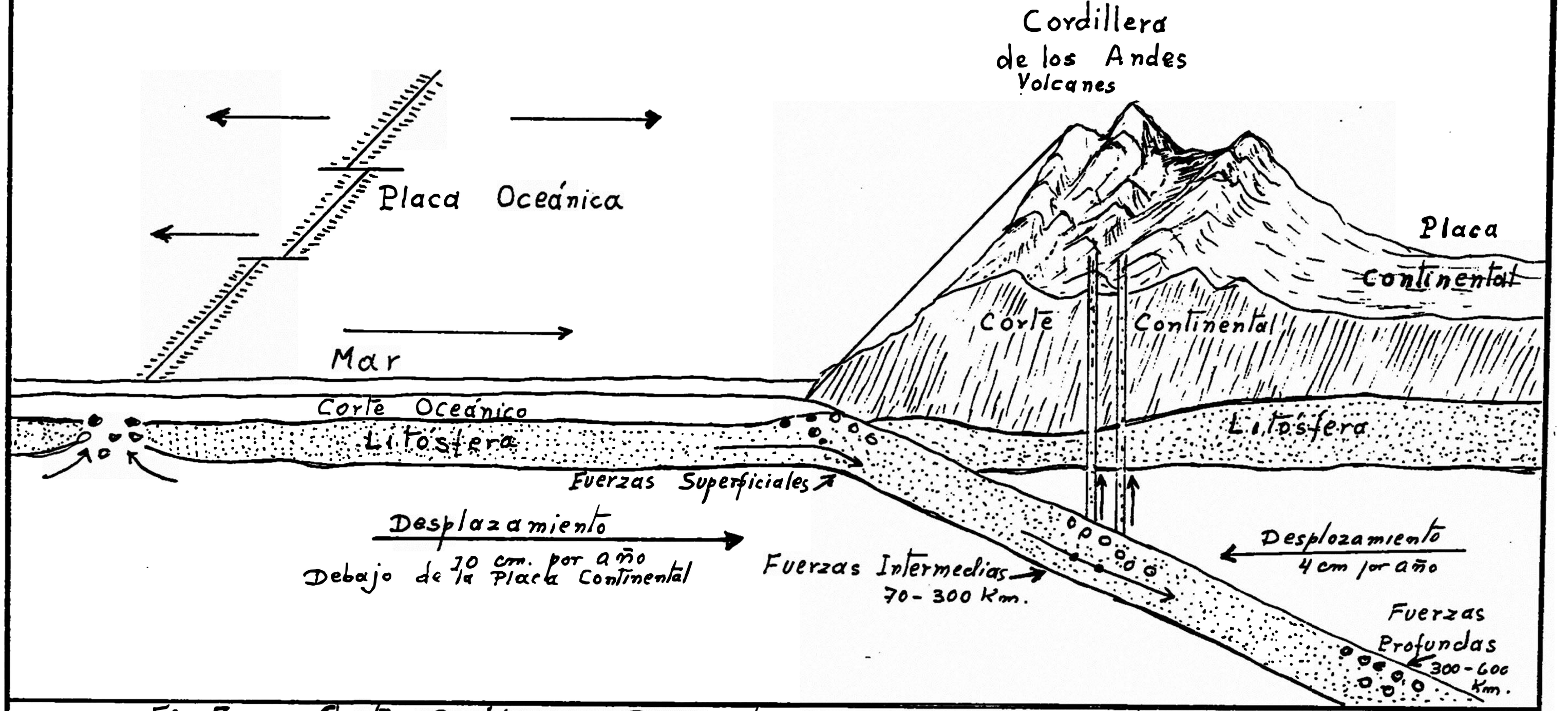


Fig: 7 Corte Geológico Placa de Nazca y Placa Continental

Hernando Tavera: La Tierra, Tectónica y Sismicidad - Inst. Geofísico del Perú - 1,993

8.5 CONSECUENCIAS

- Genera sismos al levantarse e introducirse debajo del suelo peruano.
- Se está levantando el suelo peruano en la Costa Central.

CAPITULO VII

VIRUS INFORMATICO

1. GENERALIDADES

El avance de la Informática y sus aplicaciones en las diversas actividades públicas y privadas del mundo moderno; ha dado lugar a intereses económicos y políticos contradictorios. El producto de dicha contradicción es la creación de los virus informáticos deliberadamente destructivos en la informática.

Ante los graves problemas generados por los virus en los programas de software, los investigadores han creado programas anti-virus con técnicas de protección y prevención, los que cada vez son más sofisticados.

2. CONCEPTOS

2.1 En atención a la complejidad de la ciencia de la informática, considero que los virus informáticos: Son simples programas de

computación elaborados por especialistas en informática muy ingeniosos. Dichos programas, altera o destruye la información de los sistemas informáticos.

2.2 Entre otros conceptos dados por investigadores tenemos:

Curso SEGURIDAD EN SISTEMA DE INFORMACION, dictado por la Compañía I.B.M. de Lima Perú, en Julio 1995 se plantea que:

Virus Informático es un "Programa que modifica a otros para incluir en ellos una copia de sí mismo". [12]

El Señor Fernando Salmerón de la Rosa especialista de la I.B.M. al explicar dicho concepto dice que los virus informático requieren tres condiciones:

- **EFECTO.-** En un momento dado, al invocarse puede realizar una función maliciosa o inesperada y por lo general esta función pasa inadvertida en los PC (computador personal).
- **PERSISTENCIA.-** Puede permanecer activo sólo en los backup's de data.

[12] SALMERON DE LA ROSA, FERNANDO: Curso Seguridad en Sistema de Información, IBM del Perú, Junio 1995.

- **PERNICIOSIDAD.-** La amplitud de infección depende del entorno que tantos problemas genera.

2.3 El CONCYTEC, en el libro, VIRUS INFORMATICOS EXPERIENCIAS Y SOLUCIONES, de los ingenieros Walter Iriarte, Raúl Nombera y Manuel Rodríguez, presentan tres conceptos diferentes de virus de computadora que se complementan: [13]

- "Son generalmente programas muy cortos que contienen instrucciones que atacan a determinadas interrupciones y luego efectúan su acción, creando copias de sí mismo para luego propagarse y alojarse en los sectores del Boot, la Fat y/o en cualquier otro lugar".
- "Son pequeños programas que pueden permanecer "dormidos" durante un período de tiempo determinado (horas, días, meses o años); y una vez que ciertas condiciones se han cumplido, empieza la función para la que han sido creadas".
- "Son segmentos de código autorreplicativos, que atacan a programas de aplicación o

---

[13] IRIARTE, NOMBERA Y RODRIGUEZ: Virus Informáticos, Experiencias y soluciones, CONCYTEC, 1990, p. 17, 18.

sistemas ejecutables".

Las tres definiciones compiladas tienen el mérito de ser, el producto del Symposium realizado en marzo de 1990, en la Facultad de Petróleos de la Universidad Nacional de Ingeniería.

2.4 Richard B. Levin al responder ¿Qué es un virus informático? en su libro VIRUS INFORMATICO, dice:

"Los virus informáticos son programas de software del mismo modo que los procesadores de texto, hojas de cálculo, gestores de bases de datos, etc., son programas informáticos. Esto significa que son simplemente listas de instrucciones que dicen a las computadoras que acciones hay que ejecutar y precisamente cómo ejecutarlas...Hay una descripción: un virus es un programa que modifica a otros programas al incluir una copia de él mismo ejecutable y posiblemente alterada...". [14]

2.5 Gonzalo Ferreyra Cortés, en su libro VIRUS EN LAS COMPUTADORAS, define a los virus informático de

---

[14] LEVIN, RICHARD B.: Virus Informáticos, Mc Graw-Hill Interamericana de España, S.A., 1991, p. 6.

la siguiente manera:

"Los virus de las computadoras no son más que programas, ¡Sí,simples programas de computación elaborados por programadores! Son programas similares al de un procesador de textos o de una hoja de cálculo, a un programa de base de datos o a un programa de control de inventarios, es decir, programas que contiene instrucciones para que las ejecute la computadora". [15]

También Ferreyra nos da a conocer otras definiciones, tales como:

- **De Ralph Burger en su libro WHAT YOU SHOULD KNOW ABOUT COMPUTER VIRUSES:**

  "Un programa que puede insertar copias ejecutables de sí mismo en otros programas. (El programa infectado puede infectar a su vez otros programas)". [16]

- **De Alberto Rojas, en su artículo ¿Ya Vacuno a su PC?, publicado en la revista mexicana PC/TIPS:**

  "Todo aquel código que al ser ejecutado

---

[15] FERREYRA C., GONZALO: Virus en las Computadoras, Macrobit, Mexico, p. MF3-1.

[16] Ibid, p. MF3-2.

Figura 8. Se comparan los virus informáticos con los biológicos

altera la estructura del software del sistema y destruye programas o datos sin autorización ni conocimiento del operador". [17]

Analizando las definiciones tenemos las siguientes coincidencias:

- Son pequeños o simples programas de computación.
- Se presentan en forma inesperada.
- Al modificar su estructura se reproducen automáticamente para evitar ser detectados.
- Se presentan en forma anónima, a pesar de tener autor.
- Al propagarse a través del sistema se multiplican con asombrosa rapidez.
- Su comportamiento viral altera o destruye los programas de computación.

3. CARACTERISTICAS DE UN PROGRAMA VIRUS

Al describir las características o propiedades del programa virus, se presentan dos análisis que son semejantes:

---

[17] FERREYRA C.,GONZALO: Virus en las Computadoras, Macrobi, Mexico, 1991, p. MF3-2.

3.1 Los tratadistas en ciencia de la Informática:

Afirman que los programas virus deben reunir las siguientes propiedades:

- Poder de modificar el software, que no pertenece al programa virus, uniendo sus estructuras dentro de otros programas.
- Facultad para ejecutar la modificación en varios programas.
- Capacidad para reconocer una modificación en uno o más programas.
- La habilidad de impedir o prevenir que vuelva a ser modificado el mismo programa al reconocer que ya está infectado.
- El software modificado, adquiere los atributos anteriores y como consecuencia, iniciar el mismo proceso con otros programas en otros discos.

3.2 La IBM al referirse a la Anatomía de un virus, explica que un programa virus debe reunir cuatro componentes básicos, estos son:

- **MECANISMO DE REPLICACION**

  Parte de su código dedicada a reproducir a sí mismo.

- **MECANISMO DE PROTECCION**

  Parte de su código que lo protege y esconde

muy sofisticados en las últimas generaciones de virus (poliformicos stealth).

- **MECANISMO DE ACTIVACION**

  Código que activa el mecanismo de Carga Util ante condición dada. Con frecuencia se relaciona con fechas y horas determinadas también con cantidad de booteos, secuencia de fechas y/o comandos.

- **MECANISMO DE CARGA UTIL**

  Lo que el virus realmente hace. Varía desde un mensaje curioso o trivial hasta destrucción total o parcial de datos captura de password.

4. PROPAGACION DE LOS VIRUS

Ante el problema de la propagación de los virus informaticos, nos preguntamos ¿Por qué y Cómo se propagan?.

La respuesta al por qué? está dada por las características o propiedades del virus y el cómo se propagan se menciona a continuación:

- Por copia o compartir programas.
- Al compartir Worksktation/PC's.
- Por transporte de programas.
- Propagación en LAN (Redes); esta se dá desde el

SERVER, desde PC 1 del LAN y desde el PC 2 del LAN.

- Por propagación compartiendo programas; esta se dá: De PC 1 al PC 2, del PC 2 al PC 3 y desde el PC 3.
- Por propagación estadística; fuente PC World.
- Propagación por tendencias recientes; esta se dá: Infecciones a LAN's (Redes), virus clandestinos diseñados para evitar detección, virus protegidos diseñados para evitar análisis, más acciones destructivas (mayoría a través de errores de código) y los métodos de infección más complejos (insidiosos).

5. ESTADISTICAS REPORTADAS 1994: ESTUDIO DE NCSA/ DATAQUEST [18]

5.1 EFECTO EN EMPRESAS AFECTADAS POR VIRUS

68% Archivos perdidos o malogrados.

62% Pérdida de productividad

41% Computador bloqueado

24% Aplicaciones de SW no confiables

23% Caída de la Red (LAN)

20% Usuario pierde confianza en los sistemas.

---

[18] SALMERON DE LA ROSA, Fernando: Curso Seguridad en Sistemas de Información, IBM del Perú, Junio 1995.

5.2 COMO INGRESAN LOS VIRUS A LAS EMPRESAS

65% DISKETTES INCLUYENDO:

43% Del hogar (usada en PC del hogar o en la de algún amigo, juegos, archivos de datos, SW pirata).

6% Diskettes de demostración.

6% Diskettes de Servicio Técnico.

3% En tienda (el usuario no sabía que los diskettes del SW que compraba o archivos de datos había sido devueltos por otro usuario).

2% Diskettes de compañero de trabajo.

1% Visitante desconocido a PC del usuario.

1% Del administrador de la Red.

1% De PC's de universidades, institutos,etc.

1% De un cliente o proveedor.

1% De un consultor.

7% SERVICIO DE BULLETIN BOARD VIA MODEM.

25% COPIADO DE LA RED.

1% SOFTWARE PRECARGADO EN PC NUEVA.

6. TIPOS DE VIRUS

- La primera clasificación los agrupa en dos categorías: Caballos de Troya y Bombas de tiempo.

- Alberto Rojas (México) presenta tres grupos: Caballos de Troya, Autorreplicables y Esquemas de Protección.
- La Computer Virus Industry Association integrado por Compañías y programadores presenta tres clases: Infectores del área de carga inicial [boot infectors] infectores de sistemas e Infectores de programa ejecutables (extensión COM o EXE).
- Otra clasificación los llamados: gusanos y virus lógicos.

Del resultado de las investigaciones se dan las siguientes categorías:

6.1 CABALLOS DE TROYA

Se introducen al sistema, con una apariencia diferente al objetivo final como información perdida sin sentido. Después de un tiempo actúan y destruyen la información de los discos.

6.2 BOMBAS DE TIEMPO

Son programas ocultos en la memoria del sistema o discos, en los archivos de programas ejecutables con extensión COM o EXE. Esperan una fecha determinada y explotan.

6.3 AUTORREPLICABLES

Son parecidos a los virus biológicos, ya que se autorreproducen e infectan los programas del disco. Se activan en fechas programadas y se replican a partir de la última actividad. Ejemplo: Virus del viernes 13.

6.4 ESQUEMAS DE PROTECCION

No son propiamente virus, pero su acción dañina se activa al copiar un programa protegido contra copia. El resultado, se bloquea a sí mismo, alterando su estructura original o dañando los archivos y muy difícil su recuperación.

6.5 INFECTORES DEL AREA DE CARGA INICIAL

Infecta los diskettes, disco duro y se alojan en el área de carga 0 sector 0. Toman el control al encender la computadora y lo conserva todo el tiempo.

6.6 INFECTORES DEL SISTEMA

Se introducen en los programas de sistema. Ejemplo el COMAND.COM. Otros se alojan como residentes de memoria. Los comandos del DOS, como COPY, DIR o ERASE, que se introducen en la memoria al cargar el sistema operativo. El virus

adquiere el control del disco.

6.7 INFECTORES DE PROGRAMAS EJECUTABLES

Son los virus mas peligrosos. Se diseminan fácilmente hacia cualquier programa (hojas de cálculo, juegos, procesadores de textos, etc.). Ejemplo: Virus Jerusalén.

6.8 GUSANOS

Programas que se reproducen así mismo, no necesitan de un anfitrión. Infectan todo el sistema por "arrastre" y por donde pasan borran los programas o información.

6.9 VIRUS LOGICOS

Programas normales que si no son manejados con cuidado pueden dañar la información, modificándola o borrándola y tomando su lugar.

Marco A. Merino, de acuerdo al sentir del usuario publicó en la revista Expansión de la Universidad Autónoma de México los siguientes grupos de virus: benigno, burlones, caóticos, crecidos, descarados, estadísticos, físicos, juguetones, malditos, mentirosos, mutantes, resentidos, simples,

supervisores, temporales, vengadores, viajeros. [19]

7. VIRUS COMUNES

La Computer Virus Industry Associatrivon, estudió y catalogó cerca de 250 virus.

Patricia M. Hoffman en California Estados Unidos elaboró una lista con más de 900 virus.

Dave Ferbrache (Inglaterra), Gonzalo Ferreyra Cortés (México) y otros investigadores siguen estudiando el problema de los virus y diseñando programas antivirus.

[19] FERREYRA C. GONZALO: Virus en las Computadoras, Macrobi, Mexico, 1991, p. MF4-14; MF4-15; MF4-16.

7.1 REPORTE PARCIAL DE VIRUS COMUNES DETECTADOS EN EL PERU [20]

Nombre : 1530 / HACKER-II

Alias : SVC.2936

Tamaño : 2,936 bytes

Origen : (?) Perú.

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	NO	NO	SI	SI	SI	SI

Descripción:

Fué detectado por primera vez en el Perú en Setiembre de 1991 en la ciudad de Lima. Es residente en memoria e infecta archivos .COM y .EXE utiliza técnicas de **stealth** para no poder ser fácilmente detectado. Maneja marcas especiales en los archivos que infecta,lo que teóricamente hace que un archivo infectado no pueda ser reinfectado. Este virus es sumamente destructivo y se activa a partir de 1992 los días 4 y 25 de Junio, fecha en la que procede a destruir el disco duro formateándolo. Su origen es desconocido aunque ha sido **bautizado** como **virus nacional** por no poder ser detectado en su momento por algunos antivirus internacionales SCAN, CPAV.

[20] MARTINEZ, José A.: The Hacker, Antivirus V3.1, 1992-1995.

Nombre : 1784 / MUTATION ENGINE

Alias : FLIP 2, THREE TUNES, V-1784

Tamaño : 1,784 bytes

Origen : (?) (USA)

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	SI	NO	NO	SI	SI	SI

Descripción:

Este virus fué uno de los primeros virus auto-encriptables que se han encontrado en el Perú.

Tiene un cargador variable lo que hace que no pueda ser detectado fácilmente con rutinas standares de búsqueda de cadenas, ya que cada archivo infectado es diferente de otro.

Fué detectado por primera vez en Agosto de 1993 en Lima.

No es residente en memoria e infecta archivos .COM y .EXE.

Se activa en el mes de Junio emitiendo sonidos musicales en forma continua, es muy común en nuestro medio.

Se conocen 2 variantes de este virus:

- V-1792
- V-1784.B

Nombre : CACO

Alias : GENE-101, AFM, RAFAEL

Tamaño : 2,675 bytes

Origen : (?) Perú

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	SI	NO	SI	SI	SI	SI

Descripción:

Fué detectado por primera vez en el Perú en Julio de 1994 en la ciudad de Lima. Es una variante del virus SVC.

Infecta archivos ejecutables EXE y COM, puede infectar el COMMAND.COM.

Es residente en memoria y utiliza técnicas de **stealth** para evitar ser detectado mientras está en memoria.

Muchas partes del virus original (SVC) han sido torpemente modificadas. Este virus puede dañar al momento de la infección archivos que manejan overlays internos.

Se activa a partir de noviembre de 1994, mostrando en la primera línea de la pantalla el siguiente mensaje en forma permanente:

CACO VIRUS GENE-101.COCO, ALDO, CHINO, OTTO

DOOM-TEAM &CREADORES DE VIRUS&

Este mensaje es mostrado en la primera variante conocida, pero se conocen otras variantes:

- **A&F&M&**

Casi idéntico al supuesto original, con la diferencia que los mensajes están encriptados.

Contiene el texto:

A&F&M&T&1&f:2&7&-6&9&9&1 (?)

- **RAFAEL**

Esta variante muestra el mensaje:

TIENES EL VIRUS RAFAEL

LLAMAME PARA ELIMINACION

TLF:27-????

en el centro de la pantalla después de 2 horas de haber ejecutado un programa infectado.

- Existen algunas **variantes** donde sólo se ha modificado el mensaje de CACO ... por otros mensajes, por lo demás el virus es idéntico al original ó variantes.

Nombre : CPW_CHILENO

Tamaño : 1,459 bytes

Origen : Chile

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	NO	NO	NO	SI	SI	SI

Descripción:

Este virus fué detectado en el Perú en Mayo de 1993.

Infecta archivos ejecutables (EXE, COM), no utiliza técnicas de **stealth.**

Como parte del virus se puede encontrar el siguiente mensaje:

Este programa fué hecho en Chile en 1992 por CPW.

You are here CPW!

Las iniciales CPW son encontradas también en el virus VIVA CHILE!!!

Se activa el 27 de mayo presentando el siguiente mensaje:

¡Feliz cumpleaños CPW!

Nombre : DEC3

Alias : VIKING

Tamaño : 1,333 bytes

Origen : USA

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	NO	NO	NO	SI	SI	SI

Descripción:

DEC3 fué detectado en el Perú en marzo de 1994 en la ciudad de Huanuco.

Este virus se auto-encripta, infecta archivos ejecutables (EXE, COM), no utiliza técnicas de **stealth**.

Cuando se ejecuta un programa infectado el virus vé la versión del sistema operativo, si no es 3.2, 3.3, 4.0 ó 5.0 muestra el siguiente mensaje:

Dec 3 92 is my 20th birthday (V6)

Es un virus dañino, cuando se intenta borrar un archivo, primero serán borrados todos los archivos COM y EXE del directorio por defecto.

Nombre : JERUSALEM.AGUILAR

Alias : JERUSALEM.ALTERADO II

JERUSALEM.ESPEJO II

Tamaño : 1,894 bytes

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	SI	NO	NO	SI	SI	SI

Descripción:

Este virus es una variación del virus JERUSALEN ESPEJO. **Fué detectado por primera vez en el Perú el Abril de 1993 en la ciudad de Chiclayo.**

Es residente en memoria e infecta archivos .COM y .EXE, como la mayoría de los virus variantes del JERUSALEM no infecta el COMMAND.COM. Para los archivos tipo .COM maneja una marca especial 03-93 al final de los mismos, los archivos tipo EXE no tienen marca y pueden ser re-infectados un número ilimitado de veces. Destruye programas que trabajen con overlays internos, haciéndolos irrecuperables una vez eliminado el virus. Se activa los días 17 y 30 de cada mes, presentando en forma permanente en la primera línea de la pantalla el siguiente mensaje : AGUILAR FERNANDEZ V.F.

FONO: 22_6929

MARZO/1993

Nombre : JUNIO_1530

Alias : SVC.3241

Tamaño : 3,241 bytes

Origen : (?) Perú.

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	NO	NO	SI	SI	SI	SI

Descripción:

Fué detectado por primera vez en el Perú en Enero de 1993 en la ciudad de Lima.

No es residente en memoria. Infecta archivos .COM y .EXE, utiliza técnicas de **stealth** para no poder ser fácilmente detectado.

Maneja marcas especiales en los archivos que infecta, lo que teóricamente hace que un archivo infectado no pueda ser re-infectado.

Es un virus muy parecido al virus 1530, con la diferencia que las rutinas para destruir discos han sido deshabilitadas.

Su origen es desconocido aunque ha sido **bautizado** como **virus nacional** por no poder ser detectado en su momento por algunos antivirus internacionales (SCAN, CPAV).

Nombre : Junkie

Alias : Dr.White

Tamaño : 1,037 bytes

Origen : Suiza

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
SI	SI	SI	NO	NO	SI	NO	SI

Descripción:

Este virus fué descubierto por primera vez en el Perú en diciembre de 1994.

Puede infectar archivos .COM, así como la tabla de partición y boot sectors de discos duros y diskettes.

Como parte del virus se pueden encontrar los siguientes mensajes:

- Dr White - Sweden 1994
- Junkie Virus - Written in Malmo

No utiliza técnicas de **stealth**.

Nombre : M.G. EXTEND

Tamaño : 2,597 bytes

Origen : (?)

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
SI	SI	NO	NO	SI	SI	SI	SI

Descripción:

Infecta archivos ejecutables, así como el MBR del disco duro y BOOT SECTOR de los diskettes.

Este virus contiene rutinas para evitar ser analizado/depurado.

Fué detectado por primera vez en el Perú, en Enero de 1995 en un conocido Instituto de Lima.

Su origen es desconocido, como parte del virus se encuentra:

26/02/93

M.G.

G.M.

Aparentemente estas son las iniciales del autor del virus.

¡ NOTA: ¿

Cuando infecta el MBR de un disco duro sobrescribe la tabla de partición, el virus simula N particiones extendidas.

Si se butea la computadora desde un diskette, el DOS no encontrará datos válidos en la partición

y no reconocerá el disco duro como un disco DOS (no hay unidad C:).

En cambio cuando se butea desde el disco duro, el virus se ejecuta antes que cualquier otro programa y simulará en todo momento que la partición no ha sido modificada.

Si se carga el sistema desde un diskette DOS y se ejecuta el programa TH.EXE para la eliminación del virus MONKEY, la unidad C: no estará disponible en la opción ¡DISCO ¿por lo ya explicado. En estos casos se tiene que utilizar la opción ¡MBR en disco duro que permite detectar virus en el MBR aún si el DOS no reconoce el disco duro como unidad C:

Nombre : NATAS

Tamaño : 4,744 bytes

Origen : USA

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
SI	SI	SI	SI	SI	SI	SI	SI

Descripción:

Este virus es totalmente poliformico y fué detectado por primera vez en Lima en Noviembre de 1994.

Puede infectar el Master Boot Record (MBR), BOOT SECTOR y archivos ejecutables. Utiliza avanzadas técnicas de **stealth** para evitar ser detectado, las rutinas de **stealth** son desabilitadas si el nombre de un programa efectuado comienza con: AR, LH, PK, MODEM,BACK.

Es un virus altamente dañino. Posee una rutina de activación que formatea el disco duro.

Existe 1 en 512 posibilidades que formatee el disco duro al ejecutar un programa infectado.

El disco duro también es formateado si el virus intenta ser analizado mientras esta en memoria.

Como parte del virus se puede encontrar un texto al final que dice:

Natas

Existe una variante de 4,746 bytes.

Nombre : STEALTH BOOT, KATHIA

Alias : STEALTH BOOT, PRINTER

Origen : Perú

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
SI	SI	SI	NO	NO	SI	NO	NO

Descripción:

Este virus es una variante del virus STEALTH_BOOT y puede infectar MBRs y Boot sectors. Se activa en el mes de diciembre presentando el siguiente mensaje:

¡¡Tienes el virus Kathia!!

¡Quedas invitado(a) a su fiesta el 26 !

¡No tomes mucho !

Este programa fué creado en el Laboratorio Luz de Luna en Lima-Perú (c) 1993 - Por Angel X.

El citado **Laboratorio Luz de Luna** también es encontrado como parte del virus JUSTICIERO 3L.

Variantes: - STEALTH-BOOT, PRINTER

Se puede encontrar como parte del virus los siguientes mensajes:

- ALFREDO
- LIMA - PERU
- (c) Laboratorio Luz de Luna
- ANGEL X TE SALUDA

Algunos de estos mensajes pueden ser enviados a la impresora en forma aleatoria.

Nombre : STONED.ESPEJO

Alias : Mensaje

Origen : Perú

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
SI	SI	NO	NO	SI	SI	NO	NO

Descripción:

Infecta el MBR de los discos duros y BOOT SECTOR de los diskettes.

Es una POBRE y TORPE modificación del virus STONED

Fué detectado en Lima en Junio de 1991.

Se activa mostrando el siguiente mensaje en la pantalla:

ROGER ESPEJO M.

Telef. 45-1838

Lima - Perú

Un texto parecido puede ser encontrado también en los virus JERUSALEM.ESPEJO y STONED.ESPEJO.112.

Nombre : SVC 5.0

Alias : SVC.3103

Tamaño : 3,103 bytes

Origen : Rusia

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	NO	NO	SI	SI	SI	SI

Descripción:

Es uno de los virus más comunes en Lima, infecta archivos ejecutables (EXE Y COM), no infecta el COMMAND.COM.

Utiliza técnicas de **stealth** para evitar ser detectado.

Como parte del virus se encuentra el siguiente texto :

(c) 1990 by SVC, Vers 5.0

Nombre : ROGUE

Tamaño : 1,213 bytes

Origen : (?) Perú

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	NO	NO	SI	SI	SI	SI

Descripción:

Infecta archivos ejecutables EXE y COM, puede infectar el COMAND.COM, es residente en memoria y maneja algunas técnicas de **stealth**.

Fué detectado por primera vez en Lima en Marzo de 1993.

Se activa a partir del mes de Julio de 1993, todos los días lunes, mostrados en pantalla el siguiente mensaje en forma permanente:

Now you goy a real virus !, I' m the ROGUE...

Además dañará todos los archivos .DBF accesados en ese día.

Se conocen algunas variantes de este virus:

- ROGUE.STANDARD.A

Aparentemente es la primera versión del virus malogra archivos, COM menores a 400 bytes, debido a un error en el virus.

- ROGUE.STANDARD.B

Es una versión modificada casi idéntica original de 1,225 bytes.

■ Caligula, Cachete, Angel vengador, etc

Son idénticos al ROGUE.STANDARD con la diferencia que el mensaje de:

Now you got a real virus! ....

a sido modificado por:

Muerte a Caligula. El Angel Vengador.

Angel vengador II....

Nombre : ROGUE IV

Tamaño : 1,810 bytes

Origen : (?) Perú

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	SI	NO	SI	SI	SI	SI

Descripción:

Infecta archivos (EXE Y COM), **fué detectado por primera vez en Lima en Mayo de 1993.**

Una característica de este virus es que utiliza el método de inserción para infectar archivos tipo EXE. Utiliza algunas técnicas de **stealth**.

Es un virus altamente destructivo, se activa a partir de setiembre de 1993. Muestra el siguiente mensaje:

MS-DOS starting

Please Wait...

y empieza a borrar todos los archivos del disco duro. Finalizada la destrucción muestra el siguiente mensaje:

You Catchet.

I'm The Rogue.

Nombre : VCL.JUSTICIERO

Tamaño : 674 bytes

Origen : Perú

Características:

MBR	BS	ENC	POL	STE	RES	EXE	COM
NO	NO	SI	NO	NO	NO	NO	SI

Descripción:

Es un virus simple, derivado de la herramienta VCL (virus creation library), infecta sólo archivos COM y NO es residente en memoria.

La totalidad del virus se encuentra encriptada.

Cuando se ejecuta un programa infectado, el virus infectará todos lo archivos .COM del disco.

Dentro del virus se puede encontrar el siguiente mensaje en forma codificada:

! (c)Copyright Laboratorio Luz de Luna.

Todos los derechos reservados.

JUSTICIERO V1.00.

Sr. Espejo: Deje de crear mas virus o si no se la verá con nosotros...

El citado **Laboratorio Luz de Luna** también es encontrado en el virus STEALTH-BOOT.KATHIA.

8. PROTECCION Y PREVENCION DE LOS CENTROS INFORMATICOS

La política contra los virus informáticos, es no utilizar copias ilegales o **piratas** de ningún programa; para lo cual hay que tomar en cuenta lo siguiente:

8.1 APLICAR MEDIDAS DE SEGURIDAD

- Consiste en hacer copia de respaldo del trabajo diario y de cada disco.
- Apagar la computadora si ha sido infectado.
- En tercer lugar proteger los diskettes de programas originales, para evitar la contaminación.

8.2 LEGISLACION SOBRE DERECHO DE AUTOR

- Se debe castigar el delito de piratería sobre los programas de computación.

8.3 EQUIPOS DE RESPALDO

- Es una medida de protección que consiste en hacer copias de respaldo-backup, en forma periódica de los discos que contiene las informaciones. Dicho trabajo debe estar a buen recaudo.
- Con las copias de respaldo se recupera los archivos originales y para su confiabilidad emplean los siguientes equipos: discos

flexibles de extra alta densidad, discos tipo winchester, sistemas de cintas y casetes, discos ópticos y magneto-ópticos.

8.4 PROGRAMAS ANTIVIRUS

- Son diseños de técnicos especiales de seguridad, cuyo fin es combatir el peligro de alteración o destrucción de los programas de software.
- Se comporta como una vacuna ya que su objetivo es detectar, erradicar y prevenir la acción de los virus informáticos.
- Relación de Programas Antivirus:

Nombre	Elimina Virus
Rombicilina	Turín/pelotita
PCcilina	cualquier virus
No_Viernes	Jerusalén
Clean-up Virus Remover	167 virus
Jerusalén Virus Desinfector	Jerusalén
Netscan	virus en redes
SCANRES.EXE Versión 54	cualquier virus
VirusScan Versión 6.3V72	251 virus
VShield Versión 2.8V72	cualquier virus
Central Point Anti-Virus 2.5 For NetWare	virus en redes
Dr.Solomon's Anti-Virus	cualquier virus

Nombre	**Elimina Virus**
Dr.Solomon's Anti-Virus Toolkit 6.69	cualquier virus
The Hacker AntiVirus V3.1	cualquier virus
PER-AntiVirus V3.1	cualquier virus
PC-Doctor	cualquier virus

Figura 9. PC - Doctor es un programa antivirus que se debe incluir en la primera línea del archivo AUTOEXEC.BAT

CAPITULO VIII

PLAN DE CONTINGENCIA

OFICINA DE SISTEMAS - 1993

SEDAPAL

1. OBJETIVO

La intención del presente plan tiene **alternativas estratégicas que permiten el funcionamiento del Procesamiento de Datos,** de tal manera que pueda operar en un nivel aceptable cuando las facilidades de procesamiento no están disponibles.

¿ Qué hacer cuando deja de operar el Sistema por alguna circunstancia ante un evento no deseado, hasta recuperar el funcionamiento normal ?

2. METAS

Identificar las Aplicaciones Críticas, que

permiten que nuestra capacidad operativa a nivel de servicio no se debilite por los hechos.

3. FACTORES QUE AMENAZAN LA SEGURIDAD

- Fuego
- Inundación
- Vandalismo

4. CONSIDERACIONES PARA LA NOTIFICACION DEL SINIESTRO

Pasos iniciales a dar en ausencia de las autoridades normalmente responsables :

- Se coordina con Departamento de Seguridad y el Destacamento de la Policía Nacional, dependiendo del factor que amenace.
- Se notifica al Jefe de la Oficina de Sistemas

5. ORGANIZACION DEL EQUIPO DE TRABAJO

- Operaciones de Computo.
- Administración de la Seguridad de Datos.
- Comunicación y Redes Locales.
- Programación de Sistemas.
- Administración de Base de Datos.
- Desarrollo de las Aplicaciones.

- Administración del Centro de Información.
- Areas de Aplicaciones Claves.

6. RECURSOS DISPONIBLES

- Backup VSAM de Archivos de Contingencia.
- Backup VSAM de Librería (book's - phases - subrutinas).
- Backup DITTO de las Tablas de Comercial.
- Backup de Librería ICCF.

7. PLANIFICACION DE ESPACIO

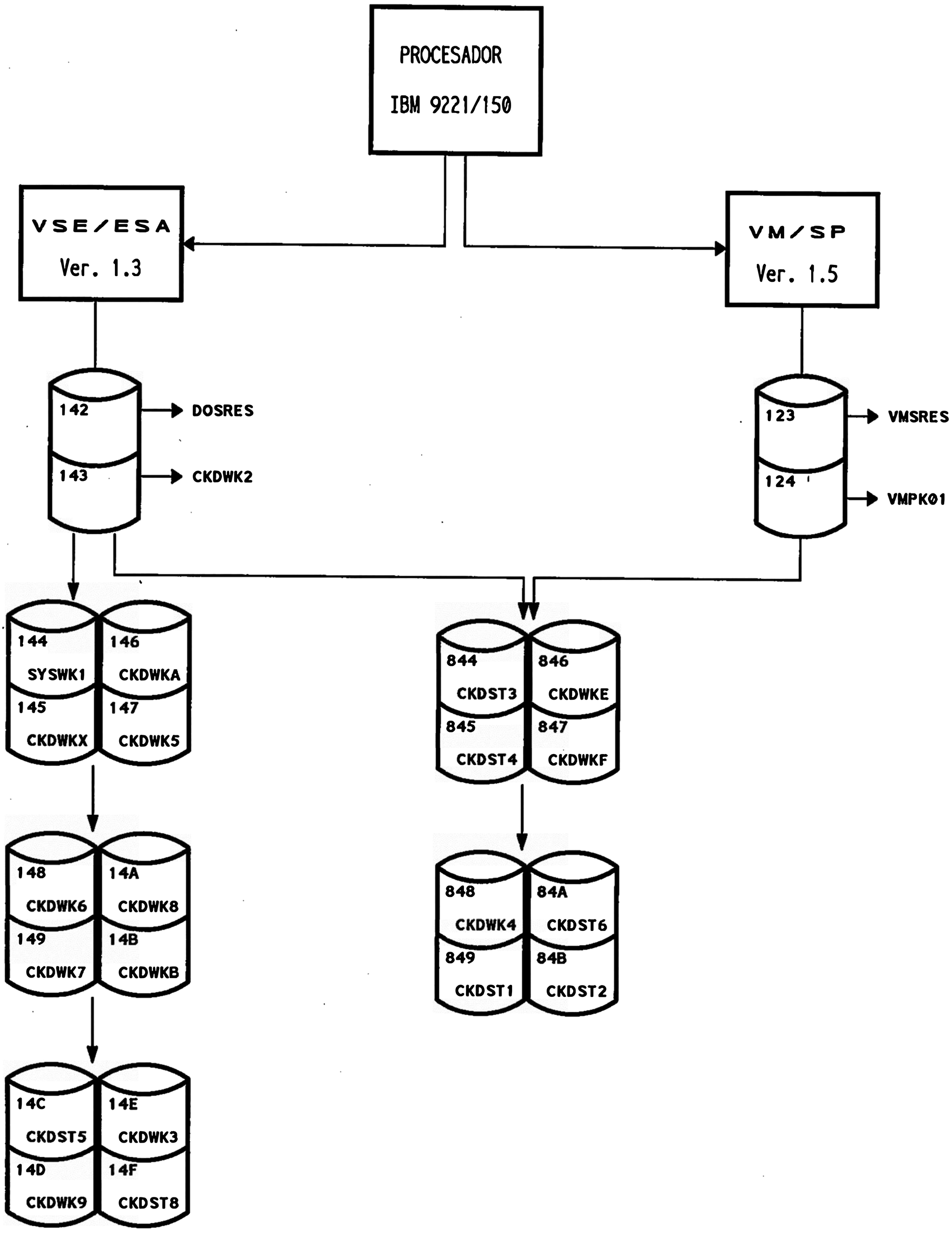
7.1 ANALISIS DE RIESGO

Considerando la Información histórica del año 1993 de los archivos de Contingencia se ha preparado el **Resumen de Archivos Plan de Contingencia en caso de Siniestros (Nivel de Contingencia)** en el que se detalla :

- Nombre de cluster.
- Longitud de la key.
- Posición de la key en cluster.
- Número de registros estimado.
- Longitud de registro.
- Longitud máxima de registro.

DISTRIBUCION DE DISCOS 3380

CONFIGURACION DE LA INFORMACION



- Share option : modalidad de acceso a otros sistemas.
- Nombre de la data.
- Nombre del index.
- Total Tracks usados.

8. DEFINICIONES

8.1 PROCESOS VITALES

Todo sistema que engloba la representatividad para que la empresa mantenga sus ingresos por los servicios que presta.

8.2 NIVEL DE CONTINGENCIA

Operatividad de la contingencia según el grado de necesidad de la información, medido en días:

PRIMER NIVEL	**:**	**2**	**DÍAS**
SEGUNDO NIVEL	**:**	**7**	**DÍAS**
TERCER NIVEL	**:**	**15**	**DÍAS**
CUARTO NIVEL	**:**	**30**	**DÍAS**

OFICINA DE SISTEMAS
UNIDAD DE PRODUCCION

PLAN DE CONTINGENCIA

(Nivel vs Procesos)

NIVEL	PERIODO (dias)	PREVIOS						T.E.		PAGOS					FACTURAC			OPERATIVO CIERR.	FUENTE PROPIA					ESTATALES	MENSUAL DE CREDITOS			ESTADISTICAS MENSUALES		
		CATAST	CIERR	REC DEC	CREDITO BIC BAC	CREDITO EMIS CUOTA	COLAT	UNI	CONS PROM	BCOS	REG	TP	FARMAC	S/TP	EMISI RECIB	SUBIDA CTA. CTE.	MICROF CTA. CTE.		H.T.E LECT.	H.T.E. RELECT	VALID LECT.	PRE- EMIS	EMIS	EMISION RECIBOS	LIQUID COBRANZ	MENSUAL CREDIT	DIRECT CREDIT	ESTADIS CATASTRO	ESTADIS CTA.CTE	ESTADIS CATAST. CTA.CTE
1	5					X			X	X					X															
2	10					X			X	X	X				X															
3	15	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X													
4	30	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

OFICINA DE SISTEMAS
Unidad de Produccion

DISTRIBUCION DE ESPACIOS PARA PRODUCCION (VSE/ESA)

CATALOGOS

- USER.CATALOG.BATCH.DINAMI
  - CKDWKA - 6,505 Tracks (Dataspace)
  - CKDWKA - 150 Tracks (Catalogo)
- USER.CATALOG.BATCH.PERMAN
  - CKDWK3 - 270 Tracks (Catalogo)
  - CKDWK3 - 12,824 Tracks (Dataspace)
- USER.CATALOG.LIBRARY
  - CKDWK2 - 60 Tracks (Catalogo)
  - CKDWK2 - 13,095 Tracks (Dataspace)
  - CKDWK6 - 4,035 Tracks (Dataspace)
- USER.CATALOG.ONLINE
  - CKDWK5 - 400 Tracks (Catalogo)
  - CKDWKB - 13,259 Tracks (Dataspace)
  - CKDWK4 - 13,139 Tracks (Dataspace)
  - CKDWK5 - 12,619 Tracks (Dataspace)
  - CKDWK6 - 8,000 Tracks (Dataspace)
  - CKDWK7 - 13,259 Tracks (Dataspace)
  - CKDWK8 - 13,259 Tracks (Dataspace)
  - CKDST4 - 13,259 Tracks (Dataspace)
- USER.CATALOG.TDESARR.ONLINE
  - CKDST1 - 284 Tracks (Catalogo)
  - CKDST1 - 9,135 Tracks (Dataspace)
  - CKDST3 - 13,259 Tracks (Dataspace)
- USER.CATALOG.CONTING
  - CKDWKE - 30 Tracks (Catalogo)
  - CKDWKE - 13,229 Tracks (Dataspace)
  - CKDWKF - 13,259 Tracks (Dataspace)
- VSAM.MASTER.CATALOG
  - DOSRES - 120 Tracks (Catalogo)
  - DOSRES - 2,505 Tracks (Dataspace)
  - SYSWK1 - 2,115 Tracks (Dataspace)
- VSESP.USER.CATALOG
  - SYSWK1 - 150 Tracks (Catalogo)
  - DOSRES - 4,260 Tracks (Dataspace)
  - SYSWK1 - 975 Tracks (Dataspace)

POWER

- VSE.POWER.ACCOUNT.FILE
  - CKDST1 - 90 Tracks
- VSE.POWER.DATA.FILE
  - CKDST1 - 3,500 Tracks
- VSE.POWER.QUEVE.FILE
  - CKDST1 - 5 Tracks

ICCF

- SYSWK1 - 4,000 Tracks

TOTAL DE ESPACIOS EN VSE/ESA

- CATALOGOS
  - TRACKS (CATALOGO) → 1,464
  - TRACKS (DATASPACE) → 184,045
- POWER = 3,595 TRACKS
- ICCF = 4,000 TRACKS

TOTAL TRACKS PARA PRODUCCION → 193,104

RESUMEN DE ARCHIVOS - PROCESOS DE CONTINGENCIAS
HOST DE PRODUCCION AL 28 - AGOSTO - 1993

NOMBRE CLUSTER	LONGITUD KEY	POSICION KEY	NRO.REG. UTILIZADO	NRO.REG. ESTIMADOS	LONG. REGIST.	LONG. MAXIMA	SRH	SRH	NOMBRE DATA	NOMBRE INDEX	TOTAL TRACKS USADOS
ARCH.CINTAS.CLUSTER	5	59	4988	4988	130	130	2	3	ARCH.CINTAS.DATA	ARCH.CINTAS.INDEX	17.66
CCA.D.BOLETIN.CATASTRO.INTER.KSDS.CLUSTER	11	0	32736	35000	40	40	2	3	CCA.D.BOLETIN.CATASTRO.INTER.KSDS.DATA	CCA.D.BOLETIN.CATASTRO.INTER.KSDS.INDEX	29.49
CCA.D.CCAF07.HISTORI.ALTERA.KSDS.CLUSTER	18	0	10773	15000	45	45	2	3	CCA.D.CCAF07.HISTORI.ALTERA.KSDS.DATA	CCA.D.CCAF07.HISTORI.ALTERA.KSDS.INDEX	14.22
CCA.D.DOCUMEN.CATASTRO.INTER.KSDS.CLUSTER	12	0	33	300	470	470	2	3	CCA.D.DOCUMEN.CATASTRO.INTER.KSDS.DATA	CCA.D.DOCUMEN.CATASTRO.INTER.KSDS.INDEX	2.97
CCA.D.HISTORI.CATASTRO.INTER.KSDS.CLUSTER	17	0	16838	15000	420	420	2	3	CCA.D.HISTORI.CATASTRO.INTER.KSDS.DATA	CCA.D.HISTORI.CATASTRO.INTER.KSDS.INDEX	132.70
CCM.D.CATAST.CONSULTA.MATTO.KSDS.CLUSTER	15	0	30	50	90	90	2	3	CCM.D.CATAST.CONSULTA.MATTO.KSDS.DATA	CCM.D.CATAST.CONSULTA.MATTO.KSDS.INDEX	0.09
CMO.D.CNCR51.CREDITOS.MOVIM.KSDS.CLUSTER	13	0	2701	3000	260	260	2	3	CMO.D.CNCR51.CREDITOS.MOVIM.KSDS.DATA	CMO.D.CNCR51.CREDITOS.MOVIM.KSDS.INDEX	16.43
CNC.B.ALTOS.CONSUMO.MAESTRO.ESDS.CLUSTER	0	0	14884	15000	50	50	2	3	CNC.B.ALTOS.CONSUMO.MAESTRO.ESDS.DATA		15.80
CNC.B.ARCHI.LISTADOR.BANCOS.ESDS.CLUSTER	0	0	0	5000	69	69	2	3	CNC.B.ARCHI.LISTADOR.BANCOS.ESDS.DATA		7.27
CNC.B.ARCHI.LISTADOR.RECIBO.SAMM.CLUSTER	0	0	331598	1000	4096	4096	1	3	CNC.B.ARCHI.LISTADOR.RECIBO.SAMM.DATA		86.28
CNC.B.ARCHIVO.CONTROL.BACKP.KSDS.CLUSTER	1	0	1	1	1981	1981	2	3	CNC.B.ARCHIVO.CONTROL.BACKP.KSDS.DATA	CNC.B.ARCHIVO.CONTROL.BACKP.KSDS.INDEX	0.04
CNC.B.ARCHIVO.CONTROL.MAEST.KSDS.CLUSTER	1	0	1	1	1981	1981	2	3	CNC.B.ARCHIVO.CONTROL.MAEST.KSDS.DATA	CNC.B.ARCHIVO.CONTROL.MAEST.KSDS.INDEX	0.04
CNC.B.CATAS.ULTI.CICLO.FACT.KSDS.CLUSTER	7	1	30181	42000	1014	1014	2	3	CNC.B.CATAS.ULTI.CICLO.FACT.KSDS.DATA	CNC.B.CATAS.ULTI.CICLO.FACT.KSDS.INDEX	897.04
CNC.B.CATASTRO.CARGOS.FACTU.ESDS.CLUSTER	0	0	780	780	470	470	2	3	CNC.B.CATASTRO.CARGOS.FACTU.ESDS.DATA		7.72
CNC.B.CATASTRO.LISTADOR.ACT.ESDS.CLUSTER	0	0	0	100	350	350	2	3	CNC.B.CATASTRO.LISTADOR.ACT.ESDS.DATA		0.74
CNC.B.CATASTRO.LISTADOR.MED.ESDS.CLUSTER	0	0	8	100	350	350	2	3	CNC.B.CATASTRO.LISTADOR.MED.ESDS.DATA		0.74
CNC.B.CATASTRO.MOVIM.DOCU12.ESDS.CLUSTER	0	0	780	100	470	470	2	3	CNC.B.CATASTRO.MOVIM.DOCU12.ESDS.DATA		0.58
CNC.B.CATASTRO.MOVIM.VALIDO.ESDS.CLUSTER	0	0	0	3000	470	470	2	3	CNC.B.CATASTRO.MOVIM.VALIDO.ESDS.DATA		29.70
CNC.B.CCMCODDCO.CENTRO.COBZA.KSDS.CLUSTER	0	0	642	700	40	40	2	3	CNC.B.CCMCODDCO.CENTRO.COBZA.KSDS.DATA	CNC.B.CCMCODDCO.CENTRO.COBZA.KSDS.INDEX	0.59
CNC.B.CIERRES.MOVIM.VALIDOS.ESDS.CLUSTER	0	0	0	2000	350	350	2	3	CNC.B.CIERRES.MOVIM.VALIDOS.ESDS.DATA		14.74
CNC.B.COLATERA.CIERRE.BACKP.ESDS.CLUSTER	0	0	3067	2000	350	350	2	3	CNC.B.COLATERA.CIERRE.BACKP.ESDS.DATA		14.74
CNC.B.COLATERA.CIERRE.MOVIM.ESDS.CLUSTER	0	0	0	3000	350	350	2	3	CNC.B.COLATERA.CIERRE.MOVIM.ESDS.DATA		22.12
CNC.B.COLATERA.MOVIM.VALIDO.ESDS.CLUSTER	0	0	3806	4000	350	350	2	3	CNC.B.COLATERA.MOVIM.VALIDO.ESDS.DATA		29.49
CNC.B.CONTROL.DIGITAC.HISTO.KSDS.CLUSTER	3	0	846	1000	878	878	2	3	CNC.B.CONTROL.DIGITAC.HISTO.KSDS.DATA	CNC.B.CONTROL.DIGITAC.HISTO.KSDS.INDEX	18.49
CNC.B.CREDITOS.ARCH.MENSUAL.KSDS.CLUSTER	7	0	13439	15000	1150	1150	2	3	CNC.B.CREDITOS.ARCH.MENSUAL.KSDS.DATA	CNC.B.CREDITOS.ARCH.MENSUAL.KSDS.INDX	363.34
CNC.B.CREDITOS.ARCHI.CARGOS.ESDS.CLUSTER	0	0	0	42	38	38	2	3	CNC.B.CREDITOS.ARCHI.CARGOS.ESDS.DATA		0.03
CNC.B.CREDITOS.CANCELAD.MES.ESDS.CLUSTER	0	0	6217	8000	95	95	2	3	CNC.B.CREDITOS.CANCELAD.MES.ESDS.DATA		16.01
CNC.B.CREDITOS.CATAST.MOVIM.ESDS.CLUSTER	0	0	0	2000	85	85	2	3	CNC.B.CREDITOS.CATAST.MOVIM.ESDS.DATA		2.58
CNC.B.CREDITOS.CATAST.UNIFI.ESDS.CLUSTER	0	0	350	100	85	85	2	3	CNC.B.CREDITOS.CATAST.UNIFI.ESDS.DATA		0.18
CNC.B.CREDITOS.CIC.CON.CRED.ESDS.CLUSTER	0	0	376	500	1528	1528	1	3	CNC.B.CREDITOS.CIC.CON.CRED.ESDS.DATA		16.09
CNC.B.CREDITOS.LIST.MENSUAL.ESDS.CLUSTER	0	0	1595	500	92	92	2	3	CNC.B.CREDITOS.LIST.MENSUAL.ESDS.DATA		0.97
CNC.B.CREDITOS.MOVIM.VALIDO.ESDS.CLUSTER	0	0	350	80	85	85	2	3	CNC.B.CREDITOS.MOVIM.VALIDO.ESDS.DATA		0.14
CNC.B.CREDITOS.PREVIO.ARCH1.ESDS.CLUSTER	0	0	80176	100000	15	15	2	3	CNC.B.CREDITOS.PREVIO.ARCH1.ESDS.DATA		31.59
CNC.B.CREDITOS.PREVIO.ARCH2.ESDS.CLUSTER	0	0	80176	100000	15	15	2	3	CNC.B.CREDITOS.PREVIO.ARCH2.ESDS.DATA		31.59
CNC.B.CREDITOS.PROYE.MAEANT.KSDS.CLUSTER	2	2	194	200	234	234	2	3	CNC.B.CREDITOS.PROYE.MAEANT.KSDS.DATA	CNC.B.CREDITOS.PROYE.MAEANT.KSDS.INDEX	0.99
CNC.B.CREDITOS.PROYE.MOVVAL.ESDS.CLUSTER	0	0	19	50	234	234	2	3	CNC.B.CREDITOS.PROYE.MOVVAL.ESDS.DATA		0.25
CNC.B.CREDITOS.SITUAC.DEUDA.ESDS.CLUSTER	0	0	76933	100000	107	107	2	3	CNC.B.CREDITOS.SITUAC.DEUDA.ESDS.DATA		225.38
CNC.B.DECRETOS.MOVIM.VALIDO.ESDS.CLUSTER	0	0	3241	240	54	54	2	3	CNC.B.DECRETOS.MOVIM.VALIDO.ESDS.DATA		0.27
CNC.B.LISTADOR.CIERRES.REAP.ESDS.CLUSTER	0	0	9701	10000	200	200	2	3	CNC.B.LISTADOR.CIERRES.REAP.ESDS.DATA		42.13
CNC.B.MOVIM.CONTABLE.BACKUP.ESDS.CLUSTER	0	0	0	11	27	27	2	3	CNC.B.MOVIM.CONTABLE.BACKUP.ESDS.DATA		0.01
CNC.B.MOVIM.CONTABLE.DIARIO.ESDS.CLUSTER	0	0	0	11	27	27	2	3	CNC.B.MOVIM.CONTABLE.DIARIO.ESDS.DATA		0.01
CNC.B.MOVIM.CONTABLE.HISTO1.ESDS.CLUSTER	0	0	106	121	27	27	2	3	CNC.B.MOVIM.CONTABLE.HISTO1.ESDS.DATA		0.07
CNC.B.MOVIM.CONTABLE.HISTO2.ESDS.CLUSTER	0	0	106	121	27	27	2	3	CNC.B.MOVIM.CONTABLE.HISTO2.ESDS.DATA		0.07
CNC.B.MOVIM.CONTABLE.LOGGIN.ESDS.CLUSTER	0	0	13972	20000	34	34	2	3	CNC.B.MOVIM.CONTABLE.LOGGIN.ESDS.DATA		14.32
CNC.B.MOVIM.CONTABLE.NEUTRO.ESDS.CLUSTER	0	0	0	11	27	27	2	3	CNC.B.MOVIM.CONTABLE.NEUTRO.ESDS.DATA		0.01
CNC.B.PAGOS.MOV.VALID.INPUT.ESDS.CLUSTER	0	0	0	15000	31	31	2	3	CNC.B.PAGOS.MOV.VALID.INPUT.ESDS.DATA		9.79
CNC.B.PAGOS.NO.APLICADO.ACT.ESDS.CLUSTER	0	0	0	10	51	51	2	3	CNC.B.PAGOS.NO.APLICADO.ACT.ESDS.DATA		0.01
CNC.B.PAGOS.NO.PROCESAD.ACT.ESDS.CLUSTER	0	0	239	300	31	31	2	3	CNC.B.PAGOS.NO.PROCESAD.ACT.ESDS.DATA		0.20
CNC.B.PAGOS.SI.APLICADO.ACT.ESDS.CLUSTER	0	0	144159	500000	40	40	2	3	CNC.B.PAGOS.SI.APLICADO.ACT.ESDS.DATA		421.27

RESUMEN DE ARCHIVOS - PROCESOS DE CONTINGENCIAS
HOST DE PRODUCCION AL 28 - AGOSTO - 1993

NOMBRE CLUSTER	LONGITUD KEY	POSICION	NRO.REG. UTILIZADO	NRO.REG. ESTIMADOS	LONG. REGIST.	LONG. MAXIMA	SRH	SRH	NOMBRE DATA	NOMBRE INDEX	TOTAL TRACKS USADOS
CNC.B.PAGOS.TP.TRANSIT.CAJA.KSDS.CLUSTER	17	0	379	1500	62	62	2	3	CNC.B.PAGOS.TP.TRANSIT.CAJA.KSDS.DATA	CNC.B.PAGOS.TP.TRANSIT.CAJA.KSDS.INDEX	[illegible]
CNC.B.PARA01.ARCHI.PARAMETR.SAMM.CLUSTER	1	0	3	3	600	600	2	3	CNC.B.PARA01.ARCHI.PARAMETR.SAMM.DATA		[illegible]
CNC.B.PARA02.ARCHI.PARAMETR.ESDS.CLUSTER	0	0	1	1	600	600	2	3	CNC.B.PARA02.ARCHI.PARAMETR.ESDS.DATA		[illegible]
CNC.B.PARA04.ARCHI.PARAMETR.ESDS.CLUSTER	1	0	3	3	600	600	2	3	CNC.B.PARA04.ARCHI.PARAMETR.ESDS.DATA		[illegible]
CNC.B.PARA08.BACKP.PARAMETR.ESDS.CLUSTER	0	0	2	2	600	600	2	3	CNC.B.PARA08.BACKP.PARAMETR.ESDS.DATA		[illegible]
CNC.B.PARA09.ARCHI.PARAMETR.SAMM.CLUSTER	1	0	3	3	600	600	2	3	CNC.B.PARA09.ARCHI.PARAMETR.SAMM.DATA		[illegible]
CNC.B.RESUMEN.ESTADIS.DATAS.ESDS.CLUSTER	1	0	405	1000	1754	1754	2	3	CNC.B.RESUMEN.ESTADIS.DATAS.ESDS.DATA		[illegible]
CNC.B.TOMAEST.MOVIM.FORMATE.ESDS.CLUSTER	1	0	12520	13000	128	128	2	3	CNC.B.TOMAEST.MOVIM.FORMATE.ESDS.DATA		[illegible]
CNC.B.TOMAEST.MOVIM.VALIDOS.ESDS.CLUSTER	1	0	12501	13000	63	63	2	3	CNC.B.TOMAEST.MOVIM.VALIDOS.ESDS.DATA		[illegible]
CNC.O.CNCR01.CATASTRO.MAEST.KSDS.CLUSTER	7	1	756361	900000	1014	1014	2	3	CNC.O.CNCR01.CATASTRO.MAEST.KSDS.DATA	CNC.O.CNCR01.CATASTRO.MAEST.KSDS.INDEX	[illegible]
CNC.O.CNCR02.CTACTE.MAESTRO.KSDS.CLUSTER	14	1	5650468	5700000	40	40	2	3	CNC.O.CNCR02.CTACTE.MAESTRO.KSDS.DATA	CNC.O.CNCR02.CTACTE.MAESTRO.KSDS.INDEX	[illegible]
CNC.O.CNCR04.CONEXION.MAEST.KSDS.CLUSTER	3	0	61	61	629	629	2	3	CNC.O.CNCR04.CONEXION.MAEST.KSDS.DATA	CNC.O.CNCR04.CONEXION.MAEST.KSDS.INDEX	[illegible]
CNC.O.CNCR06.CICCON.MAESTRO.KSDS.CLUSTER	4	1	1995	2500	1528	1528	2	3	CNC.O.CNCR06.CICCON.MAESTRO.KSDS.DATA	CNC.O.CNCR06.CICCON.MAESTRO.KSDS.INDEX	[illegible]
CNC.O.CNCR08.TABLAS.COMERC1.KSDS.CLUSTER	11	0	2912	2914	120	120	2	3	CNC.O.CNCR08.TABLAS.COMERC1.KSDS.DATA	CNC.O.CNCR08.TABLAS.COMERC1.KSDS.INDEX	[illegible]
CNC.O.CNCR10.TOMAESTA.MOVIM.KSDS.CLUSTER	9	0	1	12000	128	128	2	3	CNC.O.CNCR10.TOMAESTA.MOVIM.KSDS.DATA	CNC.O.CNCR10.TOMAESTA.MOVIM.KSDS.INDEX	[illegible]
CNC.O.CNCR11.TOMAESTA.SECTO.KSDS.CLUSTER	7	0	281	300	20	20	2	3	CNC.O.CNCR11.TOMAESTA.SECTO.KSDS.DATA	CNC.O.CNCR11.TOMAESTA.SECTO.KSDS.INDEX	[illegible]
CNC.O.CNCR21.CIERRESS.MOVIM.KSDS.CLUSTER	14	0	7764	12000	51	51	2	3	CNC.O.CNCR21.CIERRESS.MOVIM.KSDS.DATA	CNC.O.CNCR21.CIERRESS.MOVIM.KSDS.INDEX	[illegible]
CNC.O.CNCR22.CIERRESS.HISTO.KSDS.CLUSTER	11	0	7151	9000	100	100	2	3	CNC.O.CNCR22.CIERRESS.HISTO.KSDS.DATA	CNC.O.CNCR22.CIERRESS.HISTO.KSDS.INDEX	[illegible]
CNC.O.CNCR51.PARAM.CATASTRO.KSDS.CLUSTER	17	0	74	150	200	200	2	3	CNC.O.CNCR51.PARAM.CATASTRO.KSDS.DATA	CNC.O.CNCR51.PARAM.CATASTRO.KSDS.INDEX	[illegible]
CNC.O.CNCR41.COLATERA.MOVIM.KSDS.CLUSTER	12	0	1009	1009	400	400	2	3	CNC.O.CNCR41.COLATERA.MOVIM.KSDS.DATA	CNC.O.CNCR41.COLATERA.MOVIM.KSDS.INDEX	[illegible]
CNC.O.CNCR42.COLATERA.HISTO.KSDS.CLUSTER	11	0	795	2000	170	170	2	3	CNC.O.CNCR42.COLATERA.HISTO.KSDS.DATA	CNC.O.CNCR42.COLATERA.HISTO.KSDS.INDEX	[illegible]
CNC.O.CNCR51.CREDITOS.MOVIM.KSDS.CLUSTER	17	0	104	3000	260	260	2	3	CNC.O.CNCR51.CREDITOS.MOVIM.KSDS.DATA	CNC.O.CNCR51.CREDITOS.MOVIM.KSDS.INDEX	[illegible]
CNC.O.CNCR52.CREDITOS.HISTO.KSDS.CLUSTER	17	0	9221	12000	165	165	2	3	CNC.O.CNCR52.CREDITOS.HISTO.KSDS.DATA	CNC.O.CNCR52.CREDITOS.HISTO.KSDS.INDEX	[illegible]
CNC.O.CNCR53.CREDITOS.PROYE.KSDS.CLUSTER	2	2	194	1500	279	279	2	3	CNC.O.CNCR53.CREDITOS.PROYE.KSDS.DATA	CNC.O.CNCR53.CREDITOS.PROYE.KSDS.INDEX	[illegible]
CNC.O.CNCR55.MOLINA.MOVIMIE.KSDS.CLUSTER	7	0	10621	12000	300	300	2	3	CNC.O.CNCR55.MOLINA.MOVIMIE.KSDS.DATA	CNC.O.CNCR55.MOLINA.MOVIMIE.KSDS.INDEX	[illegible]
CNC.O.CNCR56.MOLINA.PARAMET.KSDS.CLUSTER	8	0	27	50	150	150	2	3	CIM.O.CNCR56.MOLINA.PARAMET.KSDS.DATA	CNC.O.CNCR56.MOLINA.PARAMET.KSDS.INDEX	[illegible]
CNC.O.CNCR61.RECDECRE.MOVIM.KSDS.CLUSTER	14	0	1669	3000	109	109	2	3	CNC.O.CNCR61.RECDECRE.MOVIM.KSDS.DATA	CNC.O.CNCR61.RECDECRE.MOVIM.KSDS.INDEX	[illegible]
CNC.O.CNCR62.RECDECRE.TARIF.KSDS.CLUSTER	4	0	12	100	700	700	2	3	CNC.O.CNCR62.RECDECRE.TARIF.KSDS.DATA	CNC.O.CNCR62.RECDECRE.TARIF.KSDS.INDEX	[illegible]
CNC.O.CNCR63.RECDECRE.HISTO.KSDS.CLUSTER	12	0	17069	20000	130	130	2	3	CNC.O.CNCR63.RECDECRE.HISTO.KSDS.DATA	CNC.O.CNCR63.RECDECRE.HISTO.KSDS.INDEX	[illegible]
CNC.O.CNCR72.PAGOSTP.HISTOR.KSDS.CLUSTER	11	0	26414	35000	85	85	2	3	CNC.O.CNCR72.PAGOSTP.HISTOR.KSDS.DATA	CNC.O.CNCR72.PAGOSTP.HISTOR.KSDS.INDEX	[illegible]
CNC.O.CNCR74.PAGOSTP.NPROCE.KSDS.CLUSTER	17	0	28574	35000	39	39	2	3	CNC.O.CNCR74.PAGOSTP.NPROCE.KSDS.DATA	CNC.O.CNCR74.PAGOSTP.NPROCE.KSDS.INDEX	[illegible]
CNS.B.CNCR10.TOMAESTA.MOVIM.KSDS.CLUSTER	9	0	12521	13000	128	128	1	3	CNS.B.CNCR10.TOMAESTA.MOVIM.KSDS.DATA	CNS.B.CNCR10.TOMAESTA.MOVIM.KSDS.INDEX	[illegible]
CNS.B.FACTURAD.ARCHI.CARGOS.ESDS.CLUSTER	1	0	338505	340000	38	38	2	3	T6A687E0.VSAMDSET.DF391229.T4458E7C.T6A687E0		[illegible]
CNS.O.CNCR34.PARAM.MASIVOS.KSDS.CLUSTER	25	0	5709	10000	200	200	2	3	CNS.O.CNCR34.PARAM.MASIVOS.KSDS.DATA	CNS.O.CNCR34.PARAM.MASIVOS.KSDS.INDEX	[illegible]
CNS.O.EVALC2.SISTEM.COMERC.KSDS.CLUSTER	9	0	383	400	64	64	2	3	CNS.O.EVALC2.SISTEM.COMERC.KSDS.DATA	CNS.O.EVALC2.SISTEM.COMERC.KSDS.INDEX	[illegible]
CNX.O.CNCR71.PAGOSTP.CAJASS.KSDS.CLUSTER	12	0	27	35000	62	62	2	3	CNX.O.CNCR71.PAGOSTP.CAJASS.KSDS.DATA	CNX.O.CNCR71.PAGOSTP.CAJASS.KSDS.INDEX	[illegible]
CRP.O.RP01R1.MOVIM.PAGOS.KSDS.CLUSTER	14	0	1	25000	50	50	2	3	CRP.O.RP01R1.MOVIM.PAGOS.KSDS.DATA	CRP.O.RP01R1.MOVIM.PAGOS.KSDS.INDEX	[illegible]
CRP.O.RP02R1.CONTR.PAGOS.KSDS.CLUSTER	7	0	1	25000	9	9	2	3	CRP.O.RP02R1.CONTR.PAGOS.KSDS.DATA	CRP.O.RP02R1.CONTR.PAGOS.KSDS.INDEX	[illegible]
CRP.O.RP05R.ELIMINA.PAGOS.KSDS.CLUSTER	20	0	1	1	60	60	2	3	CRP.O.RP05R.ELIMINA.PAGOS.KSDS.DATA	CRP.O.RP05R.ELIMINA.PAGOS.KSDS.INDEX	[illegible]
CTB.O.CTBA01.TABLAS.COMERCIA.KSDS.CLUSTER	8	2	402	402	100	100	2	3	CTB.O.CTBA01.TABLAS.COMERCIA.KSDS.DATA	CTB.O.CTBA01.TABLAS.COMERCIA.KSDS.INDEX	[illegible]
RZR.O.RZRR01.BANCCO.LOGGING.KSDS.CLUSTER	5	0	1488	3000	40	40	2	3	RZR.O.RZRR01.BANCCO.LOGGING.KSDS.DATA	RZR.O.RZRR01.BANCCO.LOGGING.KSDS.INDEX	[illegible]
RZR.O.RZRR02.BANCCO.MOVIMIE.RRDS.CLUSTER	0	0	75	75	8184	8184	2	3	RZR.O.RZRR02.BANCCO.MOVIMIE.RRDS.DATA		[illegible]
RZR.O.RZRR02.BANCINT.MOVIMIE.RRDS.CLUSTER	0	0	10	10	8184	8184	2	3	RZR.O.RZRR02.BANCINT.MOVIMIE.RRDS.DATA		[illegible]
RZR.O.RZRR03.BANCCO.DETALLE.ESDS.CLUSTER	0	0	2769	2979	22	22	2	3	RZR.O.RZRR03.BANCCO.DETALLE.ESDS.DATA		[illegible]
RZR.O.RZRR03.BANCINT.DETALLE.ESDS.CLUSTER	0	0	1472	1472	22	22	2	3	RZR.O.RZRR03.BANCINT.DETALLE.ESDS.DATA		[illegible]
** Total ***											23421.36

9. PRIMER NIVEL DE CONTINGENCIA (2 DÍAS)

9.1 IDENTIFICACION: PRIMER NIVEL DE CONTINGENCIA

Con el fin de mantener la productividad informática, se ha establecido como **PRIMER NIVEL DE CONTINGENCIA** a los siguientes procesos:

- Previos (Emisión de Cuotas)
- Toma de Estado (Consumo Promedio)
- Pagos (Bancos)
- Facturación (Emisión de Recibos)

9.2 CONSIDERACIONES TECNICAS

RECURSOS HARDWARE

- Capacidad de procesamiento de 4.5 Mips
- Unidades de Discos 3380 modelo BJ4
- Unidades de Cartridges 3490
- Impresoras 4245 de 2,000 l.p.m.
- Consola de operador
- Terminal de usuario
- PC con tarjeta de emulación y disco duro

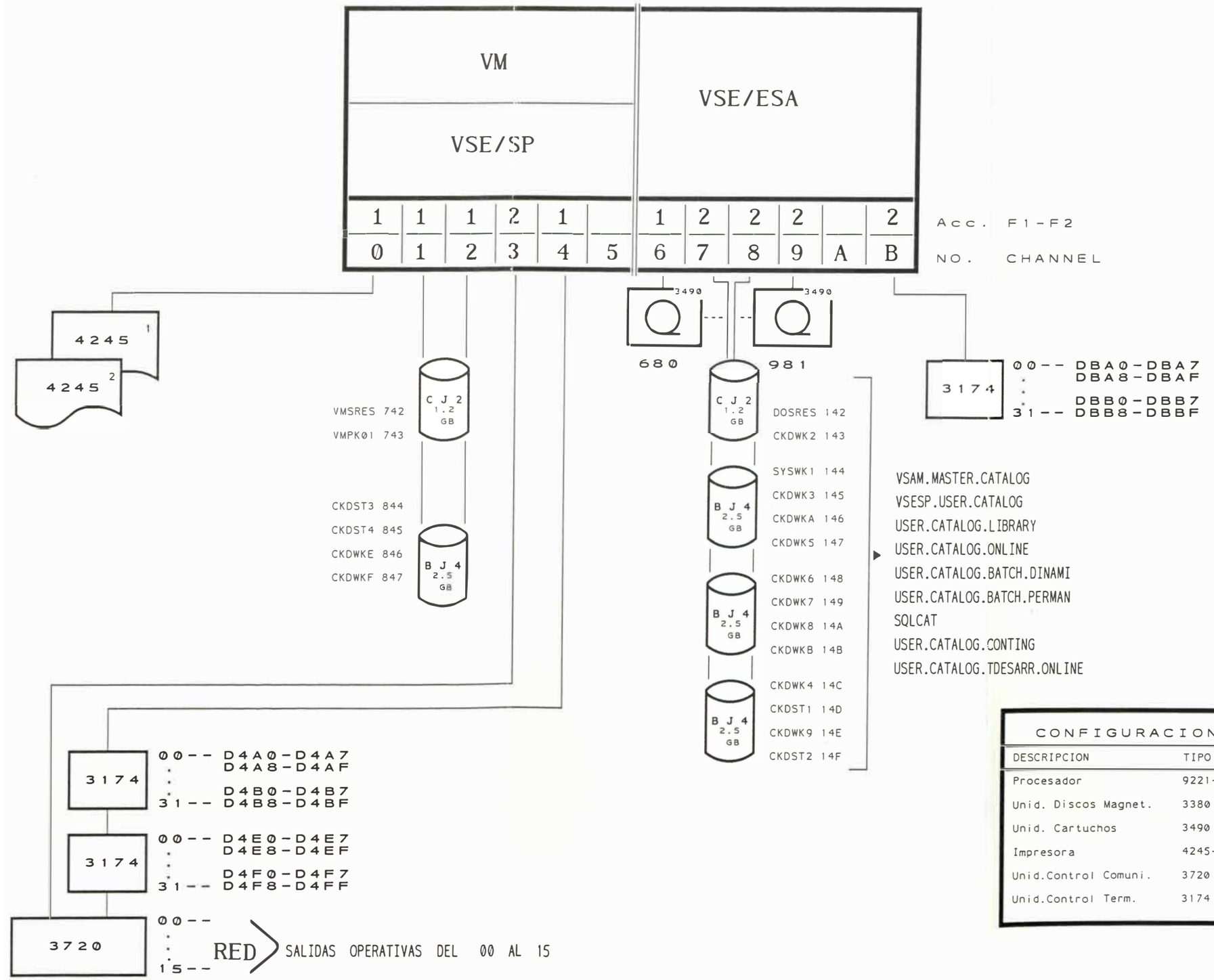
RECURSOS SOFTWARE

- Ambiente VSE
- Ambiente VSAM
- Ambiente para Librerías (book's - phases - subrutinas)
- Compilador COBOL VS 1.3

CONFIGURACION DEL COMPUTADOR CENTRAL

PROCESADOR 9291/150

HOST (1) VSEPROD HOST (2) VMDESA



CONFIGURACION

DESCRIPCION	TIPO	CANT.
Procesador	9221-150	1
Unid. Discos Magnet.	3380	6
Unid. Cartuchos	3490	1
Impresora	4245-020	2
Unid.Control Comuni.	3720	1
Unid.Control Term.	3174	3

JUNIO - 95

- Programa SORT de IBM
- Utilitario DITTO

RECURSOS HUMANOS

- Supervisor de Operaciones
- Operador de Consola
- Fiscal
- Técnico de Equipo de Hardware y Software

INFRAESTRUCTURA

- Espacio Físico de 9 metros cuadrados de almacenaje (recibos)

CAPACIDAD DE COMPUTO REQUERIDA

-	Memoria Real	:	2 MB
-	Espacio VSAM	:	1,623 MB
-	Espacio Librariam	:	15 MB
-	Espacio Area SORT	:	350 MB
-	Espacio de Editor	:	5 MB
-	Capacidad de Impresión	:	10 horas
-	Unidades de Cartridges	:	2
-	Espacio en Disco PC	:	1 MB
-	Consola de operador	:	1
-	Terminal de Usuario	:	1
-	Microcomputador	:	1

PUESTA A PUNTO

- **Preparación del Ambiente de Contingencia**

  (4 horas)

  Generación de Espacio VSAM.

  Generación de Catalogo de Contingencia.

  Restore de Archivo de Contingencia.

  Generación de Ambientes de Librería.

  Definición de Librerías de Contingencia.

  Restore de Librería (book's - phases - subrutinas).

  Compilación de Programas.

  Preparación de Librería de Editor.

  Validación y Pruebas de Job's de Contingencia.

- **Mantenimiento del Ambiente de Contingencia**

  (1 hora)

  Fastcopy de discos de contingencia.

  Generación de Microfichas (1 hora), opcional a decisión del Usuario.

9.3 DESARROLLO GENERAL: DEFINICIONES DE PROCESO

- **PREVIOS.-**

Emisión de Cuotas:

Corresponde a las Cuotas de Créditos que los usuarios suscriben con la Empresa, las mismas que se emiten de acuerdo al Ciclo a Facturar.

Consumo Promedio:

Al no haber Toma de Estado coordinamos con el Area Comercial para que los Consumos se Emitirían a Promedio.

Pagos (Bancos):

Levantamiento de información (Movimientos Diarios) y cobranza efectuada a través de los Bancos Interconectados a nuestro Centro de Cómputo.

- **FACTURACION:**

Corresponde a la Actualización de la Diferencia de Lecturas del Mes anterior con las del Mes actual aplicando la Tarifa Vigente y Factores de Morosidad de acuerdo al Indice de Precios de Consumidor del Mes anterior

Generación de Recibos:

Lista Recibos del Ciclo Facturado

- **ARCHIVOS UTILIZADOS**

SISTEMA	Nro. procesos	Nro. prog.	Nro. arch.	Nro.Trks usados	Tiempo proceso
COMERCIAL:					
Créditos	**09**	**09**	**13**		**1'30"**
Pagos	**18**	**10**	**12**		**2'00"**
Facturación	**04**	**04**	**14**		**2'00"**
T O T A L	**31**	**13**	**39**	**34,171.85**	**---**

Nota.- Estos procesos utilizan Archivos comunes por lo que no se puede detallar por proceso el Nro. de Tracks usados.

10. SEGUNDO NIVEL DE CONTINGENCIA (7 DÍAS)

10.1 IDENTIFICACION: SEGUNDO NIVEL DE CONTINGENCIA

Con el fin de mantener la productividad informática, se ha establecido como **SEGUNDO NIVEL DE CONTINGENCIA** a los siguientes procesos:

- Previos (Emisión de Cuotas).
- Toma de Estado (Consumo Promedio).
- Pagos (Bancos).
- Facturación (Emisión de Recibos).
- Pagos (Regionales).

Nota:

La inclusión del proceso de PAGOS (REGIONALES) implica el ingreso de 15,000 pagos (talones) diarios al sistema de cómputo para la actualización de la cuenta corriente, los cuales deben ser inputados en una forma eficiente. Para ello se propone tres (3) propuestas que se bosquejan continuación.

La elección de la propuesta implicará modificaciones en las consideraciones técnicas del nivel de contingencia.

DIGITACION:

Número de Pagos: 15,000 PAGOS diarios distribuídos por lotes de hasta un máximo de 200 pagos.

Propuesta 1: Ingreso Directo en Host

- Se hace necesario la instalación de Aplicaciones que realizan el ingreso de pagos al sistema.
- Se hará uso de un ambiente CICS donde ubicar las aplicaciones.
- Uso de terminales de usuario en el número necesario que permita la digitación de los pagos.

Ventaja : Todos los pagos ingresados son correctos.

Desventaja: Necesidad de un mayor ambiente Hardware y Software además de ambiente físico de digitación.

Propuesta 2: Digitación Externa

- Establecer un contrato de digitación por terceros hacia diskettes PC. Se proporcionará los diseños de registro de los pagos.

- El ingreso de los pagos al sistema se hace transferiendo los pagos desde diskettes PC al Host.
- Se tendrá en el Host un proceso de validación de pagos.

Ventajas : Ambiente de contingencia igual al nivel 1.

Desventaja: No hay posibilidad de corrección inmediata de los pagos mal digitados.

Propuesta 3: Ingreso por Software PC

- Se generará software PC de ingreso de pagos para ser manejado por las oficinas regionales en sus ubicaciones.
- Las oficinas regionales entregan diskettes PC con pagos.
- El ingreso de los pagos al sistema se hace transfiriendo los pagos desde diskettes PC al Host.
- Se tendrá en el Host un proceso de validación de pagos.
- Se tendrá software PC de control de calidad para corrección de pagos. Se necesitarán dos fiscales.

Ventaja : Ambiente de contingencia similar a nivel 1.

Desventaja: Demora (relativa) en la corrección de pagos.

10.2 CONSIDERACIONES TECNICAS

RECURSOS HARDWARE

- Capacidad de procesamiento de 4.5 Mips
- Unidades de Discos 3380 modelo BJ4
- Unidades de Cartridges 3490
- Impresoras 4245 de 2,000 l.p.m.
- Consola de operador
- Terminal de usuario
- PC con tarjeta de emulación y disco duro

RECURSOS SOFTWARE

- Ambiente VSE
- Ambiente VSAM
- Ambiente para Librerías (book's - phases - subrutinas)
- Compilador COBOL VS 1.3
- Generador de Aplicaciones CROSS SYSTEM PRODUCT
- Programa SORT de IBM
- Utilitario DITTO

RECURSOS HUMANOS

- Supervisor de Operaciones
- Operador de Consola
- Fiscal
- Técnico de Equipo de Hardware y Software

INFRAESTRUCTURA

- Espacio Físico de 9 metros cuadrados de almacenaje (recibos).

CAPACIDAD DE COMPUTO REQUERIDA

-	Memoria Real	:	2 MB
-	Espacio VSAM	:	1,548 MB
-	Espacio Librariam	:	18 MB
-	Espacio Area SORT	:	350 MB
-	Espacio de Editor	:	5 MB
-	Capacidad de Impresión	:	12 horas
-	Unidades de Cartridges	:	2
-	Espacio en Disco PC	:	1 MB
-	Consola de operador	:	1
-	Terminal de Usuario	:	1
-	Microcomputador	:	1

PUESTA A PUNTO

- **Preparación del Ambiente de Contingencia**

  (4 horas)

  Generación de Espacio VSAM.

  Generación de Catalogo de Contingencia.

  Restore de Archivo de Contingencia.

  Generación de Ambientes de Librería.

  Definición de Librerías de Contingencia.

  Restore de Librería (book's-phases-sub-rutinas).

  Compilación de Programas.

  Preparación de Librería de Editor.

  Validación y Pruebas de Job's de Contingencia.

- **Mantenimiento del Ambiente de Contingencia**

  (1 hora)

  Fastcopy de discos de contingencia.

  Generación de Microfichas (1 hr), opcional a decisión del Usuario.

10.3 DESARROLLO GENERAL: DEFINICIONES DE PROCESO

- **PREVIOS**

Emisión de Cuotas:

Corresponde a las Cuotas de Créditos que los usuarios suscriben con la Empresa, las mismas que se emiten de acuerdo al Ciclo a Facturar.

Consumo Promedio:

Al no haber Toma de Estado coordinamos con el Area Comercial y los Consumos se Emitirían a Promedio.

Pagos (Bancos):

Corresponde a la Actualización de la cobranza efectuada a través de los Bancos Interconectados a nuestro Centro de Cómputo.

Pagos (Región)

Corresponde a la Actualización de la cobranza efectuada a través de las distintas Regiones.

- **FACTURACION:**

Corresponde a la Actualización de la Diferencia de Lecturas del Mes anterior con las del Mes actual aplicando la Tarifa Vigente y Factores de Morosidad de acuerdo

al Indice de Precios de Consumidor del Mes anterior.

Generación de Recibos:

Lista Recibos del Ciclo Facturado

- **ARCHIVOS UTILIZADOS**

SISTEMA	Nro. procesos	Nro. prog.	Nro. arch.	Nro.Trks usados	Tiempo proceso
COMERCIAL:					
Créditos	**09**	**09**	**13**		**1'30"**
Pagos	**27**	**18**	**18**		**3'00"**
Facturación	**04**	**04**	**14**		**2'00"**
T O T A L	**40**	**31**	**45**	**34,210.03**	**---**

Nota.- Estos procesos utilizan Archivos comunes por lo que no se puede detallar por proceso el Nro. de Tracks usados.

11. TERCER NIVEL DE CONTINGENCIA (15 DÍAS)

11.1 IDENTIFICACION: TERCER NIVEL DE CONTINGENCIA

Con el fin de mantener la productividad informática, se ha establecido como **TERCER NIVEL DE CONTINGENCIA** a los siguientes procesos:

- Previos (Catastro, Cierres, Reclamos y Decretos, Créditos BIC BAC y Emisión de Cuotas, Colaterales).
- Toma de Estado (Unificación).
- Pagos (Bancos, Regionales, TP, Farmacias y S/TP).
- Facturación (Emisión de Recibos, Subida CTA. CTE., Microficha CTA. CTE.).
- Operativo Cierres.

NOTA :

A partir de este nivel en necesario contar con una **Red de Teleproceso de EMERGENCIA**. Para los cuales se propone la siguiente Configuración de acuerdo a la presente prioridad:

PRIORIDAD 1 :

- 3 Entidades Bancarias.

PRIORIDAD 2 :

- 3 Puntos Remotos de SEDAPAL los cuales concentrarán en forma estratégica el servicio de Teleproceso en los distritos de Surquillo, Breña y Callao.

11.2 CONSIDERACIONES TECNICAS

RECURSOS HARDWARE

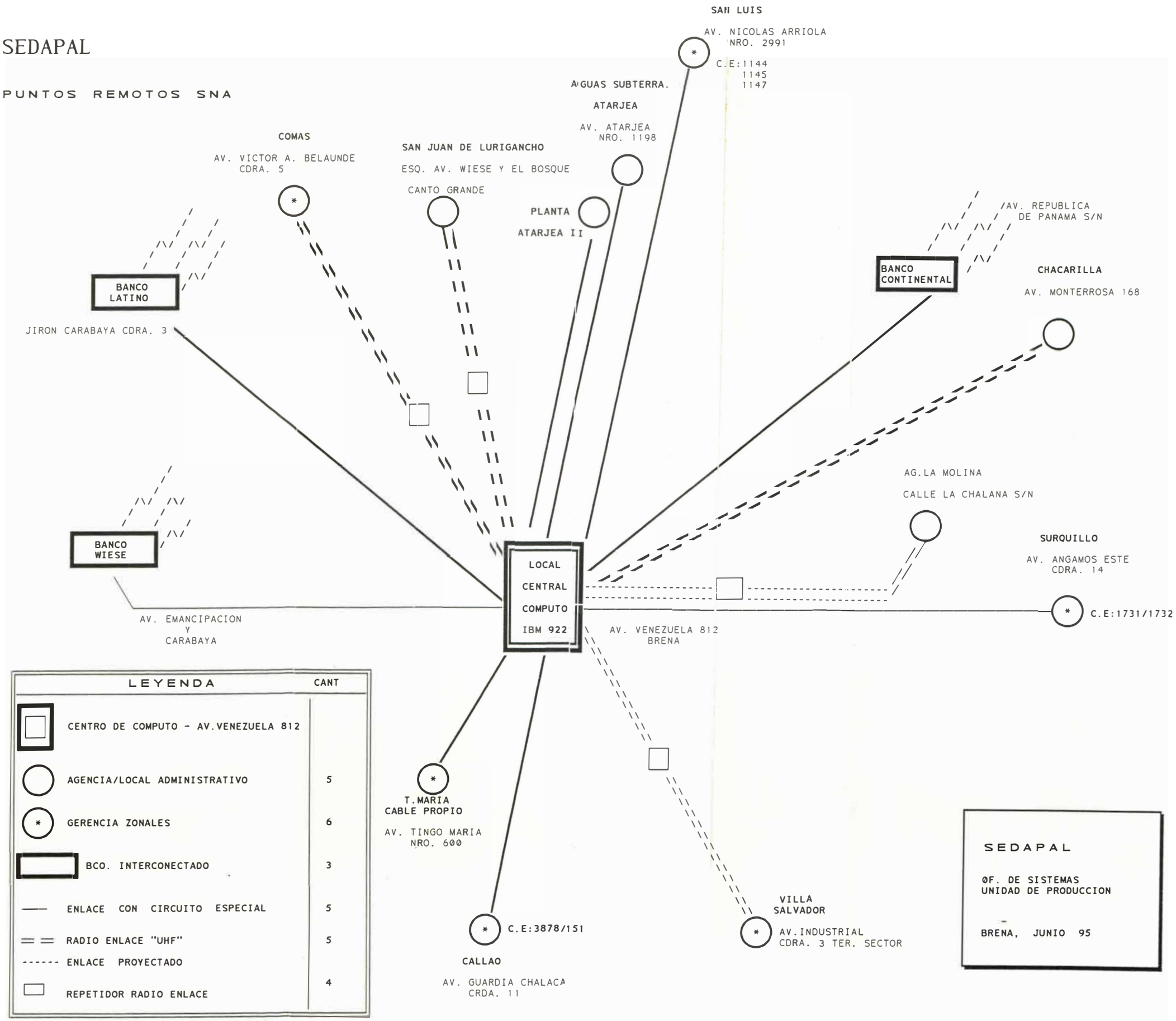
- Capacidad de procesamiento de 4.5 Mips
- Unidades de Discos 3380 modelo BJ4
- Unidades de Cartridges 3490
- Impresoras 4245 de 2,000 l.p.m.
- Consola de operador
- Terminal de usuario
- PC con tarjeta de emulación y disco duro
- Consola de Administración de red de Teleproceso
- Modems de Comunicación
- Pórticos de Salida de Controlador de Comunicaciones
- Líneas Telefónicas para comunicación de datos
- Línea Telefónica para coordinación técnica

RECURSOS SOFTWARE

- Ambiente VSE

SEDAPAL

PUNTOS REMOTOS SNA



LEYENDA	CANT
CENTRO DE COMPUTO - AV.VENEZUELA 812	
AGENCIA/LOCAL ADMINISTRATIVO	5
GERENCIA ZONALES	6
BCO. INTERCONECTADO	3
ENLACE CON CIRCUITO ESPECIAL	5
RADIO ENLACE "UHF"	5
ENLACE PROYECTADO	
REPETIDOR RADIO ENLACE	4

SEDAPAL

ØF. DE SISTEMAS
UNIDAD DE PRODUCCION

BRENA, JUNIO 95

- Ambiente VSAM
- Ambiente para Librerías (book's - phases - subrutinas)
- Compilador COBOL VS 1.3
- Generador de Aplicaciones CROSS SYSTEM PRODUCT
- Programa SORT de IBM
- Utilitario DITTO
- Ambiente CICS
- Ambiente VTAM - NCP
- Manejador de Bases de Datos SQL

RECURSOS HUMANOS

- Supervisor de Operaciones
- Operador de Consola
- Fiscal
- Técnico de Equipo de Hardware y Software
- Administrador de Red de Teleproceso
- Técnico-Supervisor de Red de Teleproceso

INFRAESTRUCTURA

- Espacio Físico de 9 metros cuadrados de almacenaje (recibos)
- Ambiente Físico para Control y Administración de la Red de Teleproceso

CAPACIDAD DE COMPUTO REQUERIDA

- Memoria Real : 8 MB
- Espacio VSAM : 2,249 MB
- Espacio Librariam : 18 MB
- Espacio Area SORT : 500 MB
- Espacio de Editor : 18 MB
- Capacidad de Impresión: 14 horas
- Unidades de Cartridges: 2
- Espacio en Disco PC : 1 MB
- Consola de operador : 1
- Consola Manejo de Red : 2
- Terminal de Usuario : 2
- Microcomputador : 1

PUESTA A PUNTO

- **Preparación de Ambiente de Contingencia**

  (6 horas)

  Generación de Espacio VSAM

  Generación de Catalogo de Contingencia

  Restore de Archivo de Contingencia

  Generación de Ambientes de Librería

  Definición de Librerías de Contingencia

  Restore de Librería (book's - phases - subrutinas).

  Compilación de Programas.

  Preparación de Librería de Editor

Validación y Pruebas de Job's de Contingencia

Preparación del ambiente de comunicaciones

Preparación del ambiente CROSS SYSTEM PRODUCT

Preparación del ambiente SQL

- **Mantenimiento de Ambiente de Contingencia**

  (2 horas)

  Fastcopy de discos de contingencia

  Generación de Microfichas (1 hora), opcional a decisión del Usuario

- **Instalación y Manejo de la red de Teleproceso**

  RED SEDAPAL.-

  - GZC. Gerencia Zonal Centro (Av. Tingo María 600) BREÑA.

    Atenderá requerimientos también de:

  - GZN. Gerencia Zonal Norte.
  - GZO. Gerencia Zonal Oeste (Av. Angamos cdra.14) SURQUILLO.

    Atenderá requerimientos también de:

  - GZS. Gerencia Zonal Sur (Av. Industrial s/n) Villa el Salvador.

- GZE. Gerencia Zonal Este (Av. Nicolás Arriola 2991) SAN LUIS.
- GZCa. Gerencia Zonal Callao (Av. Guardia Chalaca cdra 11) CALLAO.

NOTA : LINEA CONMUTADA.- Para cubrir estos tres puntos estratégicos se requiere 3 números telefónicos directos desde el centro de cómputo de contingencias hacia los puntos a servir.

RED BANCARIA.-

- **Banco Latino:**

  Soporte de Comunicaciones.-

  Comunicación vía RED MIDAS desde el centro de contingencias.

- **Banco Continental:**

  Soporte de Comunicaciones.-

  Comunicación vía radio enlace "UHF" desde el centro de contingencias.

- **Banco Wiese:**

  Soporte de Comunicaciones.-

  Comunicación vía RED MIDAS desde el centro de contingencias.

REQUERIMIENTOS Y ACTIVIDADES.-

CENTRO DE COMPUTO:

- Oficina para Control de Red
- Tres (3) Modems de Comunicaciones
- Seis (6) Pórticos de salida de Controlador de Comunicaciones (3720 o similar).
- Dos (2) Consolas de Control de red (VM y VSE).
- Una Línea Tef. CELULAR para coordinación técnica
- Una movilidad para instalación y mantenimiento de la red de Teleproceso

GERENCIAS ZONALES:

- Identificación de terminales e Impresoras en las tablas del CICS y programas manejadores de las comunicaciones.

GERENCIA ZONAL CENTRO

TIPO	ID.CICS	ID.VTAM	UBICACION
3471	UT01	LU311A01	EQUIPO COBRANZAS
4224	UP01	LU311A06	EQUIPO COBRANZAS-IMP
3471	UT06	LU311A05	EQUIPO CLIENTELA
3471	QT01	LU311A26	EQUIPO COBRANZAS (GER.Z.NORTE)
4224	QP01	LU311A25	EQUIPO COBRANZAS (GER.Z.NORTE)
3471	QT02	LU311A30	EQUIPO COBRANZAS (GER.Z.NORTE)

GERENCIA ZONAL OESTE

TIPO	ID.CICS	ID.VTAM	UBICACION
3471	TT01	LU304A02	EQUIPO COBRANZAS
4224	TP01	LU304A03	EQUIPO COBRANZAS-IMP
3471	TT03	LU304A04	EQUIPO CLIENTELA
3471	RT01	LU304A05	EQUIPO CLIENTELA (GER.Z.SUR)
4224	RP01	LU304A06	EQUIPO CLIENTELA (GER.Z.SUR)
3471	RT03	34304A07	EQUIPO FACT. Y CAT. (GER.Z.SUR)

GERENCIA ZONAL CALLAO

TIPO	ID.CICS	ID.VTAM	UBICACION
3471	WT01	LU303A05	EQUIPO COBRANZAS
4224	WP02	LU303A04	EQUIPO COBRANZAS-IMP
3471	WT05	LU303A06	EQUIPO COBRANZAS

SOFTWARE DE COMUNICACIONES:

- TCT (Terminal Control Table)
- VTAM (manejador de comunicaciones)
- NCP (Controlador de comunicaciones)
- DCT (Cola de Destino de Impresiones)
- SME (Sistema de Seguridad a nivel VTAM)

- Re-configurado de Unidades de control de terminales ubicados en las Gerencias Zonales definidas para cubrir la emergencia.

- Cableado coaxial necesario para la conexión de las pantallas e impresoras tanto en el centro de contingencias como en las Gerencias Zonales.

APLICATIVOS:

- Identificación de Aplicativos (Area Comercial)
- Identificación de Archivos de Aplicativos
- Identificación de Colas de Impresión de Aplicativos
- Identificación de módulos de

Interfases SQL para los aplicativos

TIEMPO ESTIMADO PARA OPERATIVIDAD:

- Puesta a punto del HARDWARE: 24 horas
- Puesta a punto del SOFTWARE: 8 horas

11.3 DESARROLLO GENERAL: DEFINICIONES DE PROCESOS

- **PREVIOS**

CATASTRO (Toma de Estado)

Corresponde a la medición de lecturas en el campo, realizada a través del **Convenio UNI-SEDAPAL**, tiene dos fases:

- **Lectura**

  Generación de Hojas de Toma de Estado que irán al campo.

- **Relectura**

  Actualización al Maestro de Catastro de las lecturas aplicadas.

CATASTRO (Levantamiento de Información y Actualización)

- Generación de Movimientos Válidos (Diarios)
- Actualización del Archivo de Catastro

CIERRES (Levantamiento de Información y Actualización)

- Generación Movimientos Válidos(Diarios)

- Actualización del Archivo de Catastro

RECLAMOS/DECRETOS (Levantamiento de Información y Actualización)

- Generación de Movimientos Válidos (Diarios).
- Actualización de los Archivos de Cta.Cte. y Catastro.

CREDITOS (Levantamiento de Información Bic-Bac - Emisión de Cuotas)

- Generación de Movimientos Válidos (Diarios).
- Actualización de Bic-Bac (Cta.Cte.)
- Emisión de Cuotas

COLATERALES (Levantamiento Información y Actualización)

- Generación de Movimientos Válidos (Diarios)
- Actualización de los Archivos de Cta.Cte. y Catastro.

PAGOS (Bancos y Teleproceso)

Corresponde a la Actualización de la Cobranza a través de los Bancos Interconectados a nuestro Centro de Cómputo y de las distintas Regiones.

PAGOS (Región)

Corresponde a la Actualización de la

cobranza efectuada a través de las distintas Regiones

- **FACTURACION**

Corresponde a la Actualización de la Diferencia de Lecturas del Mes anterior con las del Mes actual aplicando la Tarifa Vigente y Factores de Morosidad de acuerdo al Indice de Precios de Consumidor del Mes anterior.

GENERACION DE RECIBOS

Lista Recibos del Ciclo Facturado

SUBIDA DE CUENTA CORRIENTE

Actualización de Cta.Cte con los Cargos Facturados Generados con la Facturación.

OPERATIVO DE CIERRES

Generación de Ordenes de Cierre por Regiones.

MICROFICHAS DE CUENTA CORRIENTE

Generación de Microfichas de Cta.Cte. por Ciclo Facturado.

- **ARCHIVOS UTILIZADOS**

SISTEMA	Nro. procesos	Nro. prog.	Nro. arch.	Nro.Trks usados	Tiempo proceso
COMERCIAL:					
Catastro(T.E)	15	13	17		1'30"
Catastro(Mov)	13	18	19		30"
Cierres	13	17	19		30"
Recl/Decret.	14	16	19		30"
Créditos	56	38	25		1'30"
Colaterales	16	17	19		30"
Pagos	50	42	23		3'00"
Facturación	22	71	26		2'00"
Operat.Cierre	08	05	09		1'00"
T O T A L	207	237	176	49,676.00	---

Nota.- Estos procesos utilizan Archivos comunes por lo que no se puede detallar por proce-so el Nro. de Tracks usados.

12. CUARTO NIVEL DE CONTINGENCIA (30 DÍAS)

12.1 IDENTIFICACION: CUARTO NIVEL DE CONTINGENCIA

Con el fin de mantener la productividad informática, se ha establecido como **CUARTO NIVEL DE CONTINGENCIA** a los siguientes procesos:

- Previos (Catastro, Cierres, Reclamos y Decretos, Créditos BIC BAC y Emisión de Cuotas, Colaterales).
- Toma de Estado (Unificación).
- Pagos (Bancos, Regionales, TP, Farmacias y S/TP).
- Facturación (Emisión de Recibos, Subida CTA. CTE., Microficha CTA. CTE.).
- Operativo Cierres.
- Fuente Propia (Toma de Estado, Relectura, Pre-emisión, Emisión).
- Estatales.
- Mensual de Créditos (Liquidación de Cobranza, Créditos Directos).
- Estadísticas Mensuales (Catastro, Cta.Cte).

NOTA :

A partir de este nivel en necesario contar con una **Red de Teleproceso de EMERGENCIA**. Para los cuales se propone la siguiente Configuración de acuerdo a la presente prioridad:

PRIORIDAD 1 :

- 3 Entidades Bancarias.

PRIORIDAD 2 :

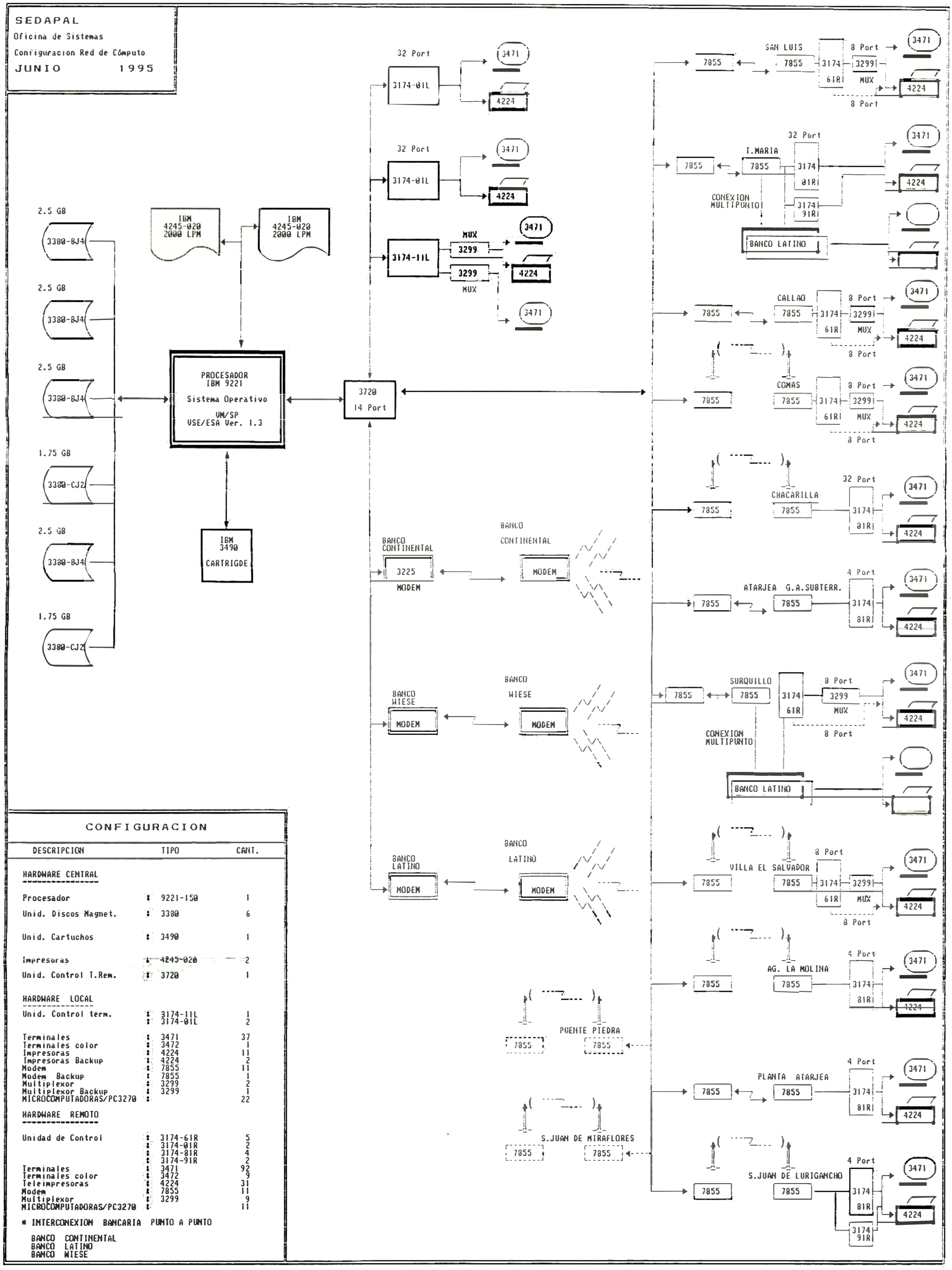
- 3 Puntos Remotos de SEDAPAL los cuales concentrarán en forma estratégica el servicio de Teleproceso en los distritos de Surquillo, Breña y Callao.

12.2 CONSIDERACIONES TECNICAS

RECURSOS HARDWARE

- Capacidad de procesamiento de 4.5 Mips.
- Unidades de Discos 3380 modelo BJ4.
- Unidades de Cartridges 3490.
- Impresoras 4245 de 2,000 l.p.m.
- Consola de operador.
- Terminal de usuario.
- PC con tarjeta de emulación y disco duro.
- Consola de Administración de red de Teleproceso.
- Modems de Comunicación.
- Pórticos de Salida de Controlador de Comunicaciones.
- Líneas Telefónicas para comunicación de datos.
- Línea Telefónica para coordinación técnica

SEDAPAL
Oficina de Sistemas
Configuracion Red de Cómputo
JUNIO 1995



CONFIGURACION

DESCRIPCION	TIPO	CANT.
HARDWARE CENTRAL		
Procesador	9221-150	1
Unid. Discos Magnet.	3380	6
Unid. Cartuchos	3490	1
Impresoras	4245-020	2
Unid. Control T.Rem.	3720	1
HARDWARE LOCAL		
Unid. Control term.	3174-11L	1
	3174-01L	2
Terminales	3471	37
Terminales color	3472	1
Impresoras	4224	11
Impresoras Backup	4224	2
Modem	7855	11
Modem Backup	7855	1
Multiplexor	3299	2
Multiplexor Backup	3299	1
MICROCOMPUTADORAS/PC3270		22
HARDWARE REMOTO		
Unidad de Control	3174-61R	5
	3174-01R	2
	3174-81R	4
	3174-91R	2
Terminales	3471	92
Terminales color	3472	9
Teleimpresoras	4224	31
Modem	7855	11
Multiplexor	3299	9
MICROCOMPUTADORAS/PC3270		11

* INTERCONEXION BANCARIA PUNTO A PUNTO

BANCO CONTINENTAL
BANCO LATINO
BANCO WIESE

RECURSOS SOFTWARE

- Ambiente VSE.
- Ambiente VSAM.
- Ambiente para Librerías (book's - phases - subrutinas).
- Compilador COBOL VS 1.3
- Generador de Aplicaciones CROSS SYSTEM PRODUCT
- Programa SORT de IBM.
- Utilitario DITTO.
- Ambiente CICS.
- Ambiente VTAM - NCP.
- Manejador de Bases de Datos SQL.

RECURSOS HUMANOS

- Supervisor de Operaciones.
- Operador de Consola.
- Fiscal.
- Técnico de Equipo de Hardware y Software.
- Administrador de Red de Teleproceso.
- Técnico-Supervisor de Red de Teleproceso.

INFRAESTRUCTURA

- Espacio Físico de 9 metros cuadrados de almacenaje (recibos).
- Ambiente Físico para Control y

Administración de la Red de Teleproceso

CAPACIDAD DE COMPUTO REQUERIDA

- Memoria Real : 10 MB
- Espacio VSAM : 2,599 MB
- Espacio Librariam : 27 MB
- Espacio Area SORT : 630 MB
- Espacio de Editor : 20 MB
- Capacidad de Impresión: 20 horas
- Unidades de Cartridges: 2
- Espacio en Disco PC : 1 MB
- Consola de operador : 1
- Consola Manejo de Red : 2
- Terminal de Usuario : 2
- Microcomputador : 1

PUESTA A PUNTO

- **Preparación de Ambiente de Contingencia**

  (6 horas)

  Generación de Espacio VSAM.

  Generación de Catalogo de Contingencia.

  Restore de Archivo de Contingencia.

  Generación de Ambientes de Librería.

  Definición de Librerías de Contingencia

  Restore de Librería (book's - phases - subrutinas).

Compilación de Programas.

Preparación de Librería de Editor.

Validación y Pruebas de Job's de Contingencia.

Preparación del ambiente de comunicaciones.

Preparación del ambiente CROSS SYSTEM PRODUCT.

Preparación del ambiente SQL.

- **Mantenimiento de Ambiente de Contingencia**

  (2 horas)

  Fastcopy de discos de contingencia

  Generación de Microfichas (1 hora), opcional a decisión del Usuario.

- **Instalación y Manejo de la red de Teleproceso**

  RED SEDAPAL.-

  - GZC. Gerencia Zonal Centro (Av. Tingo María 600) BREÑA.

    Atenderá requerimientos también de:

  - GZN. Gerencia Zonal Norte.
  - GZO. Gerencia Zonal Oeste (Av. Angamos cdra.14) SURQUILLO.

    Atenderá requerimientos también de:

  - GZS. Gerencia Zonal Sur (Av. Indus-

trial s/n) Villa el Salvador.

- GZE. Gerencia Zonal Este (Av. Nicolás Arriola 2991) SAN LUIS.
- GZCa. Gerencia Zonal Callao (Av. Guardia Chalaca cdra 11) CALLAO.

NOTA : LÍNEA CONMUTADA.- Para cubrir estos tres puntos estratégicos se requiere 3 números telefónicos directos desde el centro de cómputo de contingencias hacia los puntos a servir.

RED BANCARIA.-

- **Banco Latino:**

  Soporte de Comunicaciones.-

  Comunicación vía RED MIDAS desde el centro de contingencias.

- **Banco Continental:**

  Soporte de Comunicaciones.-

  Comunicación vía radio enlace "UHF" desde el centro de contingencias.

- **Banco Wiese:**

  Soporte de Comunicaciones.-

  Comunicación vía RED MIDAS desde el centro de contingencias.

REQUERIMIENTOS Y ACTIVIDADES.-

CENTRO DE COMPUTO:

- Oficina para Control de Red.
- Tres (3) Modems de Comunicaciones.
- Seis (6) Pórticos de salida de Controlador de Comunicaciones (3720 o similar).
- Dos (2) Consolas de Control de red (VM y VSE).
- Una Línea Tef. CELULAR para coordinación técnica.
- Una movilidad para instalación y mantenimiento de la red de Teleproceso.

GERENCIAS ZONALES:

- Identificación de terminales e Impresoras en las tablas del CICS y programas manejadores de las comunicaciones.

GERENCIA ZONAL CENTRO

TIPO	ID.CICS	ID.VTAM	UBICACION
3471	UT01	LU311A01	EQUIPO COBRANZAS
4224	UP01	LU311A06	EQUIPO COBRANZAS-IMP
3471	UT06	LU311A05	EQUIPO CLIENTELA
3471	QT01	LU311A26	EQUIPO COBRANZAS (GER.Z.NORTE)
4224	QP01	LU311A25	EQUIPO COBRANZAS (GER.Z.NORTE)
3471	QT02	LU311A30	EQUIPO COBRANZAS (GER.Z.NORTE)

GERENCIA ZONAL OESTE

TIPO	ID.CICS	ID.VTAM	UBICACION
3471	TT01	LU304A02	EQUIPO COBRANZAS
4224	TP01	LU304A03	EQUIPO COBRANZAS-IMP
3471	TT03	LU304A04	EQUIPO CLIENTELA
3471	RT01	LU304A05	EQUIPO CLIENTELA (GER.Z.SUR)
4224	RP01	LU304A06	EQUIPO CLIENTELA (GER.Z.SUR)
3471	RT03	34304A07	EQUIPO FACT. Y CAT. (GER.Z.SUR)

GERENCIA ZONAL CALLAO

TIPO	ID.CICS	ID.VTAM	UBICACION
3471	WT01	LU303A05	EQUIPO COBRANZAS
4224	WP02	LU303A04	EQUIPO COBRANZAS-IMP
3471	WT05	LU303A06	EQUIPO COBRANZAS

SOFTWARE DE COMUNICACIONES:

- TCT (Terminal Control Table)

  En esta tabla se definirán las terminales e impresoras.

- VTAM (manejador de comunicaciones).
- NCP (Controlador de comunicaciones).
- DCT (Cola de Destino de Impresiones).
- SME (Sistema de Seguridad a nivel VTAM).

- Re-configurado de Unidades de control de terminales ubicados en las Gerencias Zonales definidas para cubrir la emergencia.

- Cableado coaxial necesario para la conexión de las pantallas e impresoras tanto en el centro de contingencias como en las Gerencias Zonales.

APLICATIVOS:

- Identificación de Aplicativos (Area Comercial):

  KCA1 Sistema de Catastro

  KCA2 Calculo de Facturación Retrospectiva

KCA4 Consulta de Alteraciones

KCA5 Sistema de Catastro - Directorio de Habilitaciones

KNC2 Cierres y Reaperturas

KNC4 Colaterales

KNC5 Sistema de Créditos

KPI1 Menu Principal Interctivos de Pagos

KPI2 Pantalla de Cajas

KRP1 Recaudación de Pagos

- Identificación de Archivos de Aplicativos.
- Identificación de Colas de Impresión de Aplicativos.
- Identificación de módulos de Interfases SQL para los aplicativos.

TIEMPO ESTIMADO PARA OPERATIVIDAD:

- Puesta a punto del HARDWARE: 24 horas
- Puesta a punto del SOFTWARE: 8 horas

12.3 DESARROLLO GENERAL: DEFINICIONES DE PROCESOS

- **PREVIOS**

  CATASTRO (Toma de Estado)

  Corresponde a la medición de lecturas en el campo, realizada a través del **Convenio UNI-SEDAPAL**, tiene dos fases:

  - **Lectura**

    Generación de Hojas de Toma de Estado que irán al campo.

  - **Relectura**

    Actualización al Maestro de Catastro de las lecturas aplicadas.

  CATASTRO (Levantamiento de Información y Actualización)

  - Generación de Movimientos Válidos (Diarios)
  - Actualización del Archivo de Catastro

  CIERRES (Levantamiento de Información y Actualización)

  - Generación de Movimientos Válidos (Diarios)
  - Actualización del Archivo de Catastro

  RECLAMOS/DECRETOS (Levantamiento de Información y Actualización)

  - Generación de Movimientos Válidos (Diarios)

- Actualización de los Archivos de Cta.Cte. y Catastro

CREDITOS (Levantamiento de Información Bic-Bac - Emisión de Cuotas)

- Generación de Movimientos Válidos (Diarios)
- Actualización de Bic-Bac (Cta.Cte.)
- Emisión de Cuotas

COLATERALES (Levantamiento Información y Actualización)

- Generación de Movimientos Válidos (Diarios)
- Actualización de los Archivos de Cta.Cte. y Catastro.

PAGOS (Bancos y Teleproceso)

Corresponde a la Actualización de la Cobranza a través de los Bancos Interconectados a nuestro Centro de Cómputo y de las distintas Regiones.

PAGOS (Región)

Corresponde a la Actualización de la cobranza efectuada a través de las distintas Regiones.

- **FACTURACION**

Corresponde a la Actualización de la Diferencia de Lecturas del Mes anterior con las del Mes actual aplicando la Tarifa Vigente y Factores de Morosidad de acuerdo al Indice de Precios de Consumidor del Mes anterior.

GENERACION DE RECIBOS

Lista Recibos del Ciclo Facturado

SUBIDA DE CUENTA CORRIENTE

Actualización de Cta.Cte con los Cargos Facturados Generados con la Facturación.

OPERATIVO DE CIERRES

Generación de Ordenes de Cierre por Regiones.

MICROFICHAS DE CUENTA CORRIENTE

Generación de Microfichas de Cta.Cte. por Ciclo Facturado.

GENERACION DE RECIBOS

Lista recibos del Ciclo Facturado.

SUBIDA DE CUENTA CORRIENTE

Actualización de Cta.Cte con los Cargos Facturados Generados con la Facturación.

OPERATIVO DE CIERRES

Generación de Ordenes de Cierre por Región.

MICROFICHAS DE CUENTA CORRIENTE

Generación de Microfichas de Cta.Cte por Ciclo Facturado.

FUENTE PROPIA

Corresponde a la emisión de los Usuarios que cuentan con abastecimiento propio y que usan la red de sólo el Alcantarillado.

EMISION DE ESTATALES

Corresponde a los usuarios dependientes del Estado o Municipios, llámese Hospitales, Colegios, Universidades, Municipalidades, Empresas del Estado.

PROCESOS ESTADISTICOS

Corresponde a los procesos Mensuales (Cuadros Estadísticos)

- **ARCHIVOS UTILIZADOS**

SISTEMA	Nro. procesos	Nro. prog.	Nro. arch.	Nro.Trks usados	Tiempo proceso
COMERCIAL:					
Catastro(T.E)	15	13	17		1'30"
Catastro(Mov)	13	18	19		30"
Cierres	13	17	19		30"
Recl/Decret.	14	16	19		30"
Créditos	56	38	25		1'30"
Colaterales	16	17	19		30"
Pagos	50	42	23		3'00"
Facturación	22	71	26		2'00"
Operat.Cierre	08	05	09		1'00"
Fuente Propia	55	42	05		---
Estatales	06	04	07		2'00"
Estadísticos	54	50	11		12'00"
T O T A L	**322**	**333**	**199**	**57,421.00**	**---**

Nota.- Estos procesos utilizan Archivos comunes por lo que no se puede detallar por proceso el Nro. de Tracks usados.

Los Procesos de Fuente Propia se ejecutan por Etapas: Lecturas , Re-Lecturas , Pre-Emisión , Emisión ; por lo que no se puede dar el tiempo estimado de Proceso.

PROYECTO DEL PLAN DE CONTINGENCIA

1. GENERALIDADES

Según informes del Instituto Nacional de Defensa Civil, de Enero a la fecha (Noviembre 1995) el país ha tenido pérdidas de aproximadamente tres millones de dólares por desastres naturales y emergencias.

En el Departamento de Lima ocurrieron 81 desastres provocados por incendios y sismos en su mayor porcentaje. Ante estos desastres, se pregunta ¿Afectó a los centros informáticos? ¿Qué otros problemas dañaron el sistema?. La respuesta puede ser el silencio. Pero, la verdad, es que han tenido problemas en los sistemas informáticos.

2. TRABAJO DE CAMPO: VISITAS, ENTREVISTAS Y ENCUESTAS

El trabajo de campo se realizó para recabar informaciones de algunos centros informáticos que operan en la ciudad de Lima.

2.1 VISITAS, ENTREVISTAS Y ENCUESTAS

Estas actividades se desarrollaron del 15 de Octubre al 6 de Noviembre (1995) dirigidos a los directivos de Centros Informáticos de Entidades Financieras, de Industria y Minería, Salud Pública, Educación Superior y Servicios Básicos de la Comunidad.

Las visitas y entrevistas permiten explicar las razones de la aplicación de las encuestas por muestreo y los resultados son:

- Las entidades financieras, industria, minería, servicios básicos de la comunidad y Seguro Social del Perú, tienen Centros de Cómputo con equipos sofisticados muy costosos.
- Cuentan con ingenieros de sistemas y técnicos en computación. Entre ellos hay ingenieros egresados de la Universidad Nacional de Ingeniería.
- Tienen **Plan de Contingencia**, elaborados por especialistas de cada entidad o terceros. Telefónica del Perú, Seguro Social y Petro Perú, están preparando sus correspondientes planes.
- La interconección de los centros de cómputo tienen alcance local, nacional e

internacional.

- Las Instituciones de Educación Superior Universitaria, tienen Centros de Cómputo, equipados de acuerdo a la naturaleza de su trabajo.
- Las Universidades: Nacional de Ingeniería, Católica, "Inca Garcilaso de la Vega" y San Martín de Porres forman Ingenieros de Sistemas.
- En las universidades encuestadas trabajan ingenieros de sistemas y técnicos en computación.
- Tienen **Plan de Contingencia** las universidades: Católica, Garcilaso y San Martín de Porres y no tienen, la Universidad Nacional de Ingeniería y "Enrique Guzmán y Valle".
- Los centros de cómputo de los Hospitales Arzobispo Loayza y del Instituto del Niño, están servidos por técnicos en computación y no tienen **plan de contingencia**.
- Los problemas que han afectado a la mayoría de centros de cómputo son: Virus Informático y corte de energía eléctrica.

2.2 CENTROS DE COMPUTO DE LAS INSTITUCIONES ENCUESTADOS

INSTITUCIONES FINANCIERAS :

- Banco de Crédito del Perú.
- INTERBANC.
- Banco de Comercio.
- Banco de la Nación.

INDUSTRIA DEL PETROLEO :

- Perú - Petro.

MINERIA :

- CENTROMIN PERU S.A.
- CAMBIOR PERU S.A.
- Sociedad Minera LA GRANJA S.A.

SALUD PUBLICA :

- Instituto Peruano de Seguridad Social.
- Hospital Nacional Arzobispo Loayza.
- Instituto de Salud del Niño.

INSTITUCIONES DE EDUCACION UNIVERSITARIA :

- Universidad Nacional de Ingeniería.
- Pontificia Universidad Católica del Perú.
- Universidad Inca Garcilaso de la Vega.
- Universidad San Martín de Porres.

- Universidad Nacional de Educación "Enrique Guzmán y Valle".

INSTITUCIONES DE SERVICIOS DE LA COMUNIDAD :

- Servicio de Agua Potable y Alcantarillado de Lima - SEDAPAL.
- IBM OUTSOURCE ELECTROLIMA.
- Telefónica del Perú.

DESARROLLO DEL PROYECTO

1. GENERALIDADES

Las instituciones con centros informáticos cuentan con normas especiales de seguridad y los directivos y trabajadores comparten responsabilidades en el desempeño de sus funciones.

El resultado del trabajo permanente garantiza el cumplimiento de los objetivos propuestos.

2. ANTECEDENTES

En el país vienen ocurriendo desastres causados por la actividad geológica del Cinturón de Fuego del Pacífico Sur y la Placa de Nazca. De igual manera las inundaciones, incendios, terrorismo, sabotajes y casos fortuitos obligan adoptar medidas de contingencia a nivel nacional, regional y local para evitar pérdidas humanas y materiales.

3. FINALIDADES

Las finalidades del **Plan de Contingencia** son:

- Contribuye en forma eficaz en la protección, uso racional y recuperación de los equipos y materiales de los Centros de Informática para que sigan funcionando con normalidad.
- Garantiza y protege al personal que labora y permite la continuidad de sus funciones en los Centros de Informática.

4. ESTRATEGIAS

Se plantean las siguientes estrategias:

- Organización básica: De Conducción, equipos y brigadas de auxilio por áreas de trabajo.
- Programas de actividades de concientización para afrontar desastres.
- Normas especiales de prevención de desastres por áreas y evaluación periódica.
- Coordinaciones con organismos competentes del Estado.
- Programa de recuperación de los registros vitales, según jerarquías.
- Ensayos de prevención de desastres.
- Convenio de ayuda mutua con entidades afines.
- Póliza de Seguros.

- Presupuesto Financiero especial.
- Programas de rehabilitación y reconstrucción con proyectos de ambientes especiales para los centros de informática.
- Evaluación y replanteamiento del **Plan de Contingencia**.

5. OBJETIVOS

Para lograr los fines del plan se plantean los siguientes objetivos:

- Organizar un Comité Central, Equipos y Brigadas de Auxilio por áreas de trabajo y normar sus correspondientes tareas.
- Realizar una intensa campaña para formar conciencia cívica a fin de afrontar desastres.
- Compartir responsabilidades en la prevención, desarrollo y evaluación del **Plan de Contingencia**.
- Realizar prácticas periódicas de simulacros de desastres en coordinación con el Instituto Nacional de Defensa Civil.
- Planificar la inversión de recursos económicos destinados a las contingencias.
- Celebrar convenios de ayuda mutua con entidades afines que protejan los backup's.

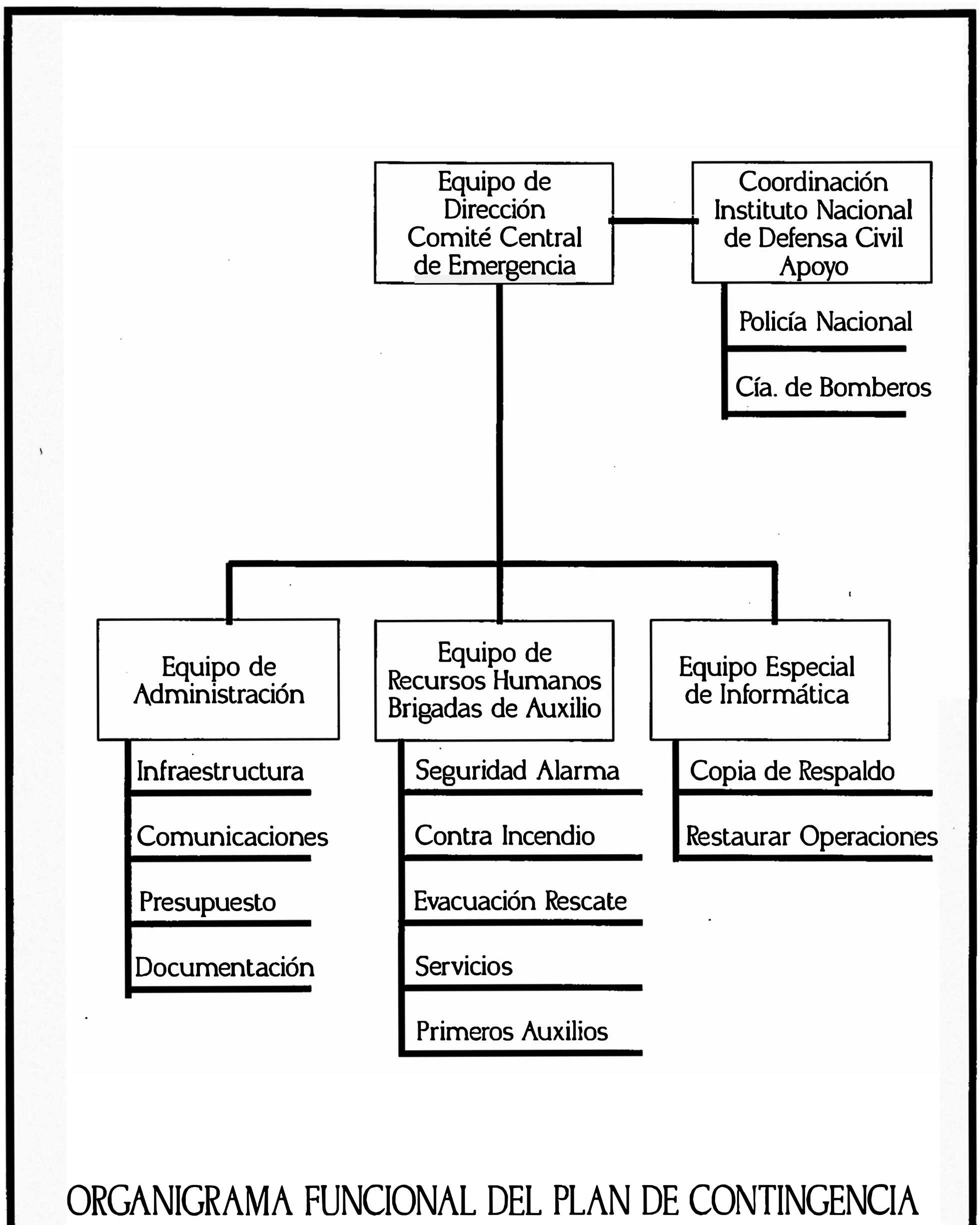
- Planificar procedimientos de mantenimiento en situaciones de emergencia.
- Establecer programas de recuperación de los registros vitales.
- Elaborar mapas de los recursos disponibles.
- Combatir la propagación de los virus informáticos, proponiendo y gestionando leyes especiales.
- Lograr que se ejecuten los programas de rehabilitación y reconstrucción de los equipos de los centros de informática.
- Lograr que se construyan ambientes adecuados que garanticen la seguridad de los equipos, materiales de trabajo y personal de los centros de informática.

6. ORGANIZACION Y FUNCIONES

6.1 EQUIPO DE DIRECCION DEL COMITE CENTRAL DE EMERGENCIA

TAREA: - Organización y dirección.

- Coordina con el Instituto Nacional de Defensa Civil.
- Coordina el apoyo de la Policía Nacional y Compañía de Bomberos.
- Elaborar los programas de acción.



ORGANIGRAMA FUNCIONAL DEL PLAN DE CONTINGENCIA

6.2 EQUIPO ADMINISTRATIVO

TAREA: - Seguridad de la infraestructura física y comunicaciones.

- Presupuesto de emergencia.
- Documentación.

6.3 EQUIPO DE RECURSOS HUMANOS

TAREA: Constituye brigadas de auxilio de:

- Seguridad y alarma.
- Contra incendios.
- Evacuación y rescate.
- Servicios - Soportes - transporte.
- Primeros Auxilios.

6.4 EQUIPO DE INFORMATICA

TAREA: - Mantener copias de respaldo.

- Restaurar las operaciones de los equipos del Centro de Informática.

7. ACCIONES PARA AFRONTAR DESASTRES

El equipo directivo del Comité Central de emergencia, planifica las acciones en el siguiente orden:

- Preventivas.
- Durante el desastre.

- De recuperación.
- De evaluación.

7.1 ACCIONES PREVENTIVAS

Las medidas preventivas son: de organización, concientización y administración.

ORGANIZACION

El equipo de recursos humanos constituirán brigadas de auxilio para realizar las siguientes tareas:

- Ensayos de alarma y verificación de los accesos del local.
- Realizar prácticas contra incendios.
- Realizar ensayos de evacuación y rescate.
- El servicio de transporte y otros deben entrenarse para actuar.
- Realizar prácticas de primeros auxilios.

ACCIONES DE CONCIENTIZACION

Tomar conciencia del problema de desastres es fundamental en la vigencia de las instituciones. Este objetivo se logra con una eficaz campaña de concientización, mediante las siguientes acciones:

- Dar a conocer las normas vigentes sobre contingencias.
- Charlas, conferencias, cine-forum.

- Imprimir boletines y confeccionar afiches de prevención de desastres.
- Publicar el mapa de recursos disponibles.
- Realizar simulacros contra desastres en coordinación con el Instituto Nacional de Defensa Civil.
- Coordinar con el Instituto Nacional de Defensa Civil para que los medios de Comunicación masiva realicen campañas periódicas de orientación contra desastres.

ADMINISTRATIVAS

El equipo administrativo cumplirá las siguientes tareas:

- Mantener la seguridad física de los ambientes del local.
- Verificar el buen funcionamiento de las comunicaciones internas y externas.
- Programar el presupuesto de contingencia.
- Preveer la seguridad de los documentos claves de la Institución.

7.2 ACCIONES DURANTE EL DESASTRE

Cuando ocurre el desastre, la organización administrativa es puesta a prueba y en la medida en que se hayan cumplido las funciones señaladas en el ANTES, el desastre será debidamente

enfocado y ejecutada las acciones prioritarias, atendiendo a la población afectada, evitando de esta manera los mayores daños que hubieran podido producirse de no haber sido debidamente prevista la emergencia y tomado las previsiones del caso.

Deberá realizarse principalmente:

- Atención de heridos.
- Búsqueda y rescate de personas.
- Distribución de alimentos y abrigo.

7.3 ACCIONES DE RECUPERACION

Después del desastre la tarea inmediata para disminuir los efectos del desastre son:

LA REHABILITACION

Se dará, principalmente, en la reanudación de los servicios de agua, luz, vías de comunicación, comercio de alimentos, atención hospitalaria, seguridad de la población.

LA RECONSTRUCCION

Es una etapa de mediano o largo plazo, en ella deberá darse atención a caminos, vías férreas, aeropuertos, hospitales, locales públicos y otros, de acuerdo con el orden de prioridades establecidas en el planeamiento administrativo de desastres.

7.4 LA EVALUACION

Es el análisis crítico de las acciones anteriores (preventiva, durante y recuperación) que se realiza para comprobar la eficiencia de la administración del desastre. El fin es reajustar y/o replantear el **Plan de Contingencia**.

7.5 PROBLEMA: PRESENCIA DE VIRUS INFORMATICO

ACCION DEL PLAN ANTIVIRUS

- Apagar las PC's.
- El especialista identifica al virus, mediante el método de detección correspondiente.
- Aplica las instrucciones para su supresión o erradicación.

RECUPERACION

- Normalizar el trabajo

EVALUACION

- Análisis cítrico.- Sugerencias, reajuste del **Plan de Contingencia**.

7.6 PROBLEMA: INCENDIO

ACCION DE LOS EQUIPOS Y BRIGADAS DE AUXILIO

- Alarma y seguridad.
- Evacuación y rescate.
- Contra incendio - extinguidores.

- Auxilio de la Compañía de Bomberos.
- Servicios.
- Primeros auxilios.

RECUPERACION

- Normalizar el trabajo.
- Uso de las cintas backup's (copia de respaldo) proporcionado en razón del Convenio de Ayuda Mutua.
- Plan de Rehabilitación y Reconstrucción.

EVALUACION

- Análisis crítico y sugerencias.
- Reajuste del **Plan de Contingencia**.

7.7 PROBLEMA: TERREMOTO 7 GRADOS ESCALA DE RICHTER

Acción de los grupos de trabajo en coordinación con Defensa Civil de acuerdo a las previsiones propuestas principalmente se atenderá:

- Evacuación.
- Atención de heridos.
- Búsqueda y rescate de personas.
- Distribución de alimentos y abrigo.
- Traslado de personas a lugares seguros.

RECUPERACION DESPUES DEL TERREMOTO

- Ejecución del Plan de Rehabilitación.
- Se emplearán las informaciones de respaldo

A C C I O N E S			
PREVENTIVAS	**DURANTE**	**RECUPERACION**	**EVALUACION**
ORGANIZACION: Equipos.- Brigadas de Auxilio de: Seguridad y alarma - Contra incendio - Evacuación y rescate - Servicios - Primeros auxilios **CONCIENTIZACION:** Conciencia cívica. Normas vigentes - Charlas - Conferencias - Cine Forum - Boletines - Afiches - mapa de recursos - Simulacros contra desastres - convenio de ayuda mutua - Póliza de seguros - Coordinación con Defensa Civil - Apoyo Policia Nacional - Compañía de Bomberos. **ADMINISTRATIVAS:** Seguridad infraestructura del local. Comunicaciones internas y externas. Presupuesto de contingencia. Seguridad de documentos claves.	TRES PROBLEMAS: 1.- Virus Informático Acción: Plan Antivirus	Normalizar el trabajo	Análisis crítico: Sugerencias Reajustar Plan de Contingencias
	2.- Incendio Acción : Equipo y Brigadas de auxilio. Intervención: Cía.de Bomberos. Apoyo : Policía Nac.	Normalizar el trabajo con apoyo del convenio-backup Ejecución del Plan de Rehabilitación y Reconstrucción.	Análisis crítico: Sugerencias Reajustar Plan de contingencia.
	3.- Terremoto: 7 Grados Escala Richter. Acción: Equipos y brigadas de auxilio. Auxilio:Defensa Civil Apoyo: Policía Nacional y Compañía de Bomberos Prioridades: Evacuación - Atención de heridos - Búsqueda y rescate de personas - Distribución de alimentos - Traslado de personas a lugares seguros.	Aplicar el Plan de Rehabilitación Convenio: cooperación y auxilio. Recuperación: Registros vitales. Normalizar el trabajo. Plan de reconstrucción: Presupuesto Especial Póliza de seguros.	Análisis crítico: Sugerencias Replanteamiento del PLAN DE CONTINGENCIA

ESQUEMA DE ORGANIZACION FUNCIONAL PARA AFRONTAR DESASTRES

para reiniciar el trabajo de informática en atención al Convenio de ayuda mutua.

- Evaluación y sugerencias.
- Ejecución del Plan de Reconstrucción de acuerdo al presupuesto contra desastres y otras partidas económicas especiales.

EVALUACION Y SUGERENCIAS

- Replanteamiento del **Plan de Contingencias**.

8. SIMULACRO DE DESASTRES

Poner a prueba el funcionamiento de los programas de acción de los recursos humanos.

En cada caso, anotar los aciertos y deficiencias.

8.1 EVALUACION

Balance crítico de las acciones de los equipos y brigadas de trabajo: aciertos, deficiencias y recomendaciones.

8.2 REAJUSTE

Replantear el programa de acción de los equipos y brigadas de trabajo.

Afinar el **Plan de Contingencia**.

9. SIMULACRO DE EVACUACION PROGRAMADO POR EL SISTEMA NACIONAL DE DEFENSA CIVIL - 31 DE MAYO DE 1995

SEDAPAL - ANTE MOVIMIENTOS SISMICOS ACTUE CON SEGURIDAD

9.1 PRESENTACION

Nuestro país está ubicado geográficamente en la parte central y occidental del continente Sudamericano, en una zona de interacción de placas que se traduce en FUENTE GENERADORA DE ACTIVIDAD SISMICA PERMANENTE, con el riesgo consiguiente de movimientos sísmicos de variada intensidad difícilmente predecibles.

Ante esta realidad, la UNIDAD DE SEGURIDAD E HIGIENE INDUSTRIAL ha preparado ésta cartilla con la finalidad que estemos preparados para actuar con seguridad: ANTES, DURANTE Y DESPUES DE UN SISMO, a los efectos de minimizar los daños personales que pudieran ocurrir como consecuencia de un sismo de fuerte intensidad.

El 31 de mayo de 1995, el Sistema Nacional de Defensa Civil ha programado un simulacro de Evacuación a las 15.2 hrs., con la participación de toda la población del Perú.

En SEDAPAL también efectuaremos dicho simulacro con la participación de todos los trabajadores y la conducción de los BRIGADISTAS

de cada centro operativo y oficinas administrativas.

9.2 LO QUE USTED DEBE REALIZAR

ANTES DEL SISMO

Conozca:

- Las áreas de Seguridad, para evacuar o refugiarse ante cualquier movimiento sísmico.
- Las rutas de salida hacia las áreas de seguridad.

Evite colocar objetos de gran peso y tamaño en estantes altos.

Asegure los estantes altos a las paredes.

Observe la ubicación de su casa y centro de trabajo en relación con otras edificaciones a fin de protegerse contra materiales que pudieran desprenderse de ellas.

Ejecute simulacros de evacuación periódicamente.

DURANTE EL SISMO

Mantenga la calma y serenidad en todo instante y recuerde que una persona serena piensa y actúa mejor.

Si está bajo techo, en los dos primeros pisos de un edificio evacue rápidamente en forma ordenada hacia la zona de seguridad, siguiendo las normas

indicadas a continuación:

- Dada la alarma o percibido el sismo, la movilización se hará en orden, a paso vivo, sin correr y sin desesperarse.
- Deje en lo posible sus cosas y objetos personales.
- Nadie debe gritar para evitar el pánico. Si alguna persona se pusiera nerviosa, los compañeros deben ayudarla a mantener la calma.
- Quiénes usen zapatos con tacones, deben quitárselos inmediatamente para una mejor movilización.
- Si alguna persona cayera durante la evacuación, debe tratar de rodar fuera de la zona de tránsito para no provocar más caídas.
- Si se le cae algún libro, zapato o cualquier otro objeto, no trate de recuperarlo.
- Quien esté más cerca de las puertas deberá abrirlas para permitir la salida rápida de las personas.
- Al evacuar un lugar siempre se debe buscar zonas abiertas (Areas de Seguridad) tales como patios, plazuelas, etc.
- Al llegar al Area de Seguridad, se constituirán en orden para verificar si todos se encuentran bien.

- Sin entorpecer la labor de las brigadas especializadas, los evacuantes permanecerán en el Area de seguridad hasta que se evalúen los daños ocasionados.

Si está bajo techo, en pisos superiores al segundo, busque refugio debajo del marco de una puerta, de escritorios o mesas resistentes o de columnas o vigas. Evite colocarse cerca de ventanas o puertas de vidrio.

Si ha logrado salir a la calle, aléjese de los alambres eléctricos, postes o edificaciones que puedan derrumbarse.

Si está en un lugar público donde hay aglomeraciones de personas, contrólese y evite contribuir al pánico general.

DESPUES DEL SISMO

Después de un sismo de considerable intensidad, pueden presentarse réplicas o temblores secundarios, por lo que se debe estar preparado para actuar con serenidad y orden.

Tenga sumo cuidado al entrar a edificios averiados por el sismo porque podrían derrumbarse.

Si al entrar a un edificación hay olor a gas:

- Abra todas las ventanas y puertas.
- Cierre la llave del gas.

- Abandone el edificio inmediatamente hasta que el gas disipe totalmente.

No prenda fuego, ni manipule interruptores eléctricos.

Si el sismo fuera de noche y la edificación estuviera averiada, use solamente linternas a pilas porque al accionar los interruptores de luz, o al usar fósforos podrían generar incendios al inflamarse líquidos o gases derramados como el alcohol, gasolina, bencina, gas propano.

Rescate de inmediato a los heridos.

No emplee el teléfono, excepto para llamadas de extrema emergencia.

Con precaución abra las puertas de los armarios y tenga cuidado con los objetos que puedan caerse de los estantes.

10. COSTOS APROXIMADOS EN DOLARES A 1995

	COSTO TOTAL	**$ 96,321.00**
1.	**Personal de Sistemas**	**1,871.00**
	Directivos	1,100.00
	Administrativos	100.00
	Analistas-programadores	200.00
	Soporte Técnico	200.00
	Operación	216.00
	Control de Calidad	55.00
2.	**Pasajes y viáticos**	**300.00**
3.	**Capacitación (por año)**	**3,000.00**
4.	**Insumos**	**2,300.00**
	Formatos y recibos	600.00
	Cintas y bandas	1,700.00
5.	**Gastos en comunicaciones**	**1,900.00**
6.	**Gastos en energía**	**1,000.00**
7.	**Software (Licencias)**	**650.00**
8.	**Equipo Central**	**44,000.00**
	Procesador	6,500.00
	Unidades de Discos	13,000.00
	Unidades de Cartridges	2,000.00
	Impresoras de Sistemas	2,500.00
	Unidad de Control de Discos	5,000.00
	Terminales	15,000.00
9.	**Equipos de Microcomputación**	**5,200.00**
10.	**Equipo de Comunicaciones**	**7,400.00**
	Unidades de Control	3,500.00
	Multiplexores	400.00
	Controladores de Comunicaciones	1,500.00
	Modems	2,000.00
11.	**Equipo de Energía**	**5,000.00**
12.	**Instalaciones**	**15,000.00**
13.	**Gastos acciones de desastres**	**1,200.00 (*)**
14.	**Convenio**	**5,000.00 (*)**
15.	**Pólizas de Seguros**	**2,500.00 (*)**

(*) Gastos adicionales para enfrentar desastres.

CONCLUSIONES

1. El Servicio de Agua Potable y Alcantarillado de Lima - SEDAPAL, entidad de propiedad del Estado, pertenece al Sector Ministerio de la Presidencia. Su misión es brindar servicio de agua potable y alcantarillado en las provincias de Lima y Callao. Para el desempeño de sus funciones cuenta con una Oficina de Sistemas que coadyuva en el desarrollo de la gestión y toma de decisión Institucional, a través de los sistemas informáticos.

2. La preocupación organizacional de primer orden es salvaguardar la disponibilidad del hardware, del software y los datos del sistema de información. La pérdida de una parte, disminuye su valor total. Por tanto la seguridad es fundamental.

3. Las medidas de seguridad garantizan el éxito de la información, la confidencialidad, el secreto y el papel de los auditores. La garantía está dada por el conocimiento y compromiso de todos los niveles

directivos y el apoyo de toda la organización.

4. El incendio inesperado es precisamente el más difícil de combatir a tiempo. Su acción devastadora provoca gran destrucción en infraestructura, equipamientos y materiales. Las quemaduras mortales y muertes del personal son daños, casi siempre irreparables.

5. El hombre constituye el elemento que más daño causa a la empresa cuando actúa malintensionadamente. Entre estos tenemos los creadores de los virus informáticos, los espías y los saboteadores.

6. En el suelo peruano ocurren terremotos con frecuencia originados por el cinturón de fuego del Pacífico Sur y el desplazamiento de la placa de Nazca. Las espantosas pérdidas de vidas humanas y materiales, han sido debido principalmente a causas secundarias, tales como; derrumbes de edificios y viviendas, desprendimiento de nieve y roca, formación de aludes, aluviones y represamiento de ríos.

7. Los virus informáticos generados por el hombre con fines perniciosos; alteran y destruyen los informes de los programas software ya que su presencia es inesperada y persiste activo en los backup's por mucho

tiempo. La Empresa pierde dinero y horas hombre.

8. El centro de informática de SEDAPAL, cuenta con sofisticados equipos que se encuentran distribuidos a través de la red de teleproceso con toda la organización. El trabajo es ejecutado por ingenieros de sistemas y técnicos en computación.

9. La Oficina de Sistemas de SEDAPAL, cuenta con PLan de Contingencia que contribuye a dar seguridad relativa a los equipos, personal y el producto del trabajo. De igual manera la mayoría de instituciones encuestadas también tienen **Plan de Contingencia** diseñados por personal propio o terceros según afirman.

RECOMENDACIONES Y SUGERENCIAS

1. **SEDAPAL**, para potenciar sus servicios requiere de mayor presupuesto ya que la población de Lima y Callao crece aceleradamente cada año, por la migración interna y los nacimientos naturales.

2. Para que se cumplan las medidas de seguridad es conveniente que los directivos de todos los niveles, los especialistas y el personal en general garanticen el éxito de las medidas de seguridad.

3. El pueblo peruano debe estar preparado para afrontar desastres, para lo cual hay que formar conciencia cívica y participar activamente en los simulacros de prevención de desastres organizado, por el Instituto Nacional de Defensa Civil.

4. Es recomendable utilizar, originales de los programas a fin de evitar la contaminación con virus informático al comprar copias sin garantía. De igual manera sancionar a los creadores y vendedores de virus

informático en el Perú.

5. Es conveniente para la empresa que los ingenieros de sistemas y los técnicos en computación se capaciten periódicamente. Los ingenieros deben realizar estudios de Post Grado en su especialidad y en administración de empresas.

6. Es necesario que las instituciones que cuentan con centros de informática diseñen **Plan de Contingencia** para asegurar la continuidad del trabajo. El plan debe ser evaluado a fin de actualizarlo y perfeccionarlo según el avance de la ciencia de la informática, la realización de simulacros de desastres y la presencia de desastres propiamente dicho.

7. Para asegurar la información de respaldo es indispensable firmar Convenio de Ayuda Mutua con un entidad afín, para que en casos de desastres el centro de informática pueda continuar sus labores sin pérdida de tiempo. Dicha entidad debe contar con una sede antisísmica, en una ciudad con mínimo riesgo de terremotos.

ANEXO N° 1

INEI

APRUEBAN RECOMENDACIONES TECNICAS PARA LA PROTECCION FISICA DE LOS EQUIPOS Y MEDIOS DE PROCESAMIENTO DE LA INFORMACION EN LA ADMINISTRACIÓN PUBLICA

RESOLUCION JEFATURAL

N°090-95-INEI

Lima, 30 de marzo de 1995

Visto el Proyecto de Directiva "Recomendaciones Técnicas para la Protección Física de los Equipos y medios de Procesamiento de la Información en la Administración Pública", propuesta por la Subjefatura de Informática del Instituto Nacional de Estadística e Informática.

CONSIDERANDO

Que, de acuerdo a lo dispuesto por el Decreto Legislativo Nº604, el Instituto Nacional de Estadística e Informática - INEI, es el organismo central y rector de los Sistemas Nacionales de Estadística e Informática, responsable de normar, supervisar y evaluar los métodos, procedimientos y técnicas estadísticas e informáticas utilizados por los órganos del Sistema.

Que, es necesario, emitir las orientaciones técnicas que garanticen la protección física de los Equipos de Procesamiento Automático de Datos y los medios de almacenamiento que contienen información especializada de la Administración Pública.

Que, conforme a lo establecido por el inciso e) del Artículo 8º del Decreto Supremo Nº 018-91-PCM, "Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática", es función del INEI, normar, conducir y supervisar el uso de la tecnología y el desarrollo de la actividad informática oficial en el país.

Estando a lo propuesto por la Subjefatura de Informática, con la opinión técnica de la Oficina Técnica de Cómputo, de Presupuesto y Planificación y con la aceptación de las Oficinas Sectoriales de Informática integrantes del Comité de Coordinación Interinstitucional de Informática (CCOI-I) y la visación de la Oficina Técnica de Asesoría Jurídica.

En uso de las atribuciones conferidas por el Artículo 6° del Decreto Legislativo N°604.

SE RESUELVE

Artículo Unico.- Aprobar la Directiva N°008-95-INEI/SJI "Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública", la que consta de siete (7) numerales y un (1) Anexo, que forman parte de la presente Resolución.

Regístrese y comuníquese.

FELIX MURILLO ALFARO

Jefe

DIRECTIVA N°008-95-INEI/SJI

"RECOMENDACIONES TECNICAS PARA LA PROTECCION FISICA DE LOS EQUIPOS Y MEDIOS DE PROCESAMIENTO DE LA INFORMACION EN LA ADMINISTRACION PUBLICA"

I. FINALIDAD

Proponer normas y procedimientos para preservar la seguridad de los equipos computacionales y medios magnéticos u ópticos utilizados.

II. OBJETIVOS

2.1 Garantizar la seguridad de la información disponible en medios de almacenamiento, ante contingencias naturales, siniestros o sabotaje.

2.2 Evitar la destrucción de equipos, componentes e insumos informáticos.

2.3 Proteger los activos informáticos de la Administración Pública.

III. BASE LEGAL

3.1 Decreto Legislativo Nº 604, Ley de Organización y Funciones del INEI.

3.2 Decreto Supremo N°018-91-PCM, Reglamento de Organización y Funciones del INEI.

3.3 Resolución Jefatural N°480-92-INEI del 2-12-92, que aprueba la Directiva "Utilización Correcta de los Equipos Informáticos del Instituto Nacional de Estadística e Informática".

3.4 Resolución Jefatural N°340-94-INEI del 21-10-94, que aprueba la Directiva "Normas Técnicas para el Almacenamiento y Respaldo de la Información que se procesa en las Entidades del Estado".

IV. ALCANCE

Comprende a las áreas responsables de las instalaciones, mantenimiento y uso de equipos computacionales, así como a todo el personal que hace uso de dichos equipos en las entidades de la Administración Pública.

V. RECOMENDACIONES GENERALES

EN RELACION A LAS INSTALACIONES ELECTRICAS

5.1 Previo a la instalación de equipos informáticos, es necesario realizar cálculos de la carga eléctrica requerida en la instalación, de los tableros de distribución, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada.

5.2 Para equipos de cómputo es conveniente disponer de circuitos alternos y tableros de distribución eléctrica independientes a cualquier otra conexión.

5.3 Deberá disponerse de un pozo a tierra conectado al Sistema Eléctrico que alimenta los equipos de cómputo. Asimismo se etiquetará el cableado, las extensiones y los tableros de distribución eléctrica.

5.4 Asegurar un suministro de energía eléctrica de voltaje con la ayuda de sistemas de estabilización de voltaje, supresores de picos y unidades de potencia contra cortes de fluidos (UPS).

5.5 Mantener en lugar visible los procedimientos de maniobras de encendido de emergencia.

5.6 Evitar los cableados sueltos o dispersos, éstos deberán entubarse.

5.7 Es necesario establecer puntos centrales de corte de fluido eléctrico, a nivel edificio o piso.

EN RELACION A LAS INSTALACIONES DE AGUA Y DESAGUE

5.8 Se recomienda que los sistemas de agua y desague se encuentren a niveles inferiores al Centro de Computo. Se verificará periódicamente el estado de las griferías y cañerías a fin de evitar

posible inundaciones.

EN RELACION A LAS INSTALACIONES DE AIRE CONTAMINADO

5.9 Es recomendable contar con servicio de aire acondicionado, evitando que este próximo a material inflamable, asimismo contará con las instalaciones de operación visibles.

5.10 Verificar que el aire acondicionado esté alimentado con agua refrigerada de un suministro confiable. Caso contrario se considerará la posibilidad de un sistema de refrigeración de agua y bombas de circulación alternativas.

5.11 Asegurar que las tomas de aire de los equipos se encuentren ubicados en zonas no susceptibles de ser obstruidas.

EN RELACION A LA PROTECCION CONTRA INCENDIOS

5.12 Capacitar al personal en el uso y mantenimiento del equipo contra incendios.

5.13 Disponer de un plano que contenga todas las fuentes de suministro posibles de agua, con su capacidad estimada en cada caso.

5.14 Evitar que las paredes, pisos y techos contengan material inflamable, recomendándose instalar equipos de alarma detectores de humo.

5.15 Para combatir los incendios producidos por equipos eléctricos se deben utilizar extintores, hechos preferentemente de bióxido de carbono, productos químicos secos y líquido vaporizado. Estos estarán al alcance inmediato, preservando la vigencia química del extintor, e identificando su localización en el respectivo plano.

5.16 Es recomendable que exista suficiente iluminación en los alrededores del edificio, las ventanas o manparas se protegerán de manera que se evite el impacto de piedras o material incendiario.

VI. RECOMENDACIONES ESPECIFICAS

6.1 Es recomendable que el acceso a los centros de cómputo sea restringido al personal autorizado, contándose con un registro de entradas y salidas de visitantes.

6.2 Que los procedimientos de limpieza de los ambientes eviten:

- Levantar el polvo en áreas donde existen éstos.
- Golpear los módulos o muebles de computadoras.
- Utilizar material inadecuado para la limpieza de los equipos.

6.3 Los equipos de cómputo no deberán estar encendidos si no van a ser utilizados.

6.4 Las microcomputadoras y terminales tendrán un soporte logístico, que permita un apropiado mantenimiento, preventivo (filtros para pantalla y kits de limpieza). Es conveniente, asimismo que las microcomputadoras tengan instalado un software de protección de pantalla.

6.5 Se recomienda que el servicio de mantenimiento de los equipos de cómputo lo realice un proveedor que garantice un buen servicio.

6.6 No es conveniente el ingreso de alimento y bebidas en las salas que cuentan con equipos de cómputo.

6.7 Disponer de los medios físicos adecuados y suficientes, así como la capacitación y reglamentación para prevenir siniestros y/o minimizar sus efectos.

6.8 Contará con un **plan de contingencias**, así como con estrategias adecuadas para hacer frente a los desastres. Entre el área de cómputo y las demás áreas, se establecerán acuerdos acerca de las condiciones bajo las cuales el plan de contingencia ha de ser activado, considerándose la duración probable de la falta de servicio, y la pérdida (total o parcial) de la capacidad de

procesamiento en una o varias instalaciones, etc.

6.9 Seleccionar organizaciones afines a la Institución y establecer con una o más de ellas convenios de mutuo apoyo, para los casos de desastres que inhabiliten el procesamiento de información. El principal criterio será la confiabilidad, también habrá que analizar la capacidad del centro de cómputo de la institución para efectuar el servicio recíproco.

VII. RECOMENDACIONES COMPLEMENTARIAS

7.1 Se constituirá un Comité de Seguridad a nivel institucional, que velará por el cumplimiento de las normas y las políticas de seguridad de los equipos y medios de procesamiento de la información, el cual se recomienda que esté presidido por el Jefe de Computo u otro funcionario a nivel equivalente.

7.2 Los Funcionarios responsables de las entidades del Estado, designarán por escrito, al personal responsable de la protección física de los equipos y medios de procesamiento de la información.

ANEXO

GLOSARIO DE TERMINOS

ACTIVO INFORMATIVO

Bienes de una organización, que se encuentran relacionados directa o indirectamente con la actividad informática, entre ellos se cuentan:

La información mecanizada (no están incluidos los documentos fuentes que la generan).

Medios de comunicación que se utilizan para la transmisión de datos mecanizados (redes de computadoras, correo electrónico, etc.).

Medios magnéticos y ópticos de almacenamiento de la información (cintas, cartuchos, diskettes, discos, etc.).

Programas y aplicaciones de la Institución, ya sea desarrollados por ésta, adquiridos o alquilados a terceros.

Manuales, procedimientos y reglamentaciones afines al área de informática (Plan de Contingencia, procedimientos de seguridad, etc.).

KIT DE LIMPIEZA

Estuche de limpieza compuesto de disk-drive limpia cabezal y líquido de limpieza.

MEDIOS MAGNETICOS

Son dispositivos que permiten el almacenamiento de programas e información. En todos los dispositivos que componen este grupo, el soporte magnético tiene la misma estructura y composición. Están formados por una base de material y formas variables, sobre las que se ha depositado una delgada capa de material magnetizable.

El registro de información se realiza mediante equipos dotados de una cabeza de grabación, el cual dispone de una bobina que produce un campo electro-magnético creando por inducción zonas puntuales magne-tizable sobre el soporte utilizado.

Los elementos más representativos de los medios magnéticos son los discos y cintas magnéticas, siendo el primero un medio de acceso seudoaleatorio y el segundo, un medio de acceso secuencial.

MEDIOS OPTICOS

Son dispositivos de almacenamiento para grandes sistemas electrónicos de archivo (programas e informa-ción). Dentro de ellos se encuentran de CD-ROM que son discos con información pregrabada y que sólo pueden ser leídas; WORM que permiten grabar información que se desee pudiendo ser leída cuantas veces sea necesario; y el EOD que son discos ópticos borrables

o reescribibles y que son de reciente aparición.

PLAN DE CONTINGENCIA

Es el plan destinado a proteger la información contra los daños producidos por hechos naturales o por el hombre, además se debe contar con estrategias de costos eficientes para hacer frente a los desastres.

ANEXO Nº 2

LISTADO RESUMEN DE VIRUS COMUNES

NOMBRE COMUN	INSTRUCCIONES PARA SU SUPRESION
1 - AIDS (SIDA)	SCAN/D o borra archivos .COM contaminados.
2 - Alabama	Clean-up, F-prot o suprimir archivos contaminados.
3 - Alameda	MDisk, Clean-ip, F-prot o DOS SYS.
4 - Amstrad	SCAN/D, F-Prot o borrar archivos contaminados.
5 - Ashar	MDisk, Clean-up, F-Prot o la orden DOS SYS.
6 - Cascade (Cascada)	M-1704, Clean-up o F-Prot.
7 - Cascade-B (Cascada-B)	M-1704, M-1704C, Clean-up o F-Prot.
8 - Cerebro	MDisk, Clean-up, F-prot o la orden DOS SYS.
9 - Chaos (Caos)	MDisk,Clean-up o la orden DOS SYS.
10- Dark Avenger (Vengador tenebroso)	M-DAV, Clean-up, F-Prot.

NOMBRE COMUN	INSTRUCCIONES PARA SU SUPRESION
11- Datacrime	AntiCrim, SCAN/D o F-Prot.
12- Datacrime II	AntiCrim, SCAN/D o F-Prot.
13- Datacrime IIB	AntiCrim, SCAN/D o F-Prot.
14- Datacrime B	AntiCrim, SCAN/D o F-Prot.
15- dBase	SCAN/D o F-Prot.
16- Den Zuk	MDisk, F-Prot o la orden DOS SYS.
17- Devil's Dance (Baile del Diablo)	SCAN/D o borrar archivos contaminados.
18- Disk Killer (Asesino del disco)	MDisk, Clean-up, F-Prot o las órdenes DOS COPY y SYS.
19- Do-Nothing Virus (Virus No Hacer Nada)	SCAN/D o F-Prot.
20- EDV	MDisk/P.
21- Friday The 13th COM Virus (Virus.COM Viernes 13)	SCAN/D o F-Prot.
22- Fu Manchu	SCAN/D o F-Prot.
23- Ghost Boot (Arranque Fantasma)	Mdisk, Clean-up, F-Prot o la orden DOS SYS.
24- Ghost COM (COM Fantasma)	Mdisk o DOS SYS y borrar archivos .COM contaminados, o Clean-up, F-Prot.
25- Golden Gate	Mdisk, F-Prot o la orden DOS SYS.
26- Halloechen	SCAN/D o borrar archivos contaminados.

NOMBRE COMUN	INSTRUCCIONES PARA SU SUPRESION
27- Holland Girl (Chica Holandesa)	F-Prot o SCAN/D.
28- Icelandic (Islandés)	SCAN/D o F-Prot.
29- Icelandic-II (Islandés-II)	SCAN/D o F-Prot.
30- Icelandic-III (Islandés-III)	F-Prot, SCAN/D o borrar archivos contaminados.
31- Jerusalem	SCAN/D/A, Sábado, Clean-up, No Virus,F-Prot.
32- Jerusalem-B	F-Prot, Sábado, Clean-up, M-JRUSLM, NoVirus.
33- Joker (Bromista)	SCAN/D o borrar archivos contaminados.
34- Lehigh	MDisk y reemplace COMMAND.COM por una copia limpia, o F-Prot.
35- Lisbon (Lisboa)	SCAN/D o F-Prot.
36- MIX/1	SCAN/D,Cazador de Virus o F-Prot.
37- New Jerusalem (Nuevo Jerusalem)	Sábado, Clean-Up, F-Prot.
38- Ohio	MDisk, F-Prot o la orden DOS SYS.
39- Oropax	SCAN/D, F-Prot o borrar archivos contaminados.

NOMBRE COMUN	INSTRUCCIONES PARA SU SUPRESION
40- Payday (Día de Paga)	M-JRUSLM, NoVirus, Sábado, Clean-Up, F-Prot.
41- Pentagon (Pentágono)	MDisk, Clean-Up o la orden DOS SYS.
42- Perfume	F-Prot o borrar archivos contaminados.
43- Ping Pong	MDisk, Clean-Up, F-Prot o la orden DOS SYS.
44- Ping Pong-B	Clean-Up, MDisk o la orden DOS SYS.
45- Saratoga	SCAN/D, F-Prot o borrar archivos contaminados.
46- SF Virus (Virus SF)	Mdisk, Clean-up, F-Prot o la orden DOS SYS.
47- Stoned (Ajumado)	Clean-Up, MDisk, F-Prot.
48- Sunday (Domingo)	Clean-Up, SCAN/D o F-Prot.
49- Suriv 1.01	SCAN/D, F-Prot o NoVirus.
50- Suriv 2.01	SCAN/D, F-Prot o NoVirus.
51- Suriv 3.00	SCAN/D, F-Prot o NoVirus.
52- Swap (Intercambio)	Mdisk, Clean-up, F-Prot o la orden DOS SYS.
53- SysLock	SCAN/D o F-Prot.
54- Taiwan	SCAN/D o borrar archivos contaminados.

NOMBRE COMUN	INSTRUCCIONES PARA SU SUPRESION
55- Traceback (Rastreo)	M-3066, VirClean, F-Prot o borrar archivos contaminados.
56- Traceback II (Rastreo II)	SCAN/D, F-Prot o borrar archivos contaminados.
57- Typo Boot (Arranque Typo)	MDisk, F-Prot o la orden DOS SYS.
58- Typo COM (COM Typo)	SCAN/D, F-Prot o borrar archivos contaminados.
59- Vacsina	SCAN/D/A, F-Prot o borrar archivos contaminados.
60- Vcomm	F-Prot o borrar archivos contaminados.
61- Vienna (Viena)	M-Viena, Clean-Up, VirClean, F-Prot.
62- Vienna-B (Vienna-B)	M-Viena, Clean-Up, VirClean, F-Prot.
63- Virus-90	SCAN/D, F-Prot o borrar archivos contaminados.
64- Virus-101	SCAN/D o borrar archivos contaminados.
65- W-13	F-Prot o borrar archivos contaminados.
66- Yankee Doodle	VirClean, F-Prot o borrar archivos contaminados.

NOMBRE COMUN	INSTRUCCIONES PARA SU SUPRESION
67- Zero Bug (Error Cero)	SCAN/D, F-Prot o borrar archivos contaminados.
68- 405	SCAN/D, F-Prot o borrar archivos contaminados.
69- 512	Clean-up V58.
70- 1260	Clean-up V57+
71- 1559	SCAN/D.
72- 1704 Format (Formateo 1704)	M-1704, Clean-up, SCAN/D, F-Prot
73- 4096	SCAN/D, F-Prot o borrar archivos contaminados.

ANEXO N° 3

REFERENCIAS CRUZADAS
DE VIRUS COMUNES

Nombres del virus	Referencia al virus en el Listado Resumen
1 - AIDS (SIDA)	AIDS (SIDA)
2 - Alabama	Alabama
3 - Alameda	Alameda
4 - Amstrad	Amstrad
5 - April 1st (1 de abril)	Surv 1.01
6 - April 1st-B (1 de abril-B)	Suriv 2.01
7 - Ashar	Ashar
8 - Austrian (Austriaco)	Vienna (Viena)
9 - Black Avenger (Vengador Tenebroso)	Dark Avenger (Vengador Tenebroso)
10- Black Friday (Viernes Negro)	Jerusalem
11- Blackjack	Cascade-B (Cascada-B)
12- Boot (Arranque)	Ping Pong-B

Nombres del virus	Referencia al virus en el Listado Resumen
13- Bouncing Ball (Pelota salatarina)	Ping Pong
14- Bouncing Dot (Punto saltarín)	Ping Pong
15- Cascade (Cascada)	Cascade (cascada)
16- Cascade-B (Cascada-B)	Cascade-B (Cascada-B)
17- Chaos (Caos)	Chaos (Caos)
18- Columbus Day (Día de Colón)	Datacrime, Datacrime II, Datacrime IIB, Datacrime-B
19- COM virus (Virus COM)	Friday The 13th COM virus (Virus COM Viernes 13)
20- Computer Ogre (Ogro Informático)	Disk Killer (Asesino del Disco)
21- Dark Avenger (Vengador Tenebroso)	Dark Avenger(Vengador Tenebroso)
22- Datacrime	Datacrime
23- Datacrime II	Datacrime II
24- Datacrime IIB	Datacrime IIB
25- Datacrime-B	Datacrime-B
26- DBase	DBase
27- December 24th (24 de diciembre)	Icelandic-III (Islandés-III)
28- Den Zuk	Den Zuk

Nombres del virus	Referencia al virus en el Listado Resumen
29- Devil's Dance (Baile del Diablo)	Devil's Dance (Baile del Diablo)
30- Disk Crunching virus (Virus Crujidor Disco)	Icelandic,Saratoga (Islandés, Saratoga)
31- Disk Killer (Asesino del Disco)	Disk Killer (Asesino del Disco)
32- Disk Ogre (Ogro del Disco)	Disk Killer (Asesino del Disco)
33- Do-Nothing virus (Virus No Hacer Nada)	Do-Nothing virus (Virus no hacer nada
34- DOS-62	Vienna (Viena)
35- DOS-68	Vienna (Viena)
36- EDV	EDV
37- Fall (Otoño)	Cascade (Cascada)
38- Falling Letters (Letras caídas)	Cascade, Ping Pong-B (Cascada, Ping Pong-B)
39- Falling Letters Boot (Arranque de Letras caídas)	Swap Boot (Arranque de Intercambio
40- Friday The 13th (Viernes 13)	Jerusalem (Jerusalem)
41- Friday The 13th COM virus (Virus COM Viernes 13)	Friday The 13th COM virus (Virus COM Viernes 13)

Nombres del virus	Referencia al virus en el Listado Resumen
42- Fu Manchu	Fu Manchu
43- Fumble (Tanteo)	Typo COM (COM Typo)
44- Ghost Boot (Arranque Fantasma)	Ghost Boot (Arranque Fantasma)
45- Ghost COM (COM Fantasma)	Ghost COM (COM Fantasma)
46- Ghostballs (Pelotas fantasmas)	Ghost Boot, Ghost COM (Arranque Fantasma, COM Fantasma)
47- Golden Gate	Golden Gate
48- Hahaha	AIDS (SIDA)
49- Halloechen	Halloechen
50- Hawaïi	Stoned (Piedra)
51- Holland Girl (Chica Holandesa)	Holland Girl (Chica Holandesa)
52- Icelandic (Islandés)	Icelandic (Islandés)
53- Icelandic-II (Islandés-II)	Icelandic-II (Islandés-II)
54- Icelandic-III (Islandés-III)	Icelandic-III (Islandés-III)
55- Israeli	Jerusalem, Suriv 1.01,Suriv 2.01, Suriv 3.00
56- Israeli Boot (Arranque Israeli)	Swap (Intercambio)
57- Italian (Italiano)	Ping Pong

Nombres del virus	Referencia al virus en el Listado Resumen
58- Jerusalem	Jerusalem
59- Jerusalem-A	Jerusalem
60- Jerusalem-B	Jerusalem
61- Jerusalem-C	Jerusalem
62- Jerusalem-D	Jerusalem
63- Jerusalem-E	Jerusalem
64- Joker (Bromista)	Joker (Bromista)
65- Lehigh	Lehigh
66- Lisbon (Lisboa)	Lisbon (Lisboa)
67- Marihuana	Stoned (Piedra)
68- Mazatlan	Golden Gate
69- Merritt	Alameda
70- Mexican (Mejicano)	Devil's Dance (Baile del Diablo)
71- Miami	Friday The 13th (Viernes 13)
72- Mistake (Error)	Typo Boot (Arranque Typo)
73- MIX1	MIX1
74- MIX/1	MIX1
75- Munich	Friday The 13th COM virus (Virus COM Viernes 13)
76- Music virus (Virus Musical)	Oropax
77- Musician (Músico)	Oropax
78- New Jerusalem (Nuevo Jerusalem)	New Jerusalem (Nuevo Jerusalem)

Nombres del virus	Referencia al virus en el Listado Resumen
79- New Zealand (Nueva Zelanda)	Stoned (Piedra)
80- Ogre (Ogro)	Disk Killer (Asesino del Disco)
81- Ohio	Ohio
82- One In Eight (Uno de Ocho)	Vienna
83- One in Ten (Uno de Diez)	Icelandic, Icelandic-II (Islandés, Islandés-II)
84- One in Two (Uno de Cada Dos)	Saratoga
85- Oropax	Oropax
86- Paskistani	Brain (Cerebro)
87- Pakistani Brain (Cerebro Pakistani)	Brain (Cerebro)
88- Palette (Paleta)	Zero Bug (Error Cero)
89- Payday (Día de Paga)	Payday (Día de Paga)
90- Peking	Alameda
91- Pentagon (Pentágono)	Pentagon (Pentágono)
92- Perfume	Perfume
93- Ping Pong	Ping Pong
94- Ping Pong-B	Ping Pong-B
95- PLO	Jerusalem
96- Russian (Ruso)	Jerusalem
97- San Diego	Stoned (Piedra)

Nombres del virus	Referencia al virus en el Listado Resumen
98- Saratoga	Saratoga
99- Seoul	Alameda
100- SF virus (Virus SF)	SF virus (Virus SF)
101- Shoe_Virus	Ashar
102- Shoe_Virus-B	Ashar-B
103- Smithsonian	Stoned (Piedra)
104- South African (Sudafricano)	Friday The 13th COM virus (Virus COM Viernes 13)
105- Stoned (Piedra)	Stoned (Piedra)
106- Sunday (Domingo)	Sunday (Domingo)
107- Sylvia	Holland Girl (Chica Holandesa)
108- System virus (Virus del Sistema)	Icelandic-II (Islandés-II)
109- Suriv 1.01	Suriv 1.01
110- Suriv 2.01	Suriv 2.01
111- Suriv 3.00	Suriv 3.00
112- Suriv01	Suriv 1.01
113- Suriv02	Suriv 2.01
114- Suriv03	Suriv 3.00
115- Swap (Intercambio)	Swap (Intercambio)
116- SysLock	SysLock
117- Taiwan	Taiwan
118- Taunt	AIDS (SIDA)

Nombres del virus	Referencia al virus en el Listado Resumen
119- The Stupid virus (El virus Estúpido)	Do-Nothing (Hacer Nada)
120- Traceback (Rastreo)	Traceback (Rastreo)
121- Traceback II (Rastreo II)	Traceback II (Rastreo II)
122- Typo Boot (Arranque Typo)	Typo Boot (Arranque Typo)
123- Typo COM (COM Typo)	Typo COM (COM Typo)
124- UIUC Virus	Ashar
125- UIUC Virus-B	Ashar
126- Unesco	Vienna
127- Vacsina	Vacsina
128- Vcomm	Vcomm
129- Vera Cruz	Ping Pong
130- VGA2CGA	AIDS (SIDA)
131- Vienna	Vienna
132- Vienna-B	Vienna-B
133- Virus-90	Virus-90
134- Virus101	Virus101
135- W13	W13
136- Yale	Alameda
137- Yankee Doodle	Yankee Doodle
138- Zero Bug (Error Cero)	Zero Bug (Error Cero)

Nombres del virus	Referencia al virus en el Listado Resumen
139- 62-B	Vienna-B
140- 405	405
141- 500 virus (Virus 500)	Golden Gate
142- 512	512a
143- 512 virus (virus 512)	Friday The 13th COM virus (Virus COM Viernes 13)
144- 632	Saratoga
145- 642	Icelandic (Islandés)
146- 648	Vienna
147- 765	Perfume
148- 867	Typo COM
149- 1168	Datacrime-B
150- 1260	1260
151- 1280	Datacrime
152- 1514	Datacrime II
153- 1536	Zero Bug (Error Cero)
154- 1559	1559
155- 1701	Cascade (Cascada)
156- 1704	Cascade, Cascade-B (Cascada, Cascada-B)
157- 1704 Format (Formateo 1704)	1704 Format (Formateo 1704)
158- 1704-B	Cascade-B (Cascada-B)
159- 1808	Jerusalem
160- 1813	Jerusalem

Nombres del virus	Referencia al virus en el Listado Resumen
161- 1917	Datacrime IIB
162- 2080	Fu Manchu
163- 2086	Fu Manchu
164- 2930	Traceback II (Rastreo II)
165- 3066	Traceback (Rastreo)
166- 3551	SysLock
167- 3555	SysLock
168- 4096	4096
169- 4711	Perfume

ANEXO N° 4

DECALOGO DE LA PREVENCION DE DESASTRES

Es prioritario estar preparados para una respuesta adecuada durante la atención de un emergencia y la reducción de los efectos de un desastre. La respuesta por sí sola no es suficiente, ya que solamente concede resultados temporales a un costo muy alto.

Las técnicas de prevención son las medidas de mayor costo-beneficio en la reducción de los desastres, porque reducen la vulnerabilidad de ingeniería y construcción, las que hacen las construcciones y estructuras más resistentes al peligro; planificación del uso de la tierra, la que limita el uso de áreas peligrosas para el desarrollo y, programas con incentivos económicos.

A partir de esta definición se presenta a continuación diez principios de la prevención.

1. Los desastres son "Ventanas de oportunidad" para mejorar la prevención.

2. La reconstrucción, la nueva construcción y el desarrollo existente ofrece diferentes posibilidades para el mejoramiento de la prevención.

3. Una prevención efectiva requiere de una acción coordinada de muchas instituciones, sectores y niveles de gobierno.

4. Es más efectivo un conjunto de medidas de prevención relacionadas entre sí (Ejm: técnicas ingenieriles, códigos de zonificación).

5. La prevención basada en incentivos es más efectiva que la prevención basada en leyes y controles restrictivos.

6. La prevención debe estar enlazada con la preparación, socorro y medidas de reconstrucción.

7. Son aspectos prioritarios para la prevención: las facilidades críticas, sectores económicos y grupos altamente vulnerables (Ejm: los niños).

8. Las medidas de prevención deberán ser ajustadas periódicamente, tanto en la evaluación de peligros y vulnerabilidades, como en actualización de los

recursos disponibles.

9. Son necesarios los mecanismos institucionales que aseguren esfuerzos de prevención que se mantengan firmes frente a los desastres.

10. El compromiso político es muy importante en el inicio y durante el sostenimiento de la prevención.

(Extraído de: "UNESCO N°5-Environment and Development Briefs- Disater Reduction-1993". I. Davis, S.P.Gupta, "Disater Mitigation in Asia and the Pacific, Asia Development Bank, 1991)

GLOSARIO DE TERMINOS

1. ACCESO

- Manera en la cual un archivo o data son referidos por un computador.
- Autorización controlada a ingresar o hacer uso de áreas u objetos.

2. ADA

Para continuar - MF1-6

3. ADAPTADOR DE LAN

Tarjeta que es instalada en un computador personal y es empleada para unir este dispositivo a una Red de Area Local.

4. ALIAS

- Nombre alternativo usado para identificar un objeto o base de datos.
- Sobrenombre establecido por un administrador de network a un archivo, impresora o dispositivo serial.

5. AMBITO DISTRIBUIDO

Comprende la red distribuida en un área geográfica.

6. AMBITO DE PROCESO DISTRIBUIDO

Ambito donde se genera y/o produce la información a transmitir, recepcionar a puntos remotos.

7. APD

Auditores de Proceso de Datos.

8. AUDITORIA

Cualquier investigación sistemática o valuación de procedimientos u operaciones con el propósito de determinar su conformidad a un criterio determinado.

9. BACKUP

- Copia de información en un diskette o disco duro para mantenimiento de registros o con propósito de recuperación posterior.
- Un comando de OS/2 para guardar archivos.
- Copia de respaldo que realizan algunos paquetes cada vez que se realiza el grabado de un archivo (en los manejadores de datos por ejemplo).

10. BACK-UP

Copia de un archivo que se mantiene como referencia en caso de que el original se pierda o destruya. A veces la palabra "back-up" se utiliza para describir una facilidad provisional de procesamiento para utilizar

en caso de desastre.

11. BACKUP

- Seguridad, respaldo.
- Recursos adicionales o copias de datos en diferentes medios de almacenamiento como prevención contra emergencia.

12. BIT (Acrónimo de Binary Digit)

Bit unidad básica de información.

Es la unidad fundamental en la "Teoría de la Información".

13. BOMBA DE TIEMPO

Programa no autorizado que se disparará en una fecha determinada o como consecuencia de una acción futura.

14. BOMBA LOGICA

Programa no autorizado que se disparará en condición o conjunto de eventos determinados o como consecuencia de una acción futura.

15. BOOT

Iniciar el funcionamiento del computador.

16. CABALLO DE TROYA

Instrucciones secretas en un programa de computación que hacen que éste ejecute funciones no autorizadas pero permite que continue cumpliendo sus objetivos originales.

17. CLAVE MAESTRA

Password de acceso.

18. CLUSTER

Racimo, grupo, conglomerado, agrupamiento.

Cantidad de sectores del disco (por lo general de 2 a 10).

19. COMPUTADORA

Máquina de propósito general que procesa datos de acuerdo con el conjunto de instrucciones que están almacenados internamente, bien sea temporal o permanentemente.

20. COMPUTADORA

Máquina o dispositivo capaz de recibir información.

21. CONTROL DE ACCESO

Utilización de controles físicos como cerraduras o controles de software como contraseña/passwords para

prevenir el acceso no autorizado a una aplicación/sistema.

22. CONTROL DE SISTEMAS

Los mecanismos dentro del entorno del sistema que ayudan a asegurar la exactitud e integridad del sistema de información computarizado y sus salidas.

23. CONTINGENCIA

Un evento, como puede ser una emergencia, que es posible pero incierto que ocurra.

24. CPD

Centro de Proceso de Datos.

25. DATA

Datos y/o información. En forma electrónica, datos se refiere a campos de datos, registros, archivos y base de datos.

26. ENCRIPTADOS

Cifrado, criptografiado, criptograficación. Codificación de datos con propósito de seguridad, convirtiendo el código estándar de datos en un código propio.

27. EPICENTRO

Punto en la superficie terrestre que se encuentra verticalmente encima del foco o hipocentro.

28. FORTRAN (acrónimo de FORmula TRANslador)

Lenguaje traductor de fórmulas.

29. HACKER

Un aficionado a las computadoras que intenta lograr acceso no autorizado a un sistema de computación, generalmente vía telecomunicaciones.

30. HIPOCENTRO

Punto o lugar donde se origina el sismo.

31. INFORMACION

En informática es sinónimo de datos (Data).

32. INFORMÁTICA

Término acrónimo - debiene de INFORmática autoMATICA.

Es todo aquello que tiene relación con el procesamiento de datos. Ciencia de la Información.

33. Kb

Mil "K" con frecuencia se refiere al valor preciso de 1,024.

34. LAVA VOLCANICA

Material volcánico compuesto de rocas y minerales al estado de fusión con altas temperaturas. Acompaña a la lava volcánica vapor de agua y gases.

35. MAGMA

Roca y minerales al estado de fusión con altas temperaturas.

36. ONDAS SISMICAS

Vibraciones de la corteza terrestre que se propagan en forma de ondas a partir del foco o hipocentro.

37. PASSWORD

Cadena de caracteres única que un programa, operador de computadora o usuario debe dar para cumplir con los requerimientos de seguridad antes de ganar acceso a la data.

38. PC (Personal Computer)

Computador personal, máquinas que se ajustan al estándar de PC. Cualquier computador personal.

39. PD

Proceso de Datos.

40. PERSONAL SENIOR

Profesional especializado y con experiencia por cuya razón es indispensable en la empresa.

41. PLANIFICACION DE RECUPERACION DE DESASTRE

El propósito de la planificación de recuperación de desastre es tomar acciones de antemano para asegurar la continuidad de la información crítica del negocio en caso de desastre. La planificación de recuperación de desastre debe ser hecha para todas las funciones operativas y de soporte de una organización.

42 PISTA DE AUDITORIA

Registro de actividad que se utiliza para vigilar el uso de un proceso computarizado o manual.

43. PRIVACIDAD

El derecho de los individuos y de las organizaciones de controlar la recolección el uso de sus datos o de datos sobre ellos mismos. Un tema social y legal.

44. PROGRAMA DE INSTALACION

Al funcionar modifican parámetros de otros programas tienen un funcionamiento especial y permiten comprender los principios en los que están basados los virus informáticos.

45. PROTECCION

Mantenimiento de la integridad de la información en el almacenamiento, previniéndola de cambios sin autorización.

46. PROTECCION DE LA PRIVACIDAD

El establecimiento de controles administrativos, técnicos o físicos para preservar un deseado nivel de privacidad.

47. PUNTOS REMOTOS

Ubicación física distante del centro de procesamiento de datos.

48. PROCESO DISTRIBUIDO

Diseminación y uso de computadoras entre localidades geográficamente separadas, las computadoras se conectan a través de una red de comunicaciones.

49. REGISTROS

En general, localidades de almacenamiento capases de guardar información. En particular, registros índice que pueden ser utilizados para modificar las direcciones de las instrucciones o registros aritméticos que realizan cambios.

50. RESPALDO

Procedimientos disponibles para uso temporal o de urgencia en caso de falla del sistema.

51. REGISTROS VITALES

Registros del negocio sin los cuales una organización: no podría reconstruir su negocio luego de un desastre, perdería mucho dinero, no podría comprobar la participación de cada accionista.

52. SISTEMA OPERATIVO

El software que controla el funcionamiento de los programas. Un Sistema Operativo debe proveer servicios tales como: ubicación de recursos, calendario, control de ingreso y salida (I/O) y manejo de data.

53. TERREMOTO

Súbito movimiento terrestre, producido generalmente por fuerzas interiores del globo terrestre o erupciones volcánicas.

54. TERRORISTAS ELECTRONICOS INTENCIONALES

Creadores de virus electrónicos maliciosamente programados de poder destructivo con motivos particulares hacia una Cía., por motivos políticos como el Virus Viernes 13, o virus Jerusalem.

55. TSUNAMIS

Olas marinas de flujo y reflujo de gran velocidad producidas por terremotos o erupciones volcánicas y de acciones desbastadoras.

56. USUARIO

Cualquiera que utilice los servicios de procesamiento de datos o una computadora. A veces es un término peyorativo utilizado por la gente de procesamiento de datos para referirse a sus clientes.

57. VACUNA

En el ámbito de seguridad de sistemas, un software de protección que "vacuna" a la computadora contra los llamados programas virus.

58. VIRUS

Programa que se copia a sí mismo y se disemina a través de una base de datos o una red. Puede causar la destrucción de la base de datos o la sobrecarga de la red, y muchos incidentes no deseados en el computador.

59. VIRUS

Simples programas de computación elaborados por programadores.

60. WORM

Programa que disemina copias de sí mismo a computadoras conectadas a una red de comunicaciones. La primera utilización de éste término aludía a un programa que se copiaba a sí mismo benignamente en una red utilizando facilidades de otra forma no utilizadas en máquinas de red, para desempeñar computación distribuida. Algunos Worms son amenazas a la seguridad que utilizan a las redes para esparcirse en contra de los deseos de los propietarios de los sistemas y los inhabilitan sobrecargándolos.

BIBLIOGRAFIA

1. **DALAL, Jagdish R.:** Gestión de Proceso de Datos, Ed. Arcadia S.A. España, 1984.

2. **FERREYRA C. Gonzálo:** Virus en las Computadoras, Macrobi, Editores, S.A. Mexico, 1991.

3. **FREEDMAN, A :** Diccionario de Computación, Universidad Austral de Chile.

4. **HANNAN, James :** Gestión de Proceso de Datos, Ed. Arcadia S.A. España 1984.

5. **HANNAN, James :** Gestión de Proceso Distribuído, Ed. Arcadia S.A. España 1984.

6. **IRIARTE W., NOMBERA R., RODRIGUEZ M.:** Virus Informático, Experiencias y Soluciones, Ed. Editec del Perú S.R. Ltda 1990.

7. **LEVIN, Richard :** Virus Informático, Mc GRAW - HILL/ Interamericana de España

S.A. 1991.

8. **LUCAS, Jr. Henry** : Conceptos de los Sistemas de Información para la Administración, Mc GRAW - HILL - Mexico S.A. 1983.

9. **MARTINEZ, José A.** : The Hacker, Antivirus V3.1 1992 - 1995.

10. **SEDAPAL** : Manual de Organización y Funciones, 1994.

11. **SEDAPAL** : Manual de Organización y Funciones, Oficina de Sistemas, 1994.

12. **SEDAPAL** : Por los caminos del Agua, 1992.

13. **SILGADO FERRO, Enrique:** Historia de los sismos más notables ocurridos en el Perú (1513-1974), Instituto de Geología y Minería, Boletín Nº3, Lima-Perú 1978.

14. **TAVERA H., Hernando:** La Tierra, Tectónica y Sismicidad, Instituto Geofísico del Perú, Observatorio Sismológico de Camacho, Nº002-93, LIMA-PERU, 1993.

15. **CONSTITUCION POLITICA DEL PERU:** Editora Perú S.A. 1993.

16. **I.B.M.** : Seguridad en Sistemas de Información, Junio 1995.

17. **I.B.M.** : Plan de Contingencia y Recuperación en Caso de Desastre, Junio 1995.

18. **PC 2000 - POPULAR COMPUTER:** Una cinta backup salvó a HOGAR, 1990.

19. **EL PERUANO** : Decreto Ley Nº19338, 1972, Gobierno Revolucionario crea el Sistema de Defensa Civil.

20. **EL PERUANO** : Decreto Legislativo Nº442, 1987 modifica Decreto Ley Nº19338.

21. EL PERUANO : Decreto Supremo N°067-DE-INDECI Reglamento de Organización y Funciones del Instituto Nacional de Defensa Civil, 1990.

22. EL PERUANO : Resolución Jefatural N°090-95-INEI, Aprueban recomendaciones técnicas para la protección física de los equipos y medios de procesamiento de la Información en la Administración Pública, marzo 1995.

23. EL PERUANO : 11 de Octubre, Día Internacional para la Reducción de los Desastres Naturales DIRDN-1990-2000, Instituto Nacional de Defensa Civil, 1995.

24. La República : Díaz Miguel, En créditos de bancos Industrial, Minero y Agrario, Estado pierde dos mil millones de dólares, 10 Octubre 1995.