**IPN**
**ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA**
**UNIDAD CULHUACAN**

**TESIS INDIVIDUAL**

Que como prueba escrita de su Examen Profesional para obtener el Título de **INGENIERO EN COMUNICACIONES Y ELECTRÓNICA** deberá desarrollar el C.:

**LUIS MANUEL AVELAR ALFEREZ**

**"METODOLOGÍA DE PLANES DE RECUPERACIÓN EN CASO DE DESASTRES PARA EL SECTOR FINANCIERO MEXICANO".**

Durante los últimos 30 años en la Industria de Servicios Financieros (Bancos y Casa de Bolsa), surgió la necesidad de mantener el mayor tiempo posible activa la capacidad tecnológica de procesamiento de información, con la finalidad de ofrecer a su amplia gama de clientes, la disponibilidad de los servicios financieros, a través de los canales de entrega que se tienen establecidos, tales como: Red de Sucursales Bancarias, Cajeros Automáticos y en los últimos 16 años, la Banca Electrónica o en línea tanto para empresas como para individuos. Esta capacidad puede verse afectado derivado de: desastres naturales, desastres informáticos (usualmente por hackers, virus informáticos), violaciones de Seguridad, fallas críticas de infraestructura de cómputo y comunicaciones.
Con finalidad de lograr la más alta disponibilidad de la infraestructura de cómputo, las empresas Financieras y todo tipo de industrias, se han enfocado en minimizar el impacto en su infraestructura, ante los desastres mencionados.
El objetivo de este trabajo, plantea la metodología para el diseño de los Planes de Recuperación de la Infraestructura Tecnológica, en el menor tiempo posible y con la menor pérdida de datos, permitiendo la continuidad del negocio de una empresa.

**Capitulado:**
**CAPÍTULO 1. ESTADO DEL ARTE**
**CAPÍTULO 2. MARCO TEÓRICO**
**CAPÍTULO 3. DISEÑO IMPLEMENTACIÓN**
**CAPÍTULO 4. PRUEBAS Y RESULTADOS**
**CONCLUSIONES**

Ciudad de México a 02de agosto del 2016

**ING. CELEDONIO ENRIQUE AGUILAR MEZA**
**PRIMER ASESOR**

**ING. CARLOS AQUINO RUIZ**
**SEGUNDO ASESOR**

**ING. FELICIANO PRIMO ISIDRO CRUZ**
**JEFE DE LA CARRERA DE I.C.E.**

**ING. JUAN MANUEL VELAZQUEZ PETO**

# INSTITUTO POLITÉCNICO NACIONAL

**ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA**

**UNIDAD CULHUACAN**

# Metodología de Planes de Recuperación en Caso de Desastres para el Sector Financiero Mexicano

**T E S I S**

**QUE PARA OBTENER EL TÍTULO DE**

**INGENIERO EN COMUNICACIONES Y ELECTRÓNICA**

**PRESENTA:**

**Luis Manuel Avelar Alférez**

**ASESORES**

**Ing. Celedonio Enrique Aguilar Meza.**
**Ing. Carlos Aquino Ruiz.**

**Ciudad de México, Agosto 2017.**

Dedicatoria

A mi Mamá, María Antonia Alférez, que seguramente está al tanto de mi vida.

A mis hermanos; José, Martha, Adela y Marcos, que siempre los he tenido a mi lado en los momentos importantes.

A mi esposa Gaby e hijos; Bere, Luis, Mauricio y Diego, por ser parte de las motivaciones de esta existencia.

Y gracias a las personas que han influido en mí para llegar a ser lo que soy.

Luis Manuel

# Índice

# Capítulo 1.

## Estado de Arte

# **Introducción**.

En el presente capitulo, se expondrán los antecedentes que han dado orígen a las metodologías y aplicación de los avances en tecnologías de la información para responder ante desastres, ya sea naturales o de tipo informático que ponen en riesgo a todo tipo de industrias, tanto las financieras, como las de manufactura, comunicaciones, la industria conocida como retail (cadenas de Almacenes) y en general a todo tipo de industria o sector que basa la operación de su negocio, en sistemas informáticos soportados por infraestructura tecnológica y que ante una circunstancia de ese tipo, sus Centos de Datos quedan afectados total o parcialmente, provocando la suspensión de los servicios de información y afectando la actividad comercial, financera o en la producción de los bienes y servicios que consume la sociedad.

Los escenarios que cubrirá el presente planteamiento , esta orientado a la pérdedida de la capacidad de procesamiento, como consecuencia de un desastre natural (principalmente derivadio de un sismo) ó bien por fallas tecnológicas mayores que  inmpidan la continuidad de la operación de los negocios.

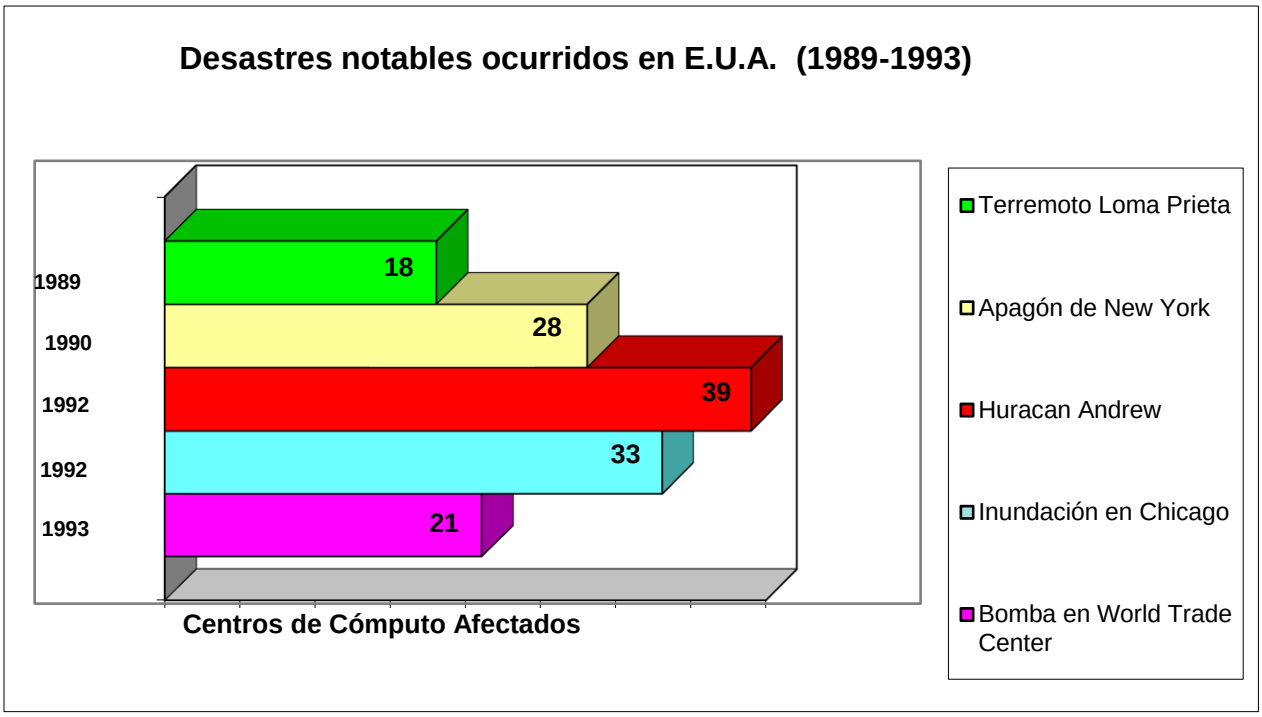
Derivado de los daños que han provocado dichos desastres, ha surgido toda un disciplina en el ámbito de las Tecnologías de la Información (TI), misma que ha venido desarrollándose, sobre todo con mayor rápidez en los Estados Unidos de América (USA), durante este capítulo haremos referencia a información estadística de éste país e información referida en periódicos y fotografías de la afrectación que sufrio nuestra ciudad de México, durante el temblor del año de 1985, que afectó varias industrias pero desafortundamente, no hay meterial estadístico disponible para saber el impacto en las diferentes industris afectadas.

## 1.1 Información Estadística en los Estados Unidos de Norteamérica.

La información estadística presentada en este documento y que cita los desastres ocurrridos en las decadas de los 80's y 90's en Estados Unidos de América, muestra el nivel de impacto de este tipo de eventos, se presentan estos datos de nuestro vecino del norte.

La información refleja los desastres que mayor impacto tuvieron en USA y que se tienen registrados formalmente, la empresa americana que recabó ésta información se llamaba SUNGARD, actualmente su nombre es: SUNGARD Availability Services[1].

En la gráfica 1.1, se pueden apreciar los desastres más notables ocurridos en el perído de 1989 a 1993 en Estados Unidos de Norteamérica y que tuvieron impacto en Centros de Cómputo afectados. Estos desastres impulsan la necesidad de crear Planes de Contingencia que incluyan la recuperación de Centros de Cómputo en otros sitios y para ello ofrecen sus servicios de Centro de Computos de Recuperación empresas como SUNGARD Availability Servicos, IBM, HP, como las más destacadas.



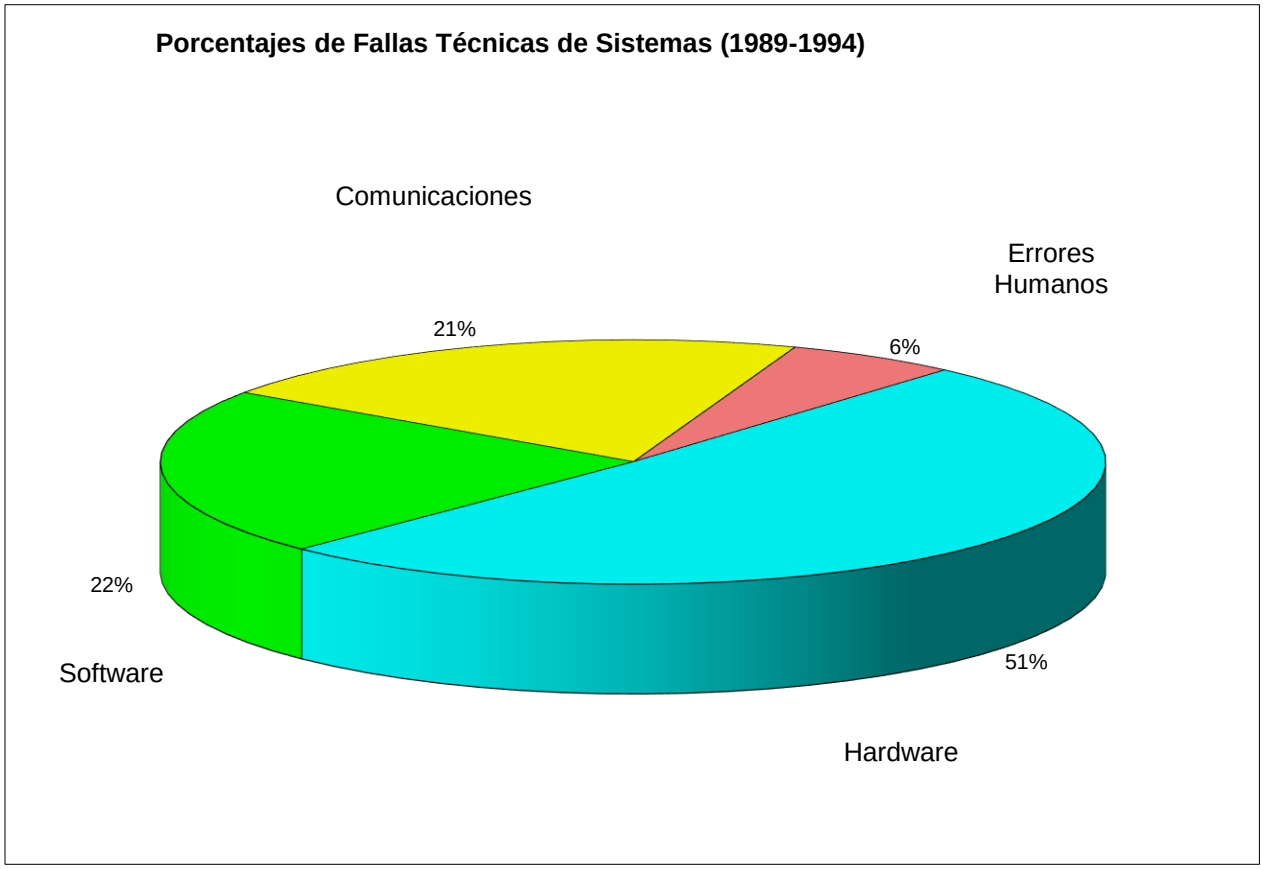

**Gráfica 1.1. Desastres Notables en Estados Unidos de Norteamérica.**

Pero no solamente los desastres naturales pueden afectar la continuidad de los servicios de cómputo e información, también fallas de tipo tecnológico como por ejemplo fallas de: Hardware,

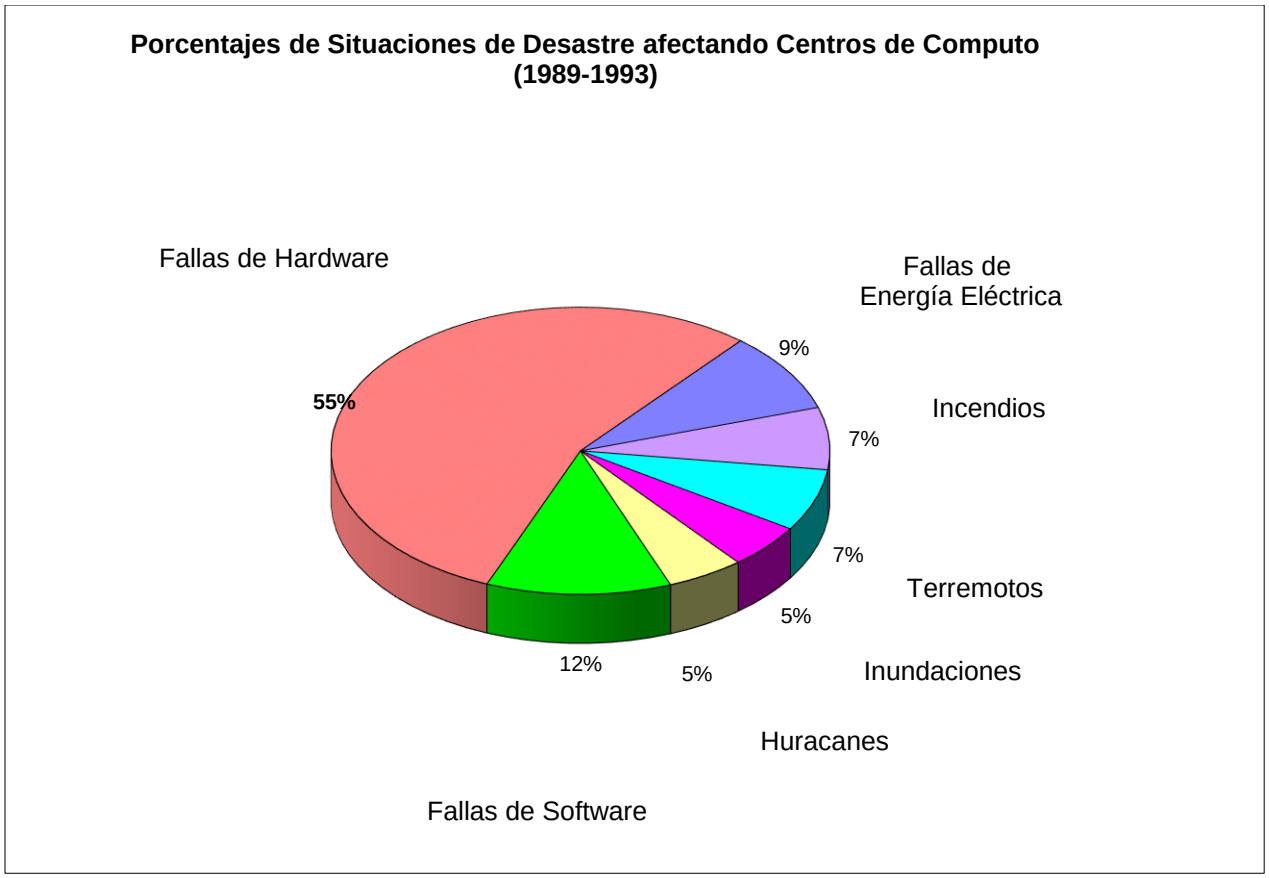
[1] **Trademark information**

Software, Comunicaciones, errores humanos y más recientemente fallas de Seguridad que permiten la infección por virus, hackeo, malware, etc.

En la gráfica 1.2, se muestra el porcentaje de fallas tecnológicas de los servicios de cómputo y en la gráfica 1.3, se muestra un comparativo porcentual entre desastres naturales y fallas tecnológicas, como se puede apreciar las fallas de tipo tecniológico son más frecuentes que los desastres naturales, ya que estos últimos son aleatorios y las fallas tecnológicas son más frecuentes derivado de varios factores como por ejemplo: desgaste de equipos, inadecuada configuración, errores humanos durante su operación, fallas en el diseño de la arquitectura de los equipos, fallas de software, huecos en la configuración de seguridad de las redes, firewalls, sitios de Internet sin adecuada seguridad, etc.




**Gráfica 1.2. Distribución de Fallas Tecnológicas.**




**Gráfica 1.3. Comparativo porcentual de fallas Tecnológicas y Desastres Naturales.**

## 1.2 Información Estadística en México.

Cabe señalar que en esas fechas en México no se contaba con estadísticas de ningún tipo y en la actualidad, tampoco existe información certera y documentada sobre el impacto de desastres naturales e informáticos en nuestro país, al visitar la página del INEGI, no se obtuvo información estadística en este sentido.

Como parte de la información periodística que se pudo obtener, ya que existe muy poca documentación en México al respecto del impacto de desastres naturales e informáticos en las décadas pasadas, en la fotos (figura 1.1 a la 1.3), mostradas a continuación, se puede apreciar el daño causado por el terremoto:

**Figura 1.1: Destrucción Edificio en Tlatelolco, en el sismo de 1985.**

**Fuente: Fundación UNAM**

**Figura 1.2: Destrucción de Edificio en Tlatelolco en el sismo de 1985.**

**Fuente: Fundación UNAM**

**Figura 1.3.: Edificio Nuevo León en Tlatelolco, destrozado por el sismo de 1985.**

**Fuente Fundación UNAM**

A continuación se citan algunos datos de la estimación de daños oficial:

- Resultaron con algún tipo de daño **(parcial o total)** alrededor de **70 mil estructuras**.
- Quedaron **destruidos o afectados más de 85 mil metros cuadrados de banquetas públicas**.
- Resultaron **afectadas más de 30 estaciones del Sistema de Transporte Colectivo Metro**.
- Se estima que se perdieron aproximadamente **2000 mil empleos a causa del terremoto** pero pudieron ser más, no se tiene datos muy concretos al respecto.[2]

## 1.3 Planes de Contingencia tecnológica en otros Paises.

Es díficil contar con información espécifica de Planes de Contingencia Tecnológica en otros países y en México, pues no es información que las empresas publiquen, derivado de sus políticas de seguridad y confidencialidad, sin embargo, en las búsquedas realizadas, encontramos un Plan de continuidad del Negocio, de una empresa Española que fabrica calzado, que muestra en una Infografía muy sencilla y resumida, las fases de su plan de Continuidad del Negocio, ver figura 1.4, cabe señalar que esta metodología se desarrolló en la última década del siglo XX.

[2] Fuentes: http://www.dfinitivo.com/archivos/2007/09/19/terremoto-de-1985-a-22-anos-de-la-pesadilla/

http://www.taringa.net/posts/videos/793741/El-Gran-Terremoto-de-Mexico-1985.html

http://www.esmas.com/noticierostelevisa/terremoto/475688.html

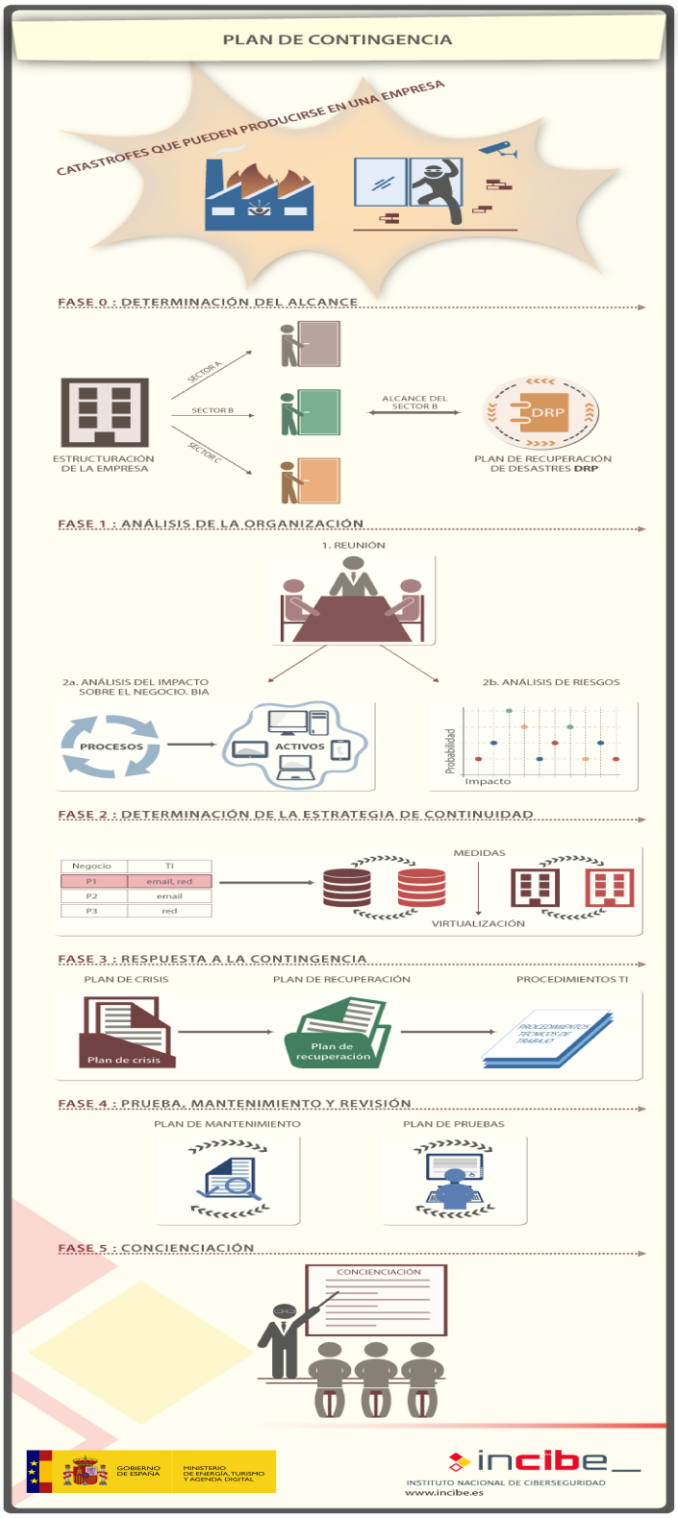



**Figura 1.4: Infografía de Plan de Continuidad del Negocio[3]**

[3] **Fuente: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio**

En dicha Infografía, se pueden observar las principales fases de su BCP[4] (Business Continuity Plan), que incluyen:

1. **Fase 0**: Determinación del Alcance: Las amenazas de desastres que pueden producirse en una Empresa (de cualquier tipo de productos y/o servicios).
2. **Fase 1:** Análisis de la Organización, desarrollo del Análisis de Impacto al Negocio (BIA) y análisis de riesgos.
3. **Fase 2:** Determinación de la Estrategia de Continuidad, replicación de Datos, Centro de Datos Alterno.
4. **Fase 3:** Respuesta a la Contingencia, Plan de Crisis, Plan de Recuperación, Procedimientos de TI
5. **Fase 4:** Prueba, mantenimiento y revisión.
6. **Fase 5:** Concientización.

En general, las Fases que definieron en esta empresa Española, se encuentran alineados a la mayoría de las metodologías de Planes de Conitnuidad del Negocio y DRP, usadas a nivel global.

Es relevante aclarar que durante el desarrollo del presente trabajo, se describirá la metodología que determinó la empresa Fianciera (Institución Bancaria) Mexicana, en la cual se basa este caso de tesis para el diseño de su Plan de Continuidad del Negocio y DRP, mismo que básicamente incluye fases similares al ejemplo descrito de la citada empresa Española.

## 1.4 Planes de Contingencia tecnológica en México

En la década de los 80's, cuando se presentó el terremoto en México, la gran mayoría de las empresas **no contaba con metodologías de Continuidad del Negocio**, no existía esa disciplina en las áreas de Sistemas, precisamente, surge la necesidad de desarrollarlas e investigar en otros países, sobre todo en USA, dada la cercanía de ese país y de la presencia en México de Compañías de Tecnología de gran renombre, como: IBM, HP, etc..

Considerando el antecedente citado, la mayoría de las empresas durante el terremoto, improvisaron planes de emergencia en ese momento pero recordemos el entorno tecnológico de aquella época:

[4] **BCP: Por sus siglas en Ingles: Business Continuity Plan: Plan de Continuidad del Negocio.**

- No existía el **Internet**, todos los enlaces se hacían vía Modem[5], con velocidades muy bajas (velocidades entre 9.6 Kbits/seg a 56.6 Kbits/seg, que al día de hoy son irrisorias) y a través de línea telefónica analógica
- No se usaba comercialmente el protocolo TCP/IP
- Las redes de datos que se usaban, la mayoría estaba basada en la arquitectura diseñada por la compañía IBM, llamada SNA[6]
- La única compañía en México que ofrecía servicios de Telecomunicaciones, era Teléfonos de México que en aquel momento, estaba en manos del Estado Mexicano.
- No existían las Computadoras Personales
- Las comunicaciones satelitales para uso comercial estaban iniciando, los Bancos, fueron de las primeras empresas que implementaron enlaces satelitales en aquellos años pero siempre se contaba con líneas de respaldo vía terrestre por las fallas que en aquellas épocas, presentaban los enlaces satelitales, todavía podemos recordar aquellas antenas parabólicas enormes que algunos Bancos tenían a unos metros de su Centro de Cómputo

Ese era el entorno tecnológico a groso modo, bajo esa situación y dado que el **escenario de desastre** que se enfrentó en ese momento, fue el siguiente:

- Algunas zonas de la ciudad, tuvieron interrupción del suministro eléctrico por varios días, esto afectó al Centro de Datos del banco a que hacemos referencia en este trabajo
- Líneas telefónicas dañadas en varias partes de la ciudad
- Algunas sucursales bancarias, estaban incomunicadas pues no tenían energía eléctrica y/o tenían fallas de comunicaciones
- Las comunicaciones hacia algunas ciudades del estado de Guerrero tuvieron fallas (recordemos que en el sismo de 1985, su epicentro se ubicó en las costas de Guerrero)

este Banco en particular, tuvo ese tipo de problemas por lo cual, se implementó de manera improvisada un **Plan de Emergencia** que consistió en las siguientes tareas, descritas de manera general:

1. Se reunieron los Directores de Áreas de Negocio con el Director de Sistemas para evaluar los daños en; el Centro de Cómputo, en los Centros de Procesamiento Remotos, en la oficinas y sucursales bancarias de las principales ciudades del estado de Guerrero y del DF y para determinar las acciones del **Plan de Emergencia**
2. Una vez identificado el impacto, se defienieron tareas específicas
3. Se solicitó suministro adicional de combustible Diesel para mantener permanentemente funcionando la planta de Emergencia del Centro de Datos, (se operó de esa manera durante 20

[5] **Modem**: acrónimo que significa **Mo**dulador **Dem**odulador
[6] **SNA: por sus siglas en Ingles: System Network Architecture, Arquitectura de Redes de Sistemas**

días posteriores al terremoto), con la finalidad de no tener interrupciones en el procesamiento de información

4. Se establecieron negociaciones con Teléfonos de México para que se proporcionaran líneas de comunicación alternas hacia las localidades efectadas, tanto en el DF (hoy Ciudad de México), como en las ciudades del estado de Guerrero en donde se tuvieron daños en Centros de Procesamiento Remotos
5. Se llevaron plantas de emergencia móviles, a las sucursales bancarias que no tenían suministro eléctrico para que pudieran operar sus equipos de comunicaciones y mantener funcionando los sistemas en línea que se tenian en aquella época en las ventanillas de las sucursales
6. En aquellas sucursales que no tenían comunicaciones, se cerraron y se le solicitó a la clientela que se dirigieran a la sucursal más cercana que contaba con energía eléctrica y con comunicaciones para que realizaran sus operaciones bancarias
7. A los proveedores de Hardware, se les solicitó personal técnico permanente en el Centro de Datos para atender cualquier falla que se presentara en ese momento y poder mantener la continuidad de la operación del Centro de Cómputo
8. Se hicieron compras de emergencia de equipos de comunicaciones y terminales (no existían las PCs) de los sistemas en línea para reemplazar los equipos dañados en las sucursales afectadas
9. Las actividades de emergencia se fueron cerrando conforme se restablecieron las comunicaciones y el suministro eléctrico, hasta llegar a la normalidad

Derivado de éste aprendizaje vivido durante ese desastre, las grandes empresas de Tecnología, fueron desarrollando metodología y tecnología que a lo largo de las décadas siguientes, han llegado a un grado de evolución que en la actualidad, permite tener Infraestructura Tecnológica alterna, permanentemente replicada para minimizar la afectación del negocio, logrando reducir el impacto a unas cuantas horas, en lugar de semanas o meses.

El presente trabajo, esta orientado a describir la metodología y las características de la infraestructura tecnológica de esta empresa Bancaria que soportan su Plan de Contingencia DRP para permitir la continuidad del negocio.

# Capítulo 2.

## Marco Teórico

# Introducción

Durante el presente Capítulo se definirán los indicadores que Internacionalmente son considerados para la determinación cuantitativa del tiempo de recuperación de la Infraestructura Tecnológica en caso de un desastre natural o tecnológico, así cómo el tiempo de recuperación de los datos o punto en el tiempo en el cual se recupera la información almacenada en el Storage del Centro de Datos Primario o Principal, lo anterior se logrará basado en el desarrollo del Análisis de Impacto al Negocio (conocido en Ingles por el acrónimo BIA[1], el cual nos permitirá conocer la visión y opinión del personal Directivo de la Empresa, sobre el tiempo máximo que podrían operar, sin tener acceso a los sistemas aplicativos que soportan los servicios financieros que ofrece cada área de Negocio a la cliente de Empresa. Esta visión de negocio alineada por el marco teórico que ofrece el proceso del BIA y la derivación de los indicadores llamados RTO[2] y RPO[3], nos permitirán definir los escenarios de recuperación y de allí derivar el Plan de Recuperación en Casos de Desastre con todas sus componentes.

**[1] BIA: por sus siglas en Ingles; Business Impact Analysis; Análisis de Impacto al Negocio.**

**[2] RTO: por sus siglas en Ingles: Recovery Time Objective; Tiempo Objetivo de Recuperación**

**3 RPO: por sus siglas en Ingles: Recovery Point Objective; Objetivo del Punto de Recuperación**

## 2.1 Análisis de Impacto al Negocio (Business Impact Analysis BIA[4]).

Se establecerán los criterios de negocio para definir las estrategias de recuperación, dichos criterios los derterminarán los indicadores siguientes:

- Impacto que recibirá el negocio en caso de una contingencia, en términos; fiancieros, reputacionales, faltas regulatorias, pérdida de posicionamiento en el mercado financiero e imagen ante su clientela
- Intervalo de Tiempo máximo que el negocio puede estar sin operar con un impacto financiero mínimo
- Intervalo de Tiempo máximo de pérdida de datos, sin que afecte la operación y a sus clientes

Para lograr identificar esos indicadores, se requiere como primer paso, desarrollar el "Análisis de Impacto al Negocio", la metodología del análisis, permitirá cuantificar las pérdidas financieras y proporcionará los elementos necesarios para esteblecer las estratregias de recuperación que le permitirán a la empresa, volver a operar de manera rápida, efectiva, con un mínimo de pérdida de información (datos) y en el lapso de tiempo que resulte del análisis citado.

## 2.2 RTO y RPO.

Para definir el **RTO** [5]y **RPO** [6] que una empresa financiera deberá seleccionar para mitigar el impacto causado por un desastre natural y/o tecnológico que impacte directamente en la continuidad del la operación del negocio y por consecuencia tenga repercusiones de pérdidas económicas severas que podrían poner en riesgo la sobrevivencia de la empresa y que deberán incluirse en el **DR Plan** (**DRP** [7]por sus siglas en Ingles) el proceso para elegirlo más usado y alineado a las mejores práticas internacionales, está basado en el **Análisis de Impacto al Negocio** (**BIA** [8] por sus siglas en Ingles).

Antes de avanzar y explicar el proceso para el desarrollo del **BIA**, es conveniente citar las definiciones de RTO y RPO:

**RTO (Recovery Time Objetive), Tiempo de Recuperación Objetivo**: es el intervalo de tiempo que transcurre, **una vez sucedido el desastre** para recuperar ó reanudar los

[4] BIA: por sus siglas en Ingles Business Impact Analysis; Análisis de Impacto al Negocio
[5] RTO: Recovery Time Objective; Tiempo Objetivo de Recuperación
[6] RPO: Recovery Point Objective; Objetivo del Punto de Recuperación
[7] DRP: Disaster Recovery Plan; Plan de Recuperación en Casos de Desastre
[8] BIA: Business Impact Analysis

servicios de la empresa, lógicamente para ello, es necesario que dentro de ése intervalo de tiempo, **se recupera la Infraestructura tecnológica y las aplicaciones** que soportan los servicios de la empresa.

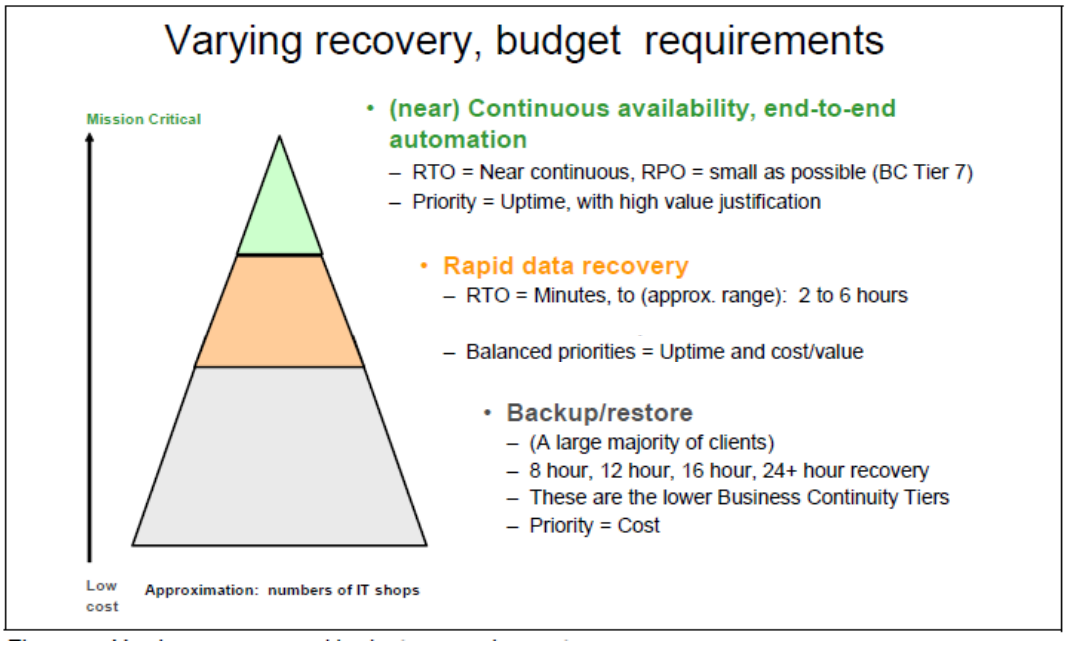
**RPO (Recovery Point Objective), Punto Objetivo de Recuperación**: Es el punto en el tiempo, en el cual se esteblece la "frescura" de los datos que deben ser restaurados, es decir, una vez sucedido el desastre, es la pérdida "aceptable" de datos a partir de la cual se reinician las operaciones, este punto puede ser desde minutos, horas ó días, eso dependerá de la estrategia que se determine como copiado de información para uso en caso de desastre ó contingencia.

Evidentemente, mientras más bajo sea el tiempo de pérdida de datos, es mejor el **RPO** y mientras más bajo sea el **RTO**, más rápido se recupera la infraestructura de cómputo y se minimiza el riesgo de pérdidas financieras de la empresa, sin embargo, un factor adicional importante que interviene en la elección del RPO y RTO, es el presupuesto que la empresa está dispuesta a proporcionar para implementar la infraestructura tecnológica para lograr el RTO y RPO resultado del BIA, básicamente existen en la industria 3 tipos de niveles de RTO y RPO:

- **Backup / Restore (Respaldo / Restauración):** en este tipo de recuperación de la infraestructura tecnológica, conlleva intervalos de tiempo de: 8, 12, 16 y 24 o más horas para restaurar la información, desde dispositivos magnéticos conocidos como Cartuchos tipo (LTO1,LTO2,LTO3….LTO7[9]), este es un tipo bajo de continuidada de negocio, la prioridad para la empresa es mantener un costo bajo de recuperación, no es usado por empresas financieras y/o casas de Bolsa.
- **Rapid Data Recovery (Recuperación de Datos Rápida):** el RTO esta en el rango de 2 a 6 horas como máximo, en este tipo de recuperación la prioridad la tiene el balance entre recuperar el servicio y el costo.
- **Continues Availability, end to end Automation (Disponibilidad Continua, automatización punta a punta):** en este tipo de recuperación la prioridad la tiene, la persistencia del servicio con la justificando su alto valor.

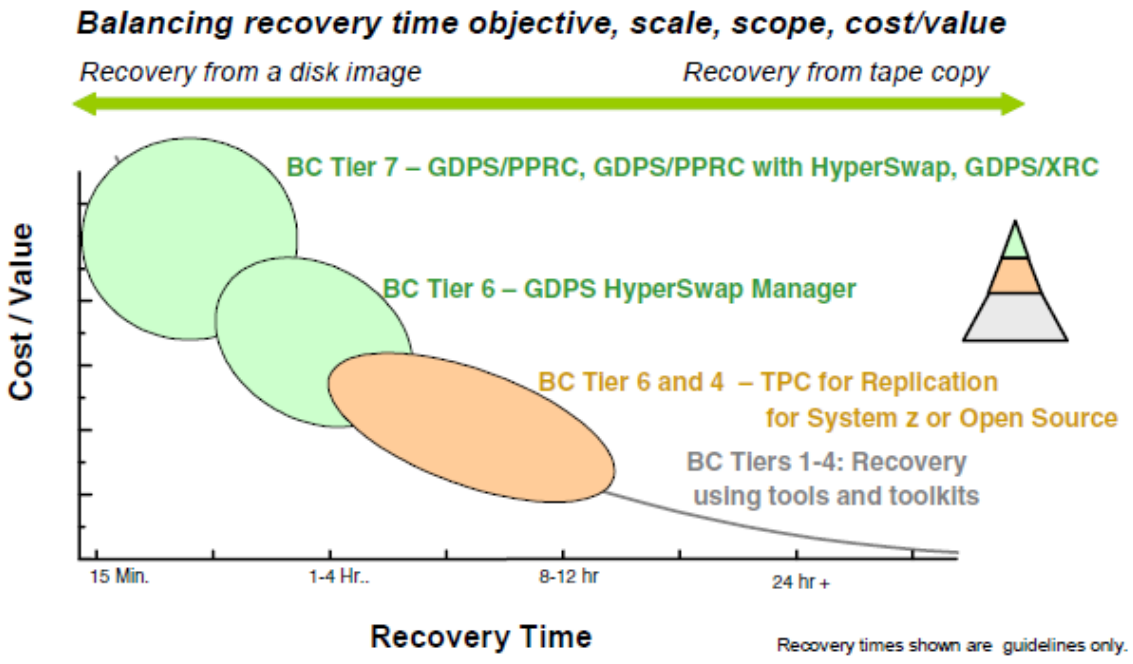
El BIA nos permitirá justificar la selección de cualesquiera de esos 3 tipos, como se muestra en la **gráfica 2.1** citada a continuación:

[9] LTO: Linear Tape Open por sus siglas en Ingles, almacenamiento de datos en cinta magnética, esta tecnología fue desarrollado a finales de la década de los 90's, del siglo XX).




**Gráfica 2.1**[10]

En la gráfica 2.2 se puede observar la relación costo / RTO – RPO:




**Gráfica 2.2**[11]

[10] [10] Fuente: IBM System Storage FlashCopy Manager and PPRC Manager Overview.
[11] Fuente: IBM System Storage FlashCopy Manager and PPRC Manager Overview.

Considerando la clasificación anterior, misma que es usada como Best Practice (Mejor Práctica en la industri de TI), se pueden establecer los escenarios de recuperación.

En la gráfica 2.1, se muestra la relación existente, entre el tiempo de recuperación, los servicios de misión crítica, así como el costo, podemos observar que entre más horas dure el tiempo de recuperación de la infraestructura (RTO), es más bajo el costo, lo anterior a que se utilizaría la técnica de BackUP/ Restore; es decir se usarían los Respaldos en cinta ó cartucho, tanto del sistema operativo como de los sistemas aplicativos y bases de datos, para llevara cabo la recpueración de la infraestructura y los datos, lo que usualmente demora entre **8 a 12 horas para activar la infraestrucutra** y para la frescura de los datos, usualmente, ésta se **encuentra entre las 24 a 72 horas,** ya que usualmente se usan los respaldos que se logran recuperar de la Bóveda externa (asumiendo que el Centro de Datos Pimario, se encuentra dañado), dichos respaldos normalmente se trasladan a la Bóveda un dia después de haber sido concluidos. La gráfica nos indica que dichos tiempos de RTO y RPO, son de prioridad baja, que normalmente no aplican para empresas financieras.

En la gráfica 2.2, se muestra básicamente lo mismo, sin embargo, en ella la diferencia consiste en que para reducir dramáticamente el RTO y por consecuencia el RPO, se logra bajo esquemas de replicación de datos (Storage), que son más costosos y que estan sustentados en tecnologías de replicación entre un Centro de Datos Primario y uno Secundario con productos de software especializado en replicación de datos de manera continua, este tipo de esquema optimiza la recuperación y aunque es más costosa, el BIA nos permitorá justificar la inversión que deberá hacer la empresa para un recuperación, eficaz y rápida que minimice el impacto financieroy operativo al negocio.

## 2.3 Escenarios de Recuperación.

Para llevar a cabo la recuperación de la operación del negocio y de la infraestructura de TI, existen varios escenarios, la selección de alguno de ellos, como ya se dijo anteriormente, dependerá del resultado del BIA y básicamente del **RPO/RTO** que se tenga establecido para evitar impactos financieros a la Empresa, en términos generales podemos explorar los siguientes escenarios:

**Escenario 1: Hot site**[12] :

Contratación de servicios de recuperación con empresas especialistas en recuperación de operación de cómputo, este tipo de sites o Data Centers, es compartido, es decir, se usa en caso de un desastre o contingencia por un cliente y por cierto período de tiempo

[12] Hot Site: Sitio Alterno de Recuperación que tiene instalada la infraestructura de cómputo que permite restaurar la información desde Respaldos en Cartucho o desde el equipo de Respaldo electrónico remoto.

determinado contractualmente por ambas partes, las características principales de este servicio son:

- ✓ Por el costo mensual, se tiene incluido una semana para recuperación en caso de contingencia, costo mensual $4,500.00 USD
- ✓ Renta anual de $54,000.00 USD
- ✓ Declaración de Contingencia[13], por un monto de $10,000.00 USD.
- ✓ Uso diario del Hot Site: $2,500.00 USD.
- ✓ Uso por semana de Hot Site: $2,500.00 USD
- ✓ Es este esquema, el cliente lo usa y una vez que el cliente regresa a su Data Center propio, los recursos tecnológicos utilizados por el cliente, son liberados y puestos a disposición de otro cliente, este servicio está conformado por los componentes siguientes:

**Componentes de Infraestructura:**

- ✓ Infraestructura tecnológica: Equipos de cómputo distribuido (Servidores Intel, Mainframe, equipos Midrange, etc…
- ✓ e-Vaulting[14]
- ✓ Storage
- ✓ Equipos de telecomunicaciones
- ✓ Recursos humanos técnicos especializados en: Soporte técnico a sistemas operativos, middleware, base de datos y operación de equipos
- ✓ Suites u oficinas de trabajo para el personal técnico de la compañía que contrata los servicios.

En el mercado de TI, existen varios proveedores especializado por ejemplo: IBM - Business Recovery and Continuity Services (IBM/BCRS – Servicios de Recuperación y Continuidad del Negocio), HP Enterprises Services (HP Servicios Empresariales), SunGard Availability Services.

Estas empresas poseen varios Data Centers[15], en diferentes ciudades de los Estados Unidos de Norteamérica y todos tiene un alto nivel de redundancia en su infraestructura de cómputo, telecomunicaciones e instalaciones físicas (Plantas Generadoras de Electricidad a base de combustible Diesel, UPSs, Acometidas eléctricas suministradas por diferentes compañías proveedores de electricidad), etc…

[13] Se considerará una declaración de contingencia por 8 semanas para efectos de evaluación en la matriz comparativa que se presentará posteriormente, en el Capítulo 3 del presente trabajo.
[14] E-Vaulting: Bóveda remota de respaldos
[15] **Data Center: Centros de Datos o Centros de Cómputo**

Lo anterior permite a dichas empresas, proporcionar estos servicios en cualquier momento en que se presente un desastre o contingencia con sus clientes.

El costo de estos servicios, dependerá de la cantidad de infraestructura que se contrate y del tiempo de contratación.

**Escenario 2. Contratación de Secundary Site[16] (Hosting / Outsourcing) ó Sitio Secundario de Recuperación:**

Este escenario consiste en contratar un Centro de Datos (Data Center) con infraestructura tecnológica **dedicada y permanentemente funcionando, bajo un esquema de replicación de datos asíncrona ó síncrona** para un cliente en específico, este escenario dependerá del resultado del **BIA** y del presupuesto que la empresa esté dispuesta a invertir para recuperar su negocio en el rango de **2 a 8 horas como máximo**, pues la decisión esta basada en el **balance de Pérdidas Financieras VS Costo del Site Secundario**.

Las componentes de infraestructura tecnológica que conforman éste escenario son:

- ✓ Equipos de cómputo dedicados, ambiente distribuido (Servidores Intel), Mainframe, equipos Midrange, etc…
- ✓ Storage permanentemente replicando datos, desde el Data Center primario ó principal hacia el Secondary Site o Sitio alterno de DRP
- ✓ Equipos de telecomunicaciones y enlaces de comunicación dedicados y permanentemente funcionando
- ✓ El personal técnico es el mismo personal que opera el Data Center primario o principal
- ✓ Suites u oficinas de trabajo para el personal técnico que contrata el sitio secundario

Las empresas que proveen este tipo de Sitio Secundarios, son básicamente las mismas que se han mencionado anteriormente y que son **líderes mundiales** en este tipo de servicio, como son: IBM-BRCS[17], HP-ES[18], SunGard-AS[19].

En el siguiente capítulo, se desarrollará el Análisis de Impacto al Negocio (**BIA** por sus siglas en Ingles) y se determinará el RTO / RPO, de la empresa financiera y con base en el resultado del análisis, **se sustentará la selección del escenario más óptimo**, desde un **punto de vista financiero y de recuperación del servicio en el menor tiempo posible**, lo que permitirá **justificar la inversión** del escenario seleccionado.

**[16] Secondary Site: Sitio Secundario o alterno de recuperación.**
**[17] IBM-BRCS: IBM Business Continuity and Recovery Services (IBM Servicios de Recuperación y Continuidad del Negocio)**
**[18] HP-ES: HP Enterprises Services (HP Servicios Empresariales)**
**[19] SunGard-AS: Sungard Availability Services (SunGard Servicios de Disponibilidad)**

**Escenario 3: Construcción o adecuación de un Secundary Site[20]ó Sitio Secundario de Recuperación por parte del Banco:**

Este escenario consiste en construir un Centro de Datos (Data Center) adicional con infraestructura tecnológica **permanentemente funcionando, bajo un esquema de replicación de datos asíncrona ó síncrona ,** este escenario dependerá del resultado del **BIA** y del presupuesto que la empresa esté dispuesta a invertir para recuperar su negocio en el rango de **2 a 8 horas como máximo, pues la decisión también esta basada** en el **balance de Pérdidas Financieras VS Costo del Site Secundario**.

**Escenario 3. Construcción de un Sitio Secundario de Recuperación (Secondary Site):**

Este escenario consiste en llevar a cabo la construcción de un segundo Centro de Datos (Data Center) por parte de la empresa, el cuál contaría con los recursos siguientes:

- tecnológica **dedicada y permanentemente funcionando, bajo un esquema de replicación de datos asíncrona ó síncrona**, este escenario dependerá del resultado del **BIA** y del presupuesto que la empresa esté dispuesta a invertir para recuperar su negocio en el rango de **2 a 8 horas como máximo**, pues la decisión esta basada en el **balance de Pérdidas Financieras VS Costo del Site Secundario**.

Las componentes de infraestructura tecnológica que conforman éste escenario son:

- ✓ Equipos de cómputo dedicados, ambiente distribuido (Servidores Intel), Mainframe, equipos Midrange, etc…
- ✓ Storage permanentemente replicando datos, desde el Data Center primario ó principal hacia el Secondary Site o Sitio alterno de DRP
- ✓ Equipos de telecomunicaciones y enlaces de comunicación dedicados y permanentemente funcionando
- ✓ El personal técnico es el mismo personal que opera el Data Center Primario o principal

Los escenarios anteriormente citados, se podrán sustentar con el la metodología del Análisis de Impacto al Negocio, la cual permite obtener de manera directa de las áreas de Negocio de la Empresa, una estimación cualitativa y cuantitativa en términos financieros de los impactos que sufriría la Empresa al dejar de funcionar, sino contara con los sistemas de cómputo que le permiten operar, tanto, en sucursales bancarias, como en la red de cajeros automáticos, así como en las bancas electrónicas, el BIA, logra establecer la correlación entre la tecnología y la generación de ingreso por cada línea de negocio.

Lo anterior es tan relevante que permitirá mostrar a la Dirección General de la Empresa, el "tamaño" del impacto por un desastre natural o informático, adicioanlmente el resultado

[20] **Secondary Site: Sitio Secundario o alterno de recuperación.**

del BIA, se proporciona de manera tal que es entendible financieramente y cualitativamente porque se pondera el daño subjetivo como son los siguientes conceptos:

- Impacto que recibirá el negocio en caso de una contingencia, en términos; fiancieros.
- Impacto reputacional; es aquel que daña el prestigio de una empresa ante sus clientes y que puede generar pérdida de clientes.
- Por consecuencai del daño reputacional, se podría tener pérdida de posicionamiento en el mercado financiero
- Faltas regulatorias, penalizaciones a las que se haría acreedor el negocio por no operar por uno o varios días, dañando el patrimonio financiero de sus clientes
- Intervalo de Tiempo máximo que el negocio puede estar sin operar con un impacto financiero mínimo
- Intervalo de Tiempo máximo de pérdida de datos, sin que afecte la operación y a sus clientes

Todo lo anterio será analizado y medible por el Análisis de Impacto al Negocio.

# Capítulo 3

## Diseño e Implementación.

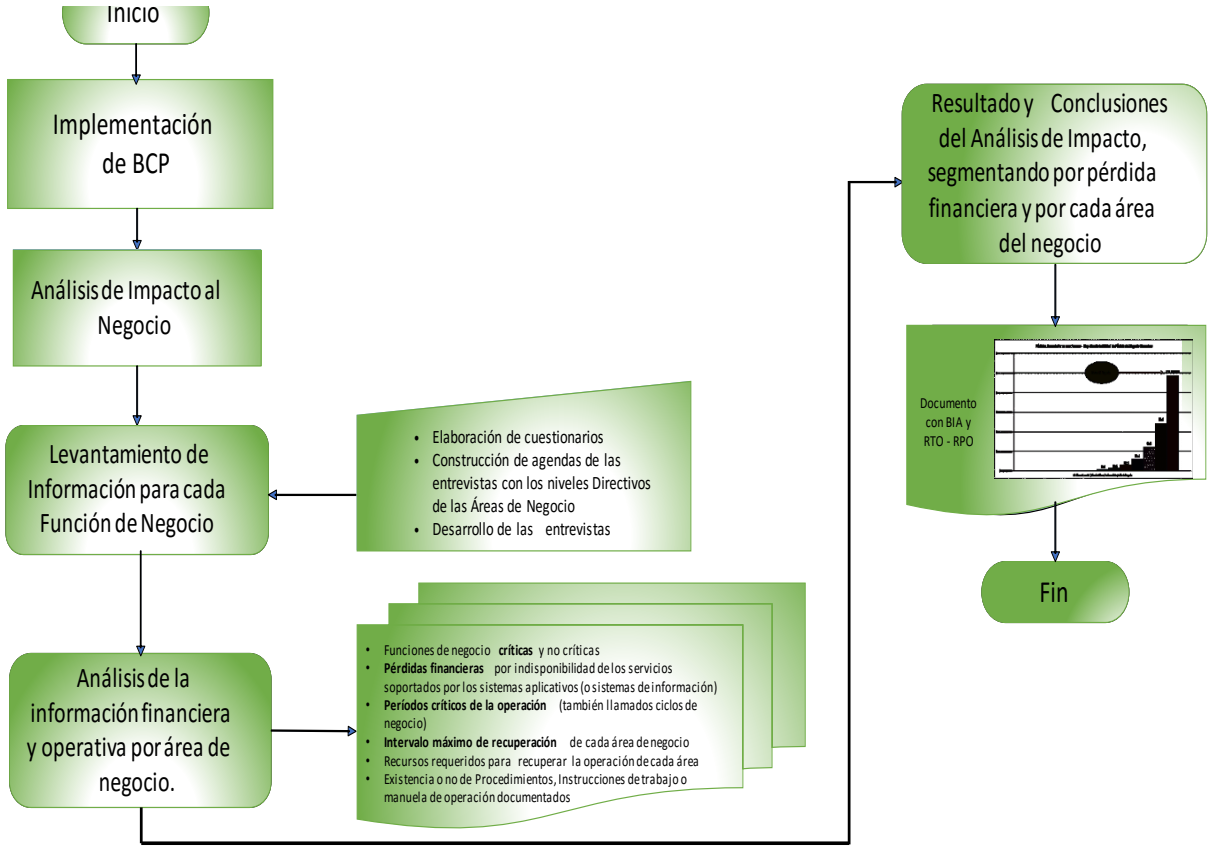
## Introducción.

En este capítulo se presentarán las etapas para desarrollar el Análisis de Impacto al Negocio (BIA) y para seleccionar la estrategia de recuperación más apropiada con base en el RTO y RPO que permita la recuperación de la operación del negocio en el menor tiempo posible, reduciendo al mínimo el impacto financiero a la empresa y por consiguiente, el impacto por la pérdida del servicio a la clientela del Banco.

En este Capítulo, se desarrollarán los Casos de Negocio de los tres Escenarios propuestos en el Capítulo 2, con la finalidad de elegir el más conveniente, en función de:

- Costo / Beneficio
- RPO / RTO
- Diagrama para el Diseño e Implementación del Plan de Continuidad del Negocio.

## 3.1 Diagrama a Bloques del Proceso para Implementar el Plan de Continuidad del Negocio.




## 3.2 Análisis de Impacto al Negocio (BIA).

El objetivo del Análisis de Impacto al Negocio consiste en evaluar y determinar el impacto financiero de cada función del nogocio crítica (es decir que tipos de servicio son los que generan ganancias al negocio):

**Ingresos** (Revenue), está directamente ligado a la captación directa de ingresos, así como identificar los diferentes sistemas aplicativos que soportan dichas funciones del negocio, para ello es necesario desasrrollarlo en 3 etapas, mismas que se citan a continuación:

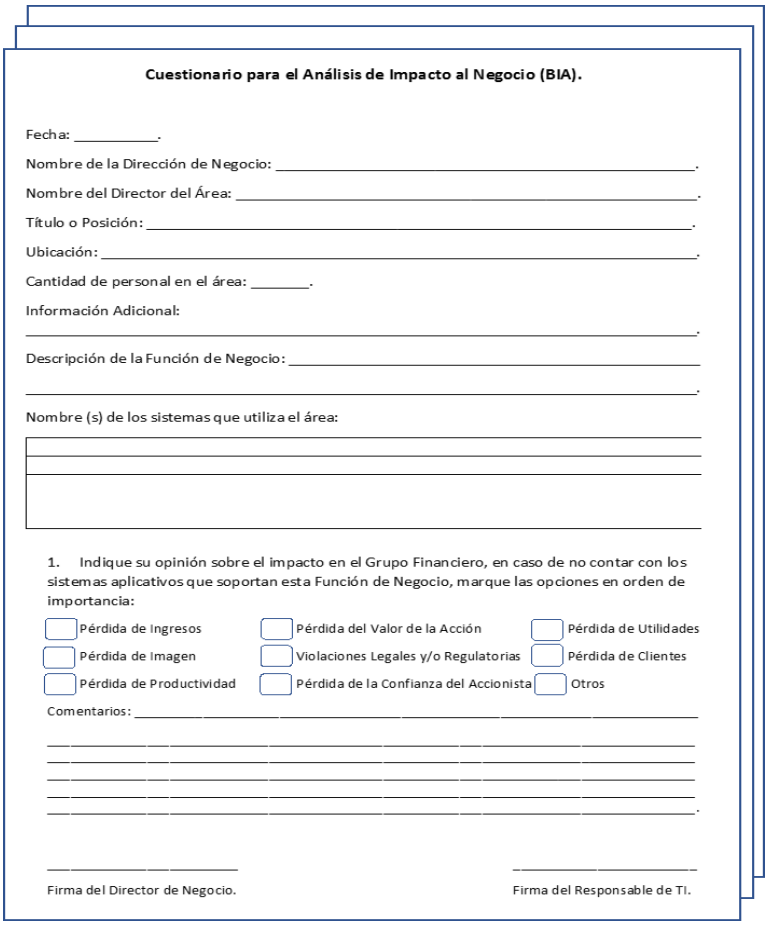
1. **Levantamiento de información para cada función del negocio.**
    a. Elaboración de cuestionarios
    b. Construcción de agendas de las entrevistas con los niveles Directivos de las Áreas de Negocio
    c. Desarrollo de las entrevistas
2. **Análisis de la información financiera y operativa por área de negocio.**
3. **Resultado y conclusiones del Análisis de Impacto, segmentando por pérdida financiera y por cada área del negocio.**

## 3.2.1. Lavantamiento de Información para Cada Función de Negocio.

## a. Elaboración de Cuestionarios.

Los cuestionarios (ver figura 3.1), deberán estar construidos y orientados de manera tal que deberán poder obtener la información mínima siguiente:

1. Descripción de la Función del Negocio.
2. Datos Generales como són: Ubicación de las oficinas, cantidad de personal en el área, cuenta con Procedimientos documentados ó Instrucciones de trabajo para llevar a cabo la función manualmente por cierto límite de tiempo.
3. Sistemas de Información (Aplicaciones) que dan soporte a su función de negocio
4. Período del día con mayor actividad transaccional u operativa.
5. Equipo utilizado para su operación normal (business as usual).
6. Tipo de impacto (desde el punto de vista del negocio) que se podría tener en caso de no contar con los sistemas aplicativos que usan en su operación ó transaccionalidad cotidiana.
7. El lapso de tiempo límite a partir del cual se podrían presentar pérdidas financieras significativas, a partir del momento que ocurriera un desastre (natural o tecnológico) que imposibilite el uso de sus sistemas aplicativos.
8. El lapso de tiempo a partir del cual se generarían pérdidas intangibles.
9. El incremento adicional de la pérdida financiera, si continuara la indisponibilidad del servicio de sus sistemas aplicativos por tiempo indefinido.



**Cuestionario para el Análisis de Impacto al Negocio (BIA).**

Fecha: _____.

Nombre de la Dirección de Negocio: _____.

Nombre del Director del Área: _____.

Título o Posición: _____.

Ubicación: _____.

Cantidad de personal en el área: _____.

Información Adicional:

_____.

Descripción de la Función de Negocio: _____

_____.

Nombre (s) de los sistemas que utiliza el área:

1. Indique su opinión sobre el impacto en el Grupo Financiero, en caso de no contar con los sistemas aplicativos que soportan esta Función de Negocio, marque las opciones en orden de importancia:

☐ Pérdida de Ingresos ☐ Pérdida del Valor de la Acción ☐ Pérdida de Utilidades
☐ Pérdida de Imagen ☐ Violaciones Legales y/o Regulatorias ☐ Pérdida de Clientes
☐ Pérdida de Productividad ☐ Pérdida de la Confianza del Accionista ☐ Otros

Comentarios: _____

_____
_____
_____
_____
_____.

_____ _____

Firma del Director de Negocio. Firma del Responsable de TI.

*Figura 3.1: Cuestionarios de Entrevistas Directivas*

## b. Construcción de Agenda de Entrevistas a Directivos.

Se debe establecer la agenda de reuniones para entrevistar a los Directores de las áreas de Negocio, con la finalidad de obtener un visión ejecutiva del impacto al negocio y también deberán participar las personas clave de la operación de cada área para obtener datos consistentes de tipo operativo.

## c. Desarrollo de las Entrevistas a los Directores de las Áreas de Negocio.

Durante el desarrollo de las entrevistas, es importante la inducción a los participantes del objetivo que se persigue con el **BIA**[1] (Business Impact Analysispor sus siglas en Ingles, Análisis de Impacto al Negocio), con la finalidad de que la información obtenida sea, confiable, veráz, sustentada y los datos financieros puedan ser demostrables en cualquier momento. Las entrevistas deberán ser desarrolladas de manera acertiva por parte del consultor de TI para obtener información vital de cada función de negocio y de las

[1] **BIA: Business Impact Analysis: Análisis de Impacto al Negocio.**

implicaciones operativas y financieras, en caso de no contar con los sistemas aplicativos que diariamente operan para realizar sus funciones, también se tendrá que obtener copia de la información que soportan las pérdidas financieras en caso de que así sea.

### 3.2.2. Análisis de la información financiera y operativa por cada área de negocio.

Es de suma importancia esta etapa, pues la toma de decisiones que se derive del certero análisis y resultado, de esta etapa, conllevará a la identificación de los factores siguientes:

- Funciones de negocio **críticas** y no críticas
- **Pérdidas financieras** por indisponibilidad de los servicios soportados por los sistemas aplicativos (o sistemas de información)
- **Períodos críticos de la operación** (también llamados ciclos de negocio)
- **Intervalo máximo de recuperación** de cada área de negocio
- Recursos requeridos para recuperar la operación de cada área
- Existencia o no de Procedimientos, Instrucciones de trabajo o manuela de operación documentados

## 2. Resultado y Conclusiones del Análisis de Impacto (Segmentando por Pérdida Financiera y por Área del Negocio).

Con base en la información recabada, se clasificó y se graficaron los aspectos más relevantes, citados a continuación:

- ✓ **Pérdidas Financieras.**

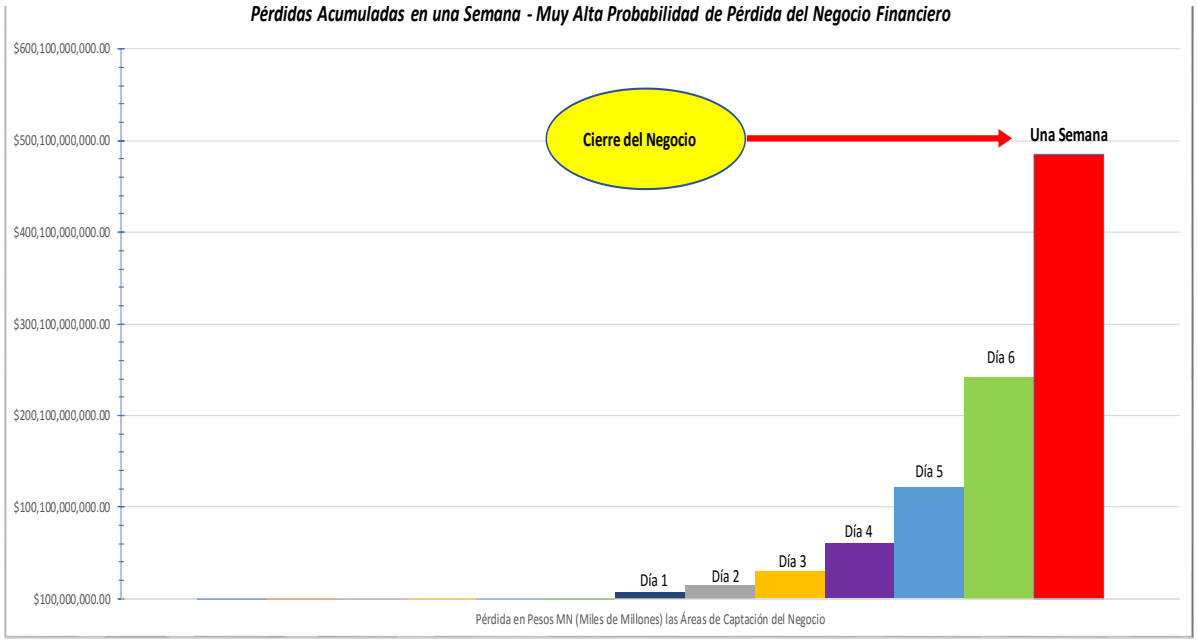
Basados en la información de captación de recursos monetarios por cada área de negocio se conformó una proyección de pérdidas por día y hasta una semana, ya que suponiendo que la empresa financiera, no contara con una **Metodología (Plan de Recuperación en caso de Desastre) y un esquema de recuperación alterno que le posibilitara la recuperación de la infraestructura tecnológica, aplicaciones en el menor tiempo posible** y por consecuencia **la recuperación de los servicios Financieros** y funciones de negocio críticas, en el **intervalo de tiempo de una semana**, la empresa en cuestión, podría quedar fuera del negocio financiero, con las consecuencias que eso implica en el mercado financiero de una país, ver Tabla 3.2 y Gráfica 3.2.

La tabla 3.2, representa el **ingreso diario del Banco** por las diferentes áreas de negocio (Captación, Colocación, Tesorería, Fondos de Inversión, etc…), este ingreso se proyecta a una semana, considerando que el negocio no pudiera operar en ella, los montos mostrados en la tabla, fueron obtenidos directamente **en las entrevistas con los Directores de las**

**áreas de Negocio** y sustentados por el sistema de **Contabilidad** de la empresa, de manera tal que es información sólida y consistente, **que muestra la dimensión del impacto financiero que sufriría la empresa por la imposibilidad de operar en una semana.**

**Tabla 3.2. Impacto Financiero Acumulado en una Semana a Partir del Desastre Natural o Tecnológico.**

| Pérdida en Pesos MN (Miles de Millones) las Áreas de Captación del Negocio | Día 1 | Día 2 | Día 3 | Día 4 | Día 5 | Día 6 | Una Semana |
|---|---|---|---|---|---|---|---|
| Desde el primer día del desastre | $ 7,231,160,552.62 | $ 14,462,321,105.23 | $ 28,924,642,210.47 | $ 57,849,284,420.94 | $ 115,698,568,841.87 | $ 231,397,137,683.75 | **$ 462,794,275,367.49** |
| Desde el día 2 del desastre | | $ 691,586,093.22 | $ 1,383,172,186.44 | $ 2,766,344,372.89 | $ 5,532,688,745.78 | $ 11,065,377,491.56 | **$ 22,130,754,983.12** |
| Desde el día 4 del .... | | | | $ 11,465,322.89 | $ 22,930,645.78 | $ 45,861,291.56 | **$ 91,722,583.12** |
| En una Semana del desastre | | | | | $ 624,223.14 | $ 1,248,446.27 | $ 2,496,892.54 |
| **Total Pesos MN (Millones)** | **$ 7,231,160,552.62** | **$ 15,153,907,198.46** | **$ 30,307,814,396.91** | **$ 60,627,094,116.72** | **$ 121,254,812,456.57** | **$ 242,509,624,913.14** | **$ 485,019,249,826.27** |

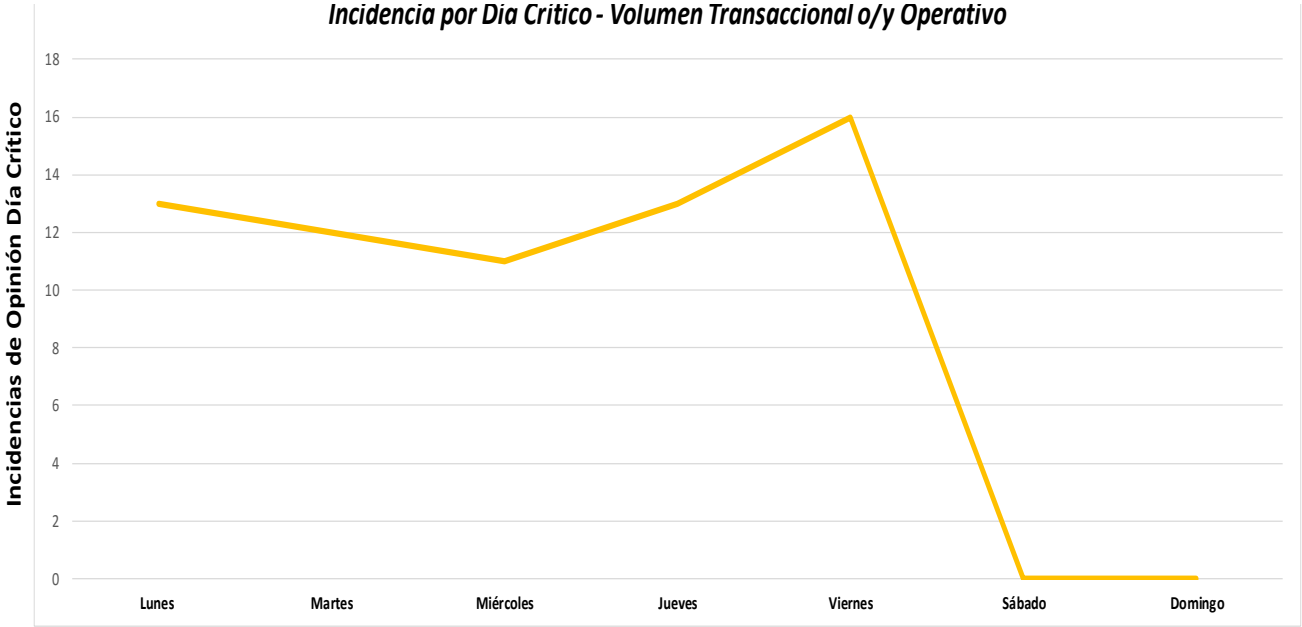



**Gráfica 3.2. Pérdida Acumuladas en una Semana a Partir del Desastre Natural o Tecnológico.**

- ✓ **Períodos Críticos de la Operación en las Principales Áreas del Negocio.**

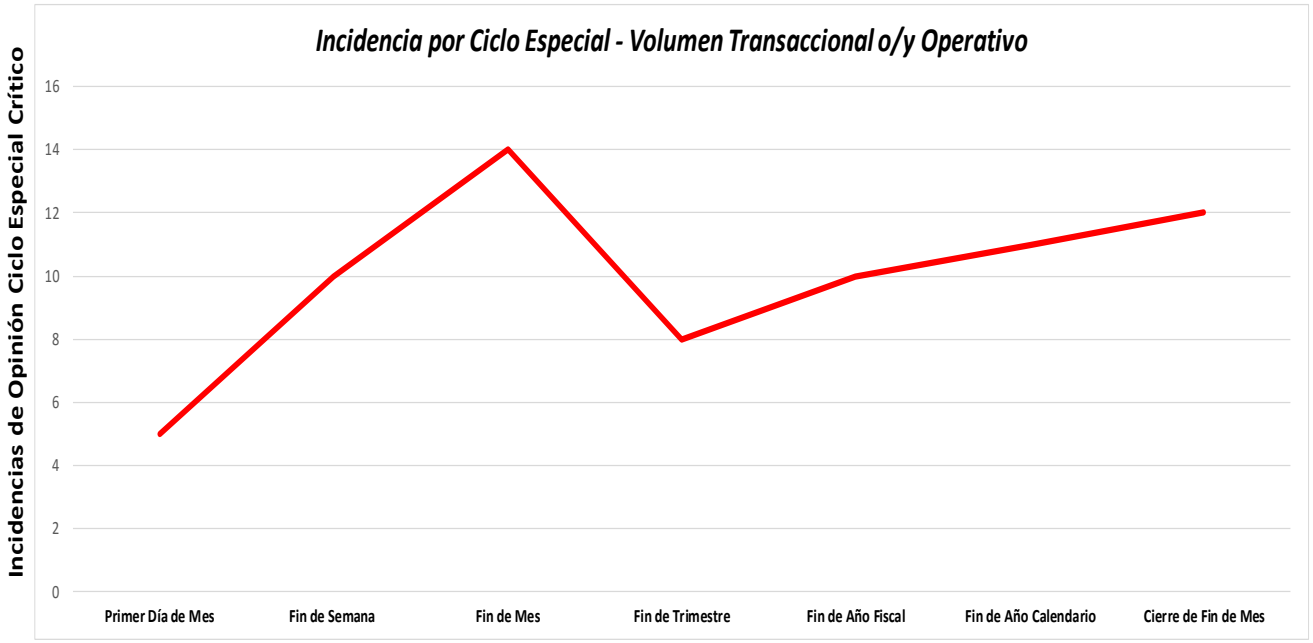
Considerando la información obtenida en las entrevistas con Direcciones Ejecutivas, se pueden establecer los días de la semana, ciclos de negocio en el mes y el año, en el cual la operación se torna más crítica por sus características de alto volumen operativo y/o

transaccional, así como de los montos financieros, mismos que se obtienen desde el **Sistema Automático de Contabilidad de la empresa**. En las gráficas siguientes se muestran los escenarios "picos de la transaccionalidad de los servicios – On Line (Banca por Internet para Empresas y personas físicas, Red de Sucursales y Red de ATM [2]– Cajeros Automáticos), con base en estos **ciclos del negocio**, podemos inferir que en caso de que una contingencia, desastre natural o tecnológico, sucediera en esos ciclos y particularmente, si sucediera bajo la siguiente condición**:** "Día Viernes, siendo fin de Mes, en el mes de Diciembre" *(ver gráficas 3.2,3.3 y 3.4)*, sería altamente riesgoso para la empresa y supondría el cierre del negocio, en caso de que no contaran con un esquema de recuperación de los servicios financieros, apoyados en la recuperación casi inmediata y eficiente de la Infraestructura tecnológica y de los sistemas aplicativos, éste Análisis de Impacto al Negocio, sustenta la toma de decisiones por parte del **CIO** [3] (Chief Information Officer por sus siglas en Ingles) o Director General de Sistemas y del Grupo Directivo del Negocio incluido el **CEO**[4] para la creación del esquema de recuperación bajo una metodología y DRP (Disaster Recovery Plan), basados en un óptimo RTO y RPO.

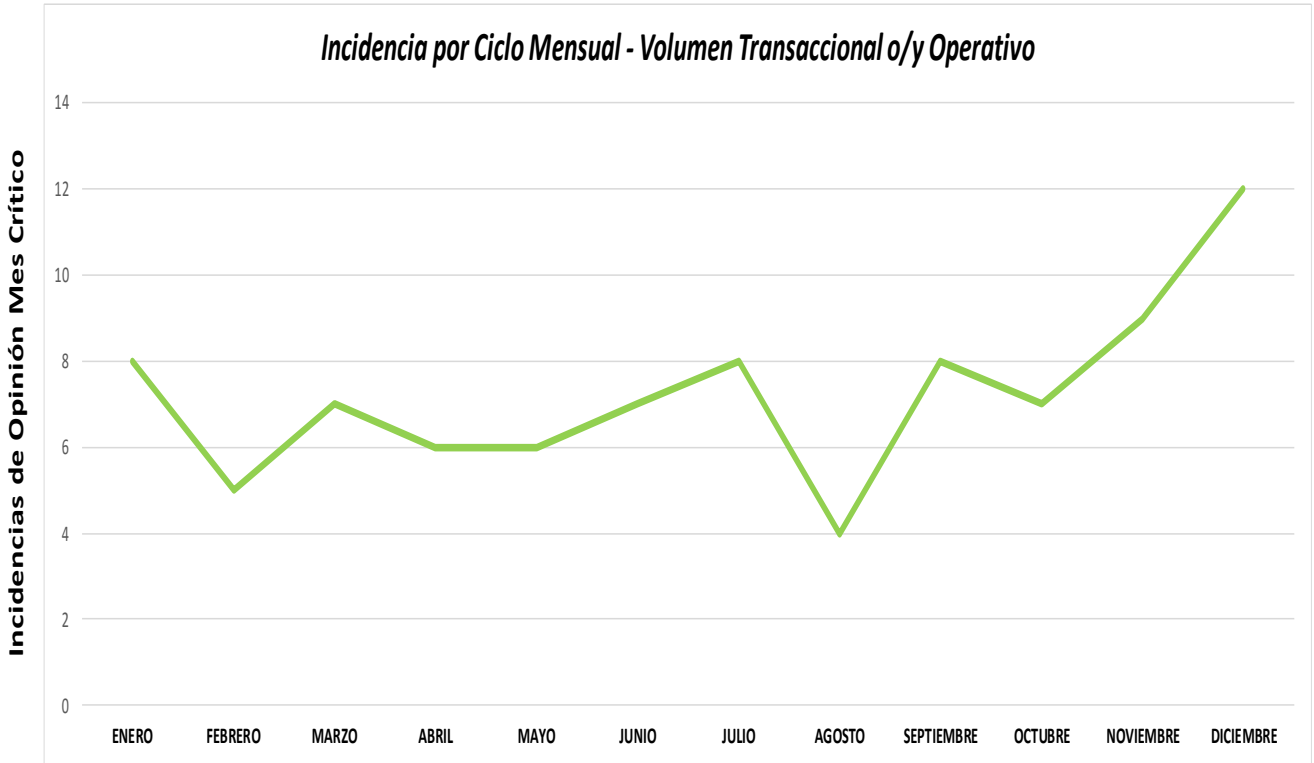



**Gráfica 3.2 Incidencia por Día Crítico de Operación y Alta Transaccionalidad.**

[2] ATM: Automatic Teller Machine (Cajero Automático)
[3] CIO: Chief Information Officer
[4] CEO: Chief Executive Officer, Director General del Grupo Financiero



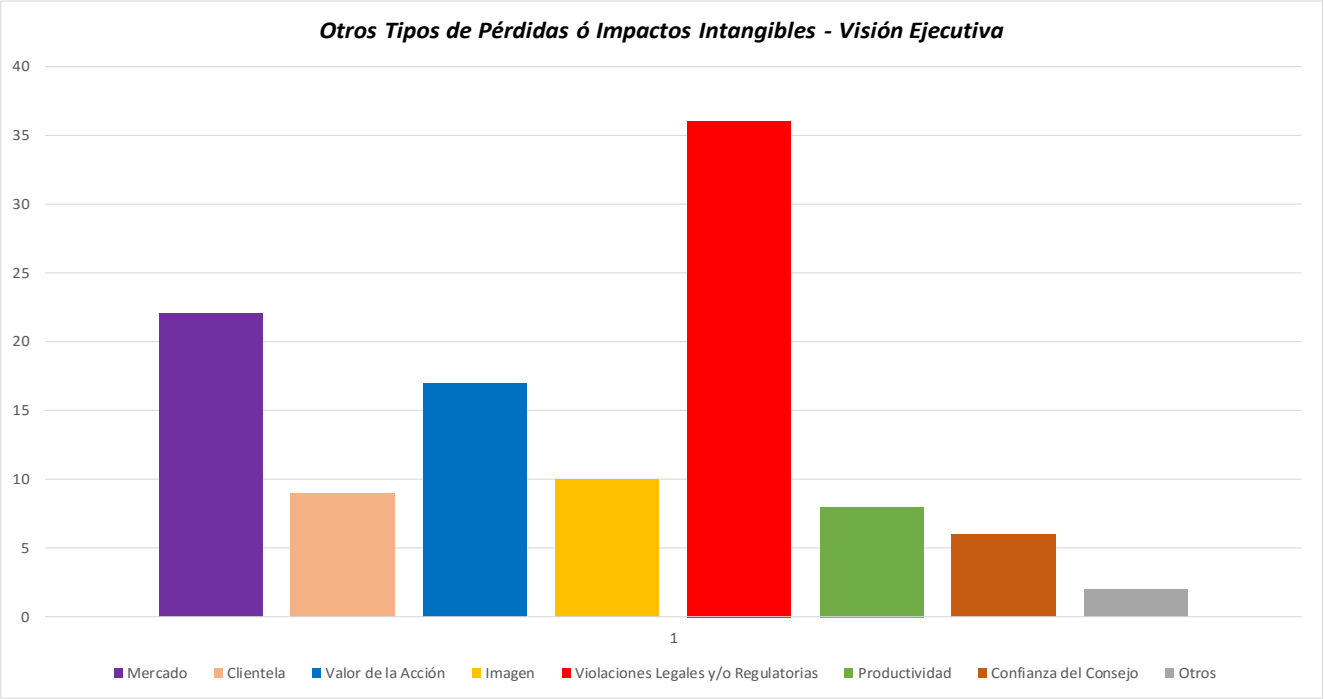

**Gráfica 3.3: Incidencia por Ciclo de Negocio (día del mes de mayor operación)**




**Gráfica 3.4: Incidencia por el Mes de Mayor Operación.**

✓ **Categorización de Impacto al Negocio por Pérdidas Intangibles.**

Existen pérdidas que no se presentan en el ámbito financiero, **son intangibles y subjetivas,** pero afectan de igual manera al negocio, pues una de las más serias es, sin duda, ***el impacto a la Reputación de la Marca y el deterioro de la Imagen***, sobre todo **cuando *se trata de una marca global***, en la gráfica 3.5, se puede observar la estimación del nivel ejecutivo del Grupo Financiero, sobre los impactos intangibles.




***Gráfica 3.5: Impactos Intangibles o Subjetivos.***

Ahora bien, como sabemos desde la perspectiva del Negocio y de los Ejecutivos que tienen bajo su cargo el crecimiento del ingreso, a través, de los instrumentos bancarios de captación de dinero, a continuación, citamos las áreas de mayor riesgo financiero por los montos que se manejan diariamente:

- Promoción y Operación Mercado de Dinero
- Banca por Internet Empresarial y Personal
- Operación de Fondos de Inversiones
- Captación y Operación de Cheques
- Tarjeta de Crédito
- Servicios Especiales

- Operación de Cartera Financiera
- Administración de Cambios de Divisas e Inversiones
- Créditos Comerciales
- Crédito Hipotecario

Estas áreas son las **más relevantes y sustantivas,** en términos de **captación de dinero,** éste es el negocio principal de la Banca.

Estas áreas de negocio, no pueden estar sin el servicio más allá de un día, pues es altamente impactante, en la **tabla 3.6,** se pueden apreciar los Intervalos de Tiempo que las áreas citadas anteriormente, necesitarían que se recuperen los servicios de Tecnologías de Información para evitar los riesgos de impacto financiero e intangibles que se han presentado en este documento.

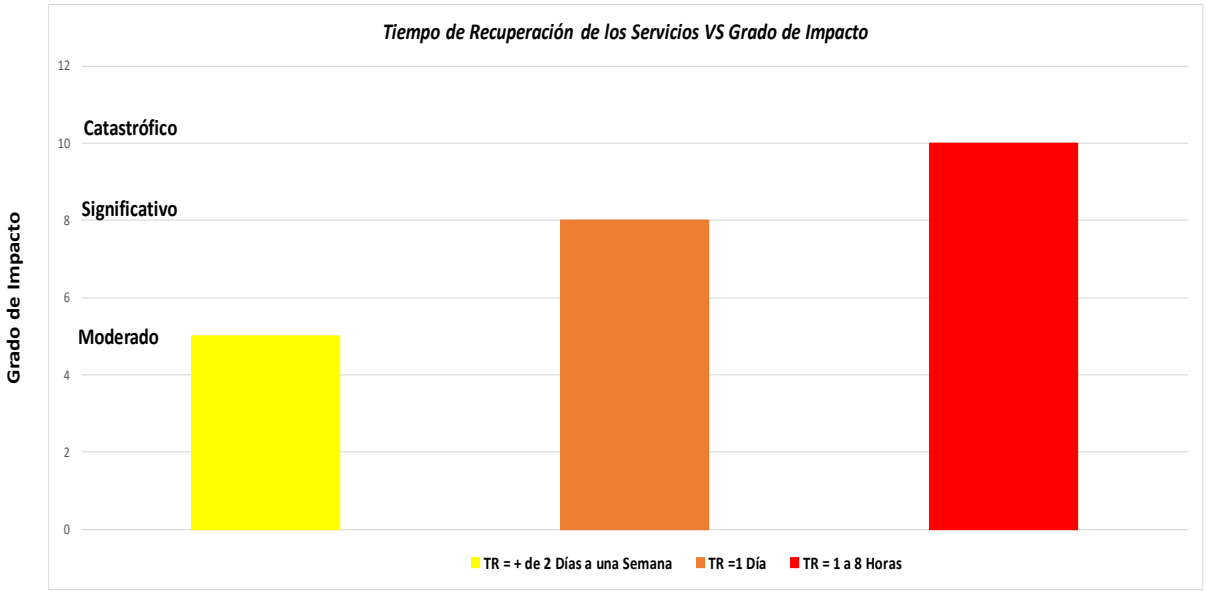
***Tabla 3.6: Tiempo Máximo Permitido de Suspensión de la Operación por Área de Negocio.***

| Área de Negocio | Área de Negocio | Área de Negocio | Área de Negocio |
|---|---|---|---|
| Banca por Internet p/ Empresas y Personal | Fondos de Inversión | Administración Cambios de Divisas | Recursos Humanos y Nómina |
| Red de Sucursales y ATMs | Operación Cartera Financiera | Aclaraciones | |
| Tarjeta Crédito | Créditos Comerciales | | |
| Promoción Mercado de Dinero | Crédito Hipotecario | | |
| SPEI Nacionales e Internacionales | Servicios Especiales | | |
| Operación Cheques | Pagos y Cobranza Institucional | | |
| Contabilidad | | | |
| Call Center Clientes | | | |
| SWIFT | | | |
| | | | |

**TR[5]= 1 a 8 Horas Máximo** **TR= 1 Día** **TR= + de 2 Días a una Semana**

En la gráfica 3.7, se puede observar el grado de impacto en función del tiempo TR de recuperación de los servicios bancarios, una vez recuperada la infraestructura Tecnológica y los Sistemas Aplicativos que hacen posibles las funciones de las áreas de negocio.

[5] TR: Tiempo de Recuperación del Servicio en las áreas de Negocio

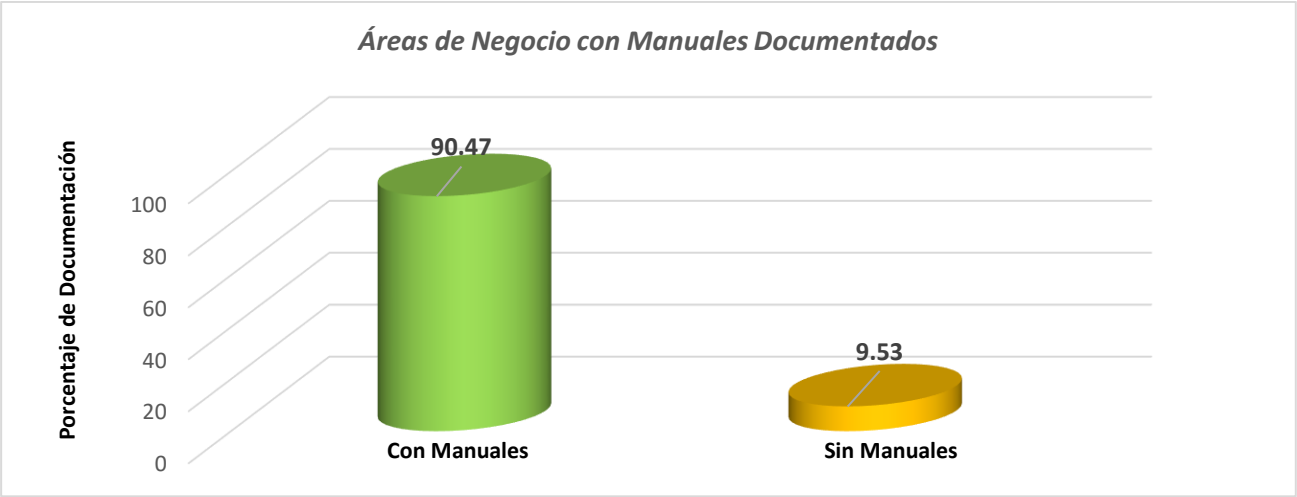



*Gráfica 3.7: Grado del Impacto VS Tiempo de Suspensión de la Operación*

Es importante que las área de negocio, tengan Procedimientos e Instrucciones de Trabajo documentadas y publicadas en algún Content Manager (**Share Point**[6] o algún otro tipo de Content Manager), y además que tengan un respaldo en los servicios de Cloud (Nube de algún proveedor de estos servicios) que les permita operar manualmente en la medida de los posible, durante el tiempo de recuperación de los servicios, con la finalidad de tener identificadas las mayor cantidad de transacciones para su posterior ingreso a los sistemas una vez restablecidos.

De acuerdo a la información analizada en el BIA, en la **Gráfica 3.8**, se muestran las áreas de Negocio que tiene manuales documentados de su operación.

[6] Share Point: Herramienta de Microsoft (© 2017 Microsoft) que es utilizada para publicar documentos para un grupo de usuarios.




*Gráfica 3.8: Áreas de Negocio con Procesos Manuales y Sin Ellos.*

Basados en el análisis realizado, sobresalen los factores siguientes desde una perspectiva de negocio:

- ✓ Altas pérdidas financieras desde las primeras 8 horas a partir del Desastre Natural o Tecnológico por un monto de: **$7,231,160,552.62 de pesos**, pérdida que se puede potenciar a valores muy preocupantes a la semana de la interrupción de los **servicios financieros, llegando a un monto de: $485,019,249,826.27 pesos, lo cual como se indicó durante el análisis, conllevaría al cierre del negocio.**
- ✓ Adicionalmente el impacto en el valor de la acción
- ✓ Las violaciones Legales y/o Regulatorias en las que se incurriría por no operar en el mercado financiero

Por último, dentro de éste análisis y con base en la información obtenida, se elabora una matriz, relacionando las funciones de las diferentes Áreas de Negocio, con los sistemas aplicativos utilizados para su operación y transaccionalidad diaria, en la **tabla 3.9**, se muestra esa **Relación Área de Negocio – Sistema (s) Aplicativo (s),** basados en dicha relación, se logrará la recuperación de los servicios de la totalidad de las áreas de negocio, con una estrategia y diseño de recuperación no mayor a las 8 horas, siendo lo más óptimo usar el rango de 2 a 6 horas, que permite una disponibilidad continua del negocio.

En resumen, la **tabla 3.9**, indica cuantos sistemas aplicativos, ya que en muchas ocasiones una línea de negocio opera, apoyándose en uno o más sistemas aplicativos, mismos que deberán estar activos y funcionando para que cada una de las áreas de negocio principales, permiten la entrada de recursos financieros al Banco, a través de los servicios que ofrecen

a sus clientes, con esta matriz, se puede asegurar que dichas líneas de negocio, recuperen su operación dentro del intervalo de tiempo máximo de recuperación, evitando mayor impacto financiero a la empresa.

***Tabla 3.9: Sistemas Aplicativos que Soportan la Operación de las Áreas de Negocio.***

| | **Sistemas Aplicativos** | |
|---|---|---|
| **Área de Negocio** | **On Line** | **Batch u Off Line** |
| Red de Sucursales y de ATMs[1] | Cheques<br>Cuenta Única<br>Giros y Cheques de Caja<br>Líneas de Servicios<br>CECOBAN[2]<br>Catálogos Generales<br>Fondos de Inversión<br>Divisas – Tipos de Cambio | Cheques<br>Giros y Cheques de Caja<br>Micro Generación de Chequeras<br>CECOBAN<br>Mesa de Inversiones |
| Banca por Internet Empresarial y Personal | Cheques<br>Cuenta Única<br>Giros y Cheques de Caja<br>Líneas de Servicios<br>CECOBAN[3]<br>Catálogos Generales<br>Fondos de Inversión<br>Divisas – Tipos de Cambio | Cheques<br>Catálogos Generales<br>Fondos de Inversión<br>Divisas – Tipos de Cambio |
| Promoción y Operación Mercado de Dinero | Mesa de Dinero<br>Fondos de Inversión | Mesa de Dinero<br>Fondos de Inversión |
| Tarjeta de Crédito | FDR[4]<br>AMEX[5]<br>PROSA[6] | FDR[7]<br>AMEX[8]<br>PROSA[9] |
| SPEI Nacionales e Internacionales | Cheques<br>Corresponsales Bancarios<br>Órdenes de Pago<br>Catálogos Generales | |
| Contabilidad | Todas las Aplicaciones Bancarias | P.A.C.O. (Paquete Contable) |
| Call Center | Clientes BD y Catálogos Generales | |
| SWIFT | Cambios de Divisas Internacionales<br>Corresponsales Bancarios | |
| Administración de Fondos de Inversión e Inversiones a Plazo Fijo | Fondos de Inversión, SIVA[10] | |
| Operación Cartera Financiera | Cartera General y Catálogos Generales | |
| Administración de Cambios de Divisas e Inversiones | Sistemas de Agencias en el Extranjero | |
| Crédito Hipotecario | Sistema de Crédito Hipotecario | |
| Créditos Comerciales | Sistema de Préstamos Personales | |
| Servicios Especiales | | Sistema Cobranza PEMEX<br>SACC[11], RECOB[12] |
| Pagos y Cobranza Institucional | Órdenes de Pago, Cheques de Viajero | |
| Aclaraciones | Clientes BD y Catálogos Generales | |
| Auditoria | | Todos los aplicativos |
| Recursos Humanos | | SISNOM[13] |

[1] ATM: Automatic Teller Machine (Cajero Automático)
[2] CECOBAN (Centro de Compensación Bancaria), entidad que depende del Banco de México.
[3] CECOBAN (Centro de Compensación Bancaria), entidad que depende del Banco de México.
[4] FDR: First Data Resources
[5] AMEX: American Express
[6] PROSA: Switch de transacciones entre Bancos a Nivel Nacional e Internacional.
[7] FDR: First Data Resources
[8] AMEX: American Express
[9] PROSA: Switch de transacciones entre Bancos a Nivel Nacional e Internacional.
[10] SIVA: Sistema de Valores
[11] SACC: Sistema de Administración de Cobranza y Crédito
[12] RECOB: Recaudación y Cobranza
[13] SISNOM: Sistema de Nómina y Compensaciones

Todo lo anteriormente concluido, nos lleva a establecer el **RTO y RPO** más indicado para la operación del Grupo Financiero que le permita a la Dirección de Tecnología, activar los servicios del Grupo **en el lapso de 8 horas o menos**, es decir, el **RTO** deberá ser igual o mucho menor a ese intervalo de tiempo y el **RPO** (punto de recuperación de los datos), máximo de **1 a 2 horas**, para poder recuperar la operación suspendida durante ese intervalo de tiempo y continuar operando, evitando el riesgo de los diferentes impactos citados en el **BIA**.

## 3.3.3.Construcción de la Solución de RPO / RTO Derivado del BIA.

Para lograr los valores de **RPO/RTO** que resultaron del **BIA** (Análisis de Impacto al Negocio), se deberán seleccionar las herramientas de replicación de datos y el esquema de Sitio Alterno, como se mencionó en el capítulo anterior, el uso de un esquema de Hot Site, no puede satisfacer los valores de **RPO / RTO**, debido a que ese esquema no proporciona la facilidad de contar con la Infraestructura Tecnológica dedicada para mantener la replicación de datos permanentemente entre el Sitio Primario y el Sitio Secundario.

Por lo anterior y considerando lo indicado en el Capítulo 2, (ver Gráfica 2.2 ***Cost / Value VS Recovery Time***), se puede utilizar una de las tecnologías de replicación de datos, entre Storage ubicados en diferentes localidades, desarrollada por la IBM y llamada **PPRC con Flash Copy**[7], desde luego conectadas por un enlace de comunicaciones dedicado para tales efectos.

A continuación, describiremos, el proceso de replicación entre Storage remotos, que típicamente soporta esta tecnología, enfocándonos a la opción de **PPRC – Flash Copy o Metro / Global Mirroring:**

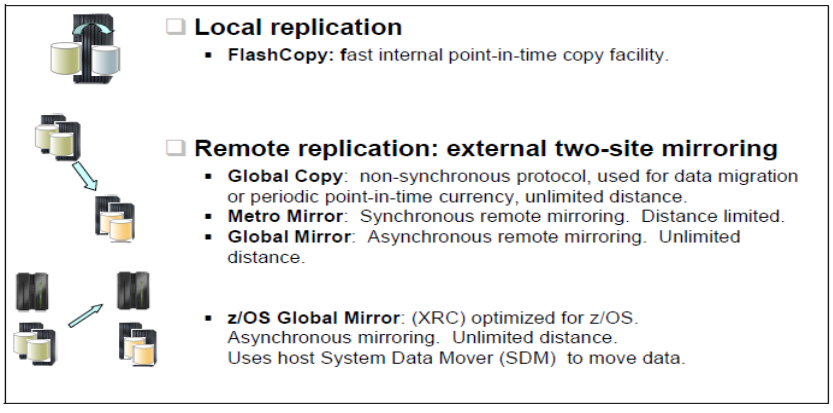



***Figura 3.10: Ejemplos de Replicación de Storage Remoto entre Dos Sitios (Site)***[8]

[7]Fuente: PPRC followed by Flash Copy: PPRC; Peer to Peer Remote Copy con Copia Instantánea, Marca registrada de IBM Corporation.
[8]Fuente: IBM Red Book Storage Infrastructure for Business Continuity.

En **la figura 3.10, se muestran tres tipos de replicación** que son usados por el PPRC (Peer to Peer Remote Copy), que es una tecnología desarrollada por IBM:

- **Replicación Local (Local Replication):** Copia en Intervalo: facilidad interna rápida de la copia del punto-en-tiempo (intervalo de tiempo).
- **Replicación Remota: duplicación externa de dos sitios (Remote Replication: External Two-Site Mirroring):** Protocolo no síncrono, usado para migración de datos o actualización de datos periódica en el tiempo, distancia ilimitada.
- **Espejo Metropolitano (Metro Mirror):** Espejeo remoto síncrono. Distancia limitada.
- **Espejeo Global (Global Mirror):** Espejeo remoto asíncrono. Distancia ilimitada.
- **Sistema Operativo/z, usado en plataforma Mainframe (z/OS Global Mirror):** (XRC) Extended Remote Copy; Copia Remota Extendida, optimizada para sistema operativo z/OS.
  Espejeo asíncrono, distancia ilimitada. Usos con SDM Anfitrión (System Data Mover: Moviendo Datos del Sistema)

La solución que abordaremos será bajo el escenario de la opción, mostrada en la **figura 3.10, como Remote Replication External Two Sites Mirroring,** para ello explicaremos brevemente cómo funciona el Flash Copy Básico o Tradicional.

**FlashCopy Básico o Típico.**

La función FlashCopy, copia datos de un origen a un destino. El tamaño del objetivo, es decir del espacio (storage en el equipo destino), debe ser Igual o de mayor tamaño que el storage origen. Una vez que la relación origen / destino se establece, tanto el origen y el destino están disponibles para los servidores para acceso de lectura y escritura.
IBM FlashCopy tiene una capacidad única llamada la opción COPY / NOCOPY. Esta función está diseñada para permitir al usuario, una flexibilidad adicional para decidir el momento en que se invoca FlashCopy. Hacer o no una copia física de los datos a través de un proceso en modo Background. Si no se realiza la Copia física, la copia física de origen se mantiene con apuntando a la copia activa de los datos, así como a la copia virtual (punto-en-tiempo, es decir al momento en que se decida hacer la copia al destino). Esta función está diseñada para hacer copias de los volúmenes completos que luego pueden ser habilitados para los sistemas y utilizados para múltiples propósitos.
Además, se puede usar un comando llamado: "Start Background Copy Now – Arrancar Copia en modo", para iniciar la copia en modo Background, cuando sea necesario.
Como resultado, la mayoría de las ejecuciones de FlashCopy son configuradas en la opción NOCOPY, en la Figura 3-11, se muestra cómo funciona el IBM FlashCopy.

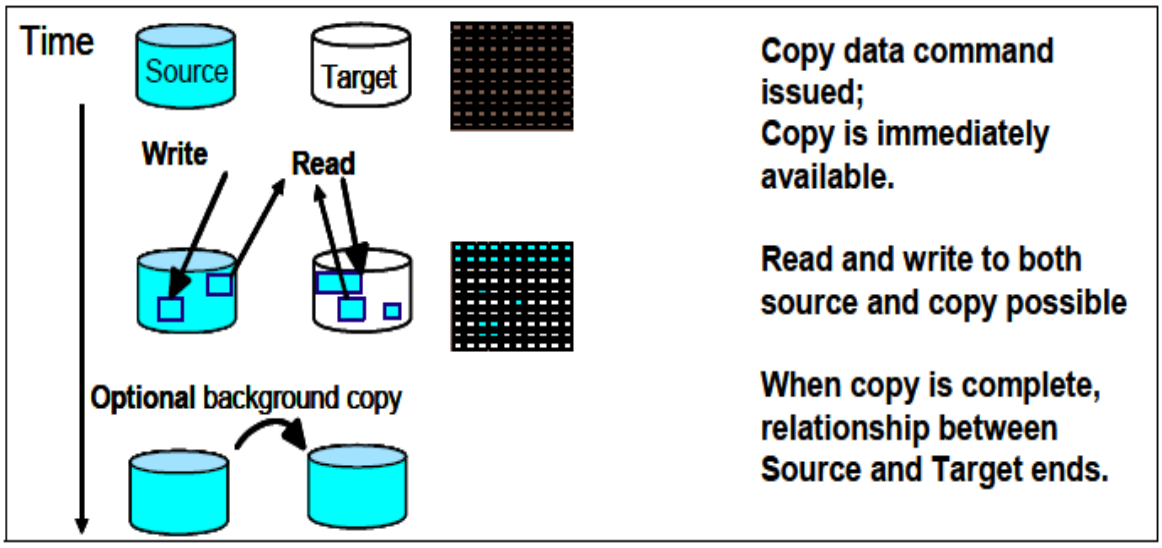



*Figura 3.11: IBM eStorage FlashCopy[9]*

Con base en esta configuración típica se llegará a la arquitectura comentada como FlashCopy o Metro Global Mirroring, misma que se puede esquematizar como se muestra en las figuras 3.12 y 3.13.

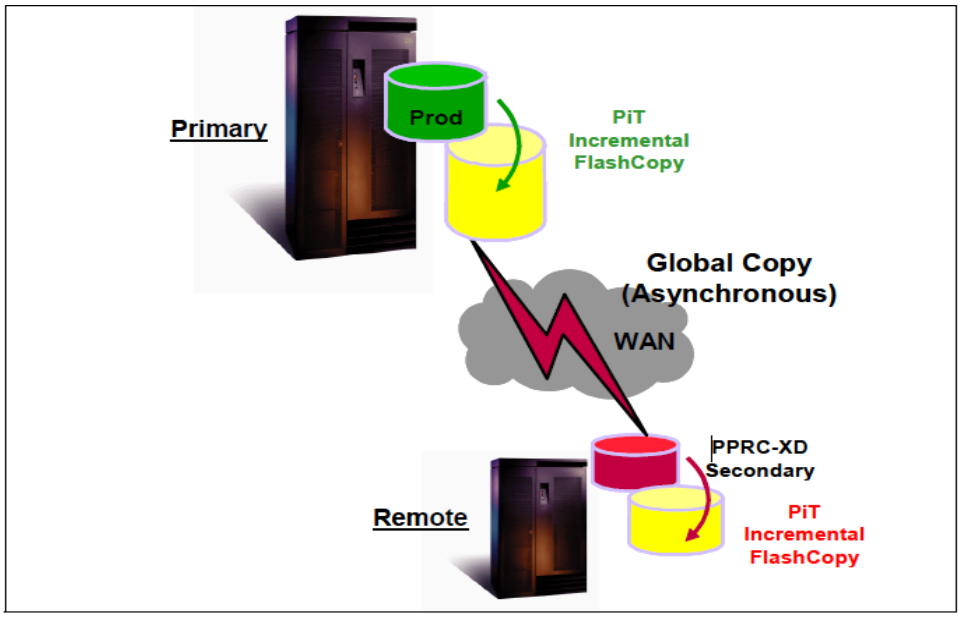



*Figura 3.12: IBM FlashCopy / Metro Global Mirroring.[10]*

[9] IBM, Red Book, Chapter 3. Part II: Storage technology for disaster recovery.
[10] IBM Red Book, IBM Storage Infrastructure for Business Continuity.

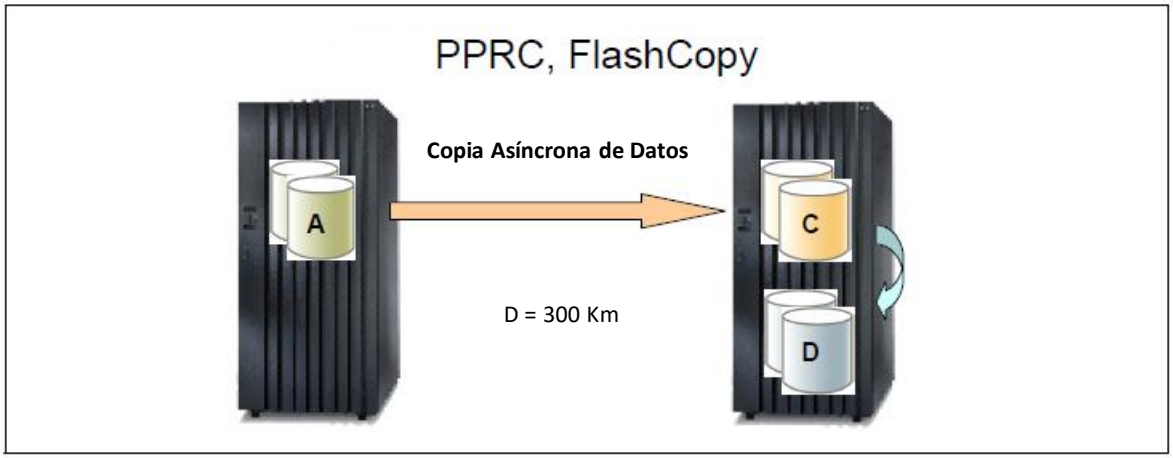



***Figura 3.13: IBM PPRC FlashCopy[11]***

A continuación, en las figuras; 3.14,3.15, 3.16, 3.17 y 3.18, se muestra un esquema típico de cómo se configura el FlashCopy a través del consola del ISFP[12] del equipo (Mainframe[13] con sistema operativo zOS[14], marca IBM), a través de los paneles mostrados, se lleva a cabo la definición y preparación de los volúmenes (discos) que serán copiados desde el Site origen hacia el Site destino, esto permitirá al FlashCopy realizar la copia remota, considerando todos los datos (Data Sets; archivos que se usarán en el Site secundario para activar la infraestructura del DRP y permitir la continuidad del negocio.

```
FLYPFC00 ---------- FlashCopy Manager -  V5R1M0  - Primary panel ---
 OPTION ===>  1

 Enter one of the following options:

FlashCopy Manager functions:

    1  ALLOCATE      - Allocate/De-allocate data sets
    2  SETUP         - Create and submit setup JOB
    3  SEL-SOURCE    - Select Source devices/volumes
    4  SEL-TARGET    - Select Target devices/volumes
    5  CONFIGURE     - Configure Source-Target environment
    6  BUILD-JOBS    - Build FlashCopy Manager Jobs

FlashCopy Manager Dataset Control Information
    High level DSN qualifier  ===> C816171
    FC Group qualifier        ===> FC2107

Service level: April 24, 2008
```

***Figura 3.14: FlashCopy Manager Menú Primario.[15]***

[11] IBM System Storage FlashCopy Manager and PPRC Manager Overview.
[12] ISPF, es un conjunto de herramienta de administración del sistema operativo zOS marca IBM, utilizado en los equipos llamados Mainframe, tiene un editor e interfaz de usuario.
[13] Mainframe, marca registrada de IBM, son computadoras de alta capacidad, su potencia de procesamiento se mide en MIPS (Millones de Instrucciones por Segundo).
[14] zOS: Sistema Operativo z para equipos de la línea zSeries de IBM, marcas registradas.
[15]Fuente: IBM System Storage FlashCopy Manager and PPRC Manager Overview

En este menú del ISPF para el FlashCopy Manager, se utilizan las siguientes funciones para configurar, un entorno de FlashCopy y crear los trabajos (JOBs) para administrar FlashCopy:

**1. ASIGNAR.**

Asignar los conjuntos de datos (Data Sets: Archivos), utilizados por FlashCopy Manager.

**2. CONFIGURACIÓN.**

Crear y enviar trabajos de grupos de datos (Data Sets) y de configuración de JOBs (trabajos).

**3. SEL-FUENTE.**

Selecciona volúmenes de origen.

**4. SEL-TARGET.**

Selecciona los volúmenes de destino.

**5. CONFIGURAR.**

Configure los entornos origen y destino de FlashCopy.

**6. Construye JOBs**

Generar trabajos de FlashCopy Manager.

Tiene la opción de que cada paso, pueda ser automatizado e incluido para ejecutarse como parte de un trabajo automatizado del sistema operativo z / OS, como parte de una cadena de trabajos (JOBs).

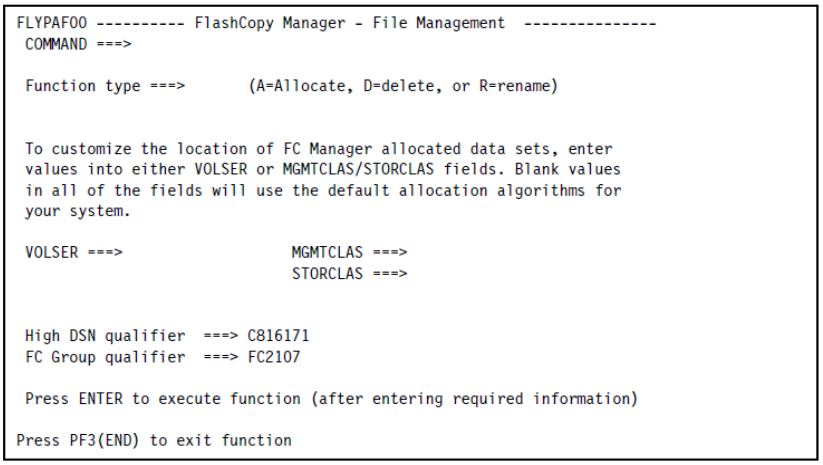



***Figura 3.15: Asignación de conjuntos de datos (Data Sets) para administrar las definiciones de FlashCopy.***[16]

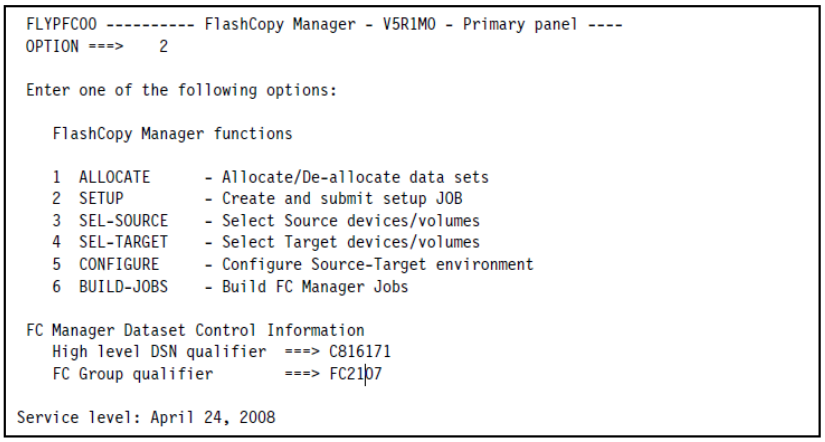



***Figura 3.16: Creación y envío del trabajo de instalación desde el panel principal.***[17]

[16] Fuente: IBM System Storage FlashCopy Manager and PPRC Manager Overview

[17] Fuente: IBM System Storage FlashCopy Manager and PPRC Manager Overview

```
Menu Utilities Compilers Help
 SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS
 BROWSE C816171.FCMGR.FC2107.NEW.DEVICE.DATA Line 000000 Columns 0001 080
 Command ===>                                                Scroll ===> CSR
 ****** ***************************** Top of Data ******************************
FLYAT03C DATE 08120 TIME: 142730 SYSTEM: MES1
DEVN MODEL... VOLSER STORAGE SSID STG CNTL. STRING STRING.... DEVICE DEVICE
.....................CONTROL .....SERIAL.......... SERIAL .......... SERIAL
D811 3390-2C. ?????? 2105F20 8102 13-00FCA81 2105. 13-00FCA81 2105.. 13-00FCA8
D812 3390-2C. ?????? 2105F20 8102 13-00FCA81 2105. 13-00FCA81 2105.. 13-00FCA8
D813 3390-2C. ?????? 2105F20 8102 13-00FCA81 2105. 13-00FCA81 2105.. 13-00FCA8
D814 3390-2C. ?????? 2105F20 8102 13-00FCA81 2105. 13-00FCA81 2105.. 13-00FCA8
D815 3390-3.. IND815 2105F20 8108 13-00FCA81 2105. 13-00FCA81 2105.. 13-00FCA8
D816 3390-3.. IND816 2105F20 8108 13-00FCA81 2105. 13-00FCA81 2105.. 13-00FCA8
D817 3390-3.. IND817 2105F20 8108 13-00FCA81 2105. 13-00FCA81 2105.. 13-00FCA8
D818 3390-3.. IND818 2105F20 8108 13-00FCA81 2105. 13-00FCA81 2105.. 13-00FCA8
D911 3390-9.. IND911 2105F20 8108 13-00FCA81 2105. 13-00FCA81 2105.. 13-00FCA8
D912 3390-9.. IND912 2105F20 8108 13-00FCA81 2105. 13-00FCA81 2105.. 13-00FCA8
etc.
```

***Figura 3.17: Conjunto de Archivos y/o Bases de Datos de salida de FlashCopy Manager (lado izquierdo del panel)[18]***

```
Menu Utilities Compilers Help
 SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS
 BROWSE C816171.FCMGR.FC2107.NEW.DEVICE.DATA Line 000000 Columns 053 132
 Command ===>                                                Scroll ===> CSR
 ****** ***************************** Top of Data ******************************

STRING.... DEVICE DEVICE.... CCA DDC LSS. CYLS T/CYL
SERIAL .......... SERIAL
13-00FCA81 2105.. 13-00FCA81 10. 10. 01.. .2226 15 .. OFF
13-00FCA81 2105.. 13-00FCA81 11. 11. 01.. .2226 15 .. OFF
13-00FCA81 2105.. 13-00FCA81 12. 12. 01.. .2226 15 .. OFF
13-00FCA81 2105.. 13-00FCA81 13. 13. 01.. .2226 15 .. OFF
13-00FCA81 2105.. 13-00FCA81 64. 64. 07.. .3339 15 .. ON
13-00FCA81 2105.. 13-00FCA81 65. 65. 07.. .3339 15 .. ON
13-00FCA81 2105.. 13-00FCA81 66. 66. 07.. .3339 15 .. ON
13-00FCA81 2105.. 13-00FCA81 67. 67. 07.. .3339 15 .. ON
13-00FCA81 2105.. 13-00FCA81 68. 68. 07.. 10017 15 .. ON
13-00FCA81 2105.. 13-00FCA81 69. 68. 07.. 10017 15 .. ON
etc.
```

***Figura 3.18: Conjunto de Archivos y/o Bases de Datos de salida de FlashCopy Manager (lado derecho del panel)[19]***

Una vez configurados los Data Sets (Archivos y Bases de Datos) que serán copiados al Sitio Secundario, ya estamos en condiciones de realizar el **Peer To Peer Remote Copy[20] con FlashCopy (PPRC – FlashCopy)** de manera permanente, esta solución de replicación de storage, **sustentará el cumplimiento del RTO y del RPO, establecido por el BIA**, ya que el storage en el sitio secundario, estará **continuamente recibiendo datos desde el Sitio Primario** y permitirá la activación de la infraestructura tecnológica, es decir, de los equipos Mainframe y del ambiente distribuido, (el ambiente distribuido, normalmente engloba servidores Intel y otros sistemas abiertos), con ésta solución, se podrá soportar la

[18] Fuente: IBM System Storage FlashCopy Manager and PPRC Manager Overview

[19] Fuente: IBM System Storage FlashCopy Manager and PPRC Manager Overview

[20] PPRC: Peer to Peer Remote Copy: Copia Remota entre Pares, IBM technologies.

Continuidad de la Operación de la Empresa, bajo las condiciones señaladas en el BIA (Business Impact Analysis), **evitando el impacto financiero** que potencialmente se podría producir **después de las primeras 8 horas de suspensión de las operaciones y que sería acumulativo**, conforme transcurra el tiempo.

### 3.3.4. Elaboración de Caso de Negocio (Business Case) para Selección de Escenario de Recuperación.

Considerando los escenarios presentados en el Capítulo 2, se procede a elaborar el Caso de Negocio para seleccionar el mejor escenario que deberá cumplir los siguientes objetivos tecnológicos y financieros:

***Criterios de Selección de Solución Tecnológica para la Metodología de Recuperación:***

- ✪ Satisfacer el criterio de RTO / RPO, derivado del Análisis de Impacto al Negocio (BIA), es decir:
  - **RTO= 0 < de 8 horas**
  - **RPO = 0 < de 2 horas**
- ✪ La inversión deberá ser **igual o menor al 10%** de las pérdidas financieras que potencialmente se presenten en caso de Desastre o Contingencia durante las primeras **8 horas de haber ocurrido el desastre**.
- ✪ Cumplir con el Standard **ANSI /TIA 942, con Tier igual o mayor a 3 (ver figura 3.19)**

| | Tier I | Tier II | Tier III | Tier IV |
|---|---|---|---|---|
| Active Capacity Components to Support IT Load | N | N+1 | N+1 | N after any failure |
| Distribution Paths | 1 | 1 | 1 active and 1 alternate | 2 simultaneously active |
| Concurrently Maintainable | No | No | Yes | Yes |
| Fault Tolerance (single event) | No | No | No | Yes |
| Compartmentalization | No | No | No | Yes |
| Continuous Cooling* | load density dependent | load density dependent | load density dependent | Yes (Class A) |

***Figura 3.19: Centro de Datos TIERs, fuente Uptime Institute[21].***

- ✪ El Site secundario en cualesquiera escenarios de los aquí descritos, deberá estar ubicado al menos a 30 millas (48 Km) de distancia del Site Primario, con la finalidad de alinearse a las mejores prácticas de la industria de TI.
- ✪ Cumplir con la normatividad establecida por la CNBV[22] para el tratamiento, resguardo y ubicación de los datos financieros de los clientes.

21 **Uptime Institute** es una organización de asesoría imparcial enfocada en mejorar el desempeño, la eficiencia y la confiabilidad de la infraestructura crítica de negocios a través de la innovación, colaboración y certificaciones independientes,
22 **CNBV**: Comisión Nacional Bancaria y de Valores de México, esta entidad es la encargada de regular las actividades financieras de los Bancos y Casas de Bolsa conjuntamente con el **Banco de México**.

- ✪ Infraestructura tecnológica dedicada; Equipos de Procesamiento (Mainframe, Servidores físicos o virtuales, Midrange, etc..), Storage, balanceadores de carga, equipos y medios de telecomunicaciones (firewalls, routers, switches, etc..), dedicados y con nivel de redundancia N +2 o bien High Availability (HA), alta disponibilidad.
- ✪ Personal técnico asignado y calificado para asistir y operar durante la recuperación en casos de Desastre o Contingencia y durante las pruebas anuales del Plan de Recuperación en Casos de Desastre (DRP).
- ✪ Actualización tecnológica continua o al menos cada 2 años.
- ✪ Capacidad para ejecutar al menos 2 pruebas de DRP al año.
- ✪ Elasticidad en la solución; es decir, la capacidad de la infraestructura para crecer o reducirse rápidamente para lograr un óptimo nivel de Costo / Beneficio.
- ✪ Cumplimiento del Standard **ISO27001**.[23]
- ✪ Cumplir con una auditoria anual de **SSAE16**[24]

Considerando los criterios antes citados, realizaremos una clasificación de ellos para establecer dos tipos de objetivos:

- ✪ ***Objetivos Obligatorios***
- ✪ ***Objetivos Deseados***

Los **Objetivos Obligatorios** son aquellos que cualquier solución o escenario deberá cubrir sin excepción alguna, aquella solución o escenario que no los cubra, será eliminada de inmediato sin evaluar los objetivos deseados.

Los **Objetivos Deseados** son aquellos que complementan a la solución y la mejoran en términos de funcionalidad o costo beneficio o sin los cuales la solución o escenario es operable y funcional.

**Objetivos Obligatorios, establecidos para la Selección de Escenarios:**

- ✪ Satisfacer el criterio de RTO / RPO, derivado del Análisis de Impacto al Negocio (BIA), es decir:
- **RTO= 0 < de 8 horas**

[23] **ISO / IEC 27001:** 2005 es una norma de seguridad de la información que fue publicada en septiembre de 2013. Sustituye a ISO / IEC 27001: 2005 y es publicada por la **Organización Internacional de Normalización (ISO)** y la **Comisión Electrotécnica Internacional (CEI)** El subcomité conjunto ISO / CEI, ISO / IEC JTC 1 / SC 27. [2] Es una especificación para un sistema de gestión de la seguridad de la información (SGSI). Las organizaciones que cumplen con la norma pueden ser certificadas como conformes por un organismo de certificación independiente y acreditado en la finalización exitosa de una auditoría de cumplimiento. Fuente: Wikipedia.

[24] **La Declaración sobre Normas para los Servicios de Certificación (SSAE) 16**, es un estándar de auditoría para las organizaciones de servicios, que **reemplaza** al **SAS 70**. El "examen del auditor de servicio" de este último, se sustituye por un informe de " SSAE 16 fue publicado en abril de 2010, y entró en vigencia en junio de 2011; Muchas organizaciones que siguieron al SAS 70 han cambiado ahora al SSAE 16. Fuente Wikipedia.

- **RPO = 0 < de 2 horas**

✪ La inversión deberá ser **igual o menor al 10 %** de las pérdidas financieras que potencialmente se presenten en caso de Desastre o Contingencia durante las primeras **8 horas de haber ocurrido el desastre**.

✪ Cumplir con el Standard **ANSI /TIA 942, con Tier igual o mayor a 3**

✪ Cumplir con el estándar SSAE16 e ISO 27001

✪ Cumplir con la normatividad establecida por la CNBV[25] para el tratamiento, resguardo y ubicación de los datos financieros de los clientes.

✪ Infraestructura tecnológica dedicada; Equipos de Procesamiento (Mainframe, Servidores físicos o virtuales, Midrange, etc..), Storage, balanceadores de carga, equipos y medios de telecomunicaciones (firewalls, routers, switches, etc..), dedicados y con nivel de redundancia N +2 o bien High Availability (HA), alta disponibilidad.

✪ Cumplimiento del Standard **ISO27001**.[26]

**Objetivos Deseados, establecidos para la Selección de Escenarios:**

✪ Personal técnico asignado y calificado para asistir y operar durante la recuperación en casos de Desastre o Contingencia y durante las pruebas anuales del Plan de Recuperación en Casos de Desastre (DRP).

✪ Actualización tecnológica continua o al menos cada 2 años.

✪ Capacidad para ejecutar al menos 2 pruebas de DRP al año.

✪ Elasticidad en la solución; es decir, la capacidad de la infraestructura para crecer o reducirse rápidamente para lograr un óptimo nivel de Costo / Beneficio.

✪ Proveer los servicios en territorio de la República Mexicana.

✪ Mecanismo para realizar cambios en el alcance contractual, establecidos en el contrato.

✪ Capacidad para proveer Soporte Técnico Especializado, desde otros países de manera remota o presencial.

El siguiente paso, consiste en realizar una matriz de Costo para cada escenario propuesto desde el Capítulo 2, página 5,6 y 7, con la finalidad de realizar la evaluación de Costo Beneficio, desarrollaremos el caso de negocio para cada escenario.

---

25 **CNBV**: Comisión Nacional Bancaria y de Valores de México, esta entidad es la encargada de regular las actividades financieras de los Bancos y Casas de Bolsa conjuntamente con el **Banco de México**.

[26] **ISO / IEC 27001:** 2005 es una norma de seguridad de la información que fue publicada en septiembre de 2013. Sustituye a ISO / IEC 27001: 2005 y es publicada por la **Organización Internacional de Normalización (ISO)** y la **Comisión Electrotécnica Internacional (CEI)** El subcomité conjunto ISO / CEI, ISO / IEC JTC 1 / SC 27. [2] Es una especificación para un sistema de gestión de la seguridad de la información (SGSI). Las organizaciones que cumplen con la norma pueden ser certificadas como conformes por un organismo de certificación independiente y acreditado en la finalización exitosa de una auditoría de cumplimiento. Fuente: Wikipedia.

## i. Casos de Negocio de los Escenarios de Solución Propuestos.

### Escenario 1: Contratación de Hot Site:

En este escenario los costos que consideraremos, son los que típicamente configuran un contrato de este tipo de Servicio de Hot Site y normalmente se establecen contratos con una duración de 5 años, ver tabla 3.20 del Caso de Negocio para Escenario 1:

***Tabla 3.20: Caso de Negocios para Escenario 1.***

| Concepto | Costo Mensual USD | Costo Anual USD | Costo de Única Vez USD | Costo recurrente Nota (**) | Subtotales USD |
|---|---|---|---|---|---|
| Renta Mensual | $4,500.00 | | | | $4,500.00 |
| Renta Anual | | $54,000.00 | | | $54,000.00 |
| Declaración de Contingencia (*) | | | $10,000.00 | | $10,000.00 |
| Uso diario de Hot Site por Declaración de Contingencia (**) | | | $2,500.00 | $12,500.00 | $2,500.00 |
| Uso por una semana de Hot Site (***) | | | $17,500.00 | | $17,500.00 |
| **Total General en USD** | | | | | **$ 88,500.00** |
| **Total General en USD por Contrato a 5 años** | | | | | **$ 442,500.00** |

**Notas:**

*(*) Se esta considerando una declración de contingencia con la finalidad de evaluar el costocompleto de la solución.*

*(**) Se considerarán 5 días de costo diario*

*(***) Se considerará una semana de costo adicional.*

### Escenario 2: Site Secundario en Esquema Hosting / Outsourcing.

Este escenario consiste en contratar un Centro de Datos (Data Center) con infraestructura tecnológica **dedicada y permanentemente funcionando, bajo un esquema de replicación de datos asíncrona ó síncrona** para un cliente en específico, este escenario dependerá del resultado del **BIA** y del presupuesto que la empresa esté dispuesta a invertir para recuperar su negocio en el rango de **2 a 8 horas como máximo,** pues la decisión esta basada en el **balance de Pérdidas Financieras VS Costo del Site Secundario**.

En la tabla 3.21 se muestra el Caso de Negocio de este escenario.

*Tabla 3.21: Caso de Negocios para Escenario 2.*

| Concepto | Costo Año 1 USD | Costo Año 2 USD | Costo Año 3 USD | Costo Año 4 USD | Costo Año 5 USD | Total a 5 años USD |
|---|---|---|---|---|---|---|
| Plataforma Mainframe (z13) | $2,239,668.00 | $2,351,651.40 | $2,469,233.97 | $2,592,695.67 | $2,722,330.45 | $12,375,579.49 |
| Plataforma Midrange (pSeries) | $302,516.00 | $317,641.80 | $333,523.89 | $350,200.08 | $367,710.09 | $1,671,591.86 |
| Servicios de Servidores Intel (iSeries) | $288,457.00 | $302,879.85 | $318,023.84 | $333,925.03 | $350,621.29 | $1,593,907.01 |
| Servicios de Telecomunicaciones | $367,287.00 | $385,651.35 | $404,933.92 | $425,180.61 | $446,439.64 | $2,029,492.52 |
| **Total cargo anual en USD** | **$3,197,928.00** | **$3,357,824.40** | **$3,525,715.62** | **$3,702,001.40** | **$3,887,101.47** | **$17,670,570.89** |

**Notas:**

* Con la finalidad de comparar adecuadamente los escenarios, los ejercicios financieros se proyectaron a 5 años.

** Este escenario consiste en el hosting de la infraestructura y su operación por parte de un Outsourcer

## Escenario 3. Construcción de un Sitio Secundario de Recuperación (Secondary Site):

Este escenario consiste en llevar a cabo la construcción de un **segundo Centro de Datos (Data Center)** por parte de la empresa, con la inversión que esto implica para la obra civil y su posterior equipamiento tecnológico.

De igual manera que en los dos escenarios anteriores, la decisión estará basada en términos de Costo / Beneficio y del cumplimiento del RPO / RTO que permita minimizar los impactos financieros y los riesgos implícitos en cada escenario.

En la tabla 3.22 se muestra el Caso de Negocio de este escenario.

*Tabla 3.22: Caso de Negocios para Escenario 3*

| Concepto | Inversión Inicial USD | Costo Mensual USD | Costo Anual USD (Año 1) | Costo Año 2 | Costo Año 3 | Costo Año 4 | Costo Año 5 | Costo Total a 5 Años |
|---|---|---|---|---|---|---|---|---|
| Construcción de Centro de Cómputo Secundario (Proyecto y Obra Civil) | $ 2,500,000.00 | | | | | | | |
| Acondicionamiento del Edificio (AA, UPS, Generadores Diesel) | $ 625,000.00 | | | | | | | |
| Adquisición de Hardware (Mainframe), Software, Equipo de Telecomunicaciones + Servidores | $ 10,102,456.00 | | | | | | | |
| Mantenimiento de equipos (HW) | | $ 150,000.00 | $ 1,800,000.00 | $ 1,890,000.00 | $ 1,984,500.00 | $ 2,083,725.00 | $ 2,187,911.25 | $ 10,096,136.25 |
| Telecomunicaciones enlaces | | $ 270,000.00 | $ 3,240,000.00 | $ 3,402,000.00 | $ 3,572,100.00 | $ 3,750,705.00 | $ 3,938,240.25 | $ 18,173,045.25 |
| **Total General en USD** | **$ 13,227,456.00** | **$ 420,000.00** | **$ 5,040,000.00** | **$ 5,292,000.00** | **$ 5,556,600.00** | **$ 5,834,430.00** | **$ 6,126,151.50** | **$ 27,849,181.50** |
| **Total General de Inversión más Costo Total a 5 años** | **$ 41,076,637.50** | | | | | | | |

**Notas:**

1) Se hace el caso de negocio hasta 5 años con la finalidad de poder comparar financieramente los escenarios de solución señalados en este capítulo del presente trabajo

## ii. Comparativo de los Escenarios de Solución Propuestos.

Para llevar a cabo una selección del mejor escenario para cubrir las necesidades de recuperación del Negocio, considerando los resultados del BIA (Business Impact Analysis)[27], se desarrolló un análisis que nos permite asignar un valor cuantitativo y cualitativo a cada escenario de recuperación, con la finalidad de ser muy objetivos en la selección del Escenario de Solución, dado que se pretende que la empresa invierta una gran cantidad de dinero para evitar impactos por falta de continuidad en sus operaciones.

Para llevar a un plano objetivo la decisión, se utilizó una metodología llamada Análisis de para la Toma de Decisiones de Kepner & Trigoe (MR) [28], la metodología nos permite asignar bajo un cierto rango, calificación y ponderación para cada alternativa analizada y permite separar los objetivos que se pretenden cubrir en dos grupos: Objetivos Obligatorios y Objetivos Deseados, los primeros (Obligatorios), son aquellas que son irrenunciables y los segundos (Deseados), son los que agregan un plus a la alternativa y complementan el análisis, puede o no que sean muy importantes pero contribuyen a enriquecer las características de cada alternativa comparada.

Con base en lo anterior, en las tablas 3.23 y 3.24, se muestran agrupados los **Objetivos Obligatorios y Deseados**, así como sus características, calificación y calificación ponderada:

[27] BIA (Business Impact Analysis): Análisis de Impacto al Negocio por sus siglas en Ingles.
[28] Análisis de Problemas y Toma de Decisiones(MR), KEPNER & TRIGOE

*Tabla 3.23: Objetivos Obligatorios que Debe Cubrir la Alternativa Elegida*

| | Alternativas de Solución | | | | | |
|---|---|---|---|---|---|---|
| **Objetivos** | **Alternativa o Escenario 1 Contratación de Hot Site** | | **Alternativa o Escenario 2 Secundary Site / Hosting Outsourcing** | | **Alternativa o Escenario 3 Construcción de Secundary Site** | |
| **Obligatorios** | **Descripción** | **Cumple / No Cumple** | **Descripción** | **Cumple / No Cumple** | **Descripción** | **Cumple / No Cumple** |
| RTO= o < de 8 horas | Este escenario por la naturaleza de los servicios, no proporciona infraestructura dedicada por lo cual no se puede lograr la recuperación de la infraestructura en 8 horas o menos. | **No Cumple** | Este escenario considera la replicación asíncronica de storage (Data), lo cual permitirá alcanzar un RTO= o < a 8 horas, permitiendo activar la infraestructura en ese lapso de tiempo. | **Cumple** | También este escenario considera la replicación asíncronica de storage (Data), lo cual permitirá alcanzar un RTO= o < a 8 horas, permitiendo activar la infraestructura en ese lapso de tiempo. | **Cumple** |
| RPO = o < de 2 horas | Al no contar con replicación síncrona o asíncrona, no se podrías tener los datos con una frescura de al menos 2 horas | **No Cumple** | Al contar con la replicación de datos a través de una enlace dedicado y con copia incremental de datos una vez realizada la primer copia , es factible contar con datos frescos y por consecuencia el RPO = o < a 2 horas. | **Cumple** | También este escenario, al contar con la replicación de datos a través de una enlace dedicado y con copia incremental de datos una vez realizada la primer copia , es factible contar con datos frescos y por consecuencia el RPO = o < a 2 horas. | **Cumple** |
| La inversión deberá ser igual o menor al 10% de las pérdidas financieras ($723´116,055.26)que potencialmente se presenten en caso de Desastre o Contingencia durante las primeras 8 horas de haber ocurrido el desastre. | $ 442,500.00 | **Cumple** | $ 17,670,570.89 | **Cumple** | $ 41,076,637.50 | **Cumple** |
| Cumplir con el Standard ANSI /TIA 942, con Tier igual o mayor a 3 | Los proveedores de Hot Site, están apegados a este estándar ya que es una Best Practice en la industria | **Cumple** | Los proveedores de Hosting y Outsourcing, están apegados a este estándar ya que es una Best Practice en la industria | **Cumple** | La construcción o adecuación de un Data Center , requerirá la certificación de este estandar y deberá incluirse en el diseño del Data Center | **Cumple** |
| Cumplir con el estándar SSAE16 e ISO 27001 | Los proveedores de este tipo de servicios, cumplen con este estándar ya que es una Best Practice de la industria | **Cumple** | Los proveedores de este tipo de servicios, cumplen con este estándar ya que es una Best Practice de la industria | **Cumple** | Los proveedores de este tipo de servicios, cumplen con este estándar ya que es una Best Practice de la industria | **Cumple** |
| Cumplir con la normatividad establecida por la CNBV para el tratamiento, resguardo y ubicación de los datos financieros de los clientes | Los proveedores de este tipo de servicios tienen instalaciones en la República Mexicana por lo que cumplirian con este objetivo | **Cumple** | Los proveedores de este tipo de servicios tienen instalaciones en la República Mexicana por lo que cumplirian con este objetivo | **Cumple** | Los proveedores de este tipo de servicios tienen instalaciones en la República Mexicana por lo que cumplirian con este objetivo | **Cumple** |
| Infraestructura tecnológica dedicada; Equipos de Procesamiento (Mainframe, Servidores físicos o virtuales, Midrange, etc..), Storage, balanceadores de carga, equipos y medios de telecomunicaciones (firewalls, routers, switches, etc..), dedicados y con nivel de redundancia N +2 o bien High Availability (HA), alta disponibilidad. | Los proveedores de Hot Site , en esta modalildad no ofrecen Infraestructura dedicada, debido a como funciona este modelo | **No Cumple** | Al establecer un contrato de Hosting / Outsourcing, el proveedor provee en sus data Centers la infraestructura dedicada que solicita el cliente | **Cumple** | Al invertir en infraestrcutura para instalarla en el Data Center | |
| Cumplimiento del Standard ISO27001 | Los proveedores de Hot Site se apegan a este standard de Seguridad | **Cumple** | Los proveedores de Hosting / Outsourcing se apegan a este standard de Seguridad | **Cumple** | La empresa puede Certificarse en este standard | **Cumple** |

## *Tabla 3.24: Objetivos Deseados que Debe Cubrir la Alternativa Elegida*

| | | Alternativa o Escenario 1 Contratación de Hot Site | | | | Alternativa o Escenario 2 Secondary Site / Hosting Outsourcing | | | | Alternativa o Escenario 3 Construcción de Secondary Site por Parte del Banco | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Objetivos Deseados** | **Peso** | **Información** | **Calf.** | **Calif . Pond.** | | **Peso** | **Información** | **Calf.** | **Calif . Pond.** | **Peso** | **Información** | **Calf.** | **Calif . Pond.** |
| Personal técnico asignado y calificado para asistir y operar durante la recuperación en casos de Desastre o Contingencia y durante las pruebas anuales del Plan de Recuperación en Casos de Desastre (DRP). | 7% | Esta alternativa si cuenta con un staff de técnico especializado en todo momento en el Hot Site para apoyar al clilente. | 10 | 0.7 | | 7% | El staff técnico especializado lo incluye como parte del alcance de servicio solicitado. | 10 | 0.7 | 7% | La empresa cuenta con staff técnico especializado para estas actividades. | 10 | 0.7 |
| Actualización tecnológica continua o al menos cada 2 años. | 20% | La actualización se solicita al proveedor e implica pagos adicionales | 7 | 1.4 | | 20% | El alcance de los servicios de Hosting en Outsourcing incluyen la cláusula de refresh tecnológico cada 2 años | 9 | 1.8 | 20% | La empresa debe considerar en su gasto de Inversión anual el presupuesto para la actualización tecnológica. | 9 | 1.8 |
| Capacidad para ejecutar al menos 2 pruebas de DRP al año | 25% | Los servicios de Hot Site, incluyen en el pago mensual una semana para realizar pruebas ó declarar contingencia | 8 | 2 | | 25% | El site bajo Hosting / Outsourcing , esta disponible siempre durante la vida del contrato y solamente se requiere aviso por escrito para usarlo. | 10 | 2.5 | 25% | La disponibilidad del sitio siempre estará presente. | 10 | 2.5 |
| Elasticidad en la solución; es decir, la capacidad de la infraestructura para crecer o reducirse rápidamente para lograr un óptimo nivel de Costo / Beneficio | 15% | Se tiene que elaborar Adendum al contrato para reducir o incrementar la infraestrcutura | 8 | 1.2 | | 15% | Se tien que elaborar un PCR (Project Change Request), Requerimiento de Cambio en el Projyecto. | 8 | 1.2 | 15% | Se tiene que relizar compra para incrementar la infraestructura. | 8 | 1.2 |
| Proveer los servicios en territorio de la República Mexicana. | 18% | Cumple | 10 | 1.8 | | 18% | Cumple | 10 | 1.8 | 18% | Cumple | 10 | 1.8 |
| Mecanismo para realizar cambios en el alcance contractual, establecidos. | 10% | Cumple | | 0 | | 10% | Cumple | | 0 | 10% | Cumple | | 0 |
| Capacidad para proveer Soporte Técnico Especializado, desde otros países de manera remota o presencial. | 5% | Limitado | 5 | 0.25 | | 5% | Amplio | 10 | 0.5 | 5% | Limitado | 9 | 0.45 |
| **Total de Calificación con Ponderación** | | | | **7.35** | | | | | **8.5** | | | | **8.45** |

**Rango de Pesos: 1 a 10**
**Ponderación: en % asignando elmayor porcentaje**
**al objetivo que tenga el mayor peso así sucesivamente**

Como se puede observar en la tabla 3.23, la única alternativa que No Cumple todos los objetivos obligatorios, es la alternativa 1, motivo por el cual, se descarta automáticamente al no cumplir con todos los objetivos obligatorios de la solución requerida.

Por lo anterior, se pasa al siguiente nivel del proceso en el cual se analizan los objetivos deseados para cada solución, con la finalidad de llevar estos objetivos a una calificación y ponderación que nos permita tomar la mejor decisión.

En la tabla 3.24, se puede observar que la alternativa 2 de Secondary Site (en un esquema de Outsourcing – Hosting), **es la alternativa que representa mayores ventajas y representa un costo menor que la alternativa 3, por lo cual surge con mejor calificación por 5 décimas contra la Alternativa 3**.

Habiendo elegido la alternativa que sustentará la solución tecnológica, se procede a desarrollar la arquitectura de solución con sus componentes de:

- ✓ Hardware (Mainframe- zSeries, servidores Intel, Equipo Midrange tipo IBM pSeries)
- ✓ Storage
- ✓ Software (Sistemas operativos, Middleware, Software de Programación, SW de Monitoreo), este software forma parte del software en el Primary Site, y dado que se replicará a través del PPRC FlashCopy (ver página 18 del presente Capítulo), no es necesario adquirirlo, solamente se especifica en el contrato de licenciamiento que deberá estar disponible para su uso en el site de DRP 2 veces al año para la ejecución de pruebas de DRP y en caso de Desastre, lo cual implica, **una pequeña cuota adicional pero no se requiere adquirir doble licenciamiento.**
- ✓ Medios de comunicación (Enlaces de comunicación, routers, switches)

para equipar el Secondary Site.

## iii. Equipamiento del Escenario 2 Seleccionado.

**Equipamiento de Cómputo Central.**

En la tabla 3.25 se muestra el equipamiento que se tendrá incluido en los servicios de Secondary Site Hosting.

*Tabla 3.25: Equipamiento de Cómputo Central (puede ser escalable en el tiempo).*

| Equipo de Cómputo | | |
|---|---|---|
| **Hardware** | **Cantidad** | **Descripción** |
| zSeries Modelo 2964-708 (z13) | **1** | 11,188 MIPS (Millones de Instrucciones por Segundo), con:<br>CPUs 8 (Tipo CPs, IFL's 4, zIIP 16), con 2 LPARS (LPARS: Logical Partitions)<br>48 Canales<br>Memoria RAM: '512 GB de memoria real y 512 GB de memoria expandida |
| Tarjetas de Comunicación tipo OSA | **3** | Modelo IBM OSA: Open System Architecture |
| Storage | **2 TB** | Modelo IBM DS8000<br>1 TB Mainframe<br>1 TB Open systmes |
| Unidades de Cartucho | **12** | Modelo 3490 B20 y 1 VTS |
| AIX | **2** | Modelo 630 C4, , 4 CPUs (3.5 GHz ) 128 GB ram, 2 X 500 GB DASD, con capacidad ON Demand por 30 días consecutivos |
| Intel Servers | **350** | 300 servidores físicos (xSeries IBM, 4 CPUs (2.67 GHz - Xeon Octa Core), 64 GB RAM, 584 GB DASD. |
| VMWare Imágenes | **500** | Wintel 200, Linux Redhat 100, Linux Suse 100 |

**Software (Sistemas Operativos y Aplicaciones.**

Considerando que la solución se basa en un esquema de replicación de Storage, desde el Data Center Primario (Pimary Site) hacia el Secondary Site (ver página 13 del presente Capítulo) bajo el esquema de PPRC FlashCopy, la totalidad de los storage groups[29], se copiarán, lo cual permitirá copiar los discos y por consecuencia, las librerías en donde radican el sistema Operativo y demás productos de software que permiten el funcionamiento del Mainframe y de los ambientes Open (Abiertos: AIX, Windows, Linux).

En la tabla 3.26 se tiene una relación de los productos de software incluyendo los sistemas Operativos.

[29] Storage Groups: Grupos de Almacenamiento

*Tabla 3.26: Equipamiento de Cómputo Central (puede ser escalable en el tiempo)*

| | Software Principal |
|---|---|
| Software | Descripción |
| z/OS V2.1 | Sistema Operativo para la z13 en ambas Lpars (LPAR: Logical Partition) |
| CICS TS V5.4 | Customer Information Control System Transaction Server (Administrador de transacciones en línea), soporta lenguajes desde Cobol Enterprise hasta Java EE7. |
| JES2 (Job Entry Subsystem) | Job Entry Subsystem is a component of z/ Operative System |
| Communication Manager (antes VTAM) | Virtual Telecommunication Access Method (a través de este método de compara comunicaciones, se pude trabajar con una tarjeta OSA: Open System Archutecture y de esta manera se puede conectar el Mainframe hacia redes TCP/IP |
| DB2 V9 | Administrador de Base de Datos de IBM |
| TWS (Tivoli Workload Scheduler) | Planificador de Trabajos (JOBS) en el ambiente Mainframe bajo z/OS |
| SMF (System Management Facility) y RMF (Resource Measurements Facility) | Componente del sistema Operativo y es monitor del rendimiento, mediante colección de registros con una Layout predefinido que permite analuzar el performance del Mainframe. |
| REXX (Restructure Extended Executor) | Leanguaje de programación de Alto Nivel que forma parte del z/OS |
| COBOL Enterprise Commun Business Oriented Languaje) | Lenguaje de programación orientado a Negocios |
| C++ | |
| TSO / SDSF (TSO: Time Sharing Option) (SDFS: Spool Display and Search Facility) | Editor del z/OS |
| File AID Compuware | Software de Administración de Edición de Archivos |
| IBM RACF | Resource Control Access Facility: Facilicidades de Control de Acceso y Recursos |
| IBM DFSMS & DFHSM | Data Facility Storage Management Subsystem: Subsistema de administración de Datos y Almacenamiento |
| TLMS CA (Computer Associate) | Tape Library Management System: Sistema de Administración y Biblioteca de Cintas, el fabricante es CA (Computer Associate) |
| AIX Operating system V5.3 | Sistema operativo para pSeries |
| Wndows Server 2012 | Sistema Operativo servidores INTEL |
| Linux Redhat V6.9 | Sistema Operativo Linux Open |
| Suse Linux Enterprise | Sistema Operativo Linux Open |
| Sybase ASE V15.7 | Administrador de Base de Datos |
| Informix Seerver V11.70 IBM | Administrador de Base de Datos |
| IBM Tivoli Monitoring V6.3 | Suite de Prodcutos de IBM para monitoreo de ambientes Mainframe, Windows, Linux, Unix. |

## 3.3.5. Arquitectura de Comunicaciones.

El Centro de Datos Secundario (Secondary Site), se conectará a la Red de Comunicaciones del Banco a través de uno de los 2 Nodos Centrales, dado que la topología de la Red es centralizada:

- El Edificio Corporativo – 1, representa al Nodo A.
- El Edificio Corporativo -2, representa al Nodo B.
- También se tendrán Nodos Regionales.

En la figura 3.27 mostrada a continuación, se esquematizan ambos Nodos las funciones de comunicaciones que soportan.

## Edificio Corporativo -1 Nodo A.

- Recibirá todos los enlaces terrestres de alta velocidad a las plazas del interior de la República, 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 vía satélite
- Está enlazado vía microondas digitales, a los edificios corporativos 2 y 3, formando un triángulo. Cada enlace individual, tiene capacidad de transmitir 4 canales de 2 Mbps (E1's) 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[30] 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 Bancarias en zona metropolitana, actualmente enlazadas a través de 2 DSO's (64 Kbps) (RDI).[31]

[30] DACS: Digital Access Cross-Connect System (DACS, por sus siglas en inglés), Sistema de Conexión de Acceso Digital.
[31] RDI: Red Digital Integrada.
SAC: Satellite Access Controller: Control de Acceso al Satélite.

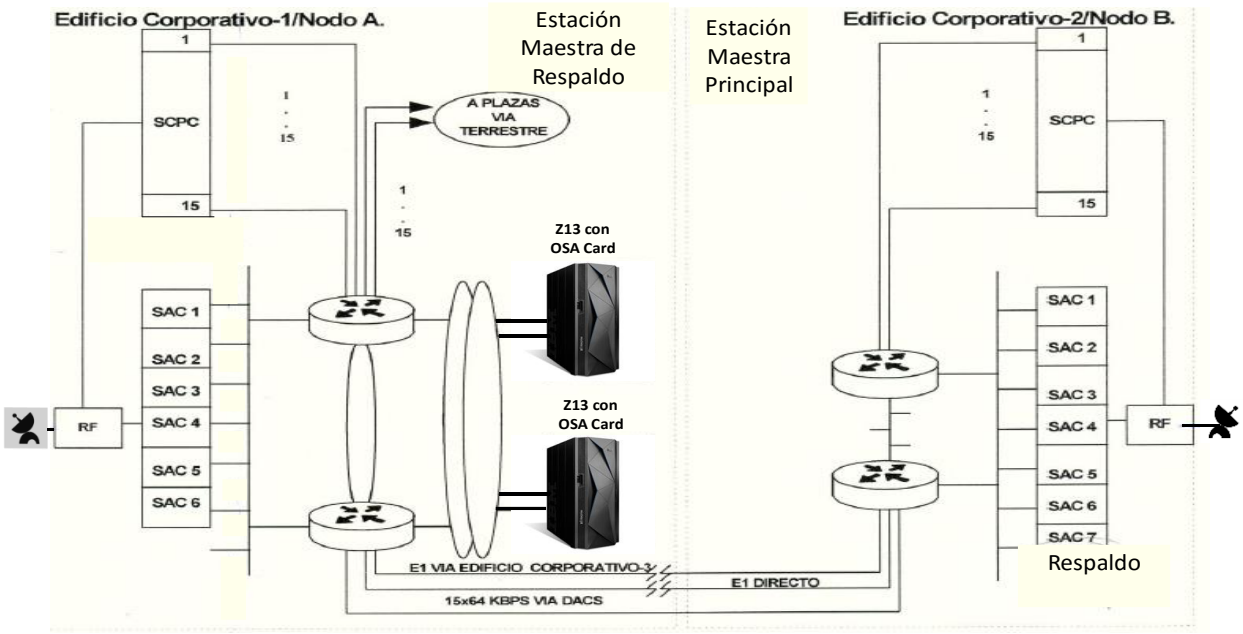



*Figura 3.27: Esquema de Comunicaciones entre Nodo A y Nodo B.*

## Nodos Regionales.

En la figura 3.28, se muestra el esquema de comunicaciones de los nodos regionales y sus funciones serán:

- 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"X64 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.[32]

[32] SCPC: Single Carrier Per Channel: Canal Único por Portadora.
POS: Point of Sale Terminal: Terminal Punto de Venta
NAC: Network Access Controller (Controlador de Acceso a la Red)

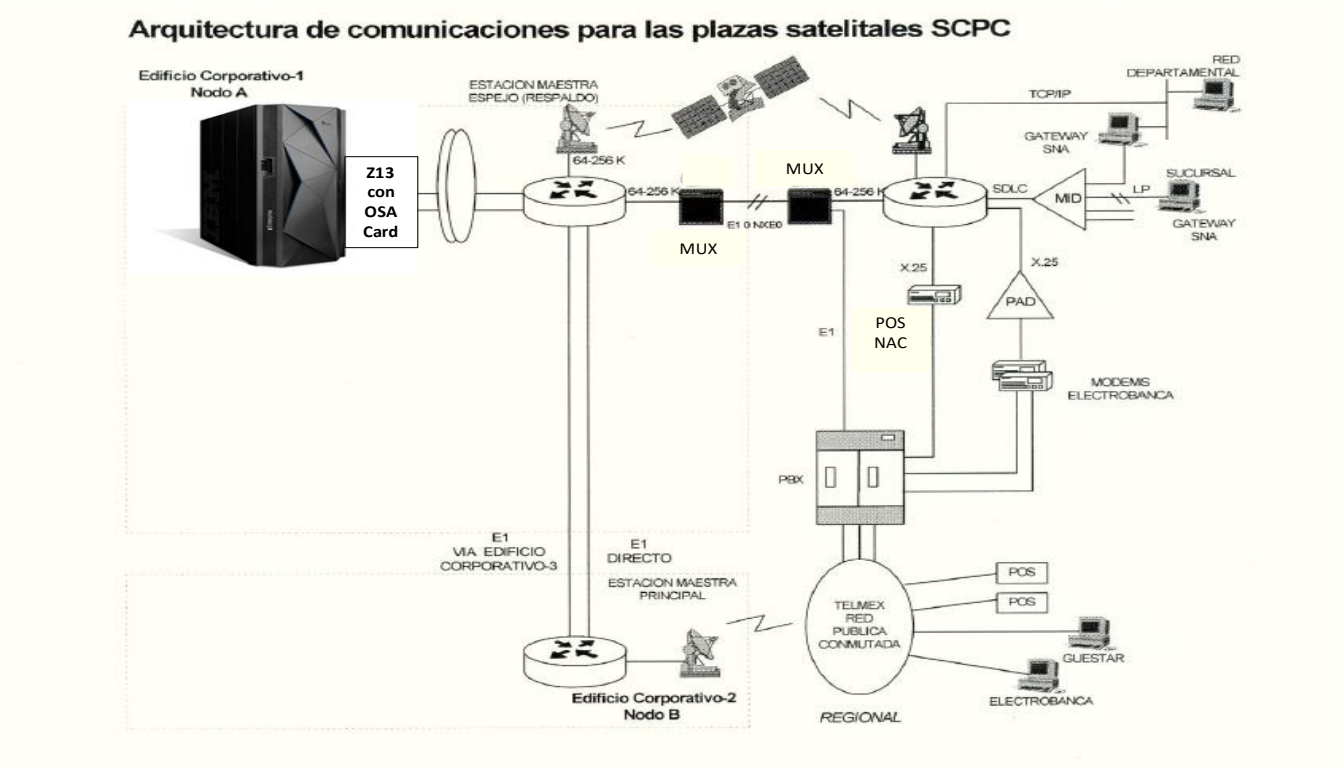



***Figura 3.28: Esquema de Enlaces Satelitales.***

## Sucursales Metropolitanas.

- En la ciudad de México, las sucursales tendrán como enlace principal un DS0 (64 Kbps) al Nodo A (Edificio Corporativo - 1), a través de la RDI de Telmex, éste enlace podrá ser re-direccionado al Nodo B (Edificio Corporativo – 2), en caso de desastre en el Nodo A (Edificio Corporativo – 1), ver figura 3.29.
- Su enlace de respaldo será una línea analógica privada.

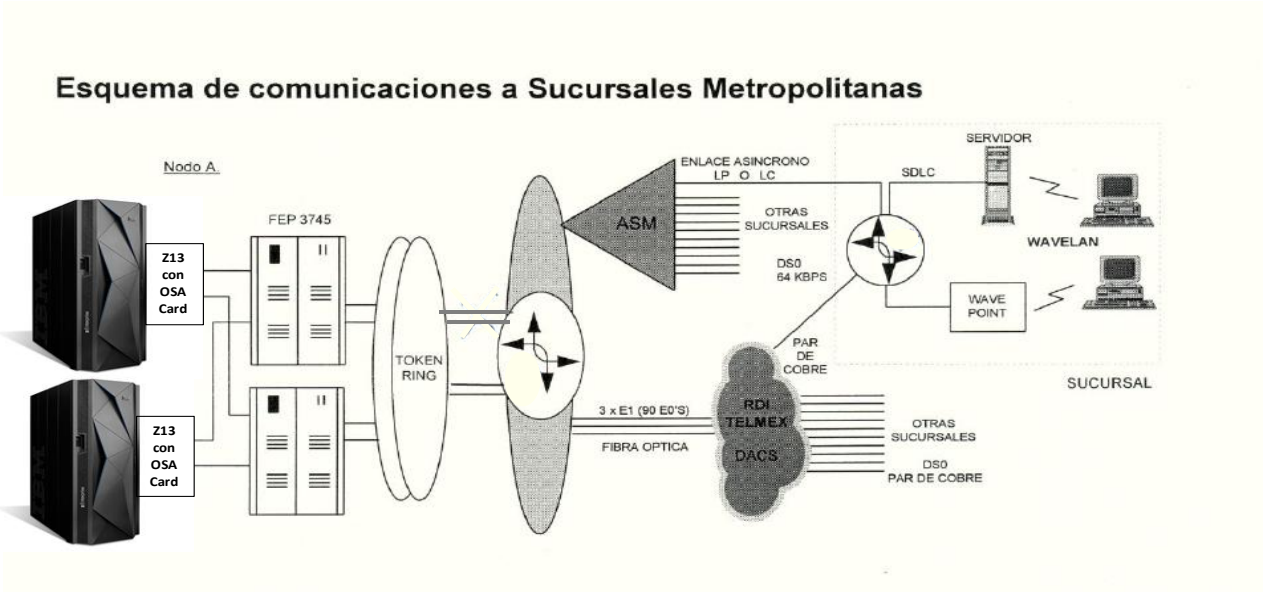



*Figura 3.29: Esquema de Enlaces Zona Metropolitana (Sucursales).*

## Plazas con VSAT TDMA

- Su enlace principal será a través de la red satelital, ver figura 3.30.
- Su enlace de respaldo será a través de un circuito de microondas analógico o a través de línea conmutada al nodo concentrador o directamente hacia la Cd. De México.

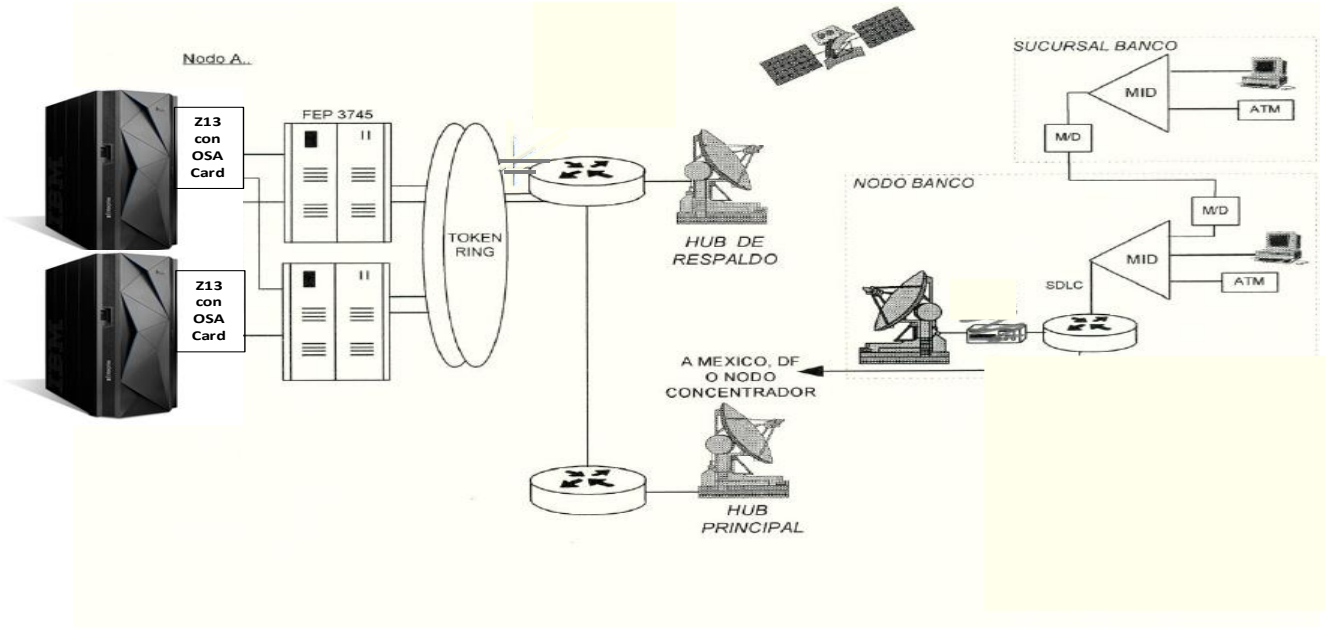



*Figura 3.30: Esquema de Enlaces Plazas del Interior de la República con VSAT TDMA[33].*

[33] TDMA: El **acceso múltiple por división de tiempo** (*Time Division Multiple Access* o **TDMA**) es una técnica de modulación que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal (normalmente de gran capacidad) de transmisión a partir de

El diagrama mostrado en la figura 3.31, muestra el esquema global de comunicaciones para:

- Edificios Corporativos y Sucursales Bancarias en zona Metropolitana
- Plazas del interior de la República enlazadas con VSAT[34]
- Plazas del interior de la República enlazadas con SCPC[35].

También se muestra el enlace de comunicaciones, saliendo desde el Edificio Corporativo – 2, a través de RDI de Telmex hasta Reynosa y de allí hacia Mc Allen a través de MCI, llegando a New York, y por último hasta el Business Recovery Center de IBM, cada uno de estos segmentos tendrá una capacidad de 2.5 Mbps, únicamente manejando señal de datos entre el Secondary Site y las Sucursales en México y Centros Operativos instalados para soportar la Continuidad de la Operación del Negocio (Business Continuity Plan).

distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de transmisión. El **Acceso múltiple por división de tiempo** (TDMA) es una de las técnicas de TDM más difundidas.

[34] VSAT: **VSAT** son las siglas de **Terminal de Apertura Muy Pequeña** (del inglés, *Very Small Aperture Terminal*). Designa un tipo de antena para comunicación de datos vía satélite y por extensión a las redes que se sirven de ellas, normalmente para intercambio de información punto a punto, punto a multipunto (*broadcasting*) o interactiva.

[35] SCPC: Single Carrier Per Channel: Canal Único por Portadora.

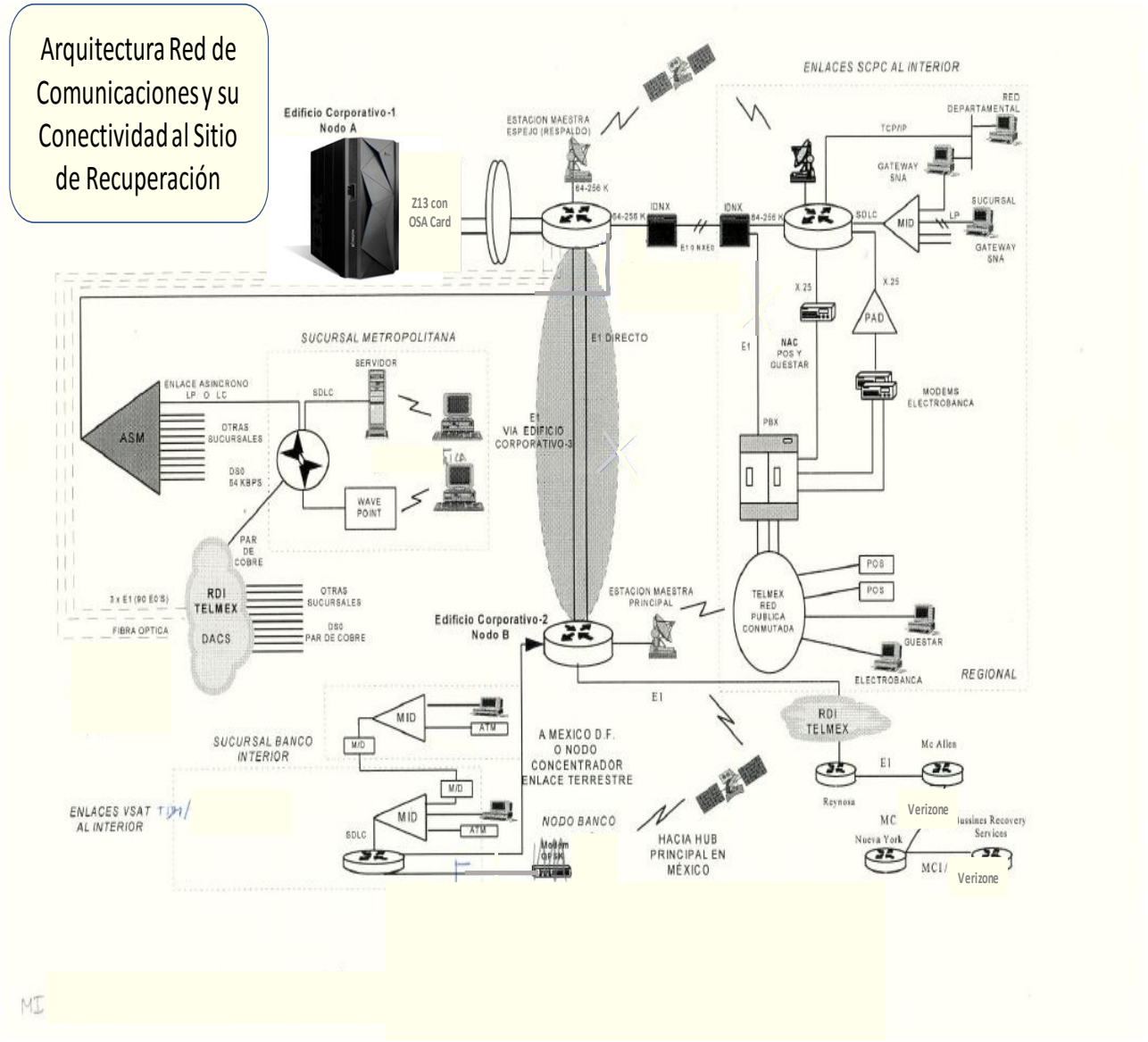



***Figura 3.31: Diagrama General de Comunicaciones y su Conectividad al Secondary Site.***

# Capítulo 4

## Pruebas y Resultados.

## Introducción.

En este capítulo se desarrollarán las componentes del Plan de Recuperación en Casos de Desastre DRP[1], así como, los grupos de especialidades tecnológicas que ejecutarán la recuperación de la infraestructura tecnológica y los datos, tanto para las pruebas de recuperación como para la recuperación de las operaciones de Cómputo y por ende del negocio en un caso real de desastre.

También se desarrollarán los procesos que tendrán como objetivo, mantener el Plan de Recuperación (DRP), siempre vigente y actualizado conforme a la evolución de la tecnología, ya que cualquier ambiente operativo es un ecosistema tecnológico vivo y dinámico, por lo cual los procesos de mantenimiento al plan deben cumplir la misión de mantenerlos vivos para garantizar los resultados esperados.

Adicionalmente como parte del alcance de este capítulo, se incluye el proceso para desarrollar las pruebas periódicas del Plan de Recuperación y la forma en que los resultados de las pruebas retroalimentan al plan de recuperación y sus procesos de mantenimiento.

## 4.1 Desarrollo del Plan de Contingencias.

Como primer paso, debemos establecer la **misión** que debe cumplir el Plan de Recuperación en Casos de Desastre (Disaster Recovery Plan):

### MISIÓN.

Definir, implementar y probrar periódicamente el Plan de Recuperación de las operaciones de cómputo que permita la continudad de los servicios vitales del negocio Bancario ó de cualquier otro tipo de industria, ante un desastre natural o informático, minimizando el impacto financiero.

Para lograr la misión establecida, se requiere contar con ***varias componentes*** que permitan articular la recuperación de manera eficiente y dentro de los límites establecidos por el RTO y el RPO, dichas componentes serán:

- Equipos de Recuperación
- Tareas por Equipos de Recuperación
- Procedimiento de Evaluación, Escalación y Declaración del Desastre
- Procedimiento de Respaldo ó Replicación de datos vitales
- Procedimiento de Recuperación
- Procedimientos de Mantenimiento al Plan de Recuperación
- Inventarios

[1] DRP: Disaster Recovery Plan por sus siglas en Ingles: Plan de Recuperación en Casos de Desastre

## 4.2 Equipos de Recuperación y sus Responsabilidades.

Establece la estructura de los equipos de trabajo para la recuperación, asignando sus responsabilidades de acuerdo a las siguientes disciplinas (ver Tabla 4.1):

***Tabla 4.1. Equipos de Recuperación.***

| Disciplina | Función Básica |
|---|---|
| Sistemas Operativos y software de terceros, programas producto. | Recuperar y activar los sistemas operativos en las diferentes plataformas tecnológicas (Mainframe, Distribuido, Midrange, etc..) |
| Sistemas Aplicativos | Recuperar y activar la funcionalidad de los sistemas aplicativos para soportar los servicios de negocio. |
| Base de Datos y Middleware (Interfaces) | Recuperar y activar la funcionalidad de las Bases de Datos y del Middleware que permite interfacear con la capa de presentación de los servicios y soportar la transaccionalidad del negocio. |
| Storage | Recuperar y activar el almacenamiento usado por las diferentes plataformas de Procesamiento. |
| Comunicaciones | Recuperar y activar los medios de comunicación y enlaces para garantizar la correcta comunicación con las áreas operativas del negocio y sus puntos de venta de servicios. |
| Operación | Toma control de la operación en el Sitio Secundario ó Site Alterno de DR. |
| Recuperación | Evalua la naturaleza del Desastre e informa al Equipo Gerencial de Recuperación para determinar la declaración del desastre de acuerdo al Plan. |
| Instalaciones Físicas (Facilities), Hardware y Equipo de Cómputo Personal (Lap Tops) | Asegura que las instalaciones esten preparadas y el equipo disponible y activo para la recuparción |
| Administración y Soporte a Usuarios Finales | Asegura que el Sitio Secundario de Recuperación este preparado para la alojar a los equipos de recuperación, coordina y mantiene comunicación con los usuarios internos (áreas del negocio) de la empresa. |
| Equipo Gerencial de Recuperación | Recibe evaluación de daños, analiza la situación y declara la contingencia ó desastre, notificando a la totalidad de la Empresa. |

En el organigrama mostrado en la figura 4.2, se puede apreciar de manera sintetizada, la estructura organizacional de los equipos de recuperación para lograr la misión de recobrar la operación del negocio en los tiempos estipulados.

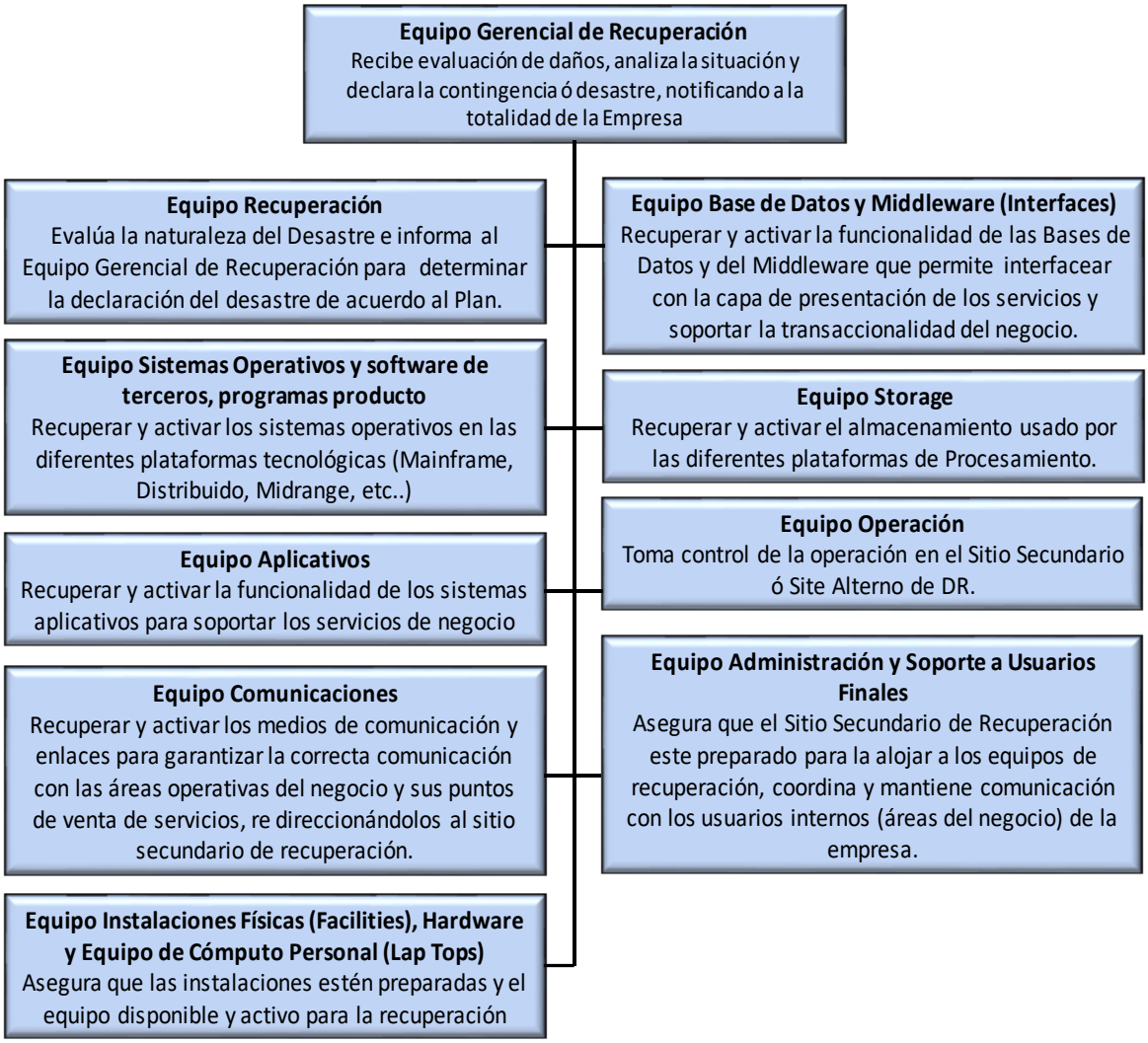



**Figura 4.2. Equipos de Recuperación.**

Es de vital importancia que el Plan de Recuperación en casos de Desastre (DRP; Disaster Recovery Plan por sus siglas en inlges), este realacionado con los Inventarios (Harware, Software, Medios de Comunicación), o en su defecto, en caso de existir, con la CMDB[2] , con la finalidad de que cada cambio de tecnología en el ambiente productivo (Primary Data Center; Centro de Datos Primario) , se realice en el Sitio Secundario de Recuperación (Site Secuendario) para evitar problemas durante las pruebas de recuperación o en un Desastre real.

## 4.3 Representación Esquemática del Plan de Recuperación, Sus Componentes y Modelo Conceptual de la Recuperación.

[2] CMDB: Configuration Management Data Base: Base de Datos para la Administración de la Configuración.

El contenido mínimo que debe tener un Plan de Recuperación para garantizar su funcionalidad y vigencia en el tiempo, se cita a continuación:

- Misión
- Equipos de Recuperación
- Tareas por Equipos de Trabajo
- Procedimientos de Evaluación, Escalamiento y Declaración de Desastre
- Procedimiento de Replicación de Datos Vitales
- Procedimientos de Recuperación (Sistemas Operativos, Aplicaciones, Bases de Datos)
- Procedimientos de Mantenimiento al Plan
- CMDB o Inventarios (Hardware, Software, Equipos de Comunicaciones, Proveedores)

En la figura 4.3, se puede representa de manera gráfica las componentes del Plan de Recuperación, **las cuales están interconectadas entre sí, con la finalidad de que esa articulación, permita que el plan sea eficente, coordinado y de los resultados esperados por la Organización (Empresa)** para la recuperación de las operaciones del negocio en caso de contingencia.


***Figura 4.3: Representación Esquemática del Plan.***

Cada una de las componentes del plan mostradas en el esquema gráfico se explican a continuación:

- Equipos de Recuperación

Se establecen los equipos de trabajo por especialidad o disciplina tecnológica que permitirán ejecutar las actividades del plan con el suficiente conocimiento y experiencia técnica que se requiere.

- Procedimientos de Evaluación, Escalamiento y Declaración de Desastre

Contiene el proceso de evaluación de daños en las instalaciones físicas del Centro de Cómputo y en los equipos instalados en él, permite identificar el grado de daño y determina si es funcional o no, y si la función que realiza puede ser soprotada por otro equipo en redundancia con la carga de trabajo que se tiene en condiciones normales.

- Procedimiento de Replicación de Datos Vitales

Describe el proceso para sincronizar los volúmenes (LUNs) o Storage Gropus, establecidos en el PPRC FlashCopy para realizar la copia de datos desde el Site Primario hacia al Site Secundario y realizar la última sincronización al 100% e indica el proceso para detener de manera controlada y apropiada la replicación de Datos.

- Procedimientos de Recuperación (Sistemas Operativos, Aplicaciones, Bases de Datos)

Contiene el proceso paso a paso para activar el sistema operativo una vez que el storage se encuentra habilitado y disponible para las diversas plataformas (Mainframe, Distribuido y Midrange).

También establece la secuencia apropiada para activar las aplicaciones y las interfaces que permiten la habilitación de los servicios de cara al negocio.

- Procedimientos de Mantenimiento al Plan

Estos procedimientos contiene el proceso para mantener permanentemente **actualizados y vigentes** los procesos de recuperación, pues controlan y monitorean los cambios en las componentes de Hardware, Software y Middleware, Comunicaciones, Aplicaciones, Almacenamiento (Storage) y proveedores, que evitarán que durante una prueba de recuperación o en un desastre se encuentren desactualizados los procedimientos de recuperación. Estos procedimientos son vitales para el Plan.

- CMDB o Inventarios (Hardware, Software, Equipos de Comunicaciones, Proveedores).

La CMDSB[3], permite correlacionar a través de los CI[4], el Hardware, los sistemas operativos, productos de Software, Midlleware, Aplicaciones, medios de Comunicación y demás componentes que finalmente soportan uno o varios servicios de las funciones de Negocio, estableciendo una clara correlación entre la infraestructura de TI con el catálogo de servicios del Negocio. En caso de no tener una CMDB, se puede optar por integrar los Inventarios que se tengan disponibles, tanto de Hardware, Software, Middleware, Aplicaciones, Comunicaciones y proveedores para consolidar esta información y que el Plan de Recuperación tenga visibilidad de los cambios que se presenten en la Infraestrcutura para retroalimentar al Plan.

Con este contenido el Plan de Recuperación, podrá ser funcional y efectivo para los fines que fue creado, finalmente a manera de resumen, se muestra en la figura 4.4, un esquema Conceptual de la representación del Plan y su Sitio Secundario de Recuperación y los puntos de venta y operación (Back Office), basado en los diagramas de comunicaciones descritos en el Capítulo 3 del presente trabajo, **a manera de mostrar al negocio en un lenguaje no técnico como operaría la recuperación en caso de desastres para que no se interrumpa la prestación de los servicios y por ende el negocio siga funcionando**.

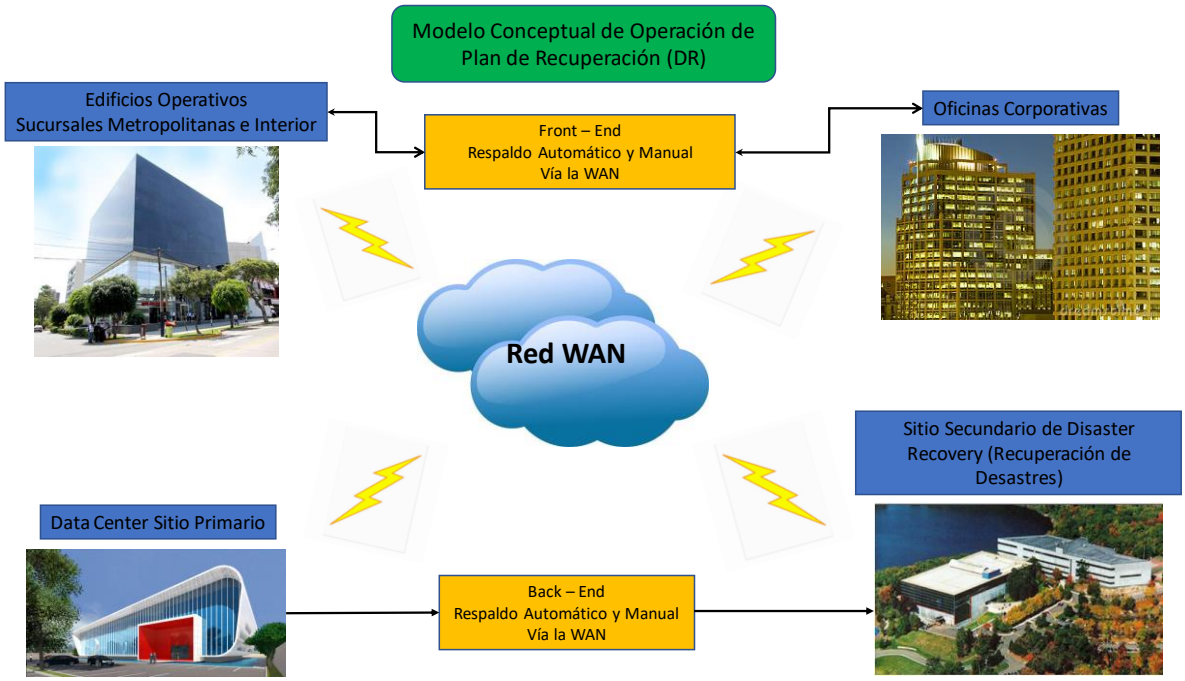



***Figura 4.4: Modelo Conceptual de Operación del Plan de Recuperación(DR).***

[3] CMDB: Configuration Data Base Management (por sus siglas en Ingles), Base de Datos para la Administración de Configuraciones.
[4] CIs: Configurations Items (por sus siglas en Ingles), Artículos o Componentes de la Configuración.

## 4.4 Prueba del Plan de Recuperación.

No basta con tener documentado y actualizado el Plan de Recuperación en casos de Desastre o Contingencia para **garantizar su funcionalidad y éxito**, es necesario realizar pruebas periódicamente, **normalmente se ejecutan dos pruebas al año**, con la participación de las áreas de Negocio **(dado que el Plan de Recuperación en Casos de Desastre forma parte del Plan para Continuidad del Negocio, BCP[5]),** desde luego usando los servicios de Site Secundario de Recuperación (Secondary Site), esto permitirá mantener ***vivo*** al Plan de Recuperación y permitirá la mejora continua del mismo.

Para llevar a cabo las pruebas, se requiere definir los alcances de la misma con el reporesentante del BCP por parte del Negocio, lo anterior para coordinar adecuadamente a las áreas del negocio que participarán en las pruebas.

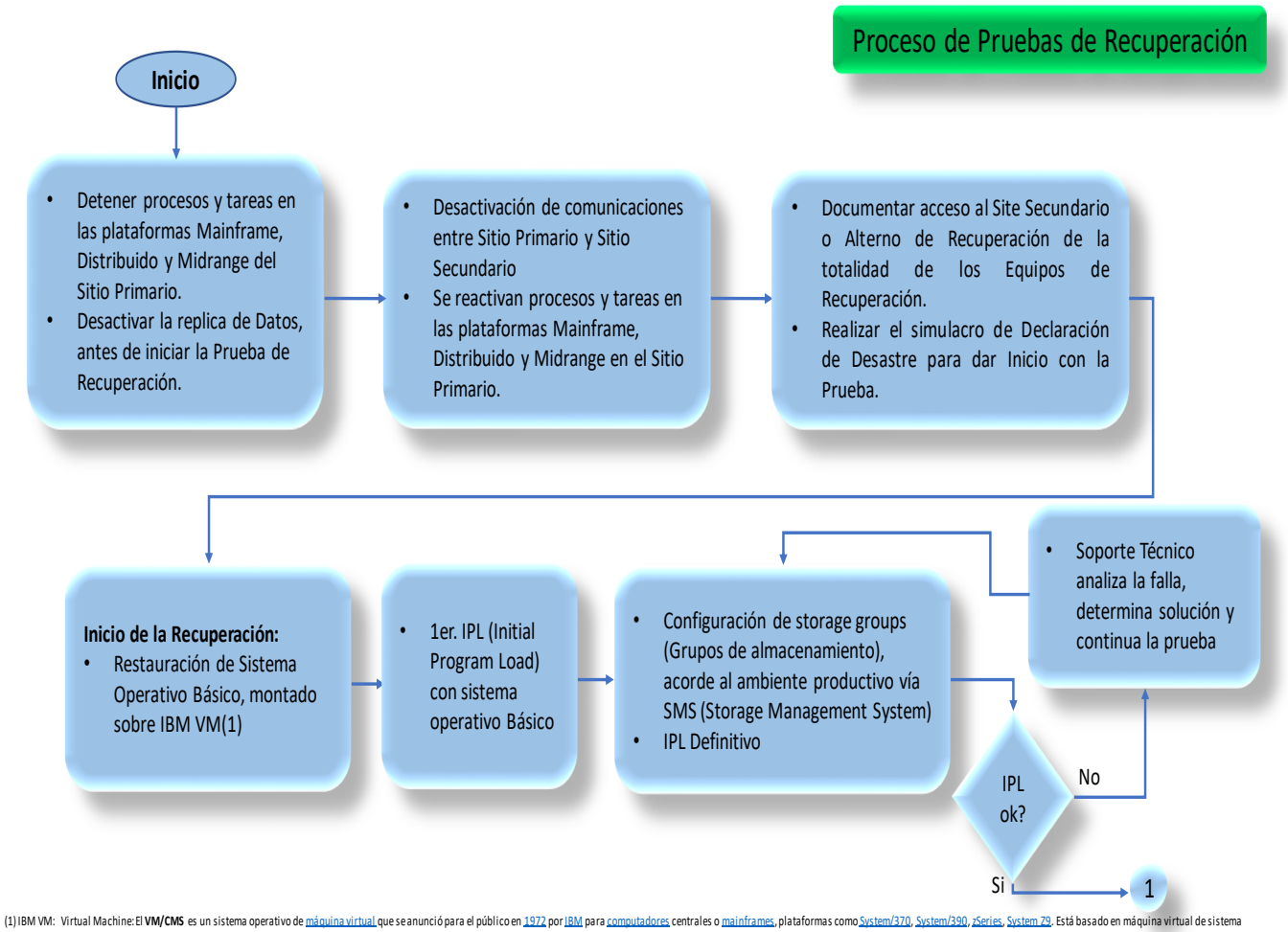
Es conveniente establer 2 tipos de Objetivos para mediar más facilmente en dos etapas la prueba, en resúmen, el contenido del Plan de Pruebas deberá contener como mínimo:

- Alcance
- Objetivo Primario
- Objetivos Secundarios
- Recursos Humanos
- Programa de Actividades detallado especificando:
  - ✓ Inicio y fin de cada tarea por día y hora
  - ✓ Responsable de cada tarea
  - ✓ Referencia a la documentación y procedimiento del Plan de Contingencia que se utilizará para ejecutar la tarea señalada
- Coordinación del uso del Site Secuendario con la empresa que provee el Data Center Secundario para tener acceso a las Suites (Salas de Recuperación), en donde se contará con equipamiento conectado directamente a la Infraestructura (Hardware, comunicaciones, Equipo de oficinas, tales como, Lap Tops y Desk Tops)
- Normalmente se establece que se usará este espacio por un intervalo de tiempo de 48 horas.
- Revisión por parte del líder del Equipo de Administración (ver página 4 del presente Capítulo) que los equipos que se encuentran Hosteados en el Siste Secundario, se encuentren en óptimas condiciones para llevar a cabo su encendido
- El lider del Equipo de Administración, deberá verificar con el Líder del Equipo de Storage que se haya detenido la réplica de datos en el día y hora acordados y de haberse ejecutado la última sincronización para garantizar el RPO de máximo 2 horas, establecido por el BIA (ver página 13 del Capítulo 3 del presente trabajo)

[5] BCP; Business Continuity Plan, por sus siglas en Ingles.

- El líder del Equipo de Administración deberá ejecutar reuniones previas de trabajo en donde se dará el Kick Off de la Prueba de Recuperación con todos los integrantes de los equipos de recuperación y sus líderes, involucrando al equipo Directivo de Tecnológias de la Información para establecer el compromiso de todos y su activa participación en la prueba.

En el diagrama (figura 4.5) de flujo mostrado a continuación (Diagrama , se muestra el proceso de **Pruebas de Recuperación**:




(1) IBM VM: Virtual Machine: El **VM/CMS** es un sistema operativo de máquina virtual que se anunció para el público en 1972 por IBM para computadores centrales o mainframes, plataformas como System/370, System/390, zSeries, System Z9. Está basado en máquina virtual de sistema cuyo núcleo es un programa de control llamado CP (Control Program) o también denominado VMCP (Virtual Machine Control Program) cuya principal característica es que permite la ejecución de una máquina virtual dentro de otra máquina virtual, también es la encargada de controlar los dispositivos hardware del ordenador: CPU, discos cintas, etc.

***Figura 4.5: Diagrama de flujo del Proceso de Pruebas de Recupración.***

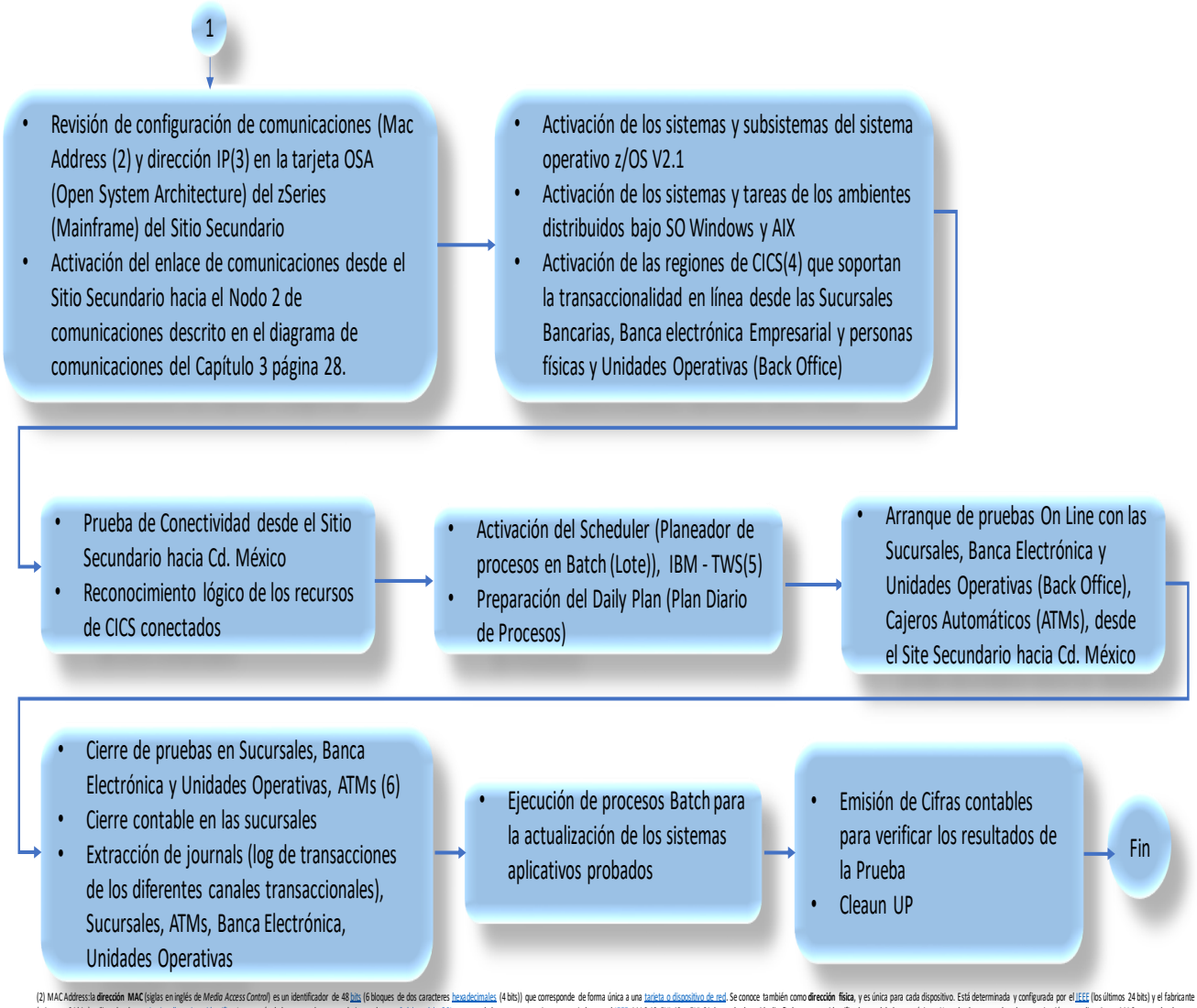



***Figura 4.5: Continuación, Diagrama de flujo del Proceso de Pruebas de Recupración.***

Durante el desarrollo de las pruebas de recuperación, el Líder del grupo de Administración, registrará en un **LOG (Bitacora cronológica para registrar cada actividad, con hora de incio y fin, así como el registro de fallas o atrasos y las soluciones aplicadas, con la finalidad de ajustar el plan de recuperación y mejorarlo con cada prueba),** la información relevante que servirá para presentar los resultados de las pruebas, hacia la Dirección General de Sistemas (CIO[6]) y hacia la Dirección General de la Empresa (CEO[7]) y se

[6] CIO: Chief Information Officer
[7] CEO: Chief Executive Officer

documentará y pondrá a disposición del área de Auditoria de la Empresa, así como a disposición de la CNBV (Comisión Nacional Bancaria y de Valores), dicho log contendrá al menos:

- Problemas presentados durante la activivación de las plataformas
- Fallas aplicativas y/o de sistema que se presentaron
- Solución a las diferentes fallas y problemas
- Tiempo de Inicio y Fin de cada actividad para poder afinar tiempos con las pruebas sucesivas
- Plan de Mejora, tanto de procedimientos de recuperación como de alcance de las pruebas.
- Evidencias de las pruebas realizadas:
    - Activación de sistemas y servicios
    - Reportes generados por los procesos Batch
    - Cifras contables de los sistemas ejecutados y que reflejan la actividad On Line, realizada con: Sucursales, Cajeros Automáticos, Banca Electrónica y Unidades Operativa
    - Clean Up[8] de los ambientes recuperados

## 4.5 Mejoramiento del Plan de Contingencias.

Cada ejecución de las pruebas de recuperación, deberá suponer una mejora en el diseño, objetivos y alcances del Plan para lograr esta mejora continua, se requiere contar con la retroalimentación de resultados, considerando la solución que se haya aplicado para cada falla ó problema presentado durante las pruebas y que se encuentra documentado en el **LOG histórico** por el Líder del grupo de Administración, este proceso se representa en el diagrama de flujo citado a continuación (ver figura 4.6):

[8] Clean Up: Limpieza de los ambientes recuperados en los equipos del Sitio Secundario.

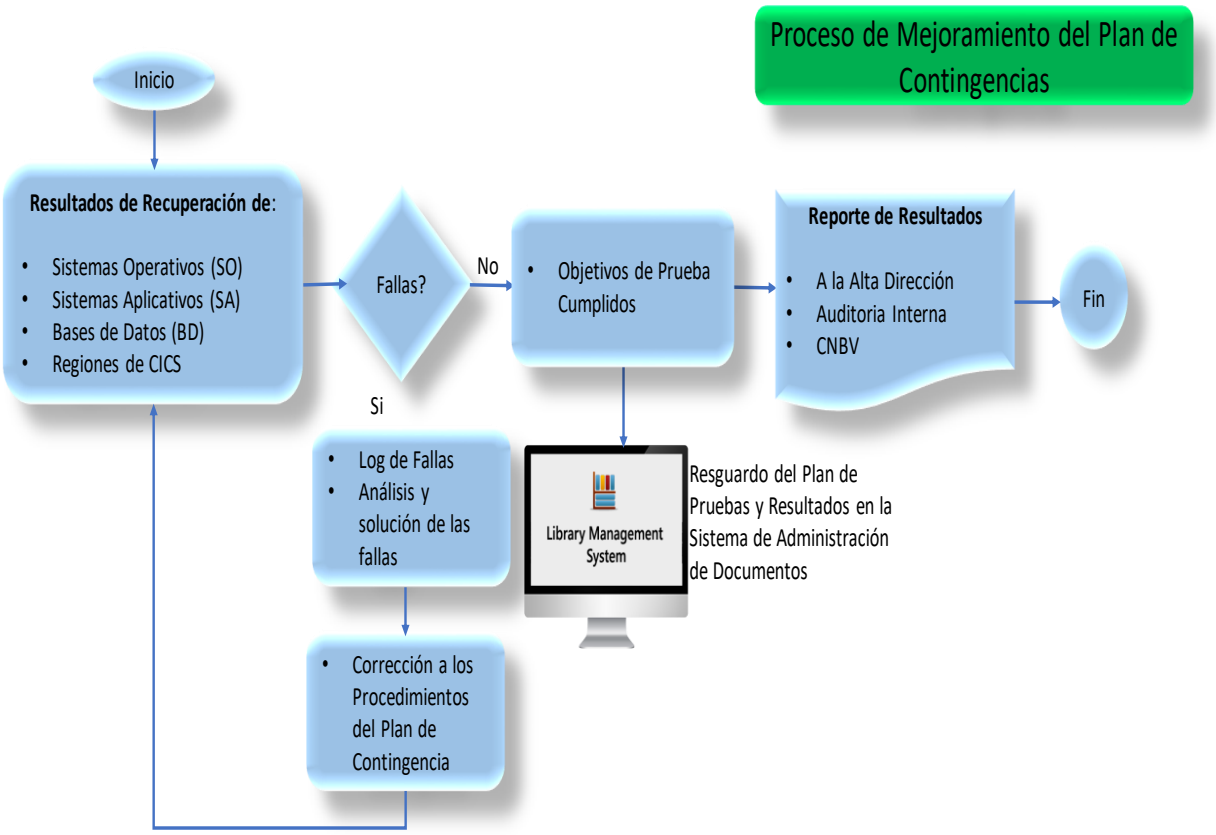



***Figura 4.6: Proceso de Mejoramiento del Plan de Contingencia.***

La mejora de los procedimientos del Plan, permitirán garantizar un alto grado de confiabilidad en la ejecuión del mismo, al momento en que se tengan que recuperar las operaciones de cómputo y la reanudación de las operaciones del negocio, en el tiempo establecido (RTO/RPO), logrando cumplir los objetivos para los cuales fue diseñado e implementado.

## 4.6 Procesos de Mantenimiento al Plan de Contingencias.

Los cambios en el entorno financiero de la empresa, derivado de nuevos servicios y/o productos financieros o de las regulaciones de la autoridad normadora de la actividad financiera o bien por los avances tecnológicos, podrán generar cambios en el Plan de Contigencia en las componentes citadas a continuación:

- Hardware y equipos de comunicación; CPUs (Procesadores), capacidad de almacenamiento, routers, switches, enlaces de comunicación, etc…
- Sistemas operativos, software o programas producto, middleware

- Nuevas versiones de Bases de Datos
- Software aplicativo; cambios o instalaciones de nuevos sistemas que soporten funciones de negocio críticas
- Personal, proveedores, etc…

Por consecuencia de los factores anteriormente citados, es necesario establecer la metodología para reflejar continuamente dichos cambios en el Plan de lo contrario, en el momento en que se presente una contingencia, **se corre el riesgo de que no se logre la recuperación del negocio**, ya que no se tendría mapeado en el Sitio Secundario las componentes identicas al ambiente Productivo, imposibilitando la continuidad de las operaciones en el tiempo establecido, materializandose los impactos citados en el BIA (Análisis de Impacto al Negocio), desarrollado en el Capítulo 3 del presente trabajo.

Por tales razones es de vital importancia, implementar el proceso de Mantenimiento al Plan de Contingencia, como se describen en los diagramas de flujo de las figuras 4.7 la figura 4.11.

### 4.6.1. Resultados de la Pruebas de Recuperación.

Con base en lo indicado en la sección "4.5 Mejoramiento del Plan de Contingencia" del presente Capítulo, al ejecutar las prueba de recuperación, se podrán presentar problemas de tipo técnico y/o logístico, que independientemente de que se solucionen satisfactoriamente, deberán ser documentadas para realizar las mejoras y/o actualizaciones al Plan.

Es importante, señalar que las correciones al Plan de Contingencia, serán responsabilidad del área de Seguridad de Información y de su líder y/o Gerente de Servicios de Continuidad y Recuperación.

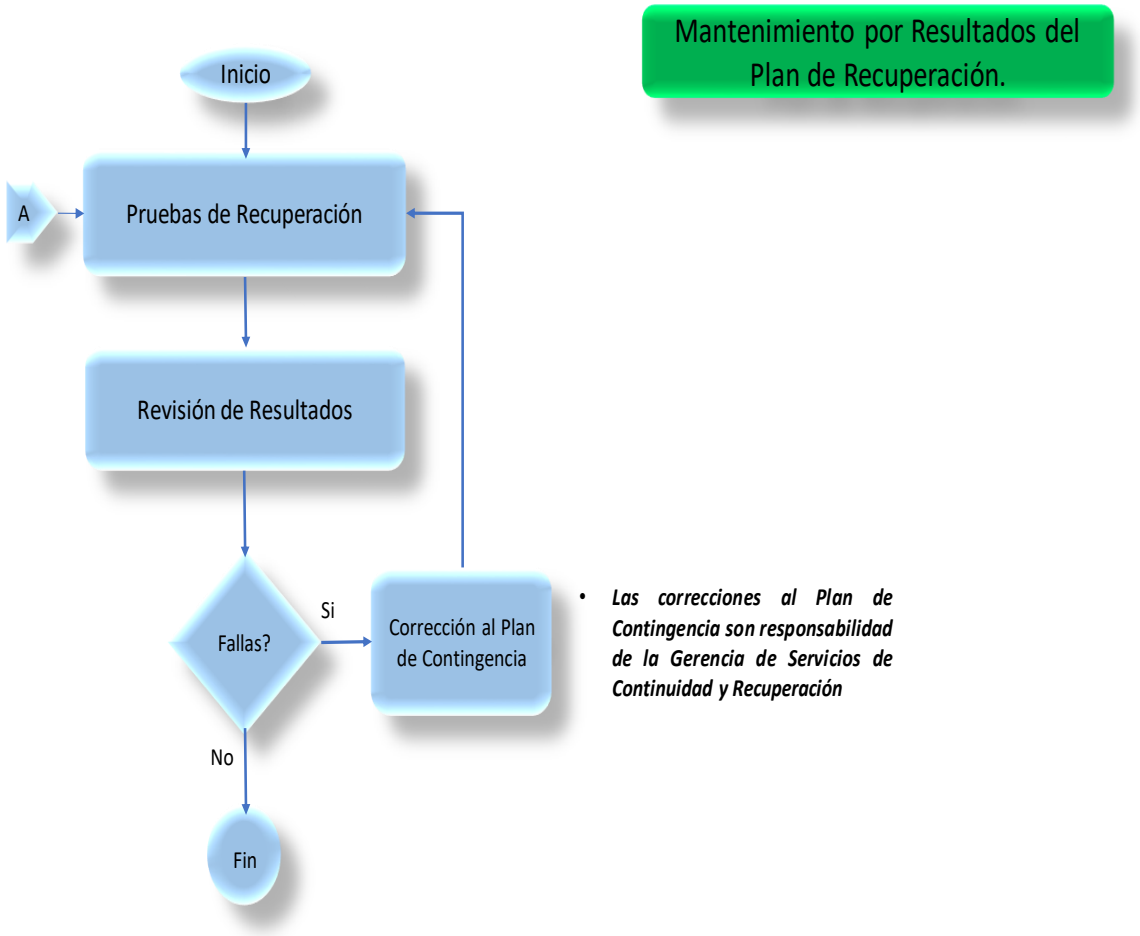



*Figura 4.7: Mantenimiento por Resultados de Pruebas de Recuperación.*

## 4.6.2. Mantenimiento al Plan por Cambios en el Software Aplicativo.

En el **Capítulo 3 de la presente Tésis**, se identificaron las funciones críticas del Negocio, así como las aplicaciones que soportan sus servicios y la interrelación de las aplicaciones con otras más que a su vez soportan otras funciones del negocio, dichas aplicaciones están incluídas en los procedimientos de recuperación del Plan, por lo cuál, todo cambio aplicativo que afecte a esas aplicaciones, así como las nuevas aplicaciones que se implementen para las funciones de Negocio críticas, deberan ser notificadas al área de Servicios de Continuidad y Recuperación del Negocio (Business Recovery and Continuity Services), para que se lleven a cabo las actualizaciones correspondientes. En el diagrama de la figura 4.10, se muestra el proceso para mantener actualizado el procediiento de recuperación del **Software Aplicativo**:

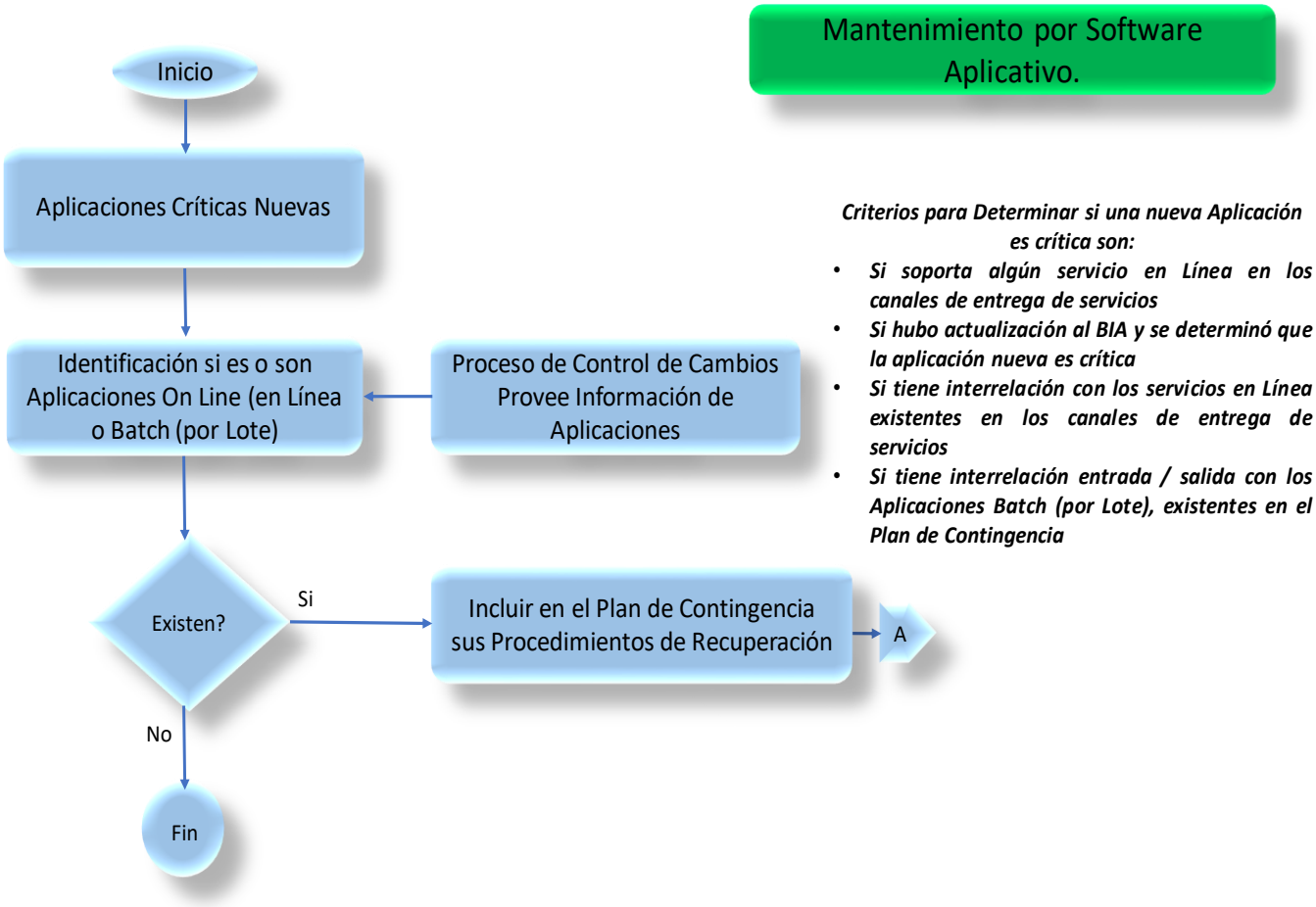



*Figura 4.8: Mantenimiento por Cambios en Software Aplicativo.*

### 4.6.3. Mantenimiento al Plan por Cambios en el Sistema Operativo.

Los sistemas operativos de la diversas plataformas también sufren cambios en sus versiones, dichos cambios son resultado de varios factores, por citar algunos:

- Mejoras a las funciones del sistema operativo para darle mayor fortaleza y compatibilidad con nuevas tecnologías de programación
- Solventar huecos de seguridad (sobre todo en las versiones del sistema operativo Windows)
- Resolver fallas de origen y para las cuales se desarrollan fixes que muchas veces dependiendo del impacto en el núcleo del sistema operativo dan por consecuencia cambios de releases[9] o versiones.

[9] Release: Lanzamiento o cambios en el sistema operativo que no requieren cambiar la versión del mismo.

No obstante que no son muy frecuentes en el lapso de tiempo corto, sí pueden afactar considerablemente al ambiente productivo, sino se prueban exhaustivamente en ambientes de **TEST y/o QA (Quality Assurance)**[10], es decir, Aseguramiento de Calidad, estos cambios son de vital importancia, dado que permitirán el cotrrecto funcionamiento de los aplicativos y de las funciones que explotan del sistema operativo en el cual se ejecutan, por lo cual cualquier cambio en el sistema operativo es delicado y debe entrar y documentarse, a través del Proceso de Control de Cambios que se tenga implementado y funcionando como parte del esquema de Gobierno de TI, que posee cualquier empresa, y deberá ser notificado a la Gerencia de Continuidad y Servicios de Recuperación.

En el diagrama de la **figura 4.11**, se muestra el proceso para mantener actualizado el Plan de Recuperación en Caso de Contingencias, derivado de los cambios en los sistemas operativos.

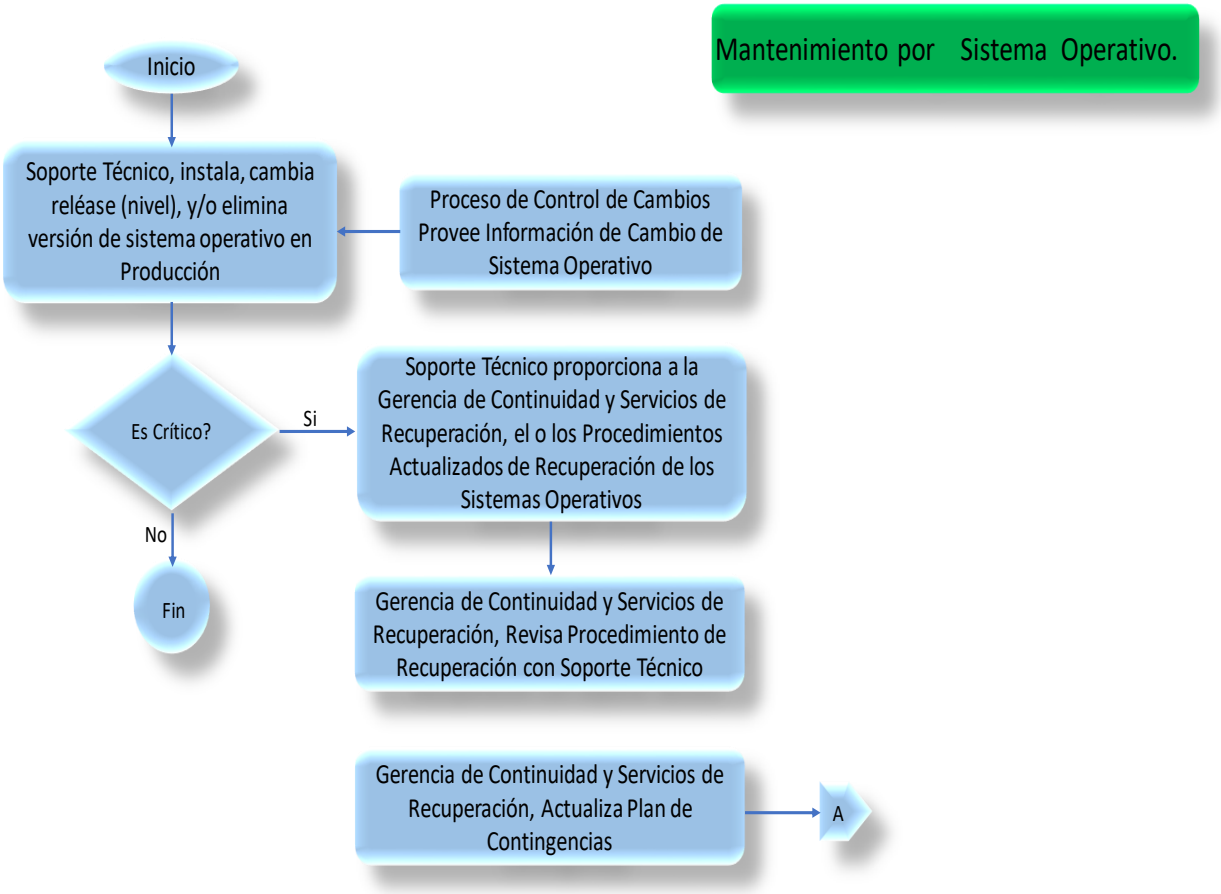



***Figura 4.9: Mantenimiento por Cambios en Sistemas Operativos.***

[10] Quality Assurance: Aseguramiento de calidad, este ambiente permite probar, no sólo, los cambios aplicativos sino también las nuevas versiones y releases de los sistemas operativos.

### 4.6.4. Mantenimiento al Plan por Cambios en Hardware y Equipo de Comunicaciones.

Actualmente producto de la evolución acelerada de la tecnología y la Empresa con la finalidad de mantenerse a la vanguardia y mejorar la entrega de los servicios Bancarios a sus clientes, requiere de invertir cada año en mejoras tecnológicas para mantener su competitividad en el sector financiero.

Estas modificaciones deben ser notificadas inmediatamente a la Gerencia de Continuidad y Servicios de Recuperación para mantener actualizado el Plan de Contingencias y por consecuencia para reflejar esos cambios en el la Infraestructura tecnológica en el Sitio Secundario (Secondary Site) para garantizar que la infraestructura sea igual a la del Sitio Primario, enla **figura 4.12,** se muestra el diagrama del Proceso de actualización al Plan de Contingencias por estos aspectos.

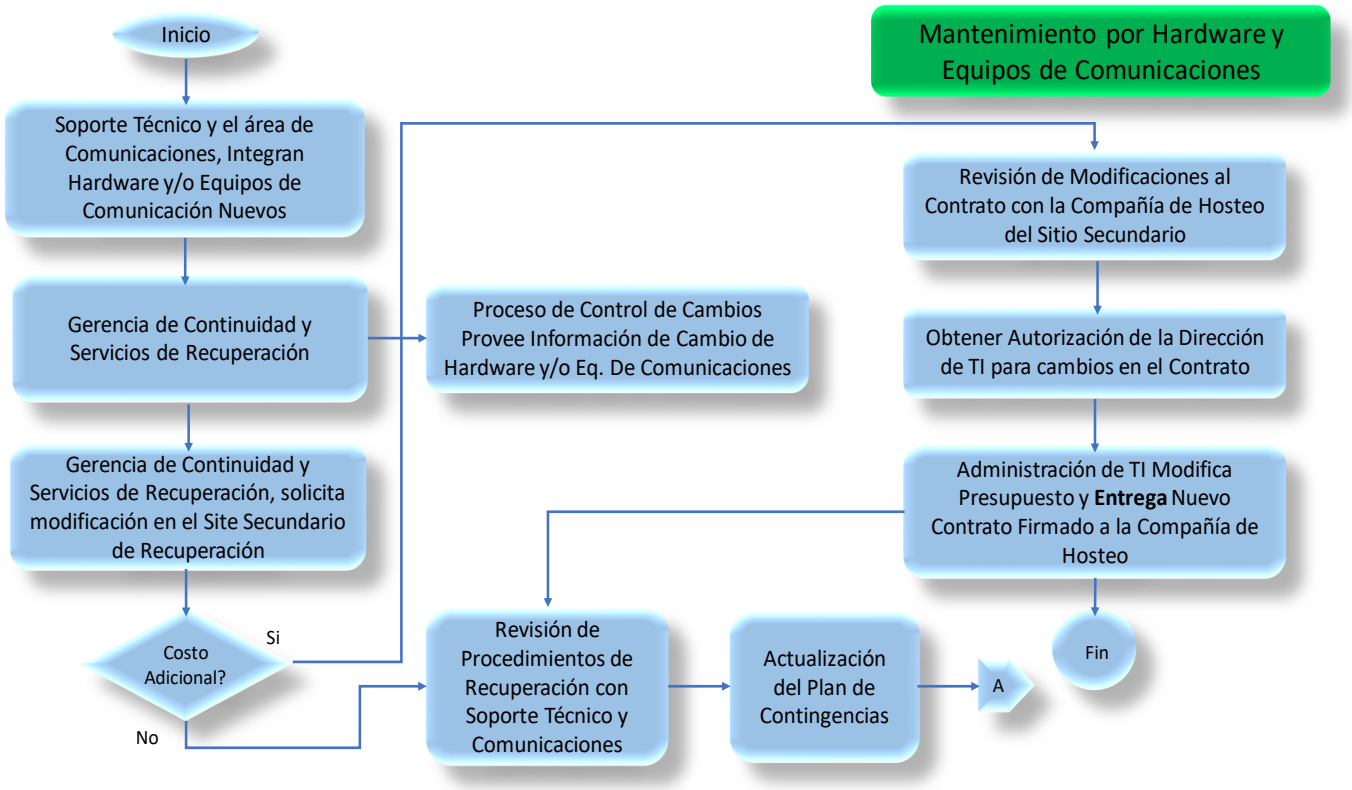



***Figura 4.10: Mantenimiento por Cambios en Hardware y Equipo de Comunicaciones.***

Las modificaciones en el costo del contrato de Hosting de la Infraestructura tecnológica se pueden deber a los siguientes factores:

- Cambio de modelo o capacidad de procesamiento en las plataformas, Mainframe (incremento en MIPS), ambiente Distribuido, Midrange
- Cambio en los modelos y/o capacidades de los equipos de ruteo (routers) y switches de comunicación.
- Cambios en el VTS (Virtual Storage Tape), que permitirá ejecutar los respaldos (BackUps), en el Sitio Secundario durante las pruebas de Recupración y/o en una contingencia real, en tanto se rehabilita el Sitio Primario.
- Incremento en el Storage que obligue a crecer a un modelo con mayor capacidad.
- Crecimiento en el ancho de banda del enlace utilizado para la replicación de storage, entre el Sitio Primario y el Secundario.

### 4.6.5. Mantenimiento por Cambios en Recursos Humanos, Proveedores e Inventarios.

Adicionalmente a los cambios que afectan al Plan de Contingencia, es necesario y crítico considerar los cambios de Recursos Humanos que se producen en las áreas involucradas en el Plan de Contingencias, ya que el Recurso Humano, forma parte de los Equipos de Recuperación (ver página 4 del presente Capítulo) y tienen responsabilidades y tareas específicas en cada grupo de recuperación, motivo por el cual:

- ✓ En caso de cambio de algún miembro de los Equipos de Recuperación, se debe conocer quien asumirá su rol y responsabilidades, ya sea para la ejecución de Pruebas de Recuperación y/o en caso de una Contingecia Real.
- ✓ Capacitar al nuevo integrante del equipo de recuperación.
- ✓ Integrarlo en las reuniones de notificación de cambios en el Plan de Contingencias y proporcionarle acceso a la biblioteca documental donde se archiva el DRP (Plan de Recuperación en Caso de Desastre)

Ahora bien, dado que una contingencia podría llegar a destruir el Sitio Primario (pensemos en un **sismo igual o superior al presentado en el siglo pasado en el año de 1985, ver Capítulo 1 de la presente Tesis**), lo cual implicaría la destucción del hardware e instalaciones del Site Primario

Por ésta razón**, es necesario contar con los Inventarios actualizados y/o una CMDB apropiadamente actualizada,** con la finalidad de proporcionar al área de Administración de TI, el Inventario de equipos con:

- ✓ sus números de serie, tipo – modelo y configuraciones

- ✓ con la finalidad de solicitar la reposición de los equipos, a la compañía Aseguradora (se llama póliza a valor reposición) para que los equipos (Hardware) sean repuestos por los Proveedores.

En la figura 4.13, se representa el diagrama del proceso de mantenimiento para actualizar el Plan de Contingencias, derivado de estos cambios.

Mantenimiento por Cambio en Recursos Humanos, Proveedores, Inventarios

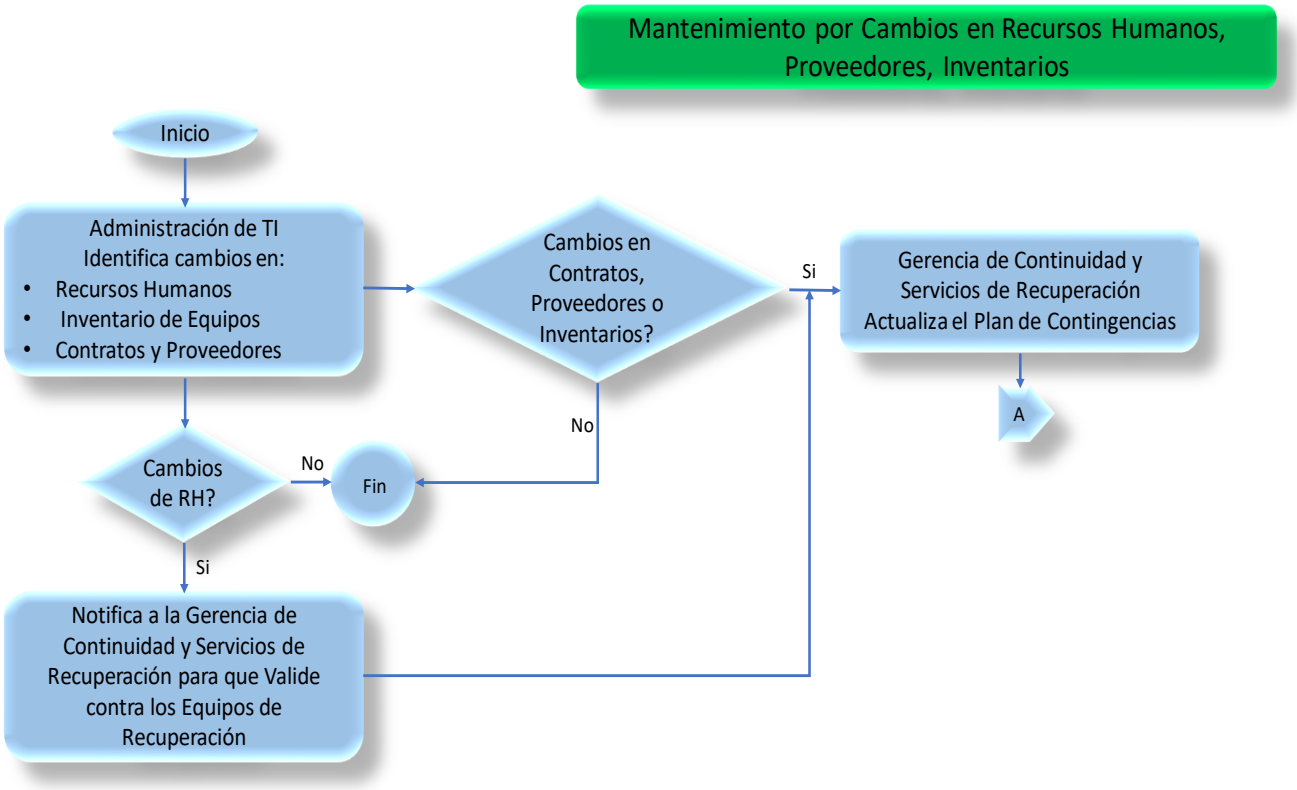



***Figura 4.11: Mantenimiento por Cambios en Recursos Humanos, Proveedores e Inventarios.***

La serie de procesos citados anteriormente, demuestran que el Plan de Recuperación en Casos de Desastre o Plan de Contingencias, no es un esfuerzo temporal ni un acto retórico de la Dirección de Tecnologías de Información, es una necesidad real, derivada del impacto que tienen los Servicios de Información en esta época de alta tecnología y su influencia en la sociedad moderna.

Desde la primer prueba realizada de este Plan de Recuperación, me surgió la necesidad de hacer de él, un documento vivo, por esa razón desarrollé los diagramas de flujo citados

en el presente capítulo con la finalidad de lograr que cada repetición de la prueba, resultara en los beneficios siguientes:

- **Reducción del tiempo** de activivación de las plataformas tecnológicas, basado en las experiencias pasadas y registradas en el LOG, citado en el presente capítulo
- **Eliminar dependencias** de personal técnico especializado que sale de la empresa por razones personales o de otra índole, **al tener permanentemente actualizado y escrito el Plan** y contar con personal con el conocimiento técnico de cada plataforma, se garantiza la transmisión del conocimiento del Plan y sus actividades y por consecuencia su ejecución exitosa
- Lo más importante para garantizar la mejora continua del Plan, radica en el hecho de **registrar cada actividad que se darrolla y cada problema ó falla que se presenta, así como, registrar la solución aplicada,** eso permitirá afinar las actividades técnicas y dejar constancia de acciones que muchas obviamos desde un punto de vista técnico cuando desarrollamos una actividad de configuración ó definición de alguna componente de software ó de sistema aplicativo.
- Durante cada prueba se documentaba el LOG o Bitácora Cronológica, **ya que es la fuente de información para las mejoras la Plan.**
- En la figura
- Esa fue la razón por la cual le llamé procedimientos de **mantenimiento** al Plan que incluyen todos los aspectos citados en este Capítulo.

## Reporte de Resultados y Desviaciones para Mejoras

Plan DRP Resultados de Prueba Activación de Infraestructura y Servicios

| Actividad | Responsable | Hora Inicio Estimada | Hora Fin Estimada | Duración Estimada (min) | Hora Inicio Real | Hora Fin Real | Duración Real (min) | Estatus |
|---|---|---|---|---|---|---|---|---|
| **VIDADES Previas 06 Nov 2015, Ambiente DRP** | | | | | | | | |
| Validar fecha y hora del sistema (02 Nov 2015) | Juan Monroy | 16:00 | 16:05 | 0:05 | 16:17 | 16:22 | 0:05 | OK |
| Validación de ambientes CPU1 y CPU2 en DRP | Juan Monroy | 16:05 | 16:15 | 0:10 | 16:22 | 16:26 | 0:04 | OK |
| Validar Activación de VTAM y TCPIP | Julio Torres | 16:15 | 16:30 | 0:15 | 16:26 | 16:30 | 0:04 | OK |
| Validar Activación de Tareas de Bases de Datos | Lydia Retana | 16:30 | 16:45 | 0:15 | 16:38 | 16:41 | 0:03 | OK |
| Validación de Activación de Regiones CICS | Ernesto Rasgado | 16:45 | 17:00 | 0:15 | 16:41 | 16:51 | 0:10 | OK |
| Validación de los recursos aplicativos utilizados por los CICS solicitados para la prueba | Ernesto Rasgado | 17:00 | 17:15 | 0:15 | 16:51 | 17:01 | 0:10 | OK |
| **VIDADES 07/Nov/2015 - Desarrollo de Prueba DRP** | | | | | | | | |
| Ejecución de Pruebas con usuarios y DPS. | DPS y Usuarios | 8:00 | 14:00 | 6:00 | - | - | - | - |
| **VIDADES 20/Ene/2016 - Fin de Prueba DRP (Fase 2)** | | | | | | | | |
| Respaldo de syslog de ambientes de DRP de Prueba Fase 2 | Juan Monroy | 16:00 | 17:00 | 1:00 | 9:00 | 11:00 | 2:00 | OK |

Plan DRP Resultados de Prueba Activación de Infraestructura y Servicios

| # | Actividad | Responsable | Hora Inicio Estimada | Hora Fin Estimada | Duración Estimada (min) | Hora Inicio Real | Hora Fin Real | Duración Real (min) | Estatus |
|---|---|---|---|---|---|---|---|---|---|
| **ACTIVIDADES Previas 06 Nov 2015** | | | | | | | | | |
| 1 | Validar el Sitio de Single Sing On DRP | Sinhué Pérez | 17:00 | 17:15 | 0:15 | 5:03 | 5:08 | 0:05 | OK |
| 2 | Validar Sito de Administración Granja DRP | Sinhué Pérez | 17:15 | 17:40 | 0:25 | 5:08 | 5:10 | 0:02 | OK |
| 3 | Validar Sitios de ambiente DRP - Intranet, Pactación de Tasas, SVC (mi pago), Scotiaweb, Inverweb, INVERTEL (CT Call Center) | Grupo Intel | 17:40 | 18:20 | 0:40 | 5:10 | 5:31 | 0:21 | OK |
| 4 | Revisión de MAC Address para direccionamientos de las PU´s de los sitios contemplados para prueba de DRP (COMTI 2098) y Host Connector. | Sinhué Pérez | 18:20 | 19:00 | 0:40 | 5:31 | 5:35 | 0:04 | OK |
| 5 | Validar configuración (HIS 2004) hacia Mainframe DRP | Sinhué Pérez | 19:00 | 19:05 | 0:05 | 5:35 | 5:35 | 0:00 | OK |
| 6 | Validar la exportación de Comtis para Call center (TLB´s) | A Garrido | 19:05 | 19:35 | 0:30 | 5:35 | 5:38 | 0:03 | OK |
| 9 | Validación de la conexión hacia los ambientes WEB a la BD's. | Sinhué Pérez | 19:35 | 19:55 | 0:20 | 5:38 | 5:57 | 0:19 | OK |
| 10 | Acceso a ODBC's para validación de conexión con los sistemas, usuarios locales y cuentas de servicios. | Grupo Intel | 19:55 | 20:15 | 0:20 | 6:00 | 6:23 | 0:23 | OK |
| **ACTIVIDADES 06 Nov 2015 - Preparación adicional Fiduciario** | | | | | | | | | |
| 11 | Validar que se encuentre configurados los datos de los OLEDB de seguridad y de catalogos para el Aplicativo Fiduciario | Sinhué Pérez | 17:00 | 17:15 | 0:15 | 6:23 | 6:44 | 0:21 | OK |

***Figura 4.12: Ejemplo de Reporte de Resultados y Desviaciones.***

# Conclusiones.

## Introducción.

A los largo de los Capítulos que conforman esta tesis, se ha venido desarrollando la metodología para el Diseño, Construcción, Implementación y Pruebas del Plan de Contingencias para una empresa bancaria en el Sector Financiero Mexicano, en el presente apartado de Conclusiones y Recomendaciones, se confirmará el porqué es necesario contar con este tipo de Planes para lograr la continuidad de la operación financiera Bancaria y cual es el futuro de este tipo de Estrategias de cara a las nuevas tendencias tecnológicas.

## Conclusiones.

El desarrollo de esta metodología, no es un tema trivial en ningún tipo de Industria del Sector Económico Mexicano, basado en mi experiencia Laboral en los últimos 36 años, he tenido la fortuna de trabajar en diferentes sectores de la Industria, durante la época que trabajé en IBM de México, como Director de Proyecto de Outsourcing, siendo el Ejecutivo reponsable de los contratos de Outsourcing, con las empresas citadas a continuación:

- Financiero y Bursatil (Inverlat -Scotiabank Banco y Casa de Bolsa, Banorte)
- Seguros (Metlife)
- Retail o tiendas de autoservicio (Grupo Gigante, Office Depot México, Toks, Elektra)
- Comunicaciones (Ferromex)

Todas ellas cuentan con **Planes de Contingencia**, cada una de éstas **Empresas prueban anualmente su Plan, con la finalidad de afinarlo y mejorarlo a lo largo del tiempo, integrando nuevas tecnologías y nuevos enfoques desde la perspectiva de los servicios de mayor impacto de cara a sus clientes.**

El factor común que tienen todas ellas, es que desde los **niveles de la Alta Dirección, se han concientizado de la importancia de contar con estos Planes y de la necesidad de invertir en ellos, ante la potencial pérdida financiera y de mercado,** que pudieran tener en caso de **una Contingencia o Desastre natural que les impida tener continuidad** en el negocio y las operacione que de él se derivan.

Saben que es necesario tenerlo y lo asumen con todo el compromiso que ello implica, no lo ven como un mal necesario, **saben que puede hacer la diferencia, entre seguir vivos o desaparecer, si eventualmente sucediera un desastre que los inhabilitara tecnológicamente**.

En síntesis, las conclusiones que podemos derivar de la presente Tesis, se pueden establecer de la manera siguiente y desde dos perspectivas:

**Desde la prespectiva Financiera:**

- ✓ Es un factor importante para la permanencia en el mercado del sector industrial en el que se encuentre, cualquier empresa de mediana a grande, **contar con una Plan**

**de Recuperación ante Contingencias que formará parte integral de su BCP[1], Plan de Continuidad del Negocio,** ya que el impacto financiero que puede llegar a sufrir, eventualmente, la podría dejar fuera del mercado y podría desaparecer la marca, con las consecuentes implicaciones en la enconomía nacional.

- ✓ Cuando se trata de una empresa del Sector Financiero y/o Bursatil, el impacto financiero podría ser brutal, dado que se mueven cantidades de dinero de inversionistas nacionales e internacionales en los Bancos y Casas de Bolsa en México, desde luego el impacto en la economía nacional sería sumamente alto.
- ✓ Por la razón anterior, la **Comisión Nacional Bancaria y de Valores (CNBV)**, audita cada año, el resultado de las prueba de Recuperación (DRP y BCP) de las Instituciones Financieras en México y cuando se da un incumplimiento, la CNBV puede llegar a imponer sanciones de diferente tipo. Como ejempo, en el país vecino del Norte, en los Estados Unidos de América, en caso de que durante una contingencia real, una empresa del sector Financiero, no pueda continuar operando, el CEO (Director General de la Empresa y el Consejo de la Empresa), pueden llegar a tener responsabilidades penales que los lleven a enfrentar la pérdida de su libertad, no es el caso en la legislación Mexicana.
- ✓ En resumen, es preferible tener implementada y probada esta metodología y sus Planes, teniendo con ello un seguro de "vida" que les permitirá seguir operando en caso de Desastre o contingencia mayores, como las descritas en el Capítulo 2 y 3 de la presente Tesis.

**Desde la prespectiva Tecnológica:**

- ✓ Es un factor esencial para la creación y desarrollo del Plan, **ejecutar de manera adecuada y sustentada financieramente, el Análisis de Impacto al Negocio (BIA: Business Impact Analysis)**, pues este proceso determinará el RTO / RPO que permitirá justificar la inversión y el óptimo tiempo de Recuperación, basado directamente de la retroalimentación del nivel Directivo de la Empresa.
- ✓ **El RTO[2] / RPO[3],** permitirá diseñar la mejor arquitectura de recuperación para cumplir el dichos tiempos
- ✓ El **Plan de Recuperación (DRP),** es un documento **vivo, dinámico,** pues es el reflejo de la Infraestructura Tecnológica de la Empresa y a su vez de los cambios en el entorno de mercado financiero, por tal motivo deben ser revitalizados, a través de:

[1] BCP: Business Continuity Plan: por sus siglas en Ingles Plan de Continuidad del Negocio.
[2] RTO: Recovery Time Objetivo: Tiempo Objetivo de Recuperación de la Infraestructura.
[3] RPO: Recovery Point Objective: Objetivo del Punto de Recuperación, este tiempo determina la frescura de los datos con el que se recuperará la información para dar continuidad al Negocio y sus operaciones.

- Los procedimientos de mantenimiento definidos en la presente Tesis, en el Capítulo 4
- De la actualilzación del **BIA** que deberá ejecutarse **cada 2 años, al menos**, para confirmar los supuestos financieros y /o agregar nuevas funciones de negocio críticas, derivadas de nuevos servicios y/o productos financieros
- De las pruebas anuales de recuperación y sus resultados
- De las observaciones realizadas por las Auditorias Internas y de la CNBV
- De los cambios tecnológicos que afecten la Infraestructura en el Sitio Primario y de Recuperación
- De las tendencias tecnológicas y evolución de este tipo de soluciones.

# Recomendaciones

## Recomendaciones.

Con la evolución de las telecomuniocaciones, las plataformas tecnológicas, los productos de Software que permiten la replicación de Datos, prácticamente, desde cualquier lugar geográfico,.y sobre todo con el surgimiento de los servicios en la NUBE, que ofrecen la mayoría de las empresas goblales de tecnología, se está dando *un cambio importante en la estrategia y Planes de Recuperación en casos de Desastre (DRP)*, pues los servicios que se ofrecen en la nube, permiten a cualquier empresa, contar con Infraestructura tecnológica que soporte la operación del negocio, desde cualquier parte del mundo, dado que los Data Center que los líderes en este tipo de servicios, tienen a lo ancho del mundo.

En la figura siguiente (figura 1), se describen los servicios que típicamente ofrecen los proveedores de NUBE:

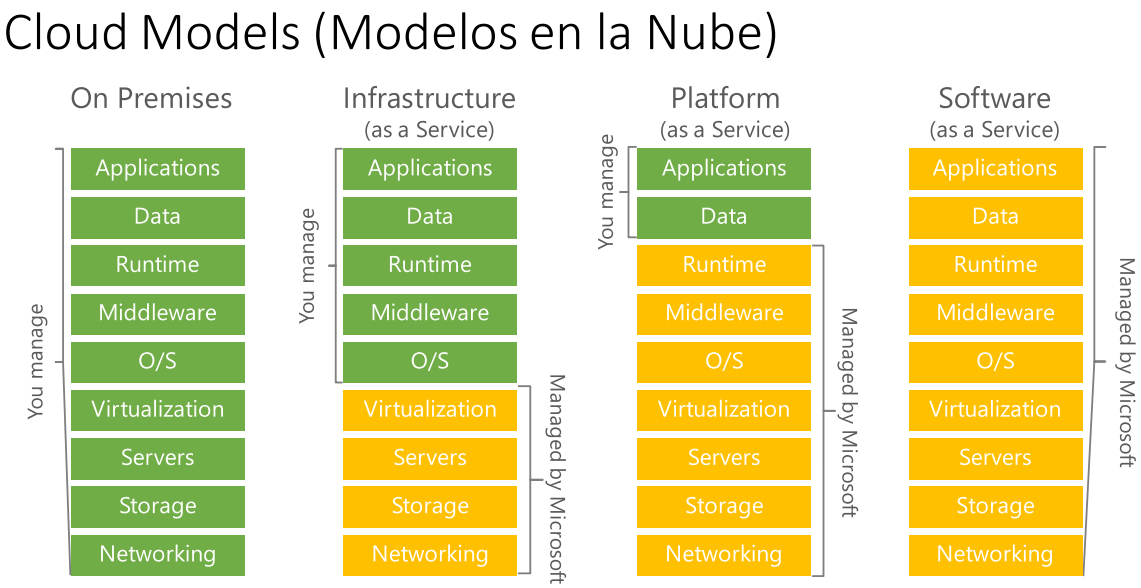



***Figura 1. Modelo de Servicios Típicos en al Nube, Fuente: Azure Microsoft (MR).***

Considerando los servicios citados en el modelo, el área de Tecnologías de la Información de cualquier empresa, podría adoptar el modelo de **IaaS**[1] ó **PaaS**[2], lo cual le permitiría tener 2 escenarios diferentes para implementar parte de su estrategia de Recuperación (DR), a continuación describiremos muy brevemente, como serían dichos Escenarios:

[1] IaaS: Infrastructure as a Service: Infraestructura como Servicios.
[2] Paas: Platform as a Service: Plataforma como Servicios

**Escenario 1:**

- Contratación de servicios de **IaaS,** con un cierto número de servidores virtuales que soporten funciones de negocio con baja criticidad, en esquema de Nube Híbrido (Privado – Público).
- Replicar hacia la Nube los datos de dichos ambientes para mantener la sincronia de la información y cumplir con el RTO/RPO que se tenga establecido.
- En este tipo de modelo, desde la capa del sistema operativo, es responsabilidad de la empresa la administración de esos ambientes, el proveedor de la Nube soporta y provee la infraestrucutra hasta la capa de virtualización, ver figura 2.

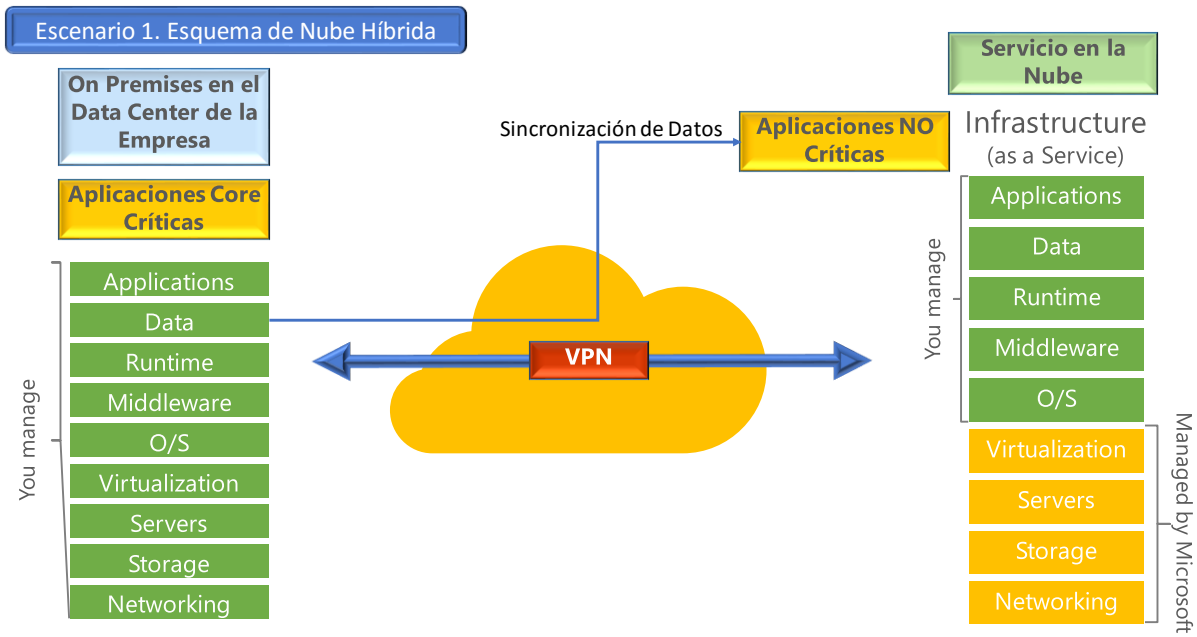



***Figura 2. Esquema de Nube Híbridas para DR de Aplicaciones NO Críticas con IaaS.***

**El Escenario 2.**

- Es muy similar pero con el servicio de PaaS en la Nube, en este tipo de servicio, la variante es que el proveedor de Nube, administra desde la capa de Red hasta el middleware y queda bajo responsabilidad del cliente (Empresa soliictante del Servicio), la admnistración de Datos y Aplicaciones, ver figura 3.

- Se trata también de un esquema de Nube Híbrida, bajo la misma consideración de tener el DR de aplicaciones No Críticas del negocio.
- Desde luego, también se requiere replicar hacia la Nube, los datos de dichos ambientes para mantener la sincronia de la información y cumplir con el RTO/RPO que se tenga establecido.

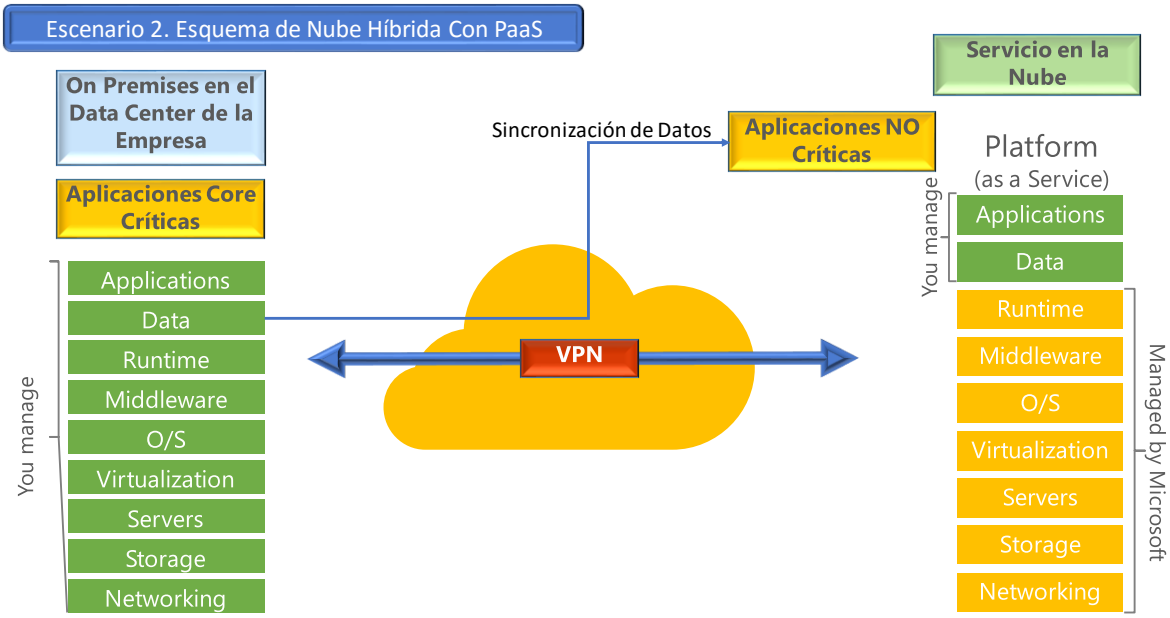



***Figura 3: Esquema de Nube Híbridas para DR de Aplicaciones NO Críticas con PaaS.***

Una de las compañías más reconocidas actualmente dedicada a la consultoría e investigación de tecnologías de la información, considera que una de las tendecnias tecnológicas que se adoptarán en el futuro cercano por muchas indutrias, consiste en la implementación de una solución "holística" de DR (Disaster Recovery: Recuperación en Desastres), que estaría formada por servicios soportados On Premise (en el Data Center Primario o local), nubes híbridas, es decir privadas y públicas, con modelo de servicios **Iaas y PaaS,** que permitirán y adicionalmente, cierto tipo de soluciones de Software como servicios (Software as a Service: **SaaS**), lo que permitiría una solución flexible en caso de Desastre.

Desde luego, se debe considera una topología de red apropiada y bien dimensionada, con esquemas redundantes de enlaces de comunicaciones con proveedores diferentes para garantizar que tienen infraestructura de comunicaciones independiente, así como la replicación de datos para soportar la recuperación en el tiempo establecido de RTO/RPO, este escenario se muestra en la figura 4.

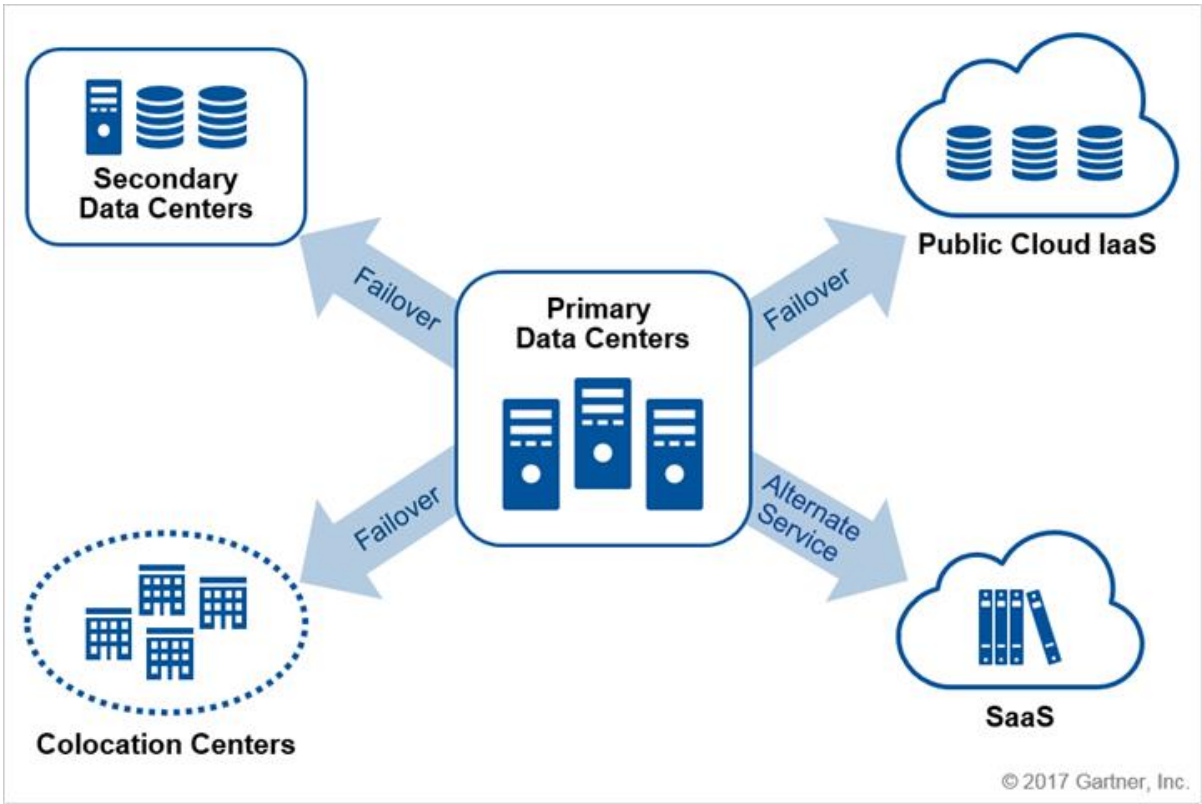



***Figura 4: Topólogía de DR (Disaster Recovery ), Recuperación en Desastres y Planes de Failover – Conmutación por Fallas, FUENTE GARTNER, Inc..***

Finalmente, durante el desarrollo de la presente Tesis, se ha presentado información estadística y documental, que soporta la necesidad de contar con Planes de Recuperación de las Operaciones de una Empresa (DRP y BCP), en caso de desastres naturales y /o tecnológicos, desarrollamos y propusimos un modelo para la creación, implementación, pruebas y mejoramiento de los planes de recuperación, todo lo anterior desde una perspectiva financiera y tecnológica, derivado de los impactos económicos que pudiera tener un desastre en la sociedad y en la economía de una Nación, ya que, en este caso en partícular, hablamos del impacto financiero que pudiera tener un Banco, pero si un desastre impactara no sólo a un Banco, sino a varios, el impacto financiero en el país podría ser altamente significativo en la economía y en la sociedad.

Derivado de lo anterior, es pertinente, incluir en las conclusiones, una visión muy rápida y resumida de las posibles tendencias que se observan y podrán marcar la evolución de los Planes de Recuperación en Casos de Desastre.

# Bibliografía y Ciberografía

# Bibliografía.


RedBooks Papers IBM:

IBM System Storage FlashCopy Manager and PPRC Manager Overview
Donald Chesarek, John Hulsey, Mary Lovelace, John Sing

IBM Storage Infrastructure for Business Continuity
R. F. Kern, V. T. Peltz

IBM DS8870 Multiple Target Peer-to-Peer Remote Copy
Warren Stanley

Communications and Networking for the IBM PC and Compatibles, Fourth Edition.

Larry Jordan and Bruce Churchill.

Brady Publishing.

Fundamentos de Comunicación de Datos

Jerry FitzGerald y Tom S. Eason.

Limusa

Análisis de Problemas y Toma de Decisiones(MR), KEPNER & TRIGOE

## Ciberografía.

Sungard Availability Services is a trademark of SunGard Data Systems Inc.

Fundación UNAM

http://www.dfinitivo.com/archivos/2007/09/19/terremoto-de-1985-a-22-anos-de-la-pesadilla/

http://www.taringa.net/posts/videos/793741/El-Gran-Terremoto-de-Mexico-1985.html

http://www.esmas.com/noticierostelevisa/terremoto/475688.html

https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

https://www.wikipedia.org/

http://www.sungardas.com/en/

https://es.uptimeinstitute.com/

# Glosario.

**Internet:**

Es el sistema mundial de redes de computadoras interconectadas que utilizan la familia de protocolos de Internet (TCP / IP) para conectar dispositivos en todo el mundo **INTER connected NETworks (Redes interconectadas)**.

**RPO**: Recovery Point Objective (Punto de Recuperación Objetivo).

**RTO**: Recovery Time Objective (Objetivo de Tiempo de Recuperación).

**Modem**: acrónimo que significa **Mo**dulador **Dem**odulador

**SNA:** por sus siglas en Ingles: System Network Architecture**,** Arquitectura de Redes de Sistemas

**CNBV**: Comisión Nacional Bancaria y de Valores**,** es el organismo del Gobierno Mexicano que rige y norma a las empresas financieras en nuestro País.

**CIO**: Chief Information Officer: Director de Información.

**CEO**: Chief Executive Officer**,** Director General del Grupo Financiero.

**BIA:** por sus siglas en Ingles Business Impact Analysis**;** Análisis de Impacto al Negocio

**LTO**: Linear Tape Open por sus siglas en Ingles, almacenamiento de datos en cinta magnética, esta tecnología fue desarrollado a finales de la década de los 90's, del siglo XX).

**PPRC**: Peer to Peer Remote Copy**;** Copia Remota entre Pares**,** tecnología desarrollada por IBM.

**E-Vaulting**: Bóveda remota de respaldos.

**Data Center**: Centros de Datos o Centro de Cómputo.

**Secondary Site:** Sitio Secundario o alterno de recuperación**.**

**IBM-BRCS**: IBM Business Continuity and Recovery Services (IBM Servicios de Recuperación y Continuidad del Negocio).

**HP-ES:** Hewlett Packard Enterprises Services (HP Servicios Empresariales).

**SunGard-AS: Sungard Availability Services (SunGard Servicios de Disponibilidad).**

**ATM**: Automatic Teller Machine (Cajero Automático).
**TR**: Tiempo de Recuperación del Servicio en las áreas de Negocio.

**Share Point:** Herramienta de Microsoft (© 2017 Microsoft) que es utilizada para publicar documentos para un grupo de usuarios.

**CECOBAN:** (Centro de Compensación Bancaria), entidad que depende del Banco de México.

**FDR**: First Data Resources.

**AMEX**: American Express.

**PROSA**: Switch de transacciones entre Bancos a Nivel Nacional e Internacional.

**SIVA**: Sistema de Valores.

**SACC**: Sistema de Administración de Cobranza y Crédito.

**RECOB**: Recaudación y Cobranza.

**SISNOM**: Sistema de Nómina y Compensaciones.

**PPRC followed by Flash Copy:** PPRC; Peer to Peer Remote Copy con Copia Instantánea, Marca registrada de IBM Corporation.

**ISPF**, es un conjunto de herramienta de administración del sistema operativo zOS marca IBM, utilizado en los equipos llamados Mainframe, tiene un editor e interfaz de usuario.

**Mainframe**, marca registrada de IBM, son computadoras de alta capacidad, su potencia de procesamiento se mide en MIPS (Millones de Instrucciones por Segundo).

**zOS**: Sistema Operativo z para equipos de la línea zSeries de IBM, marcas registradas.

**Uptime Institute:** es una organización de asesoría imparcial enfocada en mejorar el desempeño, la eficiencia y la confiabilidad de la infraestructura crítica de negocios a través de la innovación, colaboración y certificaciones independientes.

**ISO / IEC 27001:** 2005 es una norma de seguridad de la información que fue publicada en septiembre de 2013. Sustituye a ISO / IEC 27001: 2005 y es publicada por la **Organización Internacional de Normalización (ISO)** y la **Comisión Electrotécnica Internacional (CEI)** El subcomité conjunto ISO / CEI, ISO / IEC JTC 1 / SC 27. [2]. Es una especificación para un sistema de gestión de la seguridad de la información (SGSI). Las organizaciones que cumplen con la norma pueden ser certificadas como conformes por un organismo de certificación independiente y acreditado en la finalización exitosa de una auditoría de cumplimiento.

**SG**: Storage Groups: Grupos de Almacenamiento
**DACS**: Digital Access Cross-Connect System (DACS, por sus siglas en inglés), Sistema de Conexión de Acceso Digital.

**RDI**: Red Digital Integrada.

**SAC**: Satellite Access Controller: Control de Acceso al Satélite.

**SCPC**: Single Carrier Per Channel: Canal Único por Portadora.

**POS**: Point of Sale Terminal: Terminal Punto de Venta.

**NAC**: Network Access Controller (Controlador de Acceso a la Red).

**TDMA**: El **acceso múltiple por división de tiempo** (*Time Division Multiple Access* o **TDMA**) es una técnica de modulación que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal (normalmente de gran capacidad) de transmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de transmisión. El **Acceso múltiple por división de tiempo** (TDMA) es una de las técnicas de TDM más difundidas.
**VSAT**: **VSAT** son las siglas de **Terminal de Apertura Muy Pequeña** (del inglés, *Very Small Aperture Terminal*). Designa un tipo de antena para comunicación de datos vía satélite y por extensión a las redes que se sirven de ellas, normalmente para intercambio de información punto a punto, punto a multipunto (*broadcasting*) o interactiva.

**DRP**: Disaster Recovery Plan por sus siglas en Ingles: Plan de Recuperación en Casos de Desastre

**CMDB: Configuration Management Data Base**: Base de Datos para la Administración de la Configuración.

**CI's**: Configurations Items (por sus siglas en Ingles), Artículos o Componentes de la Configuración.

**BCP:** Business Continuity Plan, por sus siglas en Ingles, Plan de Continuidad del Negocio.

**IBM VM**: Virtual Machine: El **VM/CMS** es un sistema operativo de máquina virtual que se anunció para el público en 1972 por IBM para computadores centrales o mainframes, plataformas como System/370, System/390, zSeries, System Z9. Está basado en máquina virtual de sistema cuyo núcleo es un programa de control llamado CP (Control Program) o también denominado VMCP (Virtual Machine Control Program), cuya principal característica, es que permite la ejecución de una máquina virtual dentro de otra máquina virtual, también es la encargada de controlar los dispositivos hardware del ordenador: CPU, discos cintas, etc.

**MAC Address**: la **dirección MAC** (siglas en inglés de *Media Access Control*) es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales (4 bits)) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como **dirección física**, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (primeros 24 bits) utilizando el organizationally unique identifier. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64, las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

**IP Address**: Una **dirección IP** es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, *smartphone*) que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizando la red.

**CICS**: Customer Interface Control System: Sistema de Control de Interface de Cliente.

**IBM TWS**: Tivoli WorkLoader Scheduler: Agenda de Carga de Trabajos Tivoli; se usa para correr automáticamente procesos Batch conservando sus características de secuencia con predecesores y sucesores de procesos.

**Clean Up**: Limpieza de los ambientes recuperados en los equipos del Sitio Secundario.

**Release**: Lanzamiento o cambios en el sistema operativo que no requieren cambiar la versión del mismo.

**Quality Assurance**: Aseguramiento de calidad, este ambiente permite probar, no sólo, los cambios aplicativos sino también las nuevas versiones y releases de los sistemas operativos.

**IaaS**: Infrastructure as a Service: Infraestructura como Servicios.

**Paas**: Platform as a Service: Plataforma como Servicios.