



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

RECUPERACION DE OPERACIONES
DE NEGOCIO POR CONTINGENCIAS

T E S I S
Que para obtener el Titulo de:
INGENIERO EN COMPUTACION
P r e s e n t a:

TESIS CON
FALLA DE ORIGEN

GABRIELA RAMIREZ HERNANDEZ



DIRECTOR DE TESIS:
Ing. Francisco J. Rodríguez Ramírez

México, D.F.

1996

TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



Agradezco todo el apoyo brindado para la realización del presente trabajo al Ing. Luis M. Avelar Alférez, quien ha sido un factor fundamental en mi desarrollo profesional a lo largo del tiempo que hemos trabajado juntos.

También agradezco a mis Padres y abuelo materno el haberme alentado permanentemente durante mi formación académica

Índice.

Prólogo

Capítulo 1.

- 1.1. Antecedentes.
- 1.2. Análisis de la Infraestructura de Cómputo y Telecomunicaciones de la Empresa.

Capítulo 2.

- 2.1. Análisis de Riesgos de las Instalaciones de Cómputo.
- 2.2. Análisis de Impacto Financiero al Negocio.

Capítulo 3.

- 3.1. Análisis de alternativas de Recuperación del Negocio.
- 3.2. Desarrollo de la Estrategia de Respaldo.
- 3.3. Desarrollo del Plan de Contingencia.

Capítulo 4.

- 4.1. Prueba del Plan de Contingencia.
- 4.2. Retroalimentación de Resultados para la Afinación del Plan de Contingencia.
- 4.3. Mantenimiento al Plan de Contingencia.

Conclusiones.

Glosario.

Anexo.

Bibliografía.

Prólogo.

En la actualidad las empresas del ramo financiero soportan los servicios a clientes, el manejo y distribución de información, en grandes y complejas instalaciones de cómputo y comunicaciones, siendo éstas el punto de concurrencia de la totalidad de las operaciones e información de la base de clientes de dichas empresas.

Conscientes de la importancia que representa para las instituciones financieras la permanente disponibilidad de los recursos de cómputo y telecomunicaciones, durante la prestación de los servicios, el procesamiento de Información y distribución de la misma hacia los puntos de venta (sucursales) y unidades administrativas (áreas operativas sin atención al cliente), surge la necesidad de proteger la función del negocio, a través del desarrollo e implementación de **Planes de Recuperación de operaciones del Negocio por Contingencia.**

En la presente tesis se abordarán los aspectos fundamentales siguientes:

- Determinación de los escenarios de riesgos para los centros informáticos.
- Identificación del Costo/Beneficio para el desarrollo de la Estrategia de respaldo.
- La logística necesaria para establecer el Plan de Contingencia, que permita la recuperación del negocio en caso de desastre.

A lo largo del presente trabajo se probará que el contar con una metodología de **Recuperación de Operaciones del Negocio en caso de Contingencias**, es de gran importancia para las empresas financieras por los factores primordiales citados a continuación:

- Minimizar el impacto financiero a las empresas.
- Evitar la pérdida de posicionamiento en el mercado.
- Mantener la imagen de la institución ante el público.

También es conveniente considerar que en el mediano plazo, se vean obligadas las empresas del ramo financiero y bursátil, por disposiciones legales, a contar con un Plan de Recuperación del Negocio, como se encuentra establecido en los Estados Unidos de América.

Capítulo I.

A lo largo del presente capítulo se dará a conocer una panorámica de las diferentes situaciones de contingencia que pueden afectar a un centro de cómputo, inhabilitándolo para proporcionar servicios; adicionalmente se analizará la infraestructura de cómputo y comunicaciones de la empresa con la finalidad de identificar las fortalezas y debilidades de la misma.

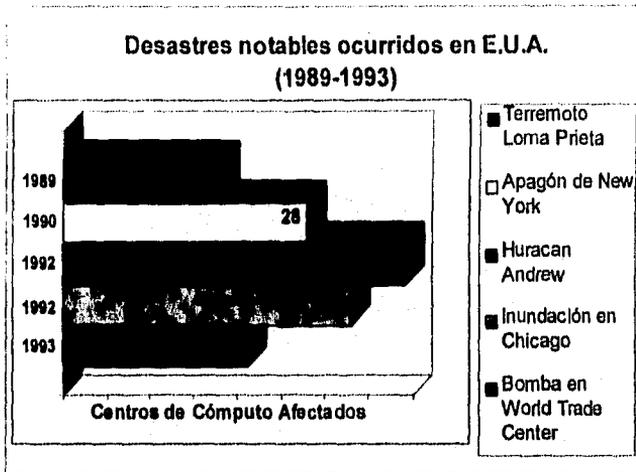
1.1 Antecedentes.

Al inicio de la década de los años ochenta en Estados Unidos de América, surgió en las empresas la inquietud de contar con la metodología e infraestructura de cómputo necesarias para respaldar las operaciones del negocio, sin embargo el sector más interesado fue el ramo Financiero y Bursátil, ya que han sufrido las consecuencias de diferentes tipos de desastres en sus instalaciones de cómputo, los cuales se pueden agrupar en dos grandes rubros; naturales y técnicos.

Entre las contingencias naturales se tiene:

- Sismos o terremotos de intensidad considerable que han causado destrozos y en algunos casos la destrucción de instalaciones de cómputo y oficinas.
- Inundaciones que afectan sus instalaciones físicas donde se encuentran ubicados sus centros de cómputo y/o sus comunicaciones o bien la imposibilidad de acceder dichas áreas operativas.

- La devastación causada por los huracanes que afectan ciertas zonas geográficas de la Unión Americana, entre otros factores de riesgo menos relevantes.
- Los atentados terroristas, aunque no son desastres naturales son importantes de considerar, como factores de riesgo.

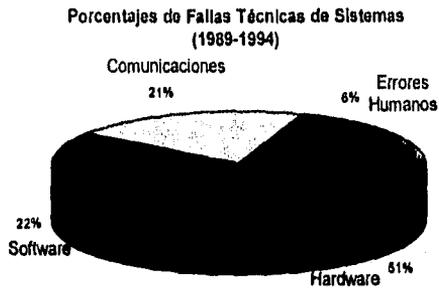


* En México no se cuenta con estadísticas confiables sobre centros de cómputo afectados por desastres naturales.

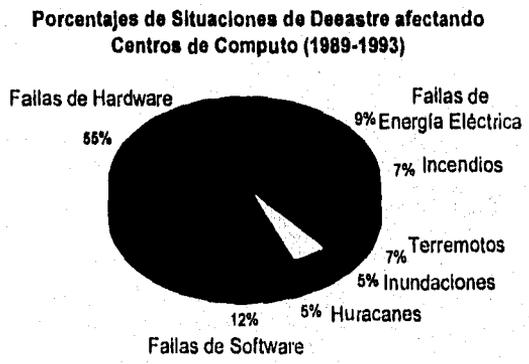
En cuanto a los problemas de origen técnico, que inutilicen con los sistemas de cómputo por más de 48 horas, se consideran los siguientes tipos de fallas:

- **Software.** Dependiendo del tipo de plataforma utilizada y de la redundancia de equipos que se tengan instalados, una falla de software puede extenderse ese tiempo.
- **Hardware.** Son los problemas más frecuentes, y en ocasiones los más difíciles de controlar, ya que se presentan regularmente en la CPU o en controladores de dispositivos periféricos (discos, unidades de cinta y/o cartucho).

- **Comunicaciones.** Se presentan en un porcentaje menor, debido a la redundancia de las comunicaciones, pero se pueden presentar en: FEPs, Ruteadores, modems, multiplexores analógicos y digitales, etc.).
- **Errores Humanos** en la operación de los equipos y sistemas. Se llegan a presentar con poca frecuencia.



Es importante señalar que comparativamente, los problemas técnicos son más frecuentes que los de origen natural, ya que estos últimos son aleatorios y los primeros son inherentes al desgaste por el uso continuo de los equipos y la operación permanente de los sistemas.



De acuerdo al entorno descrito anteriormente, la mayoría de las empresas buscó resolver esta problemática a través de:

- a) Establecimiento de convenios de Respaldo Parcial de sus operaciones con empresas de servicio del mismo tipo y con infraestructura de cómputo igual, en cuanto a Hardware y Software.
- b) Construcción de Centros de Cómputo Espejo.

Ambas alternativas conllevan grandes desventajas al ser aplicadas en una situación real.

Alternativa "A":

- Cambios en el Software Operativo que hacen incompatible el proceso de las aplicaciones en el respaldo mutuo, imposibilitando el mismo.
- Debido a las necesidades propias de cada empresa se convierte inoportuna la ventana de tiempo para realizar el respaldo.
- Capacidad de respaldo insuficiente.
- Podría presentarse la situación que ambas instituciones se hayan visto afectadas por el mismo desastre, al estar ubicadas en la misma localidad.

Alternativa "B":

- La inversión requerida para la creación de un Centro Espejo es excesivamente alta.
- El costo de mantenimiento de los equipos centrales de comunicaciones e instalaciones físicas es bastante considerable.
- La inversión que implica esta alternativa, no es rentable ante los ojos de los accionistas, esto es, dinero improductivo.

1.2 Análisis de la Infraestructura de Cómputo y Telecomunicaciones de la Empresa.

De acuerdo a la investigación realizada, en la empresa financiera en cuestión, su infraestructura de cómputo y telecomunicaciones se encuentra conformada de la siguiente manera:

Hardware

- Mainframe CPUs IBM
- 200 Giga Bytes en DASD
- Unidades de cartucho y de cintas magnéticas

Comunicaciones

- Controladores de comunicación
- Red Satelital de nodos remotos VSATs X-25 (TDM/TDMA)
- Canales de larga distancia Telmex
- Red Digital Integrada (RDI)
- Arquitecturas SNA y Ethernet
- Protocolos utilizados X-25, HDLC, TCP/IP
- Redes LAN en Sucursales
- Radio enlaces en sucursales locales D.F.
- Ruteadores
- Radio Módems.

Software

- Sistema Operativo MVS/ESA.
- Sistemas aplicativos desarrollados en: Cobol, Cobol II, Cobol comandos de Cics, IDEAL.
- Administrador de Base de Datos relacional.
- Propio de los componentes de comunicaciones.
- Redes locales.
- OS/2, CT-Ambiente gráfico tipo Windows.

Características de proceso.

Las operaciones del negocio en las sucursales a nivel nacional y en las oficinas internas están soportadas en dos mainframes IBM, de la siguiente manera:

- **Proceso en Línea Memopost.**

CPU-1 soporta los procesos en línea en base de datos en el horario de 8:00 a 21:00.

CPU-2 dedicada al proceso en línea en el intervalo de tiempo de las 6:00 a las 23:00 horas, el servicio de la red de cajeros automáticos de las 6:00 hasta las 5:00 del siguiente día.

- **Proceso Batch.**

CPU-1. A partir de las 13:00 horas se encarga de los proceso batch de la zona metropolitana y de 18 RJE's del interior.

CPU-2. Después de las 23:00 horas soporta el proceso batch de 20 RJE's del interior.

- **Proceso centralizado en la Ciudad de México.**

Es decir, la información a Nivel Nacional se actualiza y respalda en los procesos batch, en el centro de cómputo de la Ciudad de México.

- **Distribución de Información.**

Ruteada hacia los RJE's a las principales ciudades de la República, mismos que funcionan como centros de captura de datos y unidades de impresión de información para su posterior entrega a las oficinas y sucursales en dicha localidad.

- **Respaldo local de los servicios de información.**

Debido a que se cuenta con dos CPUs de las mismas características, en caso de presentarse algún problema con cualquiera de los dos equipos, se puede soportar la carga de procesamiento en la CPU que esté activa, siempre y cuando la falla del equipo en cuestión se resuelva en un lapso de tiempo máximo de 12 horas, para no generar saturación en la CPU que este procesando toda la información.

- **Respaldo de Información.**

Se procesan y administran automáticamente, mediante un software especializado en el control de:

⇒ Versiones de archivos de aplicaciones

⇒ Bibliotecas de productos

⇒ Programas

⇒ JCLs y paramétricas

⇒ Sistema Operativo

⇒ Utilerías

Que son alojados y referenciados hacia *volúmenes específicos* en cartucho magnético, los cuales son controlados por dicho software en cuanto a su vigencia, resguardo en cintoteca local, traslado a bóveda y su liberación para su reutilización.

Características de la Red de Comunicaciones.

- Enlaces RDI (DS0) hacia las sucursales metropolitanas.
- El uso de Red Conmutada de Telmex y Enlaces Privados para Voz, para respaldar las contingencias en sucursales.
- Redundancia de los elementos claves de la red para asegurar la continuidad de la operación, tales como: Ruteadores, enlaces de radio y líneas privadas.
- Infraestructura homogénea en las regiones para sucursales locales y remotas (módems, líneas privadas, ruteadores).
- Red Satelital en siete nodos principales.
- Redes SNA.
- Redes Ethernet.

De acuerdo con la plataforma de procesamiento central y la arquitectura de comunicaciones citada anteriormente podemos determinar las fortalezas y debilidades tecnológicas y de procesamiento de la Información.

Fortalezas.

- Contar con proceso centralizado para la actualización de los archivos maestros a Nivel Nacional proporciona seguridad e integridad de la información.

- Integración de nuevas versiones de software operativo y aplicativo se realiza en un sólo esfuerzo.
- No es necesaria la transferencia de información entre varios centros de cómputo para mantener la información actualizada a Nivel Nacional.
- Su red digital integrada de Telmex, líneas privadas de voz y su red satelital que cubren las principales plazas y centros remotos de la institución, así como la redundancia de Ruteadores, Módems, y enlaces de radio, garantiza la continuidad de los servicios en las Sucursales y Oficinas a Nivel Nacional.

Debilidades.

- El riesgo de perder la capacidad de procesamiento, al soportar la operación del negocio en un solo centro de cómputo, es muy alto en caso de un siniestro que inhabilite el edificio y/o los recursos informáticos que alojan estas instalaciones.

Diagnóstico.

Para proporcionar continuidad en el servicio a los clientes y en la operación del negocio en caso de una contingencia mayor, se requiere contar con capacidad de procesamiento alternativo, en cualesquiera de las siguientes figuras:

- Diseño y construcción de centro de cómputo alternativo con una capacidad de procesamiento de por lo menos el 50% en procesador central y almacenamiento en disco.
- Contratación de capacidad de procesamiento mínimo al 50% con un proveedor externo y especializado en este tipo de servicios.

Bajo la premisa de respaldar los sistemas que soporten las principales funciones del negocio, que sean determinadas mediante el análisis correspondiente.

Capítulo 2.

Durante el presente capítulo se realizará el Análisis de riesgos de las instalaciones de cómputo, para determinar los factores que potencialmente podrían afectar a la instalación y el análisis de impacto financiero al negocio, para identificar el daño financiero que sufriría la empresa en caso de desastre.

2.1 Análisis de Riesgos de las Instalaciones de Cómputo.

Para desarrollar el análisis de riesgos potenciales que permitan determinar cuales de éstos son los de más alta peligrosidad para las instalaciones de cómputo, se deben de considerar los siguientes aspectos:

1. Ubicación de las Instalaciones:

- Geográficamente que tipo de desastres naturales se podrían presentar: terremotos, huracanes, inundaciones, ciclones, etc..
- Que tipo de industrias se encuentran ubicadas a 300 m²., identificar cuales de estas pueden resultar peligrosas, por ejemplo; Industrias químicas, gasolineras, laboratorios farmacéuticos, etc..
- Determinar si la calle sobre la que se encuentra la empresa es conflictiva, en cuanto transito vehicular, ubicación de sindicatos y/u oficinas gubernamentales, etc..

2. Medidas de seguridad de acceso y en los alrededores

- La empresa debe contar con políticas y procedimientos para el acceso a las instalaciones tanto del personal como de externos, lo anterior para evitar que introduzcan bombas o armas de fuego.
- Además dependiendo de la tensión política y económica que se viva en el país debe asegurarse de que no se estacionen autos sospechosos o bultos extraños alrededor del lugar, para evitar posibles atentados terroristas.

3. Sistemas de protección y limpieza dentro del centro de cómputo.

- Contar con un sistema de monitoreo y detección de incendios automatizado que sea 99.9% confiable.
- Instalación del equipo necesario para extinguir incendios haciendo uso de los sistemas de emisión de gas, autorizados para su uso por las autoridades sanitarias, ya que los de agua pueden generar daños en los equipos de cómputo.
- Considerar que es necesario contar con plantas de luz propia, que sean totalmente seguras, que puedan soportar la carga de todos los equipos por largo tiempo y con una configuración redundante.
- Instalación de UPSs para soportar el tiempo de transferencias hacia las plantas de energía eléctrica, en caso de interrupción del suministro eléctrico de la compañía de luz.

2.2. Análisis de Impacto Financiero al Negocio.

La finalidad del Análisis de Impacto Financiero al Negocio es analizar y evaluar las funciones del negocio críticas e identificar los sistemas de información que las soportan. Para ello es necesario dividir la tarea en las etapas siguientes:

- Estudio del Análisis de la Infraestructura de Cómputo y Telecomunicaciones, realizado anteriormente.
- Levantamiento de Información.
 - Elaboración de cuestionarios.
 - Construcción de agendas de entrevistas.
 - Desarrollo de entrevistas.
- Análisis de la Información obtenida.
- Resultados y Conclusiones del Análisis de Impacto Financiero al Negocio.

Elaboración de cuestionarios.

Estos cuestionarios deberán estar orientados a la totalidad de la funciones del negocio, con el objeto de obtener la siguiente información:

1. Descripción de la Función del Negocio.
2. Datos generales como son: ubicación, personal en el área, si cuenta con procedimientos manuales documentados.
3. Sistemas de información que dan soporte a la función del negocio.

4. Periodos del día con mayor actividad.
5. Equipo utilizado para su operación normal.
6. Tipo de impacto que se puede tener en caso de no contar con sistema de cómputo y cual sería el más significativo para el área.
7. El lapso de tiempo límite a partir del cual se generan pérdidas intangibles.
8. El monto estimado de la pérdida financiera en el periodo de tiempo establecido.
9. El incremento adicional de la pérdida, si continuara la falla de sistema por más tiempo.

Cuestionario Sobre Análisis del Impacto al Negocio

Clave: _____

Nombre del Sistema: _____

- Manifiesto (nombre de aplicaciones)
- LAN (PC Software)
- Teléfono
- Otro Equipo

Nombre del Departamento _____ Fecha: _____

Localidad: _____

Nombre de la Persona que responde _____

Título: _____

Ubicación: _____

Número de empleados en el Departamento: _____

Información Adicional: _____

Descripción de la Función de Negocios: _____

1 - Indique su opinión sobre el impacto en el Grupo Financiero Inverlat, como resultado de no contar con este Proceso de Negocios. Marque las siguientes opciones en orden de importancia:

<input checked="" type="checkbox"/> Pérdida de Ingresos	<input checked="" type="checkbox"/> Pérdida del Valor de la acción
<input checked="" type="checkbox"/> Pérdida de Utilidades	<input checked="" type="checkbox"/> Pérdida de Clientela
<input checked="" type="checkbox"/> Pérdida de Mercado	<input checked="" type="checkbox"/> Pérdida de la Confianza del C.
<input checked="" type="checkbox"/> Pérdida de Imagen	<input checked="" type="checkbox"/> Pérdida de Productividad
<input checked="" type="checkbox"/> Violaciones Legales/Regulatorias	
<input checked="" type="checkbox"/> Otros (favor de especificar)	

Comentarios: _____

Grupo Financiero

Construcción de Agenda de Entrevistas.

Se debe elaborar una agenda de entrevistas perfectamente bien calendarizada, así como realizar la cita con todos y cada uno de los responsables de las funciones del negocio. En estas reuniones deberán participar tanto el responsable del área, como las personas claves en la operación del departamento.

Es recomendable se solicite y aclare la importancia de la cooperación de los integrantes en la reunión para que ésta sea exitosa. Es deseable que ambas partes cumplan con el horario establecido con anterioridad.

Desarrollo de Entrevistas.

Un aspecto de gran importancia a considerar, es la inducción a los participantes del objetivo del Análisis de Impacto al Negocio, con la finalidad de que la información proporcionada sea lo más veraz y confiable posible.

Las entrevistas tienen que desarrollarse en un ambiente ameno y asertivo por parte del entrevistador, para obtener la información vital de las funciones del negocio, debido a que estos normalmente se muestran renuentes al hablar de cantidades de dinero, e implicaciones operativas al no contar con los servicios de cómputo.

Es necesario que todos los aspectos tratados sean sumamente claros para el encuestador, y una vez terminada la reunión archive el cuestionario junto con sus comentarios personales acerca del área, así como los documentos que sustentan aspectos tales como la pérdida financiera.

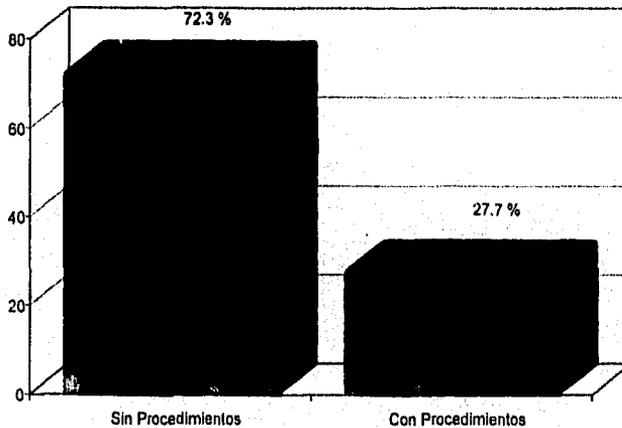
Análisis de la Información Obtenida

Esta etapa es relevante, porque de ella depende lo acertado de los resultados y las posibles decisiones que se tomen a partir de ellos, ya que se identificarán los conceptos siguientes:

- Funciones de negocio críticas y no críticas.
- Pérdidas financieras por interrupción de servicios.
- Períodos críticos de operación.
- Intervalo de tiempo de recuperación.
- Recursos requeridos para recuperar la operación.
- Procedimientos manuales documentados.

Resultados y Conclusiones del Análisis de Impacto al Negocio.

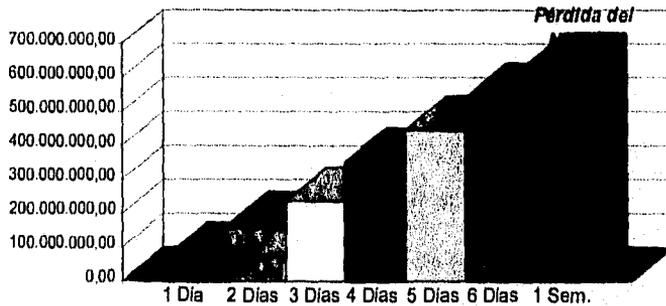
- ♦ Funciones de negocio críticas que cuentan con procedimientos manuales de operación que pudieran usarse en caso de contingencias.



♦ Pérdidas Financieras Acumuladas.

Con base en los datos proporcionados por los responsables de las funciones del negocio críticas, se determinaron las pérdidas acumuladas en una semana, de la siguiente manera.

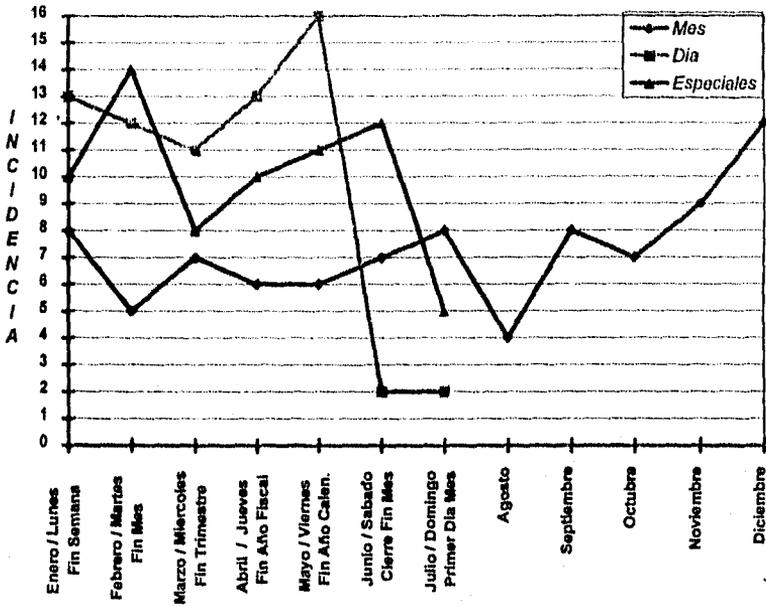
Pérdida	Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7
Desde el primer día	72,821,550.00	145,243,100.00	217,864,650.00	290,486,200.00	363,107,750.00	435,729,300.00	508,350,850.00
Apartir del 2 día		20,289,933.00	40,579,666.00	60,839,499.00	81,159,332.00	101,449,165.00	121,738,998.00
Apartir del 4 día				360,000.00	720,000.00	1,080,000.00	1,440,000.00
En una Semana					19,600.00	39,200.00	58,800.00
Total	72,821,650.00	166,532,933.00	238,164,483.00	351,716,699.00	445,006,682.00	538,297,665.00	631,688,640.00



Suponiendo que la empresa *no contara* con un plan de contingencias, que le posibilitara la recuperación de las operaciones de cómputo y por consiguiente de las funciones del negocio críticas, el monto de la pérdida financiera acumulada por una semana, podría dejar a la empresa en cuestión, fuera del negocio financiero.

◆ Periodos críticos de operación de las funciones críticas del negocio.

Basándose en la información obtenida, se debe establecer la incidencia en los periodos críticos para las funciones críticas del negocio.



Se observa que hay periodos en los cuales la carga de trabajo es mayor, lo que podría generar mayor conflicto si no se contase con el servicio de cómputo.

- ◆ Tiempo requerido de recuperación.

Dependiendo de cada una de las funciones críticas se debe establecer el tiempo requerido de recuperación, dada la importancia de ésta y la pérdida financiera que se generaría de no contar con el servicio.

OPERACION MERCADO DE DINERO	ADMON. DE VALORES	ADMON. DE CAMBIOS E INVERSIONES	FINANCIAMIENTOS ESPECIALES
INV. INSTITUCIONALES	OPERACION CAMBIOS	CREDITOS COMERCIALES	
RED SUCURSALES BANCA METRO / INT.			
OPERACIONES INVERSIONES			
OPERACION CHEQUES			
TARJETA BANCARIA			
PROMOCIÓN M.D.			
7 FUNCIONES DEL NEGOCIO EN 1 DIA	2 FUNCIONES DEL NEGOCIO EN 2 DIAS	2 FUNCIONES DEL NEGOCIO EN 4 DIAS	1 FUNCION DEL NEGOCIO EN 1 SEM.

Como se muestra en la gráfica anterior para la mayoría de las funciones del negocio críticas de la empresa financiera, es de vital importancia que se recupere la operación en un lapso de 24 horas, lo cual indica que el respaldo de operaciones debe estar funcionando en ese lapso de tiempo.

- ◆ Recursos mínimos necesarios para dar continuidad a las operaciones.

Cada función del negocio debe contar con lo mínimo necesario para poder proporcionar el servicio a sus clientes. A continuación se detallan estos recursos por cada área.

Función del Negocio	Procesos Manuales Document.	Puntos críticos	Área usuaria requerida	Escritorios	Sillas	Pcs Conectadas al Sistema	Terminales Conectadas al Sistema	PCs Stand Alone	Impresoras	Telefonos	FAX	Monto de Trasacción Totales	% de Priorid.
Red Sucursales Banco Metro / Interior	SI	1 Día	*			70			35			4'487,899	
Operación Cheques	SI	1 Día	240 m ²	20	20		20			20	1	1'779,085	
Promoción MD	SI	1 Día	112 m ²	7	18		5	1		30	1		
Gar. Admón de Cambios e Inversiones	SI	4 Días	40 m ²	4	4		1	1	1	4	1		
Financiamientos Especiales	SI	1 Sem.	24 m ²	4	4			1	1	2	1		
Operación Mercado de Dinero	No	1 Día	100 m ²	6	12	12			3	20	1		
Inv. Institucionales	No	1 Día	60 m ²	4	8	2	8	1	1	8			
Dir. Operaciones e Inversiones	No	1 Día	140 m ²	50	50		7	6	3	14	1	144,128	
Tarjeta Bancaria	No	1 Día	840 m ²	75	300				3	200	18	259,243	
Admón. de Valores	No	2 Días	168 m ²	25	60		58	8	8	25	10		
Operación Cartera	No	2 Días	100 m ²	14	14		3	3	1	8	1		
Créditos Comerciales	No	4 Días	34 m ²	6	8				3	10	1		

* El personal de la(s) sucursal(es) afectada(s) se reubicará hacia la sucursal más cercana

◆ Procedimientos manuales de operación documentados.

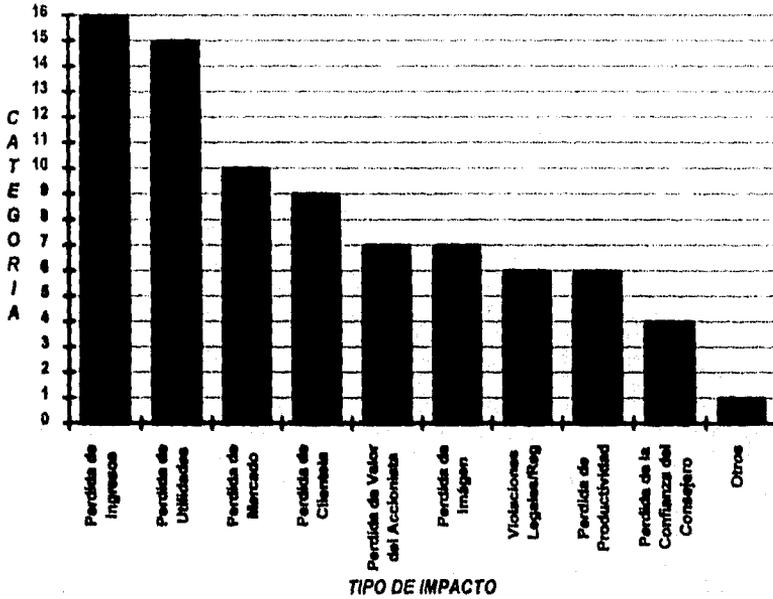
Considerando las funciones del negocio críticas, se identifica cuales de ellas cuentan con procedimientos manuales de operación documentados, lo cual les permitirá proporcionar el servicio al cliente, aún sin recursos de cómputo.

Se identificaron las funciones del negocio críticas siguientes:

1. Promoción Mercado de Dinero
2. Red de Sucursales
3. Operación Cheques
4. Administración de Cambios
5. Finanzas Especiales

♦ Categorización de Pérdidas intangibles.

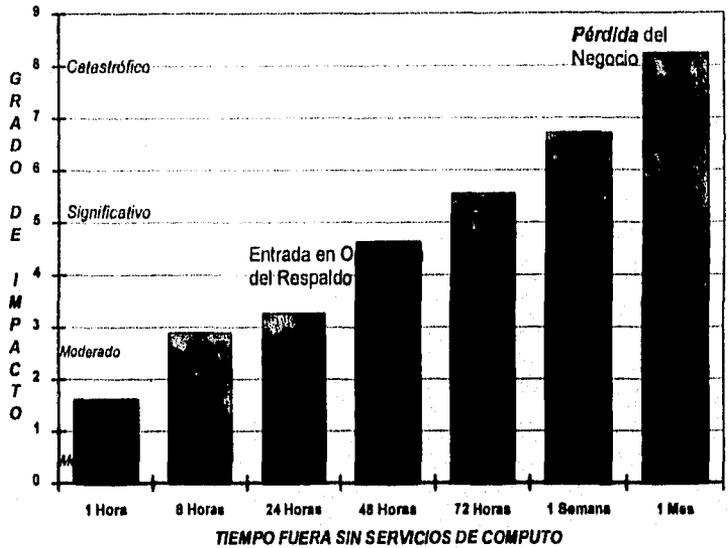
Existen otro tipo de pérdidas además de las financieras, y cada una de estas tiene un impacto diferente en cada una de las funciones del negocio.



Esta gráfica permite identificar la apreciación del nivel de Dirección y Gerencia media, en relación al daño que pudiera causarle a la empresa, un desastre que afectara las instalaciones de cómputo y con ello el soporte de las funciones de negocio críticas y es al mismo tiempo un factor importante para concientizar a la alta dirección de la importancia de implementar un Plan de Recuperación del negocio en caso de contingencia que permita darle continuidad a la operación del negocio.

◆ Tendencia de la situación del negocio.

El grado de impacto al negocio, se encuentra en función del tiempo sin servicios de cómputo que transcurra en la empresa.



Se puede observar que la situación de la empresa se agrava conforme aumenta el tiempo sin servicios de cómputo, lo que significaría quedar fuera del mercado, dada la pérdida financiera que se generaría.

◆ Sistemas vitales de proceso.

Una vez determinadas las funciones del negocio críticas, se debe investigar los sistemas de información que soportan dichas funciones de negocio, así como las interdependencias entre ellos o su relación con otros sistemas que soportan otras funciones de negocio, aunque estas no sean críticas. Con la finalidad de tener el panorama global de los procesos vitales de información.

PRIORIDAD Recuperación	FUNCION DEL NEGOCIO	SISTEMAS RELACIONADOS		ON-LINE/ BATCH
		ON-LINE	BATCH	
1	Red Sucursales Banca Metro/Interior			
2	Operación Cheques	Cheques Cargo sin Sobregiro Cuenta Maestra Chequeras Giros Control de Totales Líneas de Servicio / (T.I. CECOBAN) Catálogos Generales HOGAN	Cheques Remesas (SICOR) Giros Cuenta Maestra Complex Micro Cecoban Mesa Inversiones	Cajero Automáticos
3	Operaciones Inversiones	Ahorro Ahorro Nuevo Valores Ordenes de Pago Catálogos Generales HOGAN	Valores Metro / Interior Ahorro Ordenes de Pago Nacional	
4	Tarjeta de Crédito	Tarjeta de Crédito (FOR) / NABANCO PROSA AMEX	Tarjeta de Crédito (FOR) / NABANCO PROSA AMEX	
5	Operación Cartera	Cartera General Crédito Empresarial Cartera Hipotecaria Catálogos Generales	Sistema Cartera Crédito Hipotecario (Nvo. Sistema y Agencias Internacionales)	
8	Servicios Especiales	Servicios de Cobranza Banca Electrónica SICOPEX Nuevo Sistema Fondos en Línea Integrales para Empresas Captura American Express SACC Catálogos Generales	Multitrán SEYOTF Multinóminas RECOB SICOPEX SACC	HOGAN
7	SWIFT	Cambios de Divisas Internacional		
8	Contabilidad		Contabilidad Matriz y Sucursales (COMS) (Todas las aplicaciones que tienen liga con contabilidad) Control presupuestal	
9	Pagos y Cobranzas Institucionales		Ordenes de pago Internacionales(AS400) SICOB Oñares Cheques de Viajero SACCX PA. Co. (Contabilidad)	
10	Operación SAR		SAR / BO	
11	Gcla. Administración de Cambios		Sistema Agencias (AS400)	
12	Créditos Comerciales			

Capítulo 3.

En el presente capítulo se analizarán las alternativas de recuperación del negocio propuestas, considerando las ventajas y desventajas que conllevan cada una de ellas, para realizar la evaluación y selección de la opción óptima para la empresa. Se delineará la Estrategia de Respaldo, considerando los componentes de software, hardware y comunicaciones; finalmente se definirá el Plan de Contingencias.

3.1 Análisis de alternativas de recuperación del negocio.

De acuerdo con el diagnóstico efectuado, se realizará el Análisis Costo/Beneficio, sobre las alternativas siguientes:

Alternativa 1	Diseño y construcción de centro de cómputo espejo con capacidad de procesamiento al 50%
Alternativa 2	Contratación de procesamiento externo (Hot-Site), con capacidad al 50%.

Diseño y construcción de centro de cómputo espejo con capacidad de procesamiento al 50%.

Se realizó la investigación correspondiente, para conocer el costo de la construcción de un nuevo edificio diseñado para alojar al centro de cómputo, determinándose también la inversión necesaria para comprar el hardware, software y equipo de telecomunicaciones, así como el costo de mantenimiento y la actualización simultánea de dos centros de cómputo.

necesaria para comprar el hardware, software y equipo de telecomunicaciones, así como el costo de mantenimiento y la actualización simultánea de dos centros de cómputo.

A continuación se citan los costos sobre los conceptos antes mencionados:

Adquisición de Equipos de Hardware y Telecomunicaciones.

Detalle de Inversión en equipo.

Descripción	Precio unitario US\$	Unidades	Precio total. US\$
CPU	7,500,000.00	1	7,500,000.00
Controlador de Proceso	287,000.00	1	287,000.00
Unidad de Enfriamiento	171,000.00	1	171,000.00
Controlador de Discos	6,877.00	4	27,508.00
Unidad de Discos	10,856.00	12	130,272.00
Unidad de Cartuchos	170,819.00	4	683,276.00
Terminales	3,400.00	6	20,400.00
Controlador de comunicaciones	383,000.00	1	383,000.00
Total			9,202,456.00

Inversión Inicial.

Descripción	Importe US\$
Construcción	2,000,000.00
Acondicionamiento del edificio	500,000.00
Adquisición de Equipos de Hardware y Telecomunicaciones	9 202,456.00
Total Inversión Inicial	11,702,456.00

Gastos Anuales.

Descripción	Importe US\$
Mantenimiento de Equipos	150,000.00
Salarios del Personal	100,000.00
Renta de Comunicaciones	20,000.00
Total Mensual	270,000.00
Total Anual	3,240,000.00

Considerando los costos anteriores y el monto de las pérdidas financieras en una semana, obtenidas en el Análisis de Impacto Financiero al Negocio, se puede identificar cual es la inversión mínima que evitaría la pérdida financiera en caso de una contingencia.

Inversión inicial (US\$):	11,702,456.00
Gastos anuales (US\$):	3,240,000.00
Gasto total en un año (US\$):	14,942,456.00
Pérdidas Financieras(N\$):	631,588,648.00
(Tipo Cambio N\$7.8) (US\$)	80,972,903.59

La inversión para construir un centro de cómputo de respaldo con capacidad de procesamiento del 50% representa el:

- ◊ 14.45% de la pérdida financiera en una semana.

Contratación de procesamiento externo (Hot-Site), con capacidad al 50%.

En los Estados Unidos de América existen diversas empresas que ofrecen el servicio de procesamiento externo (Hot-Site), las cuales ofrecen lo siguiente:

- Diferentes plataformas en hardware que se adaptan a las necesidades de la empresa.
- Pruebas de procesamiento de información una o dos veces al año.
- Asesorías en el uso de las instalaciones.
- Apoyo para la instalación del software operativo.
- Integridad y seguridad en la confidencialidad de la información, etc..

Entre estos proveedores se debe elegir el que más convenga a la empresa financiera con base en los servicios que ofrezcan, y al costo de los mismos. Para poder determinar desde el punto de vista económico la conveniencia de un centro de proceso externo, se investigaron costos en los E.U.A., obteniéndose lo siguiente:

Renta mensual	4,500.00	
Renta Anual		54,000.00
Declaración de Contingencia (*)		10,000.00
Uso diario de Hot-Site	2,500.00	
Uso en una Semana de Hot-Site(*)		17,500.00
Total (US\$)		81,500.00

Nota (*): Se esta considerando una declaración de desastre para efectos de evaluación de esta alternativa.

El costo de Contratación de procesamiento externo con capacidad al 50% representa el:

◇ 0.1 % de la Pérdida financiera en una semana.

Recomendación.

Con la finalidad de tomar una decisión objetiva y no condicionada en función únicamente del costo de las alternativas, se consideraron otros objetivos:

Objetivos Obligatorios	Alternativa 1.	Alternativa 2.
Contar con la plataforma adecuada para proporcionar los servicios ofrecidos a los clientes de la institución soportados por las Funciones Críticas del Negocio.	Cumple	Cumple

Objetivos Deseados:	Alternativa 1.			Alternativa 2.	
	Peso (1-5)	Calificación (1-3)	Total	Calificación (1-3)	Total
Contar con el servicio en cualquier momento	5	2	10	3	15
Minimizar el tiempo de recuperación de información para soportar los servicios de cómputo (máximo 24 hrs.).	4	2	8	3	12
El gasto de la inversión deberá ser menor al 20 % máximo del total de la pérdida financiera en una semana.	3	2	6	3	9
La alternativa de respaldo deberá estar ubicada en una ciudad distinta y en una zona geográfica que garantice su funcionamiento.	2	3	6	3	6
Flexibilidad para responder a los cambios que sufra el ambiente de proceso (Hardware, Software, Comunicaciones).	1	2	2	3	3
Total			32		45

Al comparar los resultados de ambas alternativas, se observa que la segunda tiene mayor puntaje, debido a que satisface en mayor grado los objetivos deseados. Considerando lo anterior se propone la **Contratación de procesamiento externo (Hot-Site), con capacidad al 50%, como la estrategia más viable para garantizar la continuidad del negocio en caso de contingencia.**

3.2 Desarrollo de la Estrategia de Respaldo.

Para realizar la contratación del Servicio de Recuperación del Negocio, con la empresa elegida, se deberán cubrir los requisitos siguientes:

⇒ Definición de la configuración del equipo requerido indicando modelo y características:

- CPU
- Controladores SNA y no SNA
- Capacidad de almacenamiento en unidades de disco
- Unidades de cartucho y/o cinta magnética
- Impresoras.

⇒ Implementación del enlace de comunicaciones, que se utilizará para llevar a cabo la conexión, entre la Empresa de Servicios de Recuperación y el Banco, indicando su arquitectura, componentes y vía de acceso a las sucursales.

Por lo tanto de acuerdo al análisis efectuado en la sección 2.2, la empresa financiera en cuestión deberá establecer el contrato de Business Recovery Services con la configuración siguiente:

Cantidad	Descripción
1	CPU modelo 9121 <ul style="list-style-type: none">• 46 MIPS• 24 canales• 120 MB en memoria real• 120 MB en memoria expandida.
1	Controlador 3745-510
1	Controlador 3274
160 GB	En discos tipo 3390 modelo 2
8	Unidades de Cartucho modelo 3490-B20
2	Impresoras Láser modelo 3900 -D01

Software Operativo y Aplicativo.

La generación del sistema operativo y aplicativo en el equipo que se utilizará en el Hot-Site deberá realizarse utilizando los respaldos creados de manera periódica en las instalaciones del centro de cómputo de la empresa.

Lo anterior es con la finalidad de asegurar que en caso de una contingencia real, en la cual el Centro de Cómputo y su cintoteca local hayan quedado destruidos, la restauración del ambiente operativo y aplicativo, deberá ser con el *duplicado* que resida en *bóveda fuera de sitio*.

Para lo cual, la bóveda fuera de sitio contará con las condiciones de temperatura, humedad y seguridad recomendadas por el fabricante del medio magnético utilizado para respaldo, ya sea este cartucho o cinta de carrete, en cuanto a la seguridad de la bóveda fuera de sitio deberá apearse a las normas y procedimientos de seguridad de instalaciones y acceso establecidas por el departamento de seguridad de la Institución financiera.

Arquitectura de Comunicaciones para el respaldo.

- Solo se respaldarán los servicios de transmisión de datos.
- La topología de la red de datos es centralizada.
- Se tendrán dos nodos centrales:
 - Edificio corporativo-1, Nodo A.
 - Edificio corporativo-2, Nodo B.

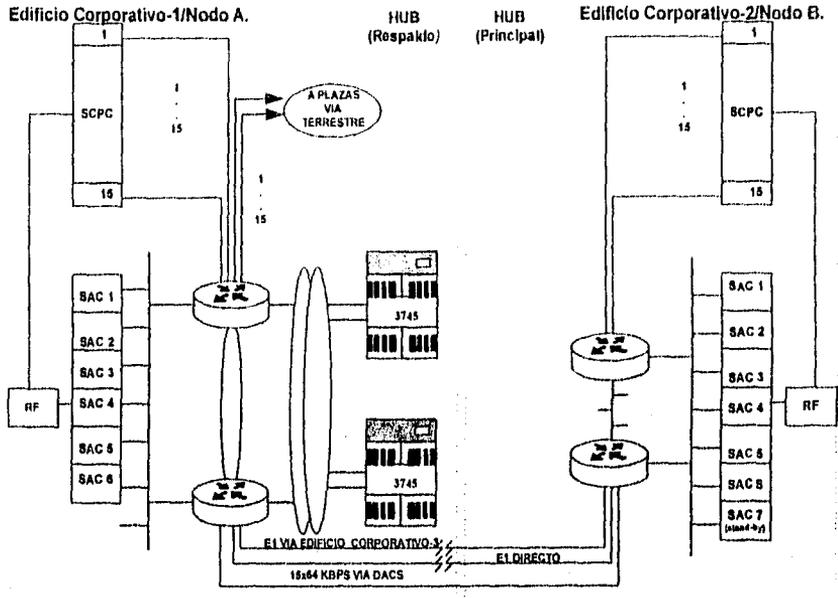
Edificio corporativo, Nodo A.

- Recibirá todos los enlaces terrestres de alta velocidad a las plazas del interior a través de RDI (u otras redes en el futuro).
- En este nodo se ubica la estación maestra espejo para el respaldo de la red de datos via satélite.
- Está enlazado via microondas digitales a los edificios corporativos 2 y 3, formando un triángulo. Cada enlace individual tiene capacidad de transmitir 4 canales de 2 Mbps (E1s) de la manera siguiente:
 - 3 asignados para transmisión de voz
 - 1 para datos.
- Adicionalmente se instalará un enlace terrestre al edificio corporativo-2 de 15x64 Kbps a través de la red de DACS de Telmex.

Edificio corporativo-2, Nodo B.

- Aloja la estación maestra principal de comunicaciones vía satélite para transmisión de voz y datos.
- Recibirá los enlaces terrestres de respaldo para las sucursales metropolitanas, actualmente enlazadas a través DSO's (RDI).
- Está enlazado via microondas digitales a los edificios corporativos 1 y 3.

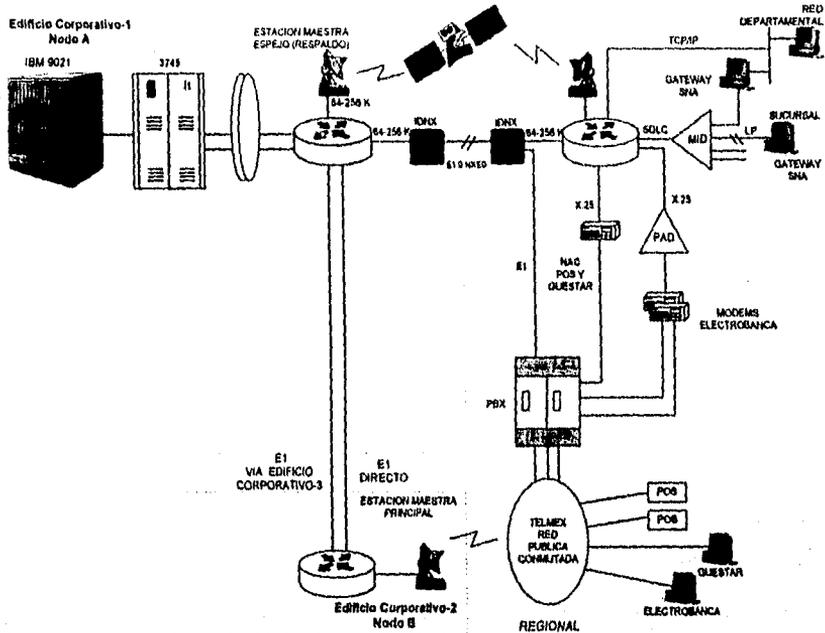
Escenario I (Token Ring).



Nodos Regionales.

- Servirán como nodos concentradores de comunicaciones de las sucursales ubicadas en sus plazas correspondientes y de aquellas plazas que no cuenten con un enlace directo al nodo A.
- Su enlace principal será terrestre, digital y de capacidades desde $n \times 64$ Kbps hasta E1. A través de éste se transmitirán señales de voz, datos e imágenes.
- Contarán con un enlace de respaldo para transmisión de datos vía satélite, con capacidades desde 64 Kbps hasta 256 Kbps con el método de acceso SCPC.

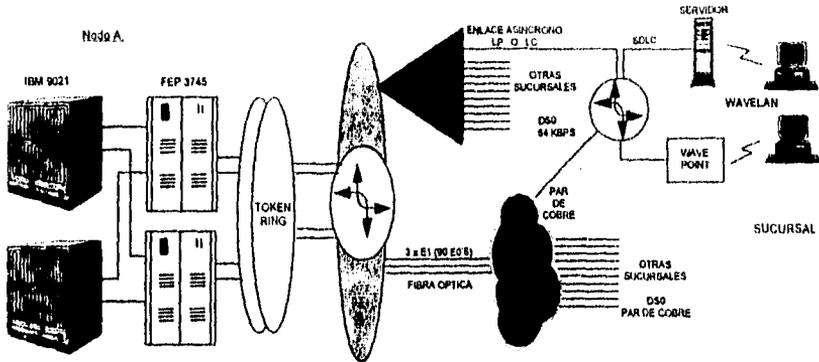
Arquitectura de comunicaciones para las plazas satelitales SCPC



Sucursales Metropolitanas.

- En la ciudad de México tendrán como enlace principal un DS0 al Nodo A (edificio corporativo-1) a través de la RDI de Telmex. Este enlace podrá ser redireccionado al Nodo B (edificio corporativo-2) en caso de siniestro en Nodo A (edificio corporativo-1).
- Su enlace de respaldo será a través de una línea analógica (privada y/o conmutada).

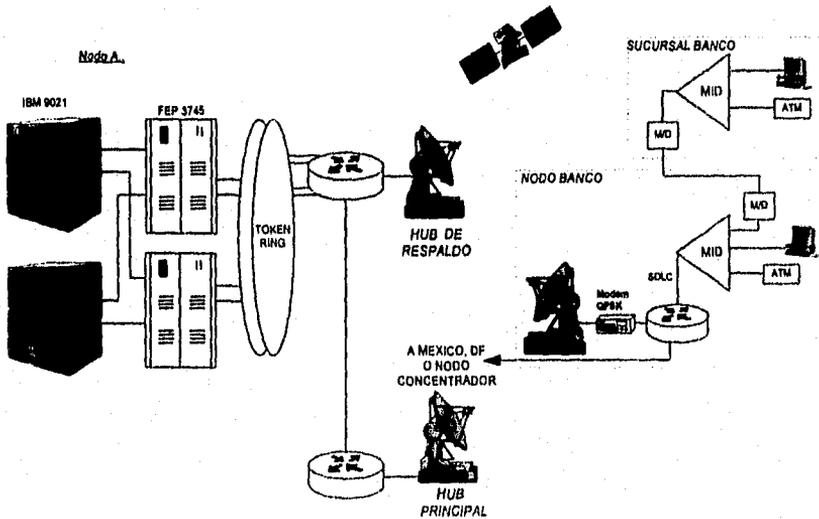
Esquema de comunicaciones a Sucursales Metropolitanas



Plazas con VSAT TDMA

- Su enlace principal será a través de la red satelital.
- Su enlace de respaldo será a través de un circuito de microondas analógico o a través de línea conmutada al nodo concentrador más cercano o directamente a la Cd. de México.

Plazas con VSAT TDMA



3.3 Desarrollo del Plan de Contingencias.

El Plan de Contingencia deberá contener el objetivo que desea alcanzar la empresa al contar con él, a través de la descripción de la misión, también deberá incluir las componentes mencionadas en esta sección, mismas que deberán apegarse a las plataformas tecnológicas y operativas de la empresa.

Misión.

Contar con un Plan de Contingencias para proporcionar continuidad a los servicios vitales para la operación **Bancaria**, minimizando el Impacto financiero en situaciones de desastre.

Procedimientos, evaluación, escalamiento y declaración

Con la finalidad de identificar y evaluar los daños a la infraestructura de Cómputo en las Instalaciones, se cuenta con procedimientos que nos permiten:

- Evaluar el impacto en instalaciones y equipos.
- Hacer el escalamiento organizacional para comunicar el estado de la situación.
- Declarar en su momento el desastre al *site* alternativo de proceso, a través de las personas autorizadas para tal efecto.

Equipos de Recuperación y responsabilidades.

Proporciona la estructura de los equipos de trabajo para la recuperación asignando sus responsabilidades de acuerdo a las siguientes disciplinas:

- Software operativo
- Operaciones
- Software aplicativo y B.D.
- Registros Vitales
- Recuperación
- Comunicaciones
- Administración
- Evaluación del Desastre
- Hardware
- Site Alterno

Procedimientos de Respaldo.

En el Plan se encuentran los procedimientos de respaldo de las aplicaciones críticas que dan soporte a las funciones de Negocio vitales de el Grupo Financiero, con la finalidad de realizar los respaldos correspondientes durante la operación en el Hot-site.

Procedimientos de Recuperación.

Los procedimientos de recuperación de los sistemas críticos que dan soporte a las funciones de negocio, se encuentran documentados en esta sección, indicando paso a paso las actividades que deberán realizarse para su restauración en el Hot-site, estos procedimientos abarcan:

- Software operativo, aplicativo y Base de Datos
- Software de Comunicaciones

Tareas por Equipos.

Con la finalidad de establecer claramente, las actividades que deberán desarrollarse durante una contingencia que nos obligue a respaldar nuestras operaciones en el Hot-site, se definieron para cada equipo de trabajo tareas, antes, durante y después de la emergencia y sus responsabilidades.

Organización de Equipos de Trabajo



Procedimientos de Mantenimiento.

Se establecieron procedimientos de mantenimiento para cada uno de los componentes del Plan, que nos permitirán mantener permanentemente actualizado el Plan de Contingencias ante cualquier cambio en el ambiente operativo, y por consiguiente garantizar su funcionalidad en cualquier momento.

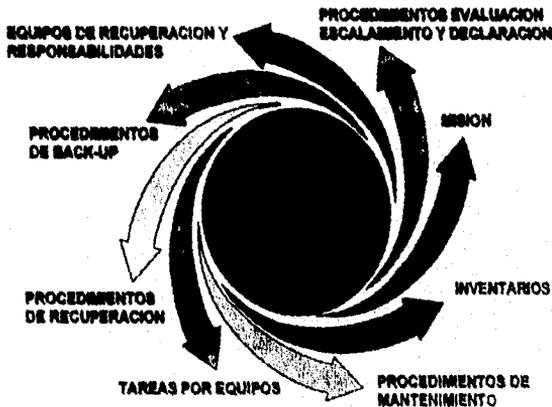
Inventarios.

Para contar con información centralizada en cuanto a las plataformas tecnológicas, software, equipos de comunicaciones, proveedores y suministros utilizados en los diferentes equipos, el Plan de Contingencias contiene un inventario de:

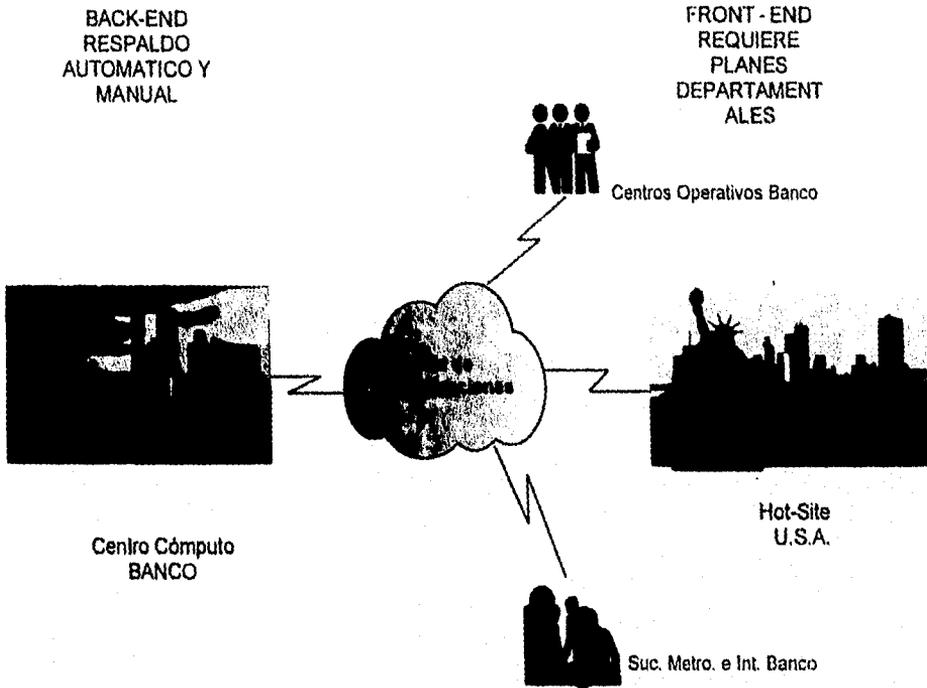
- Hardware
- Software
- Equipo de Comunicaciones
- Suministros
- Proveedores

Representación esquemática del Plan de Contingencias.

Todas las actividades antes mencionadas se pueden simbolizar de la manera siguiente, donde se observa que el Plan de Contingencias, es el conjunto de diversas actividades que ordenadas y categorizadas, forman una logística con la dinámica suficiente para responder ante las situaciones de desastre mayor en las empresas.



El resultado del análisis realizado nos muestra el escenario de respaldo siguiente:



Capítulo 4.

A lo largo del presente capítulo se verán los aspectos fundamentales para realizar las **Pruebas del Plan de Contingencia**, la importancia de la retroalimentación de resultados al realizar la prueba, así como, el mantenimiento para garantizar el funcionamiento del Plan en cualquier momento.

4.1 Prueba del Plan de Contingencia.

Con la finalidad de garantizar el funcionamiento del **Plan de Contingencia** ante cualquier situación de emergencia, es necesario realizar **pruebas periódicamente** en el **Hot-Site de proceso alterno**.

Para desarrollar exitosamente las pruebas, se tendrán que definir los aspectos siguientes:

- Alcance.
- Objetivos Primarios.
- Objetivos Secundarios.
- Recursos Humanos que serán utilizados.
- Programa de Actividades detallado, especificando:
 - Inicio y fin de la actividad en horas.
 - Responsable de la ejecución por actividad.

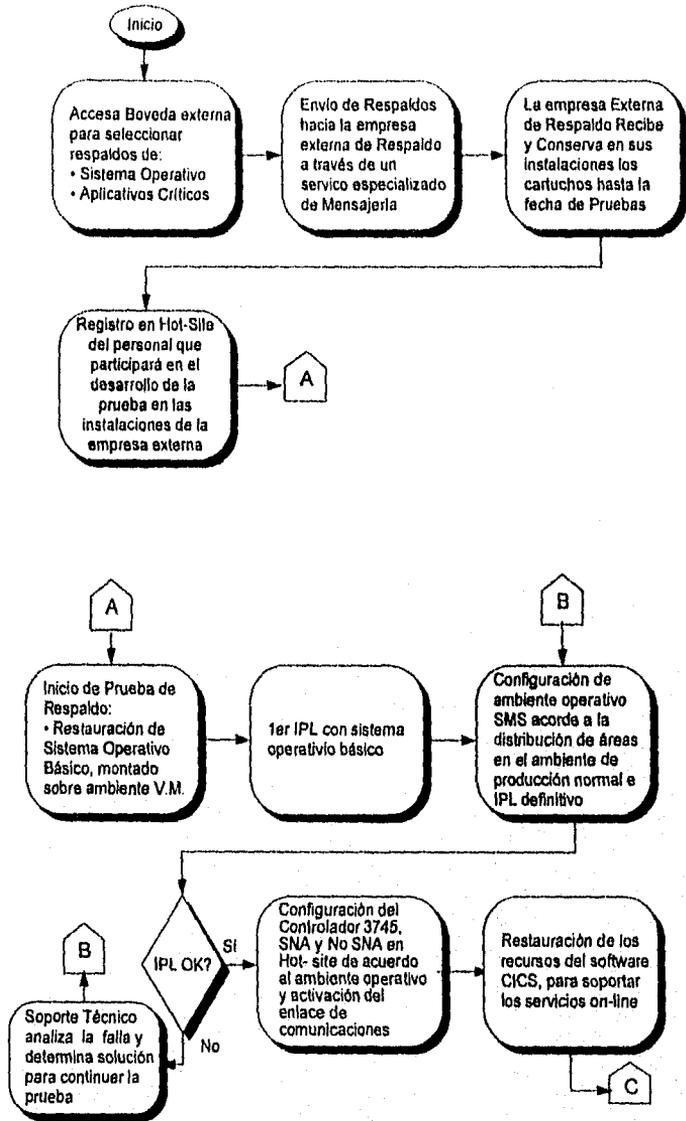
- Referencia a la documentación y/o *procedimientos* del *Plan de Contingencia* que se utilizarán para ejecutar la actividad señalada.
- Coordinación con el representante de la compañía de *Business Recovery*, de los recursos de:
 - Hardware
 - Configuraciones de los equipos
 - Esquema de conectividad que se implementará para la ejecución de las pruebas
 - Tiempo de duración de la prueba, normalmente se disponen de 24 a 48 horas para desarrollar la prueba
- Envío de cartuchos magnéticos y/o cintas magnéticas con la Información respaldada del:
 - Sistema operativo
 - Sistema aplicativo y Bases de Datos
 - Software de comunicaciones
 - Cartuchos y/o cintas scratch para su utilización durante la prueba.

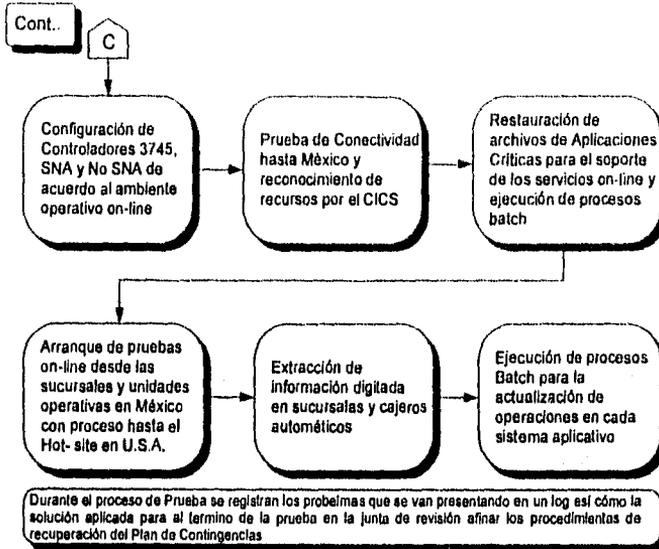
La revisión de los recursos de Hardware que se utilizarán en la prueba de respaldo es muy importante, ya que el medio ambiente de proceso sufre cambios continuamente debido a:

- Instalación de nuevos sistemas aplicativos que soporten funciones de negocio críticas
- Instalación de nuevos subsistemas de apoyo a la operación de los equipos

Invariablemente dichos cambios se reflejarán en nuevos requerimientos de espacio en disco del sistema y/o configuración de la memoria real y/o expandida, siendo estos últimos los menos frecuentes.

Proceso de Pruebas de Respaldo



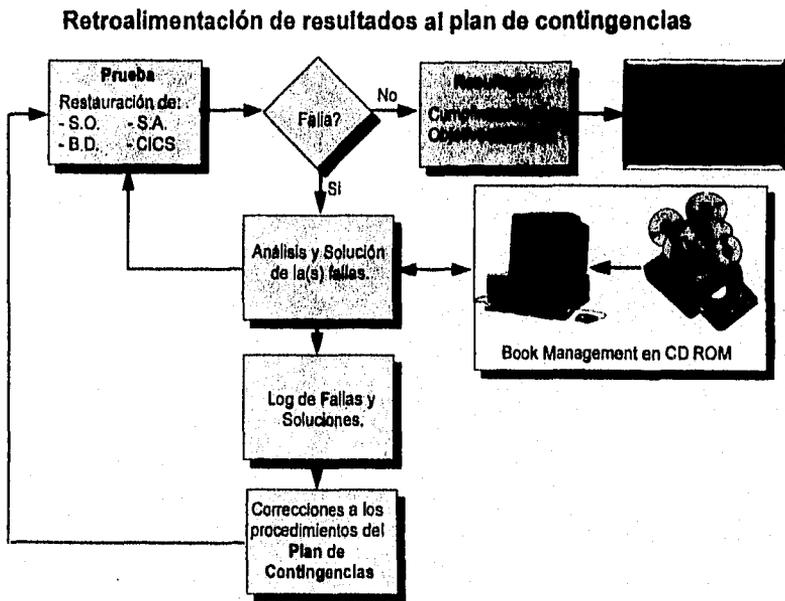


4.2 Retroalimentación de Resultados para la Afinación del Plan de Contingencia.

La satisfacción de los objetivos establecidos para la prueba de respaldo, permitirá corregir los procedimientos de:

- Restauración del sistema operativo
- Subsistemas para control y monitoreo de los recursos del equipo de cómputo
- Sistemas aplicativos

De acuerdo con las soluciones que se hayan aplicado durante la restauración del ambiente de proceso, mismas que deberán documentarse a través de un histórico al momento del desarrollo de la prueba, este proceso se representa de manera gráfica en el siguiente diagrama:



La afinación de los procedimientos del Plan, permitirán garantizar un alto grado de confiabilidad en la aplicación del mismo al momento de que sea necesario recuperar las operaciones de cómputo y del negocio en caso de un desastre, que obligue a llevar a cabo el respaldo, facilitando la habilitación del negocio en el tiempo requerido.

4.3 Mantenimiento del Plan de Contingencia.

La dinámica de cambio en la empresa, debido a la implementación de nuevos productos financieros y/o nuevos servicios, crecimiento de la cartera de clientes, o bien por los avances tecnológicos, pueden generar cambios en el Plan de Contingencias por los factores siguientes :

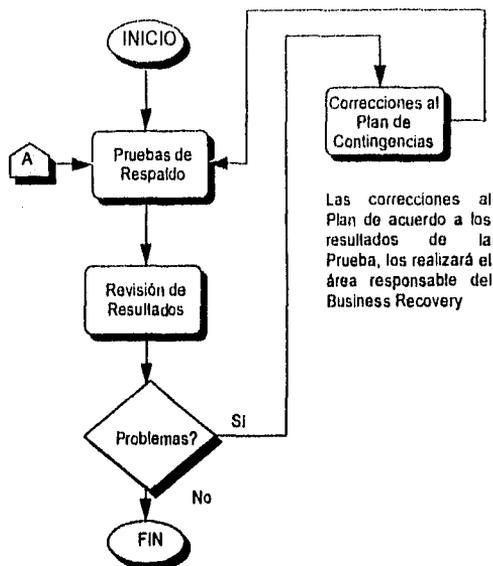
- **Resultados de pruebas de respaldo.**
- **Hardware y comunicaciones:** CPUs, capacidad de almacenamiento, etc.
- **Software operativo:** Nuevas versiones, sistemas de seguridad y control.
- **Software aplicativo:** Cambios y/o inclusión de sistemas que soportan las funciones críticas del negocio.
- **Personal, proveedores, inventario de equipos.**

Por lo tanto es importante realizar una actualización al Plan de Contingencias conforme se presente algún cambio en los aspectos anteriormente citados, ya que de no hacerlo, en el momento que se presente una contingencia, *quizás no se logre la Recuperación del Negocio*, ya que no se tendría el estado real del ambiente operativo, y no se cumpliría el objetivo de darle continuidad al negocio, a pesar de contar con un plan de Recuperación.

Resultados de pruebas de respaldo.

Como se mencionó en la sección 4.2, al desarrollar las pruebas de respaldo se pueden presentar problemas, los cuales independientemente de que sean solucionados satisfactoriamente en ese momento, deben ser documentados, para realizar las modificaciones necesarias al plan de contingencias.

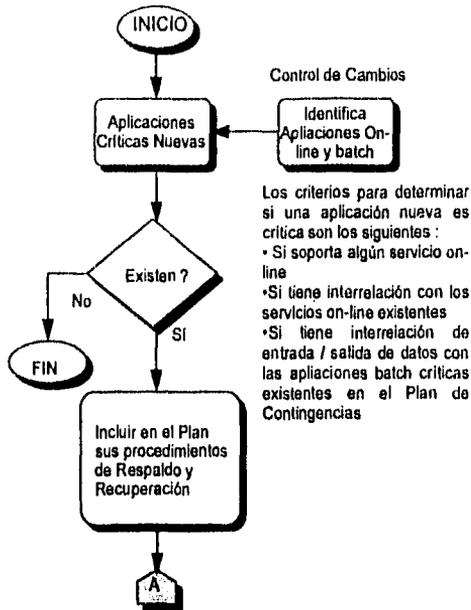
Pruebas de respaldo



Software aplicativo de funciones críticas del negocio.

En la sección 2.2 se identificaron las funciones críticas del negocio, así como las aplicaciones que las soportan y sus relaciones con otras aplicaciones, las cuales están incluidas en los procedimientos de respaldo del Plan de Contingencias, por lo tanto todos los cambios que se efectúen a estos sistemas, así como las nuevas aplicaciones, deben ser notificados al área de Business Recovery, para que se tomen las medidas necesarias para mantener permanentemente actualizado el Plan de contingencias.

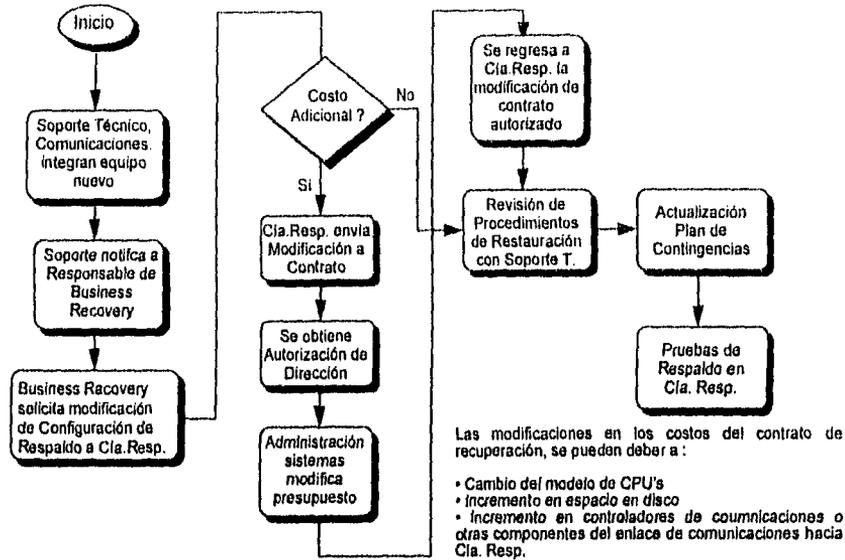
Software aplicativo



Hardware y Equipo Comunicaciones

En la actualidad los equipos de hardware y comunicaciones evolucionan rápidamente, y la empresa puede requerir cambios en este sentido para permanecer a la vanguardia. Estas modificaciones deben ser notificadas al área de Business Recovery, de inmediato, ya que puede generar modificaciones a la configuración de Respaldo en la Compañía de Respaldo Alterno, lo cual podría representar una erogación mayor a la existente y se tendría que modificar el contrato.

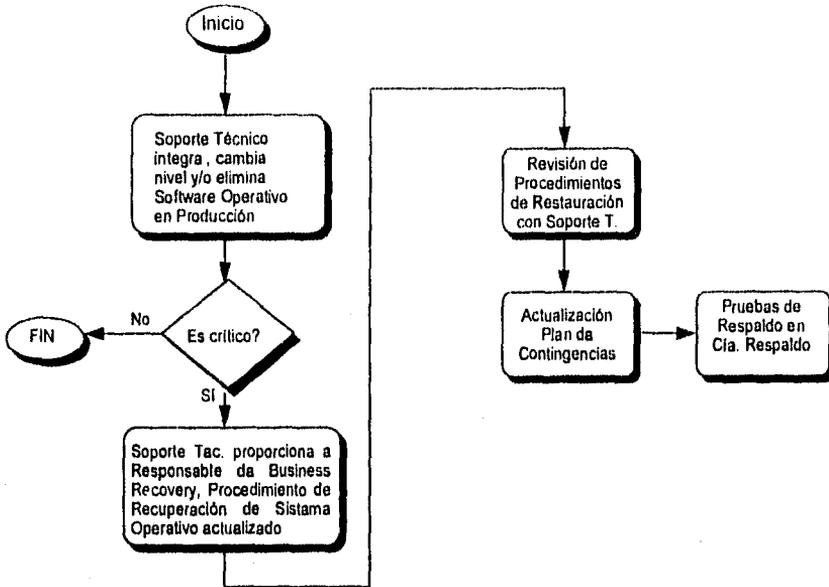
Hardware y equipo de comunicaciones



Software operativo.

El software operativo también presenta cambios, aunque no es tan frecuente como el aplicativo, la mayoría de las veces es de mayor impacto, y es un punto de vital importancia para el funcionamiento de los sistemas aplicativos, debido a que si no se restaurarán correctamente algunas herramientas de software, aunque se tengan los sistemas aplicativos, no se puede hacer nada con ellos ya que no son reconocidas por los manejadores. Por lo tanto cada cambio en el Sistema Operativo, por mínimo que ésta sea, deberá ser informado al responsable de Business Recovery, para que se actualice el Plan de Recuperación del Negocio.

Software operativo

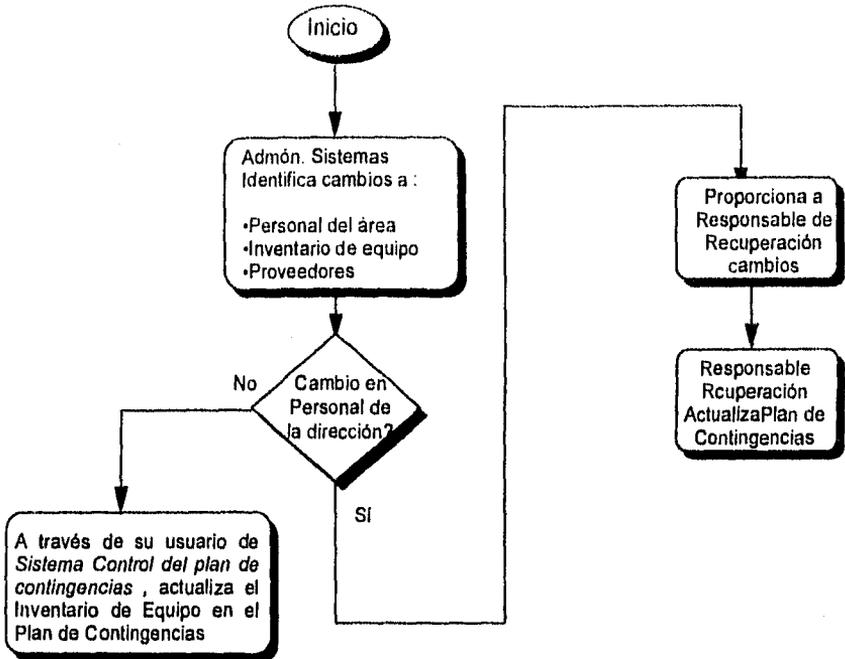


Personal, Proveedores e Inventarios.

Además de los cambios mencionados anteriormente, es importante actualizar los que ocurren en el personal del área que están involucrados con el Plan de Recuperación del Negocio, ya que cada una de estas personas es responsable de tarea(s) específica(s), y se debe saber con exactitud quien debe desarrollar la actividad en caso de que ocurra una contingencia.

Debido a que todos los equipos de hardware y comunicaciones están asegurados, al presentarse un siniestro, será necesario cobrar los seguros correspondiente, para que los equipos sean repuestos por los proveedores, por consiguiente es importante mantener actualizado el inventario de equipos y proveedores.

Personal, Proveedores e Inventarios



Como se puede apreciar en los puntos anteriores, el Plan de Contingencias *no es un esfuerzo temporal, es un proceso permanente* que permitirá a la empresa reaccionar rápida y eficazmente ante cualquier siniestro que deshabilite su capacidad de cómputo y se debe trabajar responsablemente en él para mantenerlo operable en todo momento, de lo contrario de nada serviría que se cuente con *Hot-Site alternativo, estructura de comunicaciones y la logística* necesarias para soportar el servicio a los clientes de la institución.

Conclusiones.

Durante el desarrollo del presente trabajo se determinó :

- La importancia que tiene para la empresa, **en nuestro caso del ramo financiero**, la permanente **disponibilidad de los servicios bancarios** en los puntos de venta de la empresa
- El **Impacto a la infraestructura de servicios de cómputo** (servicios de información), en caso de un **desastre mayor** y por causas técnicas y/o humanas
- Los **desastres más sobresalientes** en los **Estados Unidos de América** en los últimos años y sus consecuencias en diversas instalaciones de cómputo

Considerando ese entorno, se propuso :

- Como estrategia para proporcionar de manera continua los servicios de cómputo que dan soporte a las funciones de negocio más importantes de la empresa en cuestión, el **desarrollo de la logística, a través de un Plan de Contingencias, y la creación de la Infraestructura necesaria para soportar los servicios de cómputo, mediante la contratación de estos servicios a una compañía especializada en esta actividad (Centros de Cómputo alternos, Hot-Site)**
- Minimizando las **pérdidas financieras para la empresa**, en caso de un desastre que inhabilite sus instalaciones de cómputo
- **Garantizando la prestación de los servicios bancarios a su base de clientes**, aún en condiciones críticas

Con base en lo anterior, *pienso que es imperativo para las empresas de la Industria Financiera y Bursátil , dada la naturaleza de sus operaciones, contar con Planes de Contingencia y los recursos necesarios para soportar sus operaciones en Centros de Cómputo alternos.*

Lo cual permitirá a las empresas :

- *Dar continuidad a su negocio sin perjuicio a sus clientes*
- *No impactar al ámbito financiero del País, por las posibles pérdidas que se dieran por un desastre, tanto en su activo fijo como en recursos financieros*

No obstante lo antes citado se *deberá vencer la resistencia por parte de las empresas, en Invertir* en estas acciones ante una *posibilidad que tal vez nunca se presente.*

Por último considero que esta propuesta, no solamente la deben aplicar las empresas Financieras y Bursátiles, sino todas aquellas que son *prioritarias para la economía de un País.*

Esta logística se debe establecer como una función permanente en la empresa. para mantenerla actualizada y vigente en función de los alcances tecnológicos en materia de Servicios de Información (Informática).

Glosario.

CPU:	Unidad central de proceso
DACS:	Sistema digital de acceso Digital
DASD:	Dispositivo de Almacenamiento en Disco
FEP:	Procesador Frontal
HDLC:	High Level Data Link Control
JCL:	Job Control Language
LAN:	Red de área local
RDI o RDSI:	Red Digital Integrada
RJE:	Remota Job Entry
SAC:	Acceso de Comunicaciones Satelital
SCPC:	Por Canal una Portadora
SDLC:	Synchronous Data Link Control
SNA:	System Network Architecture
TCP/IP:	Transport Control Protocol/Internet Protocol
TDM:	Multiplexor por División de Tiempo.
TDMA:	Multiplexor por División de Tiempo Asíncrono
VSAT:	Very Small Access Telecommunications
VTAM:	Método de Acceso de Comunicaciones Virtual

Anexo.

Codificador - Decodificador (Codec):

Es un dispositivo que transforma una señal analógica en una señal digital. Realiza 8000 muestras por segundo (125 microsegundos por muestra).

Concentrador:

Su función es manejar lógicamente las señales, lo cual consiste en utilizar una línea de salida que contenga una capacidad menor que la correspondiente a la suma de las líneas de entrada, es decir, recibe mensajes desde varias fuentes y entrega menos corrientes de mensajes de las que recibe. A través de las siguientes transformaciones:

- Aumentar la velocidad de transmisión de salida sobre la de entrada.
- Cambios de codificación y detección de errores.
- Agregar datos de identificación de la fuente a los mensajes.
- Alterar de manera permanente la corriente del mensaje
- Analizar el contenido de los mensajes, reaccionan a él y almacenan datos.
- N líneas de entrada generan M salidas, donde $M < N$.

Por lo tanto mejora la eficiencia de la transmisión de datos o voz al permitir que las terminales o líneas compitan por y compartan los canales de transmisión.

Esquemas de transferencia de datos:

Existen diferentes métodos de transferencia de datos a continuación se citan los más importantes:

a) Conmutación de circuitos:

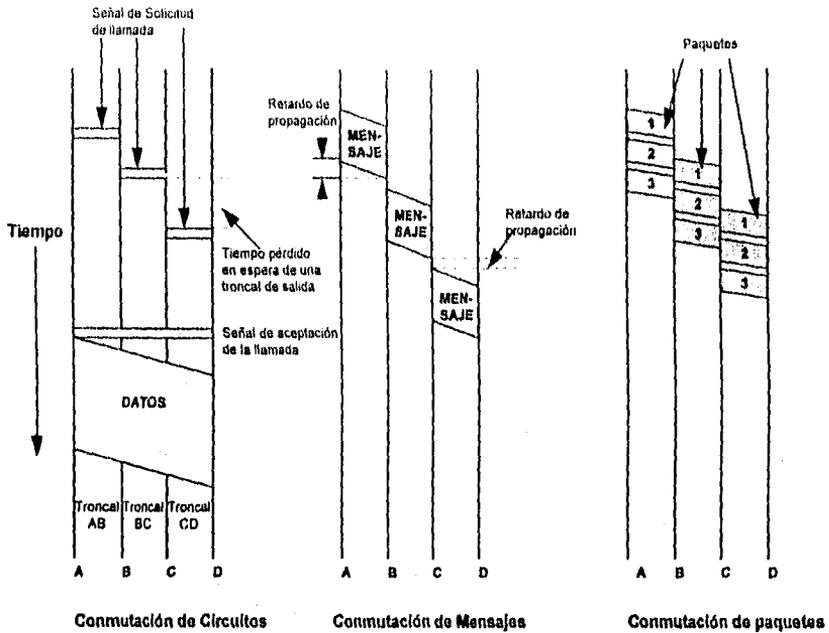
Cuando un usuario o su ordenador realiza una llamada telefónica, el equipo de conmutación, dentro del sistema telefónico, busca una trayectoria a través de una línea de transmisión que lo enlace hasta el receptor. Un factor importante es que se debe establecer una ruta de extremo a extremo antes de que cualquier conjunto de datos pueda ser enviado y se necesita que transcurra cierto tiempo esperando establecer la conexión y antes de que comience la transmisión de datos, la señal de solicitud de llamada debe propagarse hasta su destino y ser reconocida como tal.

b) Conmutación de mensajes:

En este tipo de conmutación no se necesita establecer anticipadamente la ruta entre el que envía y el que recibe. En su lugar cuando el que envía tiene listo un bloque de datos, este se almacena en la primera central de conmutación, para expedirse después dándose un solo salto a la vez. Cada bloque se recibe íntegramente, se revisa en busca de errores, y se retransmite con posterioridad. A las redes que utilizan esta técnica se les llama redes de almacenamiento y reenvío.

c) Conmutación de paquetes:

En este caso se fija el límite superior en el tamaño del bloque, permitiendo que los bloques sean almacenados en la memoria principal del equipo de conmutación de datos, en lugar de hacerlo en disco. Teniendo la seguridad de que ningún usuario puede acaparar la línea, los circuitos nunca están dedicados a una tarea en especial, estos se puede usar por otros paquetes de otro origen o con destinos que tampoco tienen ninguna relación, los equipos de conmutación de datos proporcionan una conversión de velocidad y código. También proporcionan la corrección de errores hasta cierto punto.



Líneas de punto a punto.

Estas líneas de comunicación de datos son precisamente eso, sólo tienen dos puntos extremos ocupados generalmente por una computadora y algún tipo de terminal.

Líneas de caídas múltiples o multilíneas.

Es una línea de comunicación con varios puntos de caída, en estas líneas sólo se puede transmitir en un momento dado, a menos que se utilice la multiplexión, cada terminal debe tener una dirección y además de la capacidad de reconocer que se le envía un mensaje.

Modelo de Referencia OSI.

Este modelo se refiere a la conexión de sistemas heterogéneos, es decir, a sistemas dispuestos a establecer comunicación con otros distintos. Esta formado por 7 capas, para lo que fue necesario aplicar los principios siguientes:

1. Una capa se creará en situaciones donde se necesita un nivel de abstracción.
2. Cada capa deberá efectuar una función bien definida.
3. La función que realizará cada capa deberá seleccionarse con la intención de definir protocolos normalizados internacionalmente.
4. Los límites de las capas deberán seleccionarse tomando en cuenta la minimización del flujo de información a través de las interfaces.
5. El número de capas deberá ser lo suficientemente grande para que funciones diferentes no tengan que ponerse juntas en la misma capa, y por otra parte, también deberá ser lo suficientemente pequeña para que su arquitectura no llegue a ser difícil de manejar.

Las capas son las siguientes:

a) Capa Física (Capa o nivel 1).

La capa física se ocupa de la transmisión de bits a lo largo de un canal de comunicación. Su diseño debe asegurar la integridad de la información. En esta capa se definen y materializan las características mecánicas, eléctricas, funcionales y de procedimiento para establecer, mantener y terminar la interconexión física entre un ETD y un ETCD.

b) Capa de Enlace (Capa o nivel 2).

El objetivo de esta capa es proporcionar los elementos necesarios para establecer, mantener y terminar interconexiones de enlace de datos entre entes del nivel de red. Un enlace de datos se establece siempre entre dos puntos físicos de conexión del sistema. En

todos los casos se considera que un enlace es siempre bidireccional. Esta capa tiene que resolver los problemas causados por el daño, pérdida o duplicidad de las tramas. La capa de enlace ofrece diferentes clases de servicios a la capa de red, cada uno de ellos con distinta calidad y precio.

Otra de sus funciones es lo referente a evitar que un transmisor muy rápido sature con datos a un receptor lento; para lo cual se deberá de usar un regulador de tráfico que permita que el transmisor conozca el espacio de memoria que en ese momento tiene el receptor.

c) Capa de Red (Capa o nivel 3).

Se ocupa del control de la operación de la subred. Un punto muy importante es como encaminar los paquetes del origen al destino. Las rutas podrían ser de tipo estático o dinámico. Si en un momento dado hay demasiados paquetes en la subred, ellos mismos se obstruirán mutuamente y darán lugar a un cuello de botella. El control de tal congestión dependerá también de la capa de red. El software deberá de saber cuántos paquetes, caracteres o bits se enviaron a cada cliente, con el objeto de producir información de facturación.

d) Capa de Transporte (Capa o nivel 4).

Su función principal consiste en aceptar los datos de la capa de sesión, dividirlos siempre que sea necesario, en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos ellos lleguen correctamente al otro extremo. La capa de transporte determina que tipo de servicio debe de dar a la capa de sesión y en último término a los usuarios de red.

e) Capa de sesión (Capa o nivel 5).

Permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo un transporte de datos ordinario, tal y como lo hace la capa de transporte, pero mejorando los servicios que ésta proporciona y que se

utilizan en algunas aplicaciones. Uno de los servicios de esta capa es gestionar el control de diálogo. Las sesiones permiten que el tráfico vaya en ambas direcciones al mismo tiempo.

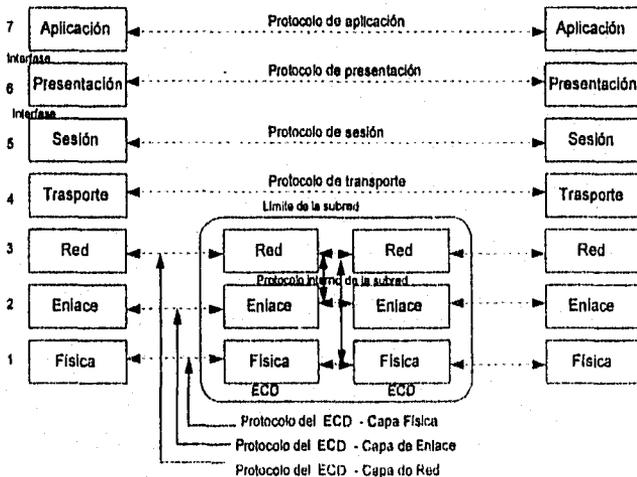
f) Capa de presentación (Capa o nivel 6).

Se ocupa de los aspectos de sintaxis y semántica de la información que se transmite. Un ejemplo es el relacionado con la codificación de datos conforme a lo acordado previamente. Esta capa esta relacionada también con la compresión de datos la cual se puede utilizar para reducir el número de bits que tienen que transmitirse, y el concepto de criptografía se necesita utilizar frecuentemente por razones de privacidad y de autenticidad.

g) Capa de aplicación (Capa o nivel 7).

Contiene una variedad de protocolos que se necesitan frecuentemente. En esta capa se llevan a cabo las funciones específicas de comunicación entre los diferentes procesos de aplicación que constituyen el sistema. Es necesario considerar que los procesos de aplicación que utilizan el mecanismo de interconexión se encuentran distribuidos y deben de considerarse para llevar a cabo objetivos comunes.

Modelo de Referencia OSI



Módem:

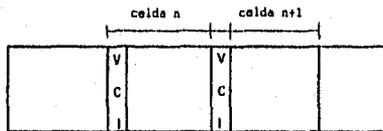
Su nombre se deriva de las palabras "Modulador - Demodulador", este dispositivo acepta como entrada los flujos de bits en serie y al mismo tiempo produce una portadora como salida, cuando actúa como demodulador recibe una portadora y genera un serie de bits en serie. Por lo general se usan en pares uno en cada extremo de la línea de comunicación.

Modo de Transferencia Asíncrono (ATM):

El término Modo de Transferencia Asíncrono (ATM del inglés Asynchronous Transfer Mode) se refiere a una técnica de conmutación de señales de banda ancha; es una tecnología asíncrona que utiliza un multiplexaje por división en el tiempo estadístico para asignar ancho de banda sobre demanda.

ATM proporciona el modo de transferencia para los servicios ofrecidos por la red digital se servicios integrados de banda ancha (B-ISDN). Segmenta el ancho de banda del medio de transmisión en unidades de tamaño fijo denominadas celdas y estas se asignan individualmente a los canales sobre demanda. Cada celda de 53 bytes consta de encabezado de 5 bytes y un campo de información de 48 bytes.

El encabezado contiene un identificador de canal virtual (VCI) que indica a que canal pertenece cada celda y se utiliza para el enrutamiento de las celdas a través de una red de conmutación ATM.



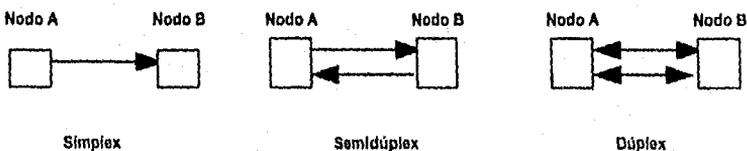
Aunque ATM surgió como el modo de transferencia de B-ISDN, puede desligarse de esta y utilizarse para crear subredes de comunicación de uso general. Una red ATM utiliza un protocolo de

conmutación de paquetes orientado a conexión para proporcionar múltiples canales virtuales a los usuarios. Como el usuario de cada canal puede variar a lo largo del tiempo la utilización del ancho de banda el ancho de banda utilizado, se dice que ATM ofrece asignación dinámica de ancho de banda sobre demanda.

En las redes ATM la unificación básica de conmutación y multiplexaje son las celdas. El tamaño fijo y reducido de las celdas hace posible la transferencia de tráfico sensible al retardo ya que reduce la varianza en el tiempo de propagación en la red (paquetes cortos no son retrasados por paquetes largos en las colas de los conmutadores) y aumenta la velocidad de conmutación de los nodos. El tamaño de las celdas en ATM se escogió considerando los siguiente:

1. Si las celdas son muy pequeñas la eficiencia de la red es baja ya que la relación entre el tamaño de los campos de control y de la carga útil es muy grande.
2. Si las celdas son grandes el retardo de la propagación en la red aumenta debido a la espera en las filas de transmisión de los nodos de conmutación.
3. Para facilitar el manejo de las celdas en los conmutadores el tamaño de la carga debe ser una potencia de 2 o por lo menos un múltiplo de 4.
4. El encabezado debe ser capaz de identificar, mediante el VCI, a que canal pertenece cada celda para propósitos de enrutamiento y contener además otras informaciones de control.

Modos de transmisión. Existen tres métodos de transmisión de información, los cuales son:



Simplex: Se transmite en un solo sentido y los papeles de transmisor y receptor están fijos. Un ejemplo puede ser un timbre de una casa.

Semidúplex (Halfduplex): Se transmite en ambos sentidos, pero solo uno a la vez, es decir, los roles de transmisor y receptor cambian. Un ejemplo puede ser una conversación sin interrupciones de ninguna de las dos partes. Se utiliza un circuito de dos alambres para realizar la transmisión.

Dúplex (Fullduplex): Se transmite en ambos sentidos a la vez. Para transmitir en dúplex se necesita un circuito de cuatro alambres.

Modulación:

Es el proceso de cambiar algunas características de la señal portadora para transmitir una señal.

Existen cuatro métodos de modulación: por amplitud, frecuencia, fase y pulso.

a) Modulación en amplitud.

El voltaje de pico a pico de la señal portadora varía con la información que se requiere transmitir. Los picos de una amplitud representan unos binarios y los de la otra representan ceros. Este tipo de modulación es adecuada para la transmisión de datos y permite usar con eficiencia el ancho de banda disponible de una línea de voz, pero es un tanto susceptible al ruido.

b) Modulación en frecuencia.

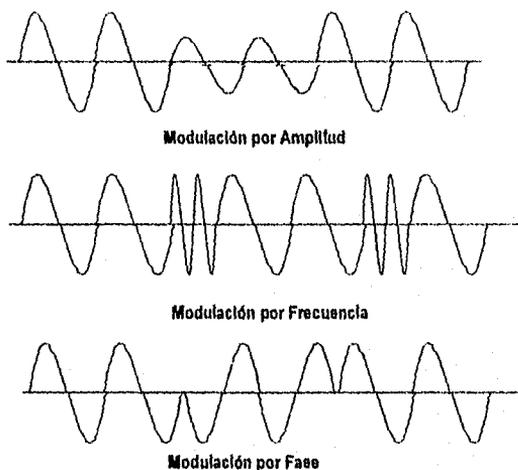
La señal portadora varía a distintas frecuencias dependiendo de la señal digital binaria, es decir, los 1's binarios tiene una frecuencia X y los 0's binarios tienen una frecuencia Y. Las frecuencias específicas utilizadas dependen del equipo receptor transmisor utilizado. Es la forma más común de modulación a velocidades de transmisión hasta de 1800 bps.

c) Modulación en fase.

En este tipo de modulación se presentan variaciones de fase en la portadora al presentarse un cambio en los binarios del mensaje, por lo que cuando cambia de 1 a 0 ó de 0 a 1 cambia la fase.

d) Modulación por codificación de pulsos (PCM).

Se emplea un impulso codificado para representar valores cuantizados de muestras instantáneas de la onda de señal, es decir, se muestrea una señal analógica continua en un flujo digital de bits.



Multiplexación:

Es combinar dos o mas señales dentro de un solo canal de comunicaciones, un multiplexor es transparente para el usuario, y N entradas producen N salidas. Existen diferentes tipos de multiplexión:

- **Por división de frecuencia.**

El espectro de frecuencias se divide en canales lógicos, es decir, en varias bandas de frecuencias más angostas, y cada usuario posee una banda dentro del espectro de frecuencias citado.

- **Por división de tiempo.**

Se asigna un canal sucesivamente a diferentes usuarios en turnos distintos, durante el cual tienen todo el ancho de banda disponible por un cierto período de tiempo.

Conmutador Privado (PBX).

Es un pequeño conmutador telefónico instalado en la oficina de un cliente para permitir la comunicación interna de una estación a otra dentro de las instalaciones del cliente y para conectar a las líneas de entrada y de salida.

Protocolo de comunicaciones.

Es un procedimiento de sincronización de manera que el receptor sepa cuando comienza y termina un bit para que pueda muestrearse, análogamente para la sincronización de caracteres de manera que el receptor pueda determinar qué bit pertenece a un carácter, y de forma parecida para la sincronización de mensajes de manera que el receptor pueda reconocer una sucesión especial de caracteres que forman los mensajes. Los protocolos típicos incluyen el bloqueaje de la transmisión en los mensajes, empleo de marcadores de principio y fin de texto o de otro tipo y algún procedimiento de reconocimiento positivo o negativo.

Protocolo X.25:

Es un protocolo para redes públicas conmutadas por paquetes de acceso o interfase entre el computador y la red específica. X.25 proporciona las funciones de control de flujo y errores, es decir, en él se definen los procedimientos que realizan el intercambio de datos entre dispositivos de usuario y un nodo de red encargado de manejar los paquetes. X.25 no incluye algoritmos de encaminamiento, los esquemas de encaminamiento estático o dinámico de paquetes se dejan a criterio de los fabricantes.

Protocolos TCP/IP (Transport Control Protocol/Internet Protocol):

La serie de protocolos TCP/IP define formatos y reglas para la transmisión y recepción de información independientemente del tipo de red o el hardware que se utilice, Esta serie de protocolos trabaja con base en paquetes, definiendo, el tamaño, tipo, origen, y destino, además de la forma en que las redes deben recibir y retransmitir paquetes cuantas veces sea necesario.

Red digital de servicios Integrados (RDSI o ISDN):

Dado que el sistema telefónico es insuficiente para las necesidades de comunicaciones actuales se generó este servicio, cuyo objetivo principal es la integración de los servicios de voz, con los de datos e imágenes. El CCITT se encarga de la coordinación internacional de ISDN. Se le considera un bus digital de bits, o bien, un conducto conceptual entre el usuario y el proveedor de servicios por el cual fluye la información. Este bus soporta varios canales a través de la multiplexión por división de tiempo. El acceso básico ofrece :

- Interfaz digital de 2 canales de tipo B a 64 Kbps para transmisión de voz o datos, por ejemplo la transportación de una conversación telefónica utilizando PCM (Modulación por impulsos codificados).
- Un canal D a 16 Kbps para la transmisión de información de control y señalización.

Este tipo de acceso ofrece al usuario una capacidad total de 144 Kbps. Los canales B y D se transmiten en tramas de 48 bits, que incluyen información de control, cada 250 seg. El multiplexaje de los canales sobre un enlace de 192 Kbps se realiza reservando cada canal y bits de control, posiciones especificadas en las tramas. Para las empresas que necesitan mayor capacidad de transmisión ISDN proporciona en su acceso primario 23 canales B y un canal D a 64 Kbps (23B+D).

Red digital de Servicios Integrados de Banda Ancha (B-RDSI o B-ISDN):

La Red Digital de Servicio Integrados de Banda ancha (Broadband-ISDN), es una extensión de ISDN en velocidades y servicios, cuyo objetivos es transportar de manera integral voz, datos y video en la misma red. los servicios que presta se agrupan en dos tipos:

1. Interactivos. En los que el intercambio de información, entre dos usuarios es bidireccional.
2. De distribución. En los que el intercambio de información es primordialmente unidireccional, de un prestador de servicios a los usuarios.

Los servicios interactivos incluyen servicios conversacionales de mensajería y de recuperación de información, mientras que los distribuidos se subdividen en servicios de difusión, en los que el usuario no tiene control sobre la presentación de la información que recibe, y servicios cíclicos que le permiten al usuario acceder a la información de manera selectiva.

Como ejemplos podemos citar videotelefonía, teleconferencia de banda ancha, vigilancia por vídeo, interconexión de redes locales, telefax de alta velocidad, transferencia de archivos voluminosos, correo electrónico con vídeo, acceso a bibliotecas, televisión de alta definición, etc.

Red de Computadoras:

Es un conjunto de ordenadores interconectados entre sí a través de uno ó más medios de transmisión de datos. Con la finalidad de transferir e intercambiar información.

Red SNA:

La arquitectura de red SNA identifica y define los posibles elementos dialogantes de una red y describe los protocolos que deben regir su diálogo. Tales protocolos consisten en unos formatos de información a intercambiar y las reglas a que deben atenerse los interlocutores, a fin de asegurar una transferencia eficaz, flexible y libre de errores, adaptada a su respectiva capacidad lógica. Ello implica, aparte de los ya mencionados formatos, unas funciones de establecimiento y terminación de diálogo, control de flujo de datos durante el mismo (en cuanto sentido, tamaño e intensidad), así como los necesarios procedimientos para detectar y recuperar cualquier tipo de error de transferencia, físico o lógico.

Esta arquitectura es absolutamente abstracta (es decir, independiente de productos y arquitecturas hard/software), y abierta, en continua evolución, a fin de adaptarse a lo que se va anticipando como factible y necesario dentro del binomio formado por el estado de la tecnología y las necesidades de los usuarios.

Al diseñar un nuevo producto para ser conectado a una red SNA, el diseñador debe seleccionar dentro de la arquitectura, cuál es la misión que va a cumplir en la red el subconjunto de funciones

que ello implica, ejecutándolas a continuación mediante programación o microcódigo, según la arquitectura y posibilidades de la propia máquina o subsistema que está desarrollando.

Existen elementos NAU (unidad direccionable de red), los cuales son un software a través del cual se utiliza la red, se dividen en las tres categorías siguientes:

- **LU: Logic Unit.** Son el elemento básico dialogante de la red, es decir, son la puerta de acceso a la red, pueden ser programas de aplicación u operadores de terminales (usuarios finales).
- **PU: Physical Unit.** Este nodo dispone de un nodo adicional de control, con capacidad de gestionar sus propios recursos (tales como línea(s) de comunicaciones), ayudar a sus LU en el establecimiento de nuevas sesiones y restaurarlas en caso de que sea necesario. Las PU se diferencian principalmente de las LU por la inexistencia de interfaces con el usuario final.
- **SSCP: System Services Control Point.** Controla todos los nodos lógicos (PU y LU), reside en el nodo físico principal del mismo ("Host"). Ese control lo ejerce mediante una serie de comandos diseñados para ese fin y que el mismo SSCP intercambia con los PU y LU a través de sesiones de modo continuo y que son prerequisites para el establecimiento de sesiones entre LUs.

Dependiendo de las agrupaciones de los elementos mencionados anteriormente, existen las categorías de nodos físicos siguientes:

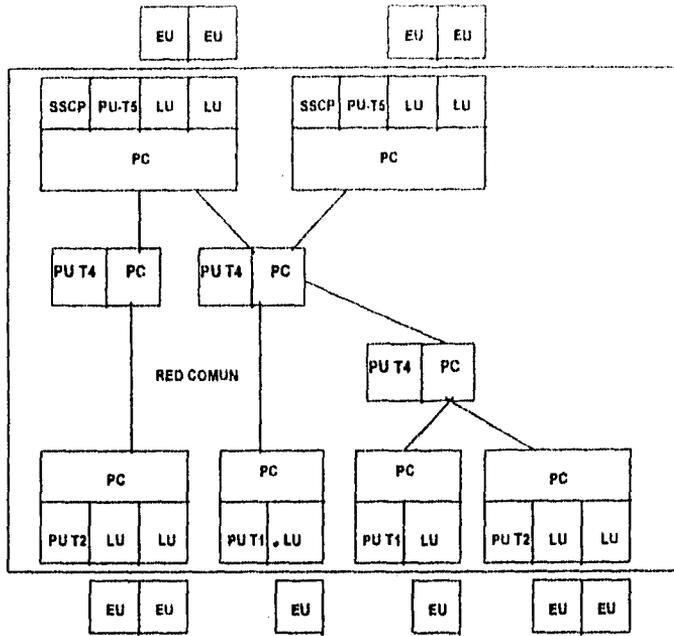
- a) **Host (PU tipo 5):** Contiene un SSCP, una PU y un número variable de LUs generalmente asociados a otros tantos programas de aplicación.
- b) **Procesador frontal o controlador de comunicaciones (PU tipo 4).** Constituye un nodo intermedio de la red, su misión principal es el control simultáneo de múltiples recursos de comunicaciones, para lo cual solo requiere de una PU.

- c) Cluster de terminales (PU tipo 2). Contiene una PU y una LU para cada usuario final que lo comparte. Si el cluster es "inteligente", estos usuarios finales pueden ser programas de aplicación que a su vez controlan dispositivos (discos, teclados, etc.), de forma externa a la arquitectura.
- d) Terminal (PU tipo 1). Generalmente asimilado a una terminal no inteligente monoestación, en tal caso contiene una PU y una LU.

Esta red tiene esta formada por capas, aunque no corresponde exactamente a las capas del modelo OSI, hay gran similitud.

Los diferentes sesiones que puede establecerse en SNA son las siguientes:

1. SSCP - SSCP: Se utiliza para el control entredominios y gestión de mensajes
2. SSCP - PU: Sirve para permitir que el SSCP, inicie, controle y pare a las PU.
3. SSCP - LU: Cede el control a las LU para manejar sesiones.
4. LU - LU: Se transmiten los datos del usuario, comunicación entre usuarios.
5. PU - PU: Control o administración de redes



Ejemplo de una Estructura de Red SNA

Synchronous Data Link Control (SDLC)

Es una norma para administrar la transferencia de datos a través de las líneas de comunicación de datos. Se encarga de la sincronización, el transmisor debe trabajar alineado con el receptor, controla y detecta los errores de transmisión, además controla la transmisión y recepción entre estaciones, y por último da aviso de procedimientos de control inapropiados en la cadena de datos.

Software Aplicativo: Conjunto de Programas de las aplicaciones, bajo los cuales tiene interacción el usuario final con los datos.

Software Operativo: Incluye los programas del sistema operativo, así como los programas de operación de cada componente en hardware.

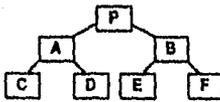
Topología de red:

Es la conectividad física de la red y se debe de considerar los siguientes objetivos:

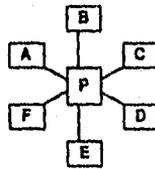
- Proporcionar la seguridad de la transmisión correcta de los datos (sin errores).
- Utilizar la ruta óptima entre el transmisor y el receptor (se debe evaluar el aspecto económico y el de integridad en los datos).
- Garantizar al usuario final un tiempo de respuesta conveniente.

Existen diversos tipos de topologías, como son: árbol, bus, estrella, anillo, malla.

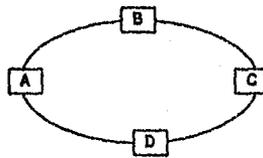
Topología de Árbol



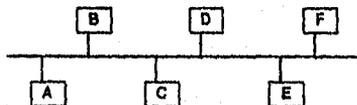
Topología de Estrella



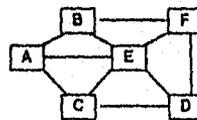
Topología de Anillo



Topología de Bus



Topología de Malla



Topología de árbol.

Su estructura parece la de un árbol, puesto que las ramas van generándose desde el nivel más alto hasta el más bajo. El nodo más alto es el concentrador de las tareas de control y resolución de errores, tiene el control de la red.

Puede tener un carácter de distribuidor, debido a que los nodos subordinados podrían controlar a los nodos que sean inferiores a éste.

- **Ventajas:**

- Fácil de controlar.

- **Desventajas:**

- Si el nodo principal falla, la red no podrá dar servicio a los demás nodos.
- Se generan cuellos de botella en los niveles superiores.
- Insuficiente delegación de responsabilidades.

Topología de bus.

Consiste de una línea troncal a la cual están conectados todos los nodos. La señal viaja en ambas direcciones del cableado y es terminada en los extremos por medio de una resistencia. Todas las estaciones reciben todas las transmisiones ya que existe un solo canal de comunicaciones para todos los dispositivos. Su ventaja principal es que el flujo de tráfico de datos es fácil de controlar.

Para evitar que una avería en el canal de comunicaciones, se pueden tomar las siguientes medidas:

- Contar con un canal redundante.
- Un conmutador que rodee un nodo en caso de falla.

Topología de Estrella.

Consta de un nodo central al cual están conectados los demás nodos que forman la red. El nodo central tiene las siguientes funciones: Contiene el software, controla el flujo de datos por lo tanto todas las terminales dependen de él, localiza las fallas en los equipos. Esta topología tiene una capacidad de procesamiento distribuido limitada.

Topología de Anillo.

Los nodos están conectados por una línea de comunicación formando un anillo o círculo. La señal viaja en una dirección y no requiere de terminadores ya que los nodos son los encargados de depurar la información que viaja por la línea. Actualmente esta topología a dado origen a otras como son el anillo modificado o anillo doble "híbrido".

Topología de Malla.

Todos los nodos están conectados a dos o mas nodos, por lo que es menos probable que presente problemas de embotellamiento y averías, dado que existe una multiplicidad de caminos, lo que garantiza que se tengan varias trayectorias alternas en caso de falla u ocupación de un camino.

Transmisión Asíncrona.

El transmisor puede transmitir un caracter en cualquier momento y el dispositivo receptor lo acepta. Los intervalos de tiempo no son importantes, lo que se requiere es que cada caracter (8 bits) tengan un bit de arranque que le precede y uno o dos de parada que siguen a los bits de datos. El bit de arranque avisa al receptor que tiene información, debe tomar tiempo para realizar funciones de sincronismo antes de que llegue el siguiente byte, el bit de parada le indica que el caracter termino, que ya esta listo para esperar la transmisión de otro dato.

Transmisión síncrona.

Este tipo de transmisión establece y mantiene la sincronización cuando la línea no está transmitiendo señales, al pasar un grupo de bytes de sincronización entre los dispositivos transmisor y receptor. La transmisión síncrona es más eficiente debido a que hay menos bits de control, en relacion a los bits transmitidos.

Virtual Telecommunication Access Method (VTAM):

Es un software de comunicaciones que administra los accesos a una red SNA. Dirige la transmisión de datos entre los programas de aplicación en el Host y los componentes de la red de comunicación de datos. Los servicios básicos que realiza VTAM incluyen establecer, controlar y terminar el acceso de entre los programas de aplicación y las terminales. Mueve los datos entre los programas de aplicación y las terminales y permite que los programas de aplicación compartan las líneas de comunicaciones, controladores de comunicaciones y terminales, VTAM controla la configuración de la red de telecomunicaciones y permite que ésta sea supervisada y alterada.

Bibliografía.

Tanenbaum Andrew

Redes de ordenadores

Ed. Prentice Hall, 2a. Edición.

FitzGerald Jerry

Fundamento se conmutación de datos.

De. Limusa, 1a. Edición.

Alabau Muñoz Antonio.

Teleinformática y redes de computadoras

Ed. Marcombo, 2a. Edición.

Black Uyles

Redes de computadoras

Ed. Macrobít. 1a. Edición.