



INTRODUCCION

A partir de eventos mundiales en donde desastres naturales o provocados han afectado centros de datos de empresas, los resultados han sido en algunos casos tan graves como la desaparición de grandes empresas y pérdidas millonarias a dueños, clientes y proveedores.

En México las regulaciones y la preocupación de los dueños de empresas de asegurar a toda costa la protección de la información ante cualquier incidente generaron que a partir del 2006 el sistema financiero mexicano replanteara los modelos tradicionales de recuperación ante un desastre y la pérdida de su centro de datos principal.

La complejidad del proyecto fue muy grande y represento un cambio total de los paradigmas de la administración de los centros de datos tradicionales.

Hoy este sistema de DRP es el único en México 100% probado, reconocido por múltiples empresas dedicadas al análisis de infraestructura y soluciones de tecnología (Gartner).

Para crear y ejecutar el proyecto, se tuvieron que gestionar sub-proyectos de renovación tecnológica que alinearan las soluciones (muchas de ellas monolíticas, sin soporte comercial y pocas posibilidades de sustitución) a una serie de objetivos (consolidación, simplificación y crecimiento de las capacidades) encaminados a que en su conjunto facilitaran la creación del DRP en una forma conjunta que cubriría el total de aplicaciones del Banco.

El presente trabajo se desarrolla en dos grande capítulos el primero describe un marco teórico de porque la necesidad de que un centro de datos o un área de tecnología que contiene información del negocio requiere crear una estrategia y un modelo de recuperación en caso de fallas; en el segundo se expone como se analizó y creo el modelo que cubría las necesidades de recuperación que la empresa requiere, detalla los procesos de análisis, diseño y construcción del proyecto y explica el modelo de operación que se logro al final del proyecto.

OBJETIVO

El objetivo de este proyecto fue analizar, diseñar, construir, administrar una solución que permita ante un caso de desastre de cualquier tipo una recuperación total del centro de datos de uno de los Bancos más importantes de México.

Respecto de mi aportación en este proyecto, comentare que fui el líder técnico y operativo; todas las decisiones de infraestructuras fueron tomadas por mi persona y las fundamente en procesos de investigación de tecnologías de punta, procesos de evaluación técnica de las soluciones, muchas pruebas y laboratorios que simularon los escenarios planteados. Los proyectos de implementación fueron coordinados, dirigidos y en varios casos supervisados por mí como Director de Infraestructura y la responsabilidad total de su éxito o fracaso dependía exclusivamente de mis decisiones. Existía un equipo alterno que se encargo de todos los aspectos de control de pruebas con toda la institución, la comunicación externa y la coordinación de los usuarios.



CAPITULO I

1. MARCO TEORICO (ITIL- PROCESO DE CONTINUIDAD)

1.1 Los Procesos de Tecnología

Todas las empresas de cualquier tamaño que de alguna forma ya cuenta con un área de tecnologías de la información (TI) o pretenden crear una nueva debe apegarse a un modelo de operación que lo oriente en las metodologías y procesos que deberá seguir. Existen muchas metodologías y documentación que dan esta orientación, pero la verdad es que las empresas que ya cuentan con áreas de sistemas fueron creando sus modelos y procesos con base a su crecimiento, a los problemas que se le fueron presentando y las formas muy particulares en como implementaron ciertos procesos, las nuevas áreas tratan de apegarse a estos modelos ya probados y documentados, pero pocas veces lograr implementarlos al 100% como se plantea en las mejores prácticas y optan por generar sus propias variantes.

1.2 ITIL

ITIL (Information Technology Infrastructure Library), es un conjunto de documentos que brinda un conjunto detallado, consistente y coherente de mejores prácticas con un enfoque hacia los procesos de la administración de los servicios de Tecnologías de Información, además promueve un enfoque de calidad para alcanzar la eficacia y eficiencia en el uso de los sistemas de información para el negocio.

Actualmente se ha difundido mucho el uso de estos lineamientos y existen cursos de certificación y/o empresas que validan el apego a estas normas dentro de los procesos y servicios que ofrece un área de tecnología. Entre los beneficios que se afirma se pueden lograr utilizando esta metodología se mencionan los siguientes:

1. Incrementar la satisfacción de usuarios y clientes mediante el uso de los Servicios de Tecnología.
2. Mejorar la disponibilidad del servicio y directamente apoyar al negocio en mejorar su eficiencia y ganancias.
3. Lograr reducciones financieras, reduciendo el re trabajo, mejorando procesos de administración y control.
4. Mejorar la salida de productos y servicios que provengan de tecnología, ejemplo nuevos desarrollos, optimización de procesos de usuario, mantenimientos más eficientes.
5. Mejorar la seguridad y optimizar el riesgo.

ITIL, está estructurado en 8 o 9 libros, varían según el autor pero en esencia cubren los siguientes aspectos de TI:

Gestión de Servicios de Tecnología (TI):

1. Mejores prácticas para la Provisión de Servicio (Desarrollo).
2. Mejores prácticas para el Soporte de Servicio (Operación y continuidad).

Otras guías operativas

3. Gestión de la infraestructura de TI.
4. Gestión de la seguridad.
5. Perspectiva de negocio.
6. Gestión de aplicaciones.
7. Gestión de activos de software.

Para asistir en la implementación de prácticas ITIL, se publicó un libro adicional con guías de implementación (principalmente de la Gestión de Servicios):

8. Planeando implementar la Gestión de Servicios.

El área que nos ocupa para entender la importancia y criticidad del DRP, es el proceso de Soporte al Servicio, es decir la segunda práctica más importante. Este proceso se fundamenta en dos grandes áreas: El **soporte al servicio** y la **entrega del servicio**.



1.2.1 Soporte al Servicio

El soporte al servicio cubre todos los aspectos de la operativa diaria de un área de tecnología y se sustenta en los siguientes procesos:

-Administración de la configuración, proporciona un modelo lógico de la infraestructura o el servicio mediante la identificación, control, el mantenimiento y la verificación de las versiones de los Elementos de Configuración existentes. En este proceso se contabilizan todos los activos de TI, las configuraciones y los servicios dentro de la organización.

-Mesa de Servicio/Centro de Servicio al Cliente, representa la cara al usuario y centra sus objetivos en manejar y mejorar el servicio para y en nombre del negocio, operativamente su objetivo es proveer un punto único de contacto para aconsejar, guiar y restaurar rápidamente los servicios normales de sus usuarios y clientes. Es el punto de contacto entre el cliente y el servicio. Esta mesa de servicio está orientada al cliente y está constituida por personas con conocimiento técnico y con habilidades para relaciones interpersonales, comúnmente este proceso se asocia a un Callcenter (Centro de Contacto Cliente- Empresa de Servicios).

-Administración de Incidentes, tiene como propósito establecer los lineamientos operativos para restaurar la operación normal del servicio lo antes posible y minimizar el impacto adverso sobre las operaciones del negocio. En este proceso se evalúan, priorizan y ordenan los eventos y se analizan los niveles de servicio que el negocio solicita a TI (Tecnologías de Información, área de Infraestructura, áreas de tecnología de las empresas).

-Administración de Problemas, proceso responsable de minimizar el impacto adverso por incidentes o problemas sobre el negocio que son causados por errores o malfuncionamiento de la Infraestructura Tecnológica, y se asegura de prevenir la repetición de los incidentes relacionados con estos errores. Este proceso introduce ampliamente los conceptos de soluciones reactivas y proactivas. En este proceso se analiza la relación entre los problemas y los cambios y se construye la base de conocimientos que ayude en temas de prevención.

-Administración de cambios, tiene el objetivo de garantizar el uso de métodos y procedimientos estandarizados para el manejo eficaz y oportuno de todo cambio en TI, minimizando el impacto de los incidentes relacionados con los cambios y mejorando la operación diaria. Se analiza la calidad del servicio buscando la reducción constante de incidentes relacionados por un cambio. En este proceso se crea un comité responsable de valorar el impacto y la relación de componentes que pueden ser afectados en el cambio. En algunos casos ciertos autores separan este proceso de Administración de liberaciones responsable de la administración, control y pruebas de los sistemas que están siendo modificados. En el caso del proyecto esta área se le denominó, Implantación.

1.2.2 Entrega al Servicio

El segundo aspecto ITIL respecto a las mejoras prácticas para el soporte al servicio, es la “entrega al servicio”, este proceso tiene como misión mantener y mejorar la calidad de los servicios de TI (Administración de Almacenamiento, administración de equipo de computo y comunicaciones, administración de las soluciones o aplicaciones, operación de centro de computo) a través de un ciclo constante de acuerdo, monitoreo, generación de reportes y planes específicos para 4 grandes áreas.

-Administración de la Disponibilidad, tiene como objetivo mantener y mejorar la calidad de los servicios de IT a través de un ciclo constante de acuerdo al monitoreo, generación de reportes; en este proceso se gestionan, acuerdan y monitorean los niveles de servicio. Aquí se desarrollan y diseñan los SLAs (Service Level Agreement, Acuerdos de Niveles de Servicio) los cuales serán revisados y evaluados de forma continua para garantizar la calidad requerida. En este proceso se listan los catálogos de servicios y se firman contratos de SLA y mejora continua.

-Administración Financiera para servicios de TI, provee una guía con respecto a la utilización eficiente de los costos de los activos y los recursos de TI empleados en la provisión de servicios, debe tener la capacidad de entregar cuentas por todo el gasto de servicios de IT y debe aconsejar sobre inversiones de IT para la mejora. En algunos casos crean modelos de costos por servicio y pueden ofrecer diferentes niveles de calidad dependiendo de los requerimientos del negocio.

-Administración de la capacidad (una de las áreas que más apoyo tuvo durante la creación del proyecto que se está analizando ya que de ésta se desprendió la necesidad de una renovación tecnológica que apalanco la creación de



proyectos de consolidación y vitalización que pretendían soportar la demanda de capacidad de cómputo con una estrategia fuerte de simplificación del Hardware), este proceso es responsable de la optimización de la capacidad de la infraestructura de TI, los servicios y el soporte a la organización para ofrecer un nivel de disponibilidad sostenido, de costo adecuado y que permita al negocio satisfacer sus objetivos. Particularmente en la Banca este es uno de los procesos más críticos ya que puede ser el determinante de que un cliente use o no sus servicios, ya que se supone que las aplicaciones siempre estarán disponibles para que el cliente pueda realizar un movimiento financiero en todo momento. En este proceso se debe asegurar que todos los aspectos de la capacidad actual y futura y aspectos de desempeño del negocio se brinden a un costo eficaz. Algunos autores mezclan mucho este proceso con el de disponibilidad asociando los costos de capacidad de redundancia ya sea al aspecto mismo de la capacidad o al de la disponibilidad. En nuestro caso ambas están estrechamente relacionadas ya que derivado de ambas se gestiono el proyecto de renovación que sirvió de base para la construcción del DRP.

-Administración de la continuidad del Negocio, en este proceso se sustenta todos los procesos y procedimientos para soportar la continua operación de los servicios que ofrecen los sistemas, asegurando que los requerimientos técnicos y las instalaciones físicas pueden ser recuperados dentro de los tiempos requeridos y acordados con el negocio. El plan de continuidad es un enfoque sistemático para la creación de un plan o procedimiento para prevenir y/ recuperarse de la pérdida de servicios críticos por períodos extensos o que en muchos de los casos represente la pérdida potencial de instalaciones o equipos derivados de un siniestro.

1.2.3 Administración de la Continuidad de los Servicios de TI

En la actualidad los clientes o usuarios esperan que tras la interrupción del servicio derivado de un siniestro grave, las organizaciones continúen operando al menos a un nivel mínimo acordado. Si no se puede cumplir con esto la insatisfacción del cliente, genera mala reputación, pérdidas a los negocios y muchas veces la pérdida del cliente en sí mismo, la competencia es muy fuerte y problemas de este tipo llegan a generar pérdidas tan graves como la desaparición del negocio. Ejemplos como servicios de búsqueda en internet YAHOO, GOOGLE, servicios de redes sociales, FACEBOOK, TWITTER, etc. Son tan vulnerables a la insatisfacción de los clientes que estas empresas hacen inversiones millonarias para establecer esquemas de respaldos muy complejos y costosos pero que se fundamente en el objetivo “SERVICIO SIEMPRE, CALIDAD DEL SERVICIO SIEMPRE”.

Los sistemas financieros sobretodo son los que en su mayoría invierten y tienen procesos y áreas dedicadas al aseguramiento principalmente de la “Información”, que es el activo más valioso de un negocio financiero y el servicio al cliente.

El proceso de administración de la continuidad de los servicios de IT también conocido por sus siglas en ingles ITSCM (Information Technology Service Continuity Managemet- Gestión de la continuidad del servicio en Tecnología), se encarga de buscar e implementar las medidas sólidas de reducción de riesgo y opciones de recuperación para poder dar el soporte y continuidad a los servicios más críticos del negocio.

ITSCM debe realizar actividades de análisis de impacto al negocio (BIA, Bussines Impact Analysis)) para determinar el daño que puede causar la interrupción del servicio según el caso. Por ejemplo en un negocio de autoservicio si los sistemas fallaran, quizás lo más importante es restablecer el sistema de los cajeros, los sistemas administrativos, recursos humanos, horarios quedarían en segundo o tercer término y todos los esfuerzos tecnológicos deben centrarse en restablecer el sistema más importante porque no podrían vender y por tanto habría pérdidas. En este análisis se evalúan los niveles de amenaza y vulnerabilidad para establecer si estos requisitos tienen un riesgo elevado. Por ejemplo, si hay muchas posibilidades de que se produzca una interrupción (amenaza) y el impacto para la organización es alto si se materializa (vulnerabilidad) entonces habrá un riesgo muy elevado.

Los datos que se conjunen del análisis de impacto y evaluación del riesgo determinaran la estrategia que la organización debe desarrollar para que en una forma adecuada use la combinación riesgo con las opciones de recuperación.

Las medidas de reducción de riesgo pueden incluir la instalación de sistemas de alta disponibilidad, mayor control de seguridad, procedimientos de escalación mejorados, servicios con terceros muy especializados y redundantes, inclusión de software especializado, etc. Se tiene que tener mucho cuidado en estos diseños evitando siempre que un riesgo no aumente a otro, por ejemplo los servicios con terceros (uso de empresas externas) pueden reducir los temas de disponibilidad de los sistemas, sin embargo, esto puede aumentar potencialmente el riesgo de comprometer información confidencial (el proyecto que se presentara en este reporte busca cubrir adecuadamente estos temas) a menos que se apliquen controles de seguridad más rigurosos.



Las opciones de recuperación pueden variar dependiendo de la velocidad con la que se deben restablecer los servicios y fundamentalmente el costo de implementación está ligado directamente con la relación, 'pérdida de información' - 'tiempo para reactivar el sistema', a mayor pérdida menor costo porque no se requieren esquemas costosos de resguardo de información, a menor tiempo de reactivación mayor costo por el tipo de equipos y soluciones que permitan una rápida reparación o la existencia de un equipo solo para utilizar en caso de un incidente mayor.

Para cumplir con todo esto es necesario el proceso de ITIL que hemos descrito anteriormente ya que en su conjunto los procesos de administración de la capacidad ofrece los recursos necesarios para dar el soporte a los requisitos de negocio, la administración de la disponibilidad provee la disponibilidad y diseño de recuperación con la intención de prevenir o reducir impacto en caso de fallas, la administración de cambios garantiza que los planes de continuidad sean correctos y que se revisen continuamente.

Para el éxito de un proyecto de este tipo es crítica la participación de la alta dirección ya que todos los participantes técnicos y usuarios deben comprometerse en conjunto para el desarrollo del proyecto y su continuo mantenimiento, pruebas y actualización. Sin esto un sistema de recuperación puede en muy poco tiempo carecer de valor y volverse obsoleto o ineficiente a los requerimientos solicitados en el BIA.

1.2.4 Definiciones Importantes

1.- Desastre: Un evento que afecta a un servicio o sistema de manera tal que es requerido un esfuerzo importante para restablecer el nivel original de operación y desempeño.

2.- Administración de Crisis: Proceso mediante el cual la organización administra el impacto del desastre, la cobertura adversa a medios de comunicación y mantenimiento continuo de información del avance del proceso de solución.

3.- Plan de recuperación de Desastre (DRP): Son los procesos que se focalizan solo en los procesos de recuperación, principalmente en respuesta a desastres físicos que son contenidos dentro del BCM

4.- Administración de la continuidad del Negocio (BMC): Se ocupa de la administración de continuidad del negocio que incorpora todos los servicios de los que depende el negocio, uno de los cuales es IT, en forma frecuente es precedida por un comité multidisciplinario y con una posición gerencial con reporte a la alta dirección y en donde se tomen decisiones importante para los procesos de prueba y la posibilidad del control en caso de un desastre real.

5.- Análisis de Riesgo y Métodos de Administración (CRAMM): Se describe como la manera de identificar las medidas preventivas justificables para proteger la confidencialidad, la integridad y la disponibilidad de la infraestructura de TI. Este análisis de Riesgo involucra la identificación y evaluación del nivel de riesgos calculados desde la evaluación del valor de los activos y nivel de amenazas hasta las vulnerabilidades de estos activos.

6.- Opciones de recuperación:

- No hacer nada.
- Solución Temporal Manual.
- Acuerdos Recíprocos.
- Recuperación gradual (Cold Standby) - 72 horas o más.
- Recuperación Intermedia (Warm Standby) entre 24 y 72 horas.
- Recuperación Inmediata (Hot Standby) < 24Horas.

1.3 Proceso de BCM (Business Continuity Management)

El proceso de BCM incluye cuatro etapas (Iniciación, Requerimientos y Estrategias, Implantación y Administración de la operación) que le permiten analizar, desarrollar, construir, mantener y operar un sistema de recuperación en caso de desastres, en forma breve explicare cada una de ellas. El presente trabajo se centra en las etapas de requerimientos, estrategias y administración, detallando y documentando como fue el proceso.

1.3.1 Etapa 1: Iniciación



Iniciar Administración de la continuidad del Negocio

Esta etapa cubre la organización del proyecto y comprende los siguientes puntos:

- Establecer la Políticas.
- Establecer los términos de Referencia y Alcance.
- Asignación de recursos.
- Definir la organización del Proyecto y la estructura de control.
- Acuerdos sobre Proyectos y Planes de Calidad.

Esta etapa es compleja porque determina el arranque formal de varios proyectos que apoyen o alineen a la estrategia que buscarían para lograr el modelo deseado de recuperación, en este no se definen los alcances pero si el marco de referencia global que con base en la regulación y objetivos que el negocio buscaría en caso de una contingencia, defina los alcances de la recuperación.

1.3.2 Etapa 2: Requerimientos y Estrategias

Requerimiento y Estrategia

En esta etapa se brindan todas las bases para realizar un buen sistema de control para la continuidad no solo en la parte técnica, si no en la operativa, y es crítica para determinar que tan bien una organización sobreviva a una interrupción del negocio o un desastre y los costos en los que pudiera incurrir.

Esta etapa es fundamental, en el presente reporte se detallan los siguientes pasos que determinan los requerimientos y estrategias que para el caso de la institución financiera que nos ocupa y en donde se realizó el proyecto que estamos documentando.

1.3.2.1 Análisis de Impacto (BIA)

Una forma esencial para determinar los requerimientos para el proceso de continuidad del negocio, es conocer la pérdida que puede soportar la organización como resultado de un desastre o interrupción del servicio y la velocidad que estas pérdidas van escalando con base en el tiempo que se tarda en reactivar la operación. El propósito de esta fase es crear un análisis del Impacto al Negocio (BIA- Business Impact Analysis) en donde a través de un proceso de evaluación se:

- Identificarán los procesos críticos del negocio, el daño o pérdida potencial que puede causar a una organización la falla de un sistema o proceso crítico del negocio, por ejemplo en un banco el sistema de cajeros o internet es más crítico que el sistema de pago a proveedores.
- El impacto que se mide en varios escenarios y por lo general caen en una o más de las siguientes categorías – imposibilidad de alcanzar los niveles de servicio internos, pérdida financiera, costos adicionales (reconstrucciones, demandas), pérdidas inmediatas o de largo plazo, pérdidas de participación de mercado, etc. El reporte, propósito de este documento, detalla el resultado de este proceso en una institución financiera.

1.3.2.2 Evaluación del riesgo

La siguiente forma que determina los posibles requerimientos del proceso de continuidad del negocio es el análisis de las posibilidades de que se produzca un desastre o una seria interrupción del servicio. Esta es una evaluación del nivel de amenaza y del grado en el que una organización es vulnerable a tal amenaza. En el reporte anexo se ejemplifica y se muestra un ejercicio completo de esta evaluación.



1.3.2.3 Estrategia de Continuidad del Negocio

La información reunida en los puntos anteriores (análisis de impacto y evaluación del riesgo), permite desarrollar una estrategia correcta para la organización con un balance óptimo de reducción de riesgo y recuperación; y una o varias opciones de continuidad, en el caso que se analiza en el documento se verán siete posibles opciones de implementación de un modelo de recuperación y el elegido fue el más completo y complejo pero con mayor alcance de recuperación y minimización del riesgo. En esta etapa también se incluyen las consideraciones de las prioridades en el proceso de recuperación del servicio y los cambios en las operativas de los servicios o procesos relacionados en un tiempo del día, en un día de la semana y/o en las variaciones del mes y anuales. Por ejemplo en el caso del una empresa de tecnología que da servicio a restaurantes tipo Bar es más crítico un problema que da por la tarde, noche o madrugada que en la mañana en donde quizás no de servicio. Otro ejemplo es una tienda de autoservicio, en caso de una falla el sistema de cobro tiene una mayor prioridad de recuperación que el sistema de nomina o pago a proveedores, por tanto se definen procesos diferentes para los sistemas menos críticos como control manual, registros en libros, etc.

En el proyecto se presentan siete escenarios ordenados por los tiempos para el restablecimiento de la información y la pérdida potencial de datos permitida, cada uno de ellos representaba un costo y un esfuerzo muy diferente, la conclusión final con base en los requerimientos del BIA fue tomar la más compleja pero con mayor alcance a la reducción del riesgo y reducción mínima a la posibilidad de pérdida de información esto determinado porque el de declaro que “el activo más importante de una institución financiera son los datos”.

1.3.3 Etapa 3: Implantación

Implantación del Modelo o Solución.

En esta etapa se construye el modelo físico que sustente los requerimientos del BIA, dependiendo de la estrategia aquí pueden solo generarse documentos, hasta construir instalaciones o soluciones de Hardware o Software que ayuden a cubrir los planteamientos del BIA.

1.3.3.1 Planeación de Organización e Implementación

Se crea el plan macro que contenga una división lógica estratégica que cubra los aspectos de la planeación global por proceso, dividiendo la implementación de procesos en áreas de apoyo, procesos de áreas técnicas, procesos de construcción, procesos de información a terceros, procesos de información a dirección, procesos operativos de contingencia. El caso que nos ocupa en este reporte se centra en la implementación y organización del área técnica.

1.3.3.2 Implantar Acuerdos en Espera

Las estrategias de los procesos de recuperación se basan en una serie de “Acuerdos de espera” (son los tiempos en que definitivamente los servicios estarán fuera y se disparan los procesos de recuperación, la fase de pruebas se responsabiliza en su momento de validar estos acuerdos y tratar de que estén por debajo de lo solicitado) que incluyen temas de la ubicación, sistemas y telecomunicaciones requeridos para el proceso, los cuales pueden ir desde rentas por evento, hasta instalaciones solo para este propósito, todas estas posibilidades de implementación dependen de lo solicitado en el BIA.

Para implantar los Acuerdos de espera es preciso llevar a cabo ciertas acciones por ejemplo:

- Contratar instalaciones físicas de recuperación con terceros (o propias si hay capacidad).
- Preparar y equipar las instalaciones en espera.
- Comprar e instalar los sistemas de computación, telefonía, redes, enlaces para la recuperación.
- Validar temas de contratos de SW para el uso de licencias en instalaciones de recuperación.
- Negociar con proveedores de servicio externo los planes y servicios requeridos.

1.3.3.3 Desarrollar los Planes de Recuperación



Estos planes se desarrollan en conjunto con todas las áreas de la empresa, en la actualidad existe software especializado que permite llevar estos procesos y mantenerlos documentados en una herramienta, proveedores como SUNGARD, LRDPS, proveen este tipo de soluciones y ayudan a con base en un flujo documentar las acciones a seguir por cada área o proceso contingente.

1.3.3.4 Implementar Medidas de Reducción de Riesgo.

En esta parte aplica la construcción física en base al diseño, cuando menor tiempo de caída resulta inaceptable, se debería implementar el almacenamiento y respaldo fuera de las instalaciones físicas productivas, utilizar tecnologías como arreglos de discos y esquemas de duplicación de discos por medio de redes extendidas o fibras ópticas, previniendo la pérdida de datos y garantizando la disponibilidad continua de los datos, también la implementación de sistemas locales con alta tolerancia a fallas.

En el caso de estudio del presente trabajo se explica a detalle las fases del diseño, la construcción e implementación de esta solución y es en donde se centra la mayor parte de información de este documento, se detalla las fases y la orientación de la decisión del modelo de DRP elegido, el cual se construyó a partir de proyectos habilitadores de la solución que fueron la consolidación y la vitalización de los sistemas, así como un proyecto de consolidación de almacenamiento, todo esto habilita la posibilidad de crear un centro de respaldos mucho más económico y funcional que el que se tenía operando y que representaba un riesgo muy alto para la institución y fue uno de los habilitadores principales del origen de este proyecto.

1.3.3.5 Desarrollar los Procedimientos

Estos procedimientos deben incluir:

- Instalación y pruebas del hardware de remplazo, almacenamiento y redes.
- Restauración del software y datos a un punto de referencia común (entre todos los sistemas o aplicaciones de una empresa o negocio buscando consistencia de datos inter-aplicaciones) y consistente.
- Calcular puntos de quiebre del negocio.
- Establecer de puntos de control en cada paso del arranque de los sistemas de recuperación.
- Crear los mecanismos de información al negocio o personaje o área que se determinó tenga esta función.

1.3.3.6 Pruebas

Implica el proceso de planeación y ejecución de una prueba completa que debe replicar la invocación de todos los acuerdos de recuperación, incluyendo la recuperación misma y participación de los procesos de negocio y de posibles externos (auditores, consultores). Esta parte es la culminación y validación del cumplimiento del BIA, en la cual se revisa la integridad de los planes y confirma los objetivos de tiempo, preparación del personal técnico y de negocio, la reacción y generación de la contingencia.

El presente documento no detalla esta fase pero la explica brevemente en el capítulo 5 ya que no estuvo ni está en mi ramo de control la coordinación de las pruebas, solo me corresponde el mantenimiento y aseguramiento de los sistemas del DRP y apoyar el constante uso del mismo en este tipo de pruebas.

1.3.4 Etapa 4: Administración de Operación

1.3.4.1 Educación y Conciencia

Esto debe cubrir y garantizar una capacitación a todo el personal para que conozca las implicaciones de la continuidad del negocio y de la continuidad del servicio, debe generar conciencia para que siempre tomen en cuenta que hay una parte de su rutina de trabajo normal y otra de que deberán aplicar en caso de un desastre. Empresas muy evolucionadas en esto crean una comunicación continua que informa como atacar estos temas incluso en forma personal, ya que muchas empresas en si tienen riesgos y deben extender el tema de la continuidad del negocio a la continuidad de sus vidas, por ejemplo, plantas atómicas, empresas que estén en zonas altamente sísmicas, etc.



1.3.4.2 Revisión y Auditoria

Se debe llevar a cabo una revisión regular de los entregables del ITSCM para garantizar la actualización continua. En el caso de TI esto pueden tener gran impacto por ejemplo en un cambio mayor de infraestructura de TI, las dependencias en las redes pueden cambiar y entonces hay que estar en constante vigilancia que el centro de respaldo sea igualmente actualizado. Los planes también tienen que considerar que las organizaciones cambian y las responsabilidades creadas deben formar ya parte del perfil de cada persona que tiene que ver con este proceso. En el caso de esta implementación el modelo cubre los aspectos de Software en su totalidad ya en el documento se explica porque y como se logra esto, pero los aspectos del Hardware deben ser muy cuidados para mantener y asegurar su funcionalidad en las pruebas y por su puesto en el posible evento.

1.3.4.3 Prueba

Sirve para establecer un programa de pruebas anual que garantice la operatividad y mantenibilidad de la infraestructura. Se recomienda al menos una vez al año.

1.3.4.4 Administración de Cambios

Debe estar incluido dentro del Proceso de Cambios para garantizar que cualquier cambio a la infraestructura se vea reflejado en los acuerdos de contingencia previstos y/o notifique de cambios inadecuados que puedan alterar la composición de la solución de DRP.

1.3.5 Etapa 5: Invocación

Esta decisión la toma el equipo de administración de crisis compuesto por gerente o directores de negocio y los departamentos de IT. Utilizan la información que se reúne de las evaluaciones de daños para determinar en qué momento invocar al plan de DRP y notificar la formalización del mismo.

En este paso se ejecuta paso a paso los procedimientos determinados en las fases anteriores, se moviliza al personal técnico que se determinó para el apoyo del evento y se determina si en incidente hay posibilidad de que el personal de la operación se incorpore al proceso de validaciones, ya que el proceso desde diseño considero la nula posibilidad de apoyo del personal que está en sitio principal, finalmente contactar y alertar a todos los proveedores, de telecomunicaciones, servicios de soporte, aplicación, etc.

A través de la recuperación inicial es importante llevar el registro de las actividades que se estén cumpliendo de acuerdo al plan, y establecer personal de apoyo en las desviaciones. El objetivo durante la invocación para todo el personal activo es restituir la continuidad del servicio, posteriormente se revisaran las necesidades o requerimientos que pudieran requerirse según sea el caso.

Una vez completa la recuperación, el negocio debería poder operar desde el lugar de recuperación al nivel determinado y acordado en la estrategia de Continuidad del Negocio y DRP. El objetivo siguiente es llevar a los niveles normales y desocupar el lugar de recuperación cuando antes. Es importante que se manejen mensajes directivos que comuniquen al personal involucrado sea consciente de sus responsabilidades para garantizar una transición sin problemas.

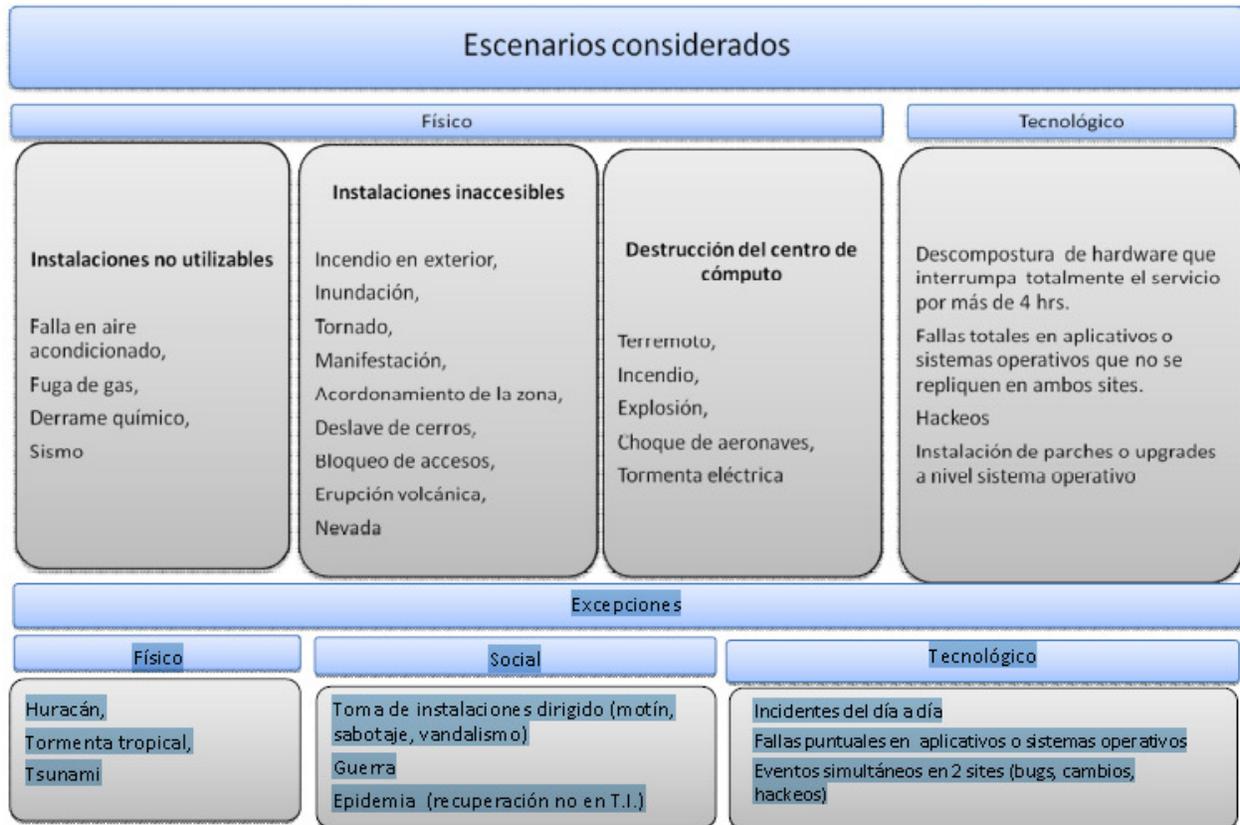


FIGURA 1: ESQUEMA DE TIPOS DE FALLAS Y ERRORES EN LOS SISTEMAS TECNOLÓGICOS

A partir de aquí me dedicaré a describir con detalle el proceso de implementación del DRP (Tercer etapa del BCM) de un grupo Financiero, el más avanzado de México y el más funcional por la cobertura que se logro con los proyectos de consolidación y virtualización que se apalancaron durante la construcción del proyecto.



2. INTRODUCCION AL PROYECTO

En el 2006 el Banco (Institución Financiera) contaba con una amplia infraestructura de equipos centrales instalados en un edificio corporativo de tecnología con más de 2200 metros cuadrados de piso falso. Aproximadamente los siguientes equipos en forma general:

- Mainframe con 3600 MIPS Modelo Hitachi Trinium.
- 2 Robots SILO Storage Tek con 1200 Slots y 8 Drives 9840 de 2GB y 100GB.
- 76 Equipos UNIX de tipo SUN, IBM y HP con discos SCSI internos y con arreglos independientes.
- 2 Equipos TANDEM NONSTOP con 6 CPUs y soporte a 2300 Cajeros y 12,000 POS.
- 362 Equipos Intel de 2 y 4 CPUs distribuidos en 26 RACK, correspondientes a varios modelos y marcas entre las que destacaban IBM, HP, SUN, Datageneral, Unisys, Compac, Lanix.
- 6 Unidades de disco Principal central con aproximadamente 20 Terabytes.

El esquema de DRP en ese momento se fundamentaba en un contrato con la empresa SUNGARD LTD que proporcionaba los servicios de DRP, los cuales consistían en un enlace de 64K con su centro de respaldo en la ciudad de Filadelfia en Estados Unidos y un máximo de 2 pruebas al año, en las que incluía un Mainframe con 2000 MIPS, 1 Robot con 64 Slot y 1 Drives 9840, un Tandem y un SUN E10K.

Las prueba de DRP se programaban solo una vez al año y el modelo se fundamentaba en tomar la base de respaldos del día definido para la prueba, tomar los cartuchos y trasladar a un equipo de soporte técnico de 8 personas a la ciudad de Filadelfia para, en un Lapso de 48 horas se tratará de levantar el ambiente central para una prueba con usuarios.

Las aplicaciones incluidas en esta prueba solo cubrían el sistema de sucursales y cajeros que representaba las dos aplicaciones más críticas y solo el 2% de todas las aplicaciones del Banco en ese momento.

Las pruebas aunque declaradas exitosas tenían serios problemas entre los que destacaban:

- Mucho tiempo incurrido en levantar los dos sistemas.
- La pérdida de operatividad e información que representaba levantar casi 3 días hábiles después de declarada la contingencia.
- Todos los sistemas operativos que requieren las sucursales no funcionaban.
- Enlace sumamente lento para una sola sucursal de prueba.
- Los usuarios no estaban satisfechos con las pruebas.
- Observaciones de las entidades regulatorias en donde no se cubrían sistemas críticos como los de internet por mencionar uno.
- Problemas técnicos asociados a parametrización, configuración dado que solo se respaldaban los datos y no las configuraciones.
- Muchos módulos del sistema de sucursales no operaban derivado de relaciones de conectividad y aplicativa con otros sistemas.
- La participación de otras áreas de tecnología era compleja porque las fallas o errores eran muchos, el análisis para corrección era complejo y muchas veces estaba asociado a recursos que no estaban en los respaldos.
- No se podía generar una operativa de más de un día porque el Batch (Procesos nocturnos basados en lotes de procesamiento paralelo) esperaba recursos o insumos de muchos sistemas y al forzar un avance fallaban de inmediato en las validaciones de consistencia (procesos de conciliación por ejemplo).

Derivado de las carencias e incumplimiento normativo esquema de DRP con el que se contaba, el banco impulsa un proyecto que asigna al área de infraestructura y que en conjunto con las áreas de negocio busquen como gran objetivo crear un DRP propio que cumpla con los requerimientos de los usuarios críticos y se ajuste al presupuesto máximo programado y que no limite a otras áreas, es decir, no debe detenerse ningún proyecto o iniciativa de las áreas de negocio que este en curso. Finalmente se plantea que este proyecto también haga un diferencial competitivo respecto de la competencia y que se use en beneficio del negocio.

Se arranca el proceso de análisis mediante el proceso BIA (Business Impact Analysis) comentado ampliamente en el marco teórico de este documento. Para realizar este análisis se contrata a una empresa externa que sirve como moderador e integrador de la información, sin embargo la decisión corre a cargo del personal de TI de la institución.



Al arrancar el proceso de análisis se habilitó una presentación a las áreas de negocio para que conocieran las posibilidades que existían y como a la suma de complejidad se le sumaba el costo de inversiones en infraestructura, esto permitió que todos los involucrados tuvieran claro el panorama y no se sesgara la criticidad de un producto o servicio a la manipulación del personal entrevistado y se limitara el análisis a los costos reales de asumir pérdida de operación, esto evita que personal de áreas de negocio o de operaciones cree supuestas pérdidas cualitativas basadas en suposiciones que no existen y aunque tienen posibilidad de suceder realmente no son críticas para la operación del negocio aunque podrían serlo para su crecimiento ejemplo sistemas de áreas de mercadotecnia. La figura 2 explica la relación de costos con base a la necesidad de protección y recuperación de información en un tiempo determinado.

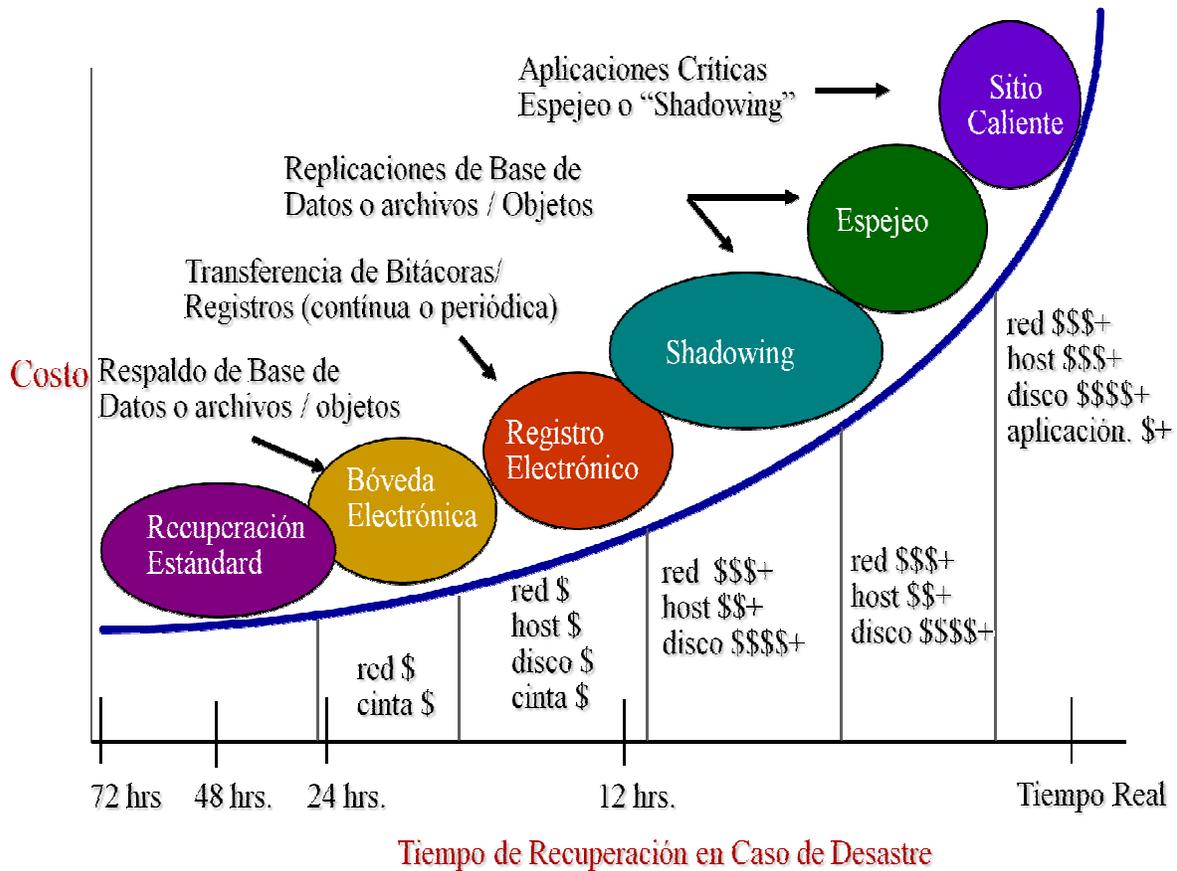


FIGURA 2: TIEMPO DE RECUPERACIÓN VS COSTO DE SOLUCIÓN

A menor tiempo de respuesta o de restauración de los sistemas en caso de falla, mayor es el costo de las tecnologías habilitadoras de una recuperación más rápida. Los mecanismos tradicionales de recuperación basados en respaldos en cintas son de lo más económico, por ejemplo un respaldo de 100 TB en cinta hoy equivale a 10 Cintas modelo T1000 o LTO (\$2,500 USD) pero su recuperación en un sistema de 40Mbps/Segundo tardaría 72 horas en recuperar los datos, en cambio un sistema de almacenamiento con espejeo para 100TB de discos de 80GB muy rápidos se elevaría a \$770,000 USD pero la recuperación local sería prácticamente instantánea.



CAPITULO II

1. ANALISIS

1.1 Introducción

El presente informe detalla el proceso de implementación de un modelo tecnológico para el DRP de una institución Bancaria.

Las regulaciones de los sectores financieros obligan a los bancos y entidades financieras de cualquier tipo tener un sistema de recuperación en caso de desastres que asegure la recuperación de la información de los clientes, el rápido restablecimiento del servicio o una parcialidad que permita al cliente obtener los servicios más críticos (ejemplo: retiros de fondos).

Como antecedente la institución ya contaba con un sistema de DRP con las siguientes características:

- Ubicación física en EU (Filadelfia).
- Número limitado de equipos cubiertos en la póliza de DRP (TANDEM y Mainframe).
- Numero de pruebas de DRP limitadas a 2 por año.
- Renta fija se use o no el sistema.
- Enlaces muy limitados solo para el soporte de terminales de áreas de operaciones (E1 2Mbps).
- Sistema basado en respaldos a cintas.
- Considera una recuperación con pérdida de datos de hasta 2 días y hasta 4 para levantar el sistema principal.
- La operación de la recuperación se fundamentaba en organización manual.

El nuevo requerimiento en principio solicita un cambio drástico en estos puntos incluyendo los siguientes objetivos:

- Minimizar la pérdida de datos a máximo una hora.
- Reducir los tiempos de recuperación a máximo 8 horas.
- Incluir todos los sistemas de BackOffice, Front-Office, y herramientas de apoyo crítico (Aplicaciones de apoyo).

El presente informe, detalla la forma en que se llevó el análisis técnico que permitiera construir una solución que cubriera los aspectos antes mencionados, minimizando riesgos, optimizando el gasto, salvaguardando la información.

1.2 Antecedentes

Derivado de una preocupación creciente en la industria financiera en cuanto a la continuidad de las operaciones ante cualquier eventualidad del tipo natural o premeditada, hay estadísticos en donde:

- ✚ Se reevalúa constantemente conceptos tales como la gestión del riesgo y la seguridad
 - Desastres Naturales
 - Terrorismo
- ✚ Desastres naturales en México y su posibilidad de ocurrencia
 - Terremotos
 - Septiembre 1985
 - Huracanes
 - Gilberto
 - Wilma

Durante los últimos años, las naciones y organizaciones se han visto orilladas a reevaluar el significado de conceptos tales como la gestión del riesgo y la seguridad debido a la creciente preocupación que en el mundo han generado hechos lamentables recientes tales como desastres naturales y actos terroristas entre otros, los que han desembocado en enormes mermas económicas, pérdida irrecuperable de información, y lo más importante, la pérdida de vidas humanas.

Un caso relativamente reciente y en la memoria de muchos de nosotros es del terremoto histórico del 19 de septiembre de 1985 que alcanzó 8.1° en la escala de Richter, generando muchas muertes y destrucción, con un saldo de 9 mil muertos y



un sinnúmero de desaparecidos; dicho terremoto afectó severamente la infraestructura de comunicaciones del centro del país y varios edificios entre los cuales se encontraban los que albergaban los centros de datos principales de algunos bancos. Otros casos como los huracanes Gilberto en 1988 y Wilma en octubre de 2005 demuestran que nuestro país es afectado con relativa frecuencia por fenómenos naturales de alto riesgo.

La creciente delincuencia, problemas políticos, la naturaleza misma generan riesgo que si no son controlados pueden generar problemas en centros de cómputo que no tengan procesos de recuperación en sitios alternos que permitan la continuidad de la operación de los sistemas.

Para minimizar estos riesgos es importante lograr mecanismos que aseguren la continuidad de la vida del negocio; la capacidad de recuperación de la información ante cualquier eventualidad en poco tiempo es mandatorio.

- ✚ Las instituciones financieras juegan un papel importante ya que tienen los registros del patrimonio económico de personas y empresas y esto los obliga a:
 - Tener una gran responsabilidad social y económica.
 - Alta dependencia de sus sistemas e infraestructura informática.
 - Tendencia a la centralización y consolidación para mejorar eficiencia operativa.
 - En la banca moderna cada vez menos operaciones dejan una huella en documentos físicos (fichas de depósito, cheques, etc.).

Ante un evento que ponga fuera de servicio un centro de datos ,el superar y salir adelante en poco tiempo de estos episodios es mandatorio, no sólo por recuperar la continuidad de la vida cotidiana, importante también es retomar las bases de estabilidad sobre las cuales se apoyan el desarrollo y el crecimiento del país. Este aspecto encierra una gran relevancia para las instituciones financieras debido a su enorme responsabilidad social y económica. Por la dependencia que éstas tienen de las tecnologías de información y por la clara tendencia a centralizar y consolidar aplicaciones y sistemas para mejorar sus índices de eficiencia, se hace muy crítico mitigar cualquier riesgo que amenace el funcionamiento continuo de sus servicios a través de la implantación de soluciones técnicas y procedimientos avanzados.

Las instituciones financieras como todas las Organizaciones, depende de recursos, personal y de actividades que son desarrolladas diariamente para permanecer sana, feliz y rentable.

La mayoría de las Organizaciones cuentan con recursos tangibles, propiedad intelectual, empleados, equipo de cómputo, enlaces de comunicación, instalaciones y servicios. Si alguno de estos componentes se daña o queda inaccesible por alguna razón, la empresa puede dejar de operar indefinidamente. Si más de uno de estos recursos son dañados, la permanencia de la empresa pueden estar en peligro. La disponibilidad de la Tecnología de Información (TI) es crucial para mantener la continuidad de las operaciones y la competitividad de la empresa.

Hoy la gran mayoría de las organizaciones requieren un alto nivel de disponibilidad de los Servicios de TI, y aún más, muchas de ellas requieren una disponibilidad continua las 24 horas del día, todos los días del año.

Una prolongada interrupción del servicio informático y/o de las operaciones de la empresa puede causar pérdidas muy significativas, no sólo financieras, si no también pérdida de la credibilidad con los clientes y/o usuarios y hasta la desaparición de la organización.

Por lo tanto, la capacidad para recuperarse, de una posible interrupción grave del servicio informático y o de las operaciones de la empresa, es un requerimiento de supervivencia de la organización.

1.2.1 Características de la información

En cualquier entorno informático es necesario estar protegido de las múltiples amenazas, garantizando fundamentalmente la preservación de tres características:

- ✚ Integridad: que se proteja la exactitud y totalidad de los datos y los métodos de procesamiento;
- ✚ Confidencialidad: que la información sea accesible sólo a las personas autorizadas.
- ✚ Disponibilidad: que los usuarios autorizados tengan acceso a la información y los recursos cuando los necesiten;

1.3 Análisis de impacto al negocio (BIA)

Para poder definir un plan estratégico que nos ayudara a entender claramente el impacto que genera al negocio un desastre de los mencionados es importante, dejar por escrito el análisis y fundamento de los requerimiento de recuperación que



cada aplicación o sistema requiere; se realizó un análisis de impacto al negocio denominado BIA que usa una metodología de entrevistas y cálculos que suponen lo que pasaría en caso de un evento grave y los tiempos máximos que el usuario o cliente requiere para que le sea restablecido el servicio. Este análisis es el fundamento de la creación de una infraestructura tecnológica que de soporte a estos requerimientos.

1.3.1 Análisis de Impacto al Negocio

1.3.1.1 Objetivos

Los objetivos principales del BIA son:

- Identificar los procesos de misión crítica del negocio y los requisitos para su recuperación.
- Identificar el impacto financiero como consecuencia de la pérdida de los sistemas de misión crítica, aplicaciones y procesos.
- Documentar los Tiempos Objetivo de Recuperación, así como los Puntos de Recuperación Objetivo y (RTO y RPO) para las aplicaciones críticas y procesos.
- Hacer las recomendaciones de como minimizar o mitigar el riesgo del impacto al negocio.
- Desarrollar una estrategia de recuperación por prioridad.
- Obtener el apoyo de las unidades de negocio dueñas de los procesos y funciones que están siendo soportadas.

1.3.1.2 Generales

- El estudio enfoca su análisis en las Unidades de Negocio, los Canales y las Aplicaciones más críticas del banco.
- El cálculo de las pérdidas potenciales de las unidades críticas de negocio, de los canales y de las aplicaciones fue complejo, debido al diseño de la organización (principalmente por la relación entre los canales y las unidades de negocio), así como también por la dificultad de conseguir la información financiera en la forma y detalle necesaria.
- El propósito de realizar el BIA en las Unidades de Negocio clave, Canales y Aplicaciones, es proporcionar una cierta perspectiva de las pérdidas financieras potenciales en el caso de una falla mayor. La información no es completamente adecuada para validar las estimaciones de pérdidas.

1.3.1.4 Análisis de Impacto al Negocio

Las consecuencias de la pérdida en caso de que de un desastre se muestran en el siguiente diagrama:

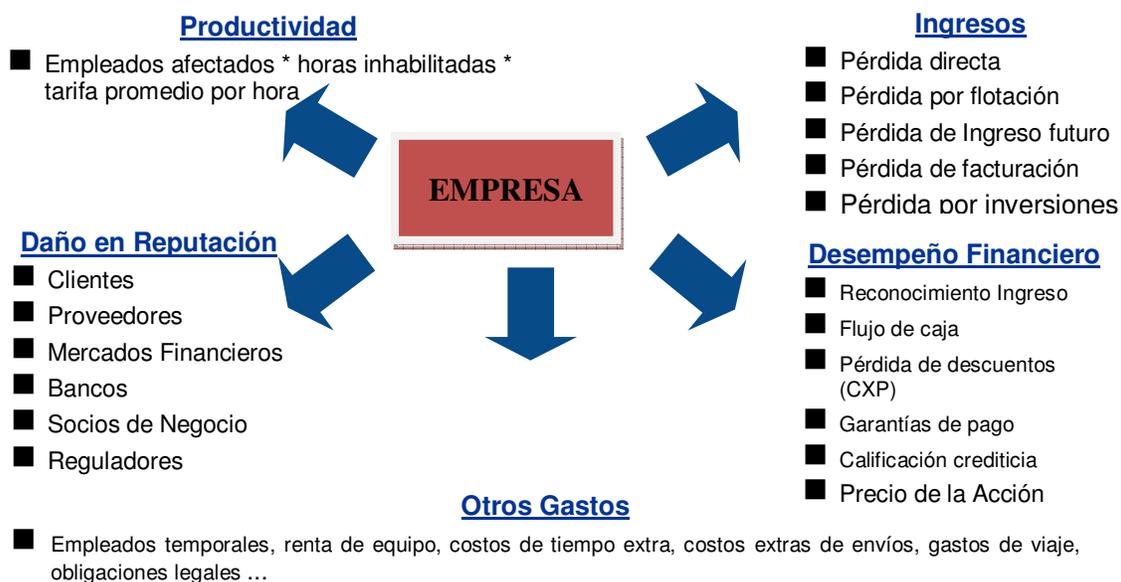


FIGURA 1.1: AFECTACIONES POSIBLES EN CASO DE UNA FALLA



Alrededor de la empresa hay una variedad amplia de factores que en caso de una falla simple impactan en algún proceso o servicio y puede generar daños económicos, pérdida de ganancia o clientes, un desastre o falla grave entonces representa el mayor daño dependiendo de tipo de negocio.

En el peor escenario en caso de un desastre mayor (como la inhabilitación total del Centro de Datos de Tlalpan, o incluso la pérdida de Edificios Corporativos importantes en Monterrey y el D.F.), las consecuencias de pérdida podían llegar a ser:

- Afectación de una cantidad muy importante de empleados (dependiendo de la criticidad del escenario).
- Pérdida de ingreso como consecuencia de la incapacidad de proveer / desempeñar los siguientes procesos que tienen alto impacto financiero: Tesorería, Operaciones Cambiarias y de Corretaje, Tarjetas de Crédito y Cajeros Automáticos, Depósitos (principalmente cuenta de cheques), etc.
- Incremento de gastos como resultado de costos de procesos manuales, costos por el control de las operaciones manuales y el costo de proveer soporte a los clientes.
- Pérdida de clientes actuales y potenciales.
- El impacto financiero estimado de la pérdida y/o falta de ingreso por cada día de interrupción, es de \$8.83 millones de pesos mexicanos.

1.3.2 Entorno Inicial (antes del proyecto)

El DRP se fundamentaba con base en respaldos de las aplicaciones más críticas, no incluía la parte de los sistemas operativos y buscaba cubrir solo la parte de operación, en resumen con el modelo que se tenía:

- La recuperación de la aplicación de Altamira (Aplicación Central del Banco) puede tomar siete días; la recuperación completa del Mainframe (Equipo de procesamiento Central principal) puede ser de varias semanas.
 - La estrategia actual del Mainframe cubre únicamente a Altamira.
 - 100% de las sucursales corren Altamira.
 - Unix y sistemas abiertos pueden tomar aproximadamente 20 días para recuperarse.
 - No existe estrategia o planes para estos sistemas.
 - Dependencia de los proveedores, ejemplo: arreglos de entregas de equipos.
 - La recuperación completa de la red puede requerir aproximadamente 20 días.
- Todos los canales, incluyendo Internet (privado, público y corporativo), puede tomar como mínimo de 10 a 20 días a recuperarse dependiendo de las tecnologías utilizadas actualmente.
- La aplicación del Centro de Llamadas (CallCenter de Institución Financiera) depende de los sistemas abiertos y puede tomar 20 días para recuperarse.
- Tesorería puede llegar a operar por dos días; sin embargo, el negocio no podrá sostener una interrupción de más de 2 días y no será capaz de seguir operando.
- Actualmente, bajo este modelo el Banco se expone a una pérdida potencial de información; específicamente, la Institución Financiera podría perder hasta 1.1 millones de transacciones diarias, que pueden no ser recuperables.
 - 60% de las transacciones actuales de los canales provienen de los Cajeros Automáticos, Terminales Punto de Venta y de Internet.
 - Las transacciones restantes pueden tener algún registro en papel; pero, puede tomar meses para recuperar la información, asumiendo que cuentan con los procedimientos apropiados.
- El plan actual no cubre muchos sistemas importantes que no se encuentran en la plataforma de Mainframe, ejemplo: Tesorería, o funciones operativas claves, ejemplo: ERP

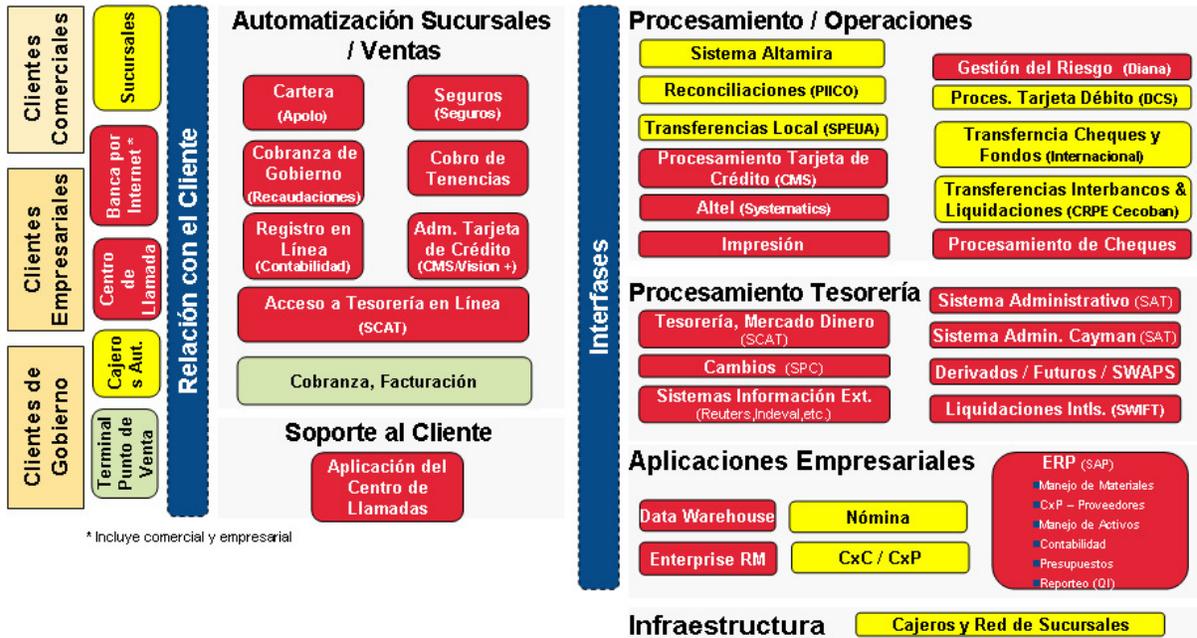


FIGURA 1.2: ESQUEMA LÓGICO DE LAS APLICACIONES DE LA INSTITUCIÓN FINANCIERA

La infraestructura es el pilar en donde las aplicaciones se sostienen, en el caso del Banco los diferentes equipos soportan todas las aplicaciones y servicios que se muestran en el diagrama. Aquí se dividen los sistemas de captación como las sucursales apoyados por las aplicaciones y el centro de atención a clientes y finalmente las actividades operativas y administrativas que soportan al negocio. Todos estas estructuras lógicas son áreas, personas y sistemas los cuales al final son ejecutadas en un equipo de computo en el centro de datos.

1.3.3 Proceso para el análisis de la situación actual.

Conceptos importantes para el análisis son RPO y RTO:

- ❖ **Recovery Point Objective (RPO)**
 - Punto en el tiempo hasta el cual será posible recuperar el registro de la información y las aplicaciones.
- ❖ **Recovery Time Objective (RTO)**
 - Intervalo de tiempo requerido para recuperar los sistemas e información.

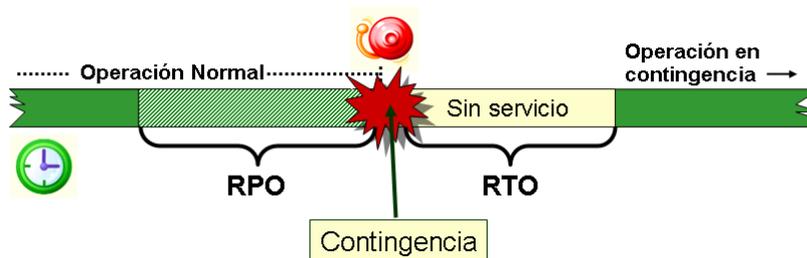


FIGURA 1.3.1: RPO VS RTO

Como primera fase se realiza una serie de entrevistas para investigar y analizar las aplicaciones más críticas y determinar los tiempos de recuperación requeridos, se denomina como RTO (Recovery Time Objective) que es el tiempo máximo deseado para recuperar un sistema en una falla.

- A través de las entrevistas a las Unidades de Negocio y de TI, se identificaron los siguientes Sistemas y Procesos como los más críticos y el RTO para cada uno.

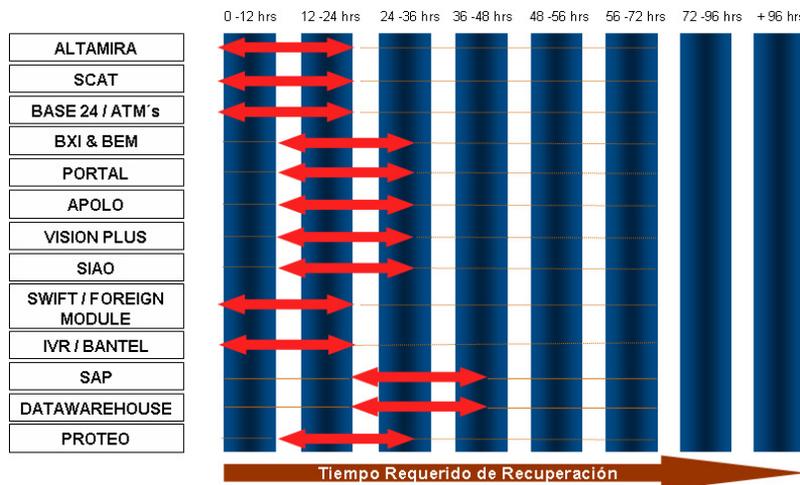


FIGURA 1.3: ANÁLISIS BIA TIEMPO REQUERIDO PARA RECUPERACIÓN DE SISTEMAS

La gráfica describe en el lado derecho las aplicaciones bancarias por su nombre y del lado izquierdo los tiempos que se consideran mínimos para recuperar el servicio. Por ejemplo Altamira es el sistema principal de cuentas sin el ningún sistema puede operar se indica que hasta en 24 horas debería de levantarse el servicio, otro caso es el sistema de Dataware House el cual podría estar fuera 24 horas y no generar impacto porque es un sistema para toma de decisiones y no interviene en las operaciones monetarias de los clientes.

Para poder clasificar todos los sistemas y determinar su criticidad se creó una estructura de categorías que nos permitirá ubicar a las aplicaciones según el tipo de proceso y el nivel de servicio.

- Los procesos más críticos de La Institución Financiera se clasificaron en cuatro categorías de acuerdo a las mejores prácticas :

	Procesos Clave de Negocio	Niveles de Servicio
Categoría 1	Funciones Críticas de Producción de Ingreso <ul style="list-style-type: none"> ■ Tesorería / Cambios / Internacional ■ Depósitos ■ Cajeros Automát. / TPV / Tarjeta Crédito ■ Centro de Llamadas (Banortel) ■ Transferencia de Fondos / Pagos 	Muy Alto impacto financiero de clientes 99.9% disponibilidad (< 45 min./mes.) RPO = Ninguno (cero segundos)
Categoría 2	Funciones Menos Críticas Prod. de Ingreso <ul style="list-style-type: none"> ■ Operaciones de Internet Externo ■ Operaciones de Cartera ■ Manejo del Riesgo 	Alto impacto financiero de clientes 99.5% disponibilidad (< 3.5 hrs./mes.) RPO = Mínimo (segundos a pocas horas)
Categoría 3	Funciones Empresariales Operativas <ul style="list-style-type: none"> ■ Sistema ERP ■ Reclamaciones ■ Procesos de Información 	Mediano impacto financiero de clientes 99.0% disponibilidad (< 5.5 hrs./mes.) RPO = Bajo (minutos a horas)
Categoría 4	Funciones Departamentales <ul style="list-style-type: none"> ■ Administración ■ Recursos Humanos ■ Finanzas ■ Internet Interno ■ Legal ■ Manejo de Filiales ■ E-mail 	Bajo impacto financiero de clientes 98.0% disponibilidad (< 13.5 hrs./mes.) RPO = Medio (horas a días)

FIGURA 1.4: ESQUEMA DE CATEGORÍAS DE IMPACTO

- Basados en las entrevistas realizadas a distintas áreas de negocio, en las cuales se manifestaron las distintas prioridades de recuperación de sus principales aplicaciones, se hizo una clasificación de la criticidad de las aplicaciones desde el punto de vista de los usuarios directos o indirectos de éstas.



Implementación de infraestructura de DRP

- Las distintas áreas usuarias manifestaron una gran variedad de niveles críticos. Sin embargo, con el fin de catalogar más fácilmente las criticidades, éstas se dividieron en tres niveles, y al mismo tiempo, para cada uno de estos niveles se realizó una clasificación en orden descendente de la prioridad de éstas aplicaciones (en función a los argumentos de los usuarios). La clasificación es numérica del 1 al 36 y los niveles de criticidad son:

Recovery Severity Level or Tier	Recovery Time (RTO)	Most Critical and Important Applications
Level 1 or Tier A (Highest Priority)	Less than 72 hours	
Level 2 or Tier B	72 to 96 hours	
Level 3 or Tier C	Beyond 96 hours	

FIGURA 1.5: ESQUEMA DE TIPOS NIVELES DE SEVERIDAD

- Se realizó el análisis con las aplicaciones más importantes que permitieran al final del mismo determinar qué porcentaje de la infraestructura representaban éstas aplicaciones (al final se observó que eran la mayoría).
- Finalmente en cada una de las aplicación se le solicitó cuál es la tolerancia máxima de pérdida de datos en el tiempo, es decir, cuánto tiempo de información podría perderse en caso de falla. A este concepto se le denomina RPO (Recovery Point Objective) que representa el tiempo o momento en que se considera que la información está perdida o ya no es recuperable de ninguna forma. Sistemas basados en cintas implica que un RPO puede ser digamos de 24 horas de información perdida suponiendo que el respaldo es de un día anterior, todas las operaciones o actualizaciones a los sistemas en las últimas 24 no tienen mecanismo alguno de recuperación.

El resultado de varias semanas de entrevistas y reuniones en donde por aplicación o sistema se realizaron cuestionarios diversos a usuarios para determinar la criticidad y tiempos de recuperación que solicitan y los impactos que cualitativamente podían tener en caso de fallas, se resumen en los siguientes cuadros.

El cuadro muestra el área que utiliza cierta aplicación, describe los tiempos que solicita el usuario para recuperar, la posibilidad de pérdida de información y los tiempos que una empresa consultora maneja como estándar mundial en situaciones de falla total y finalmente la plataforma donde corre el sistema.

Para los sistemas de sucursales el resultado es que los usuarios en lo general solicitan o manifiestan que en máximo 72 horas cualquiera de estos sistemas debe ser restablecido y no aceptan la pérdida de datos ya que implica daño al patrimonio de los clientes.

CHANNEL OR BUSINESS AREA	APPLICATIONS	DEFINITION	BUSINESS REQUIREMENTS		GARTNER ASSESSMENT OF RECOVERY CAPABILITY		COMMENT	PLATTFORM	PRIORITY RECOMMENDATION	RANK
			RTO	RPO	RTO	RPO				
DEPOSITS	Altamira	Deposits	Less than 72 hrs	0 or minimal loss of data	7+ days	1 day	Covered by Sungard at less than 100%	MAINFRAME	Level 1	1
BRANCHES	NTF	New Financial Terminal (Nuevo Terminal Financiero)	Less than 72 hrs	N/A - No data stored locally	7days +	None	Mainframe and network dependency	NT	Level 1	1
BRANCHES	Proteo	Systems of Branches Integrated Branch Network (Sistema de Sucursales Red Integrada)	Less than 72 hrs	N/A - No data stored locally	7days +	None	Mainframe and network dependency	NT	Level 1	1
BRANCHES	CT	Systems of Branches Old Branch Network (Sistema de Sucursales Red Anterior)	Less than 72 hrs	N/A - No data stored locally	7days +	None	Mainframe and network dependency	NT	Level 1	1
TREASURY	SCAT	Money Market Operations (Sistema de Captación de Mesa de Dinero)	Less than 72 hrs	TAPE BACK UP AND MAXIMUN LOST 1 DAY. NEED TO RECOVER BOTH ALTAMIRA AND DATABASE	20+ days	1 day loss of data	RUNS IN UNIX and ORACLE (THE FINAL RECORD IN ON THE MAINFRAME IN ALTAMIRA)		Level 1	2
TREASURY	Sociedades de Inversión	Mutual Funds (Productos de Soc. de Inversión de Renta Fija)	Less than 72 hrs		20+ days	1 day loss of data		UNIX (PART OF SCAT)	Level 1	2
TREASURY	Stock Market (Mercado de Capitales)	(Los 3 Corresponden a Tesorería, el SCAT a ambos)	Less than 72 hrs		20+ days	1 day loss of data		UNIX (PART OF SCAT)	Level 1	2

FIGURA 1.6: TABLA RESUMEN DE ANÁLISIS BIA DE 3 ÁREAS CRÍTICAS DE OPERACIÓN

Las siguientes figuras muestran en forma de resumen el resultado de las mismas entrevistas y análisis en las áreas más importantes. El estudio original cubrió todas las áreas por requerimiento del comité al que se reportaban los resultados en

Elaborado por:
Salvador Sierra Hernández

Revisado por:
M.I. Jorge Valeriano Assem



Implementación de infraestructura de DRP

donde participaban todos los directores generales de la institución. Aquí solo muestro las de los sistemas más críticos y se excluyen todas las aplicaciones departamentales dejando las centrales como ejemplo de este documento.

Resultados de los Sistemas de Cajeros Automáticos y POS:

CHANNEL OR BUSINESS AREA	APPLICATIONS	DEFINITION	BUSINESS REQUIREMENTS		GARTNER ASSESSMENT OF RECOVERY CAPABILITY		COMMENT	PLATTFORM	PRIORITY RECOMMENDATION	RANK
			RTO	RPO	RTO	RPO				
ATM and POS	ATM's	CMS: Management Debit Card (CMS:Administración de tarjeta de debito)	Less than 72 hrs	No loss of data accepted	50% of ATM machines can be recovered in 48 hours - ATMs not connected via F/R will take 10+days	Minimal Impact	Network, Tandem and MF dependency	EACH ATM MACHINE	Level 1	3
ATM and POS	Base 24		Less than 72 hrs	Base 24 interface with CMS and MF -IF MF is down, Base 24 will conduct authorization	Base 24 can be recovered in less than 72 hours	Minimal impact		TANDEM	Level 1	3
ATM and POS	Applications for POS		Less than 72 hrs		Same as above			TANDEM (PART OF BASE 24)	Level 1	3
ATM and POS	CMS		Less than 72 hrs		10+ days Note: internet POS Sales may take longer to recover depending on MQ recovery	1 day of data	No recovery at Sungard	BASED IN SAME PARTITION AS ALTAMIRA (RUNS IN VSAM FILE)	Level 1	3

FIGURA 1.7: TABLA RESUMEN DE ANÁLISIS BIA DEL SISTEMA DE CAJEROS

Resultados de Sistemas de Operaciones Internacionales y CallCenter:

CHANNEL OR BUSINESS AREA	APPLICATIONS	DEFINITION	BUSINESS REQUIREMENTS		GARTNER ASSESSMENT OF RECOVERY CAPABILITY		COMMENT	PLATTFORM	PRIORITY RECOMMENDATION	RANK
			RTO	RPO	RTO	RPO				
INTERNATIONAL	Módulo Extranjero	Operations in USD (Operaciones en Dolares)	Less than 72 hrs		7+ days	1 day	Covered by Sungard at less than 100%	ALTAMIRA (MAINFRAME)	Level 1	4
INTERNATIONAL	SWIFT		Less than 72 hrs		20+ days	Potentially can lose 1 week of data	High Availability Cluster	UNIX	Level 1	4
INTERNATIONAL	SCC		Less than 72 hrs		1- days +	1 day	Not covered by Sungard	ALTELL APPLICATION (MAINFRAME)	Level 1	4
INTERNATIONAL	Bank Trade		Less than 72 hrs		20+ days	1 day	No plans for DR	WINDOWS	Level 1	4
TELECOM and CALL CENTER	IVR		Less than 72 hrs		7 days +	Minimal	Call center has downstream connection to Altamira	PBX / WINDOWS	Level 1	5
TELECOM and CALL CENTER	Bantel		Less than 72 hrs		7 days +	Minimal	Call centers are fully redundant	PBX	Level 1	5
TELECOM and CALL CENTER	MemoFile		Less than 72 hrs					??? CLAIMS ???	Level 1	5

FIGURA 1.8: TABLA RESUMEN ANÁLISIS BIA BANCA INTERNACIONAL Y CALLCENTER

Resultados de los Sistemas de Internet y administración de tarjetas:

CHANNEL OR BUSINESS AREA	APPLICATIONS	DEFINITION	BUSINESS REQUIREMENTS		GARTNER ASSESSMENT OF RECOVERY CAPABILITY		COMMENT	PLATTFORM	PRIORITY RECOMMENDATION	RANK
			RTO	RPO	RTO	RPO				
INTERNET	BXI	Internet Banking (Banco por Internet)	Less than 72 hrs	No data stored	20+ days	Complete loss of data	Access depend on Portal, Depend on MQ	WIN / UNIX	Level 1	6
INTERNET	BEM	Corporate Internet Banking (Banco en su Empresa)	Less than 72 hrs	No data stored in front-end application server	20+ days	None	Consider moving to E:Risk - Access depend on portal	WIN / UNIX	Level 1	6
INTERNET	Portal	Access to Internet Portal (Acceso a Banorte en Internet)	Less than 72 hrs	Store reports from internet and back up to tapes all transactions stored in Oracle	20+ days	Complete loss of data		UNIX	Level 1	6
CREDIT CARD	Apolo	Cartera	Less than 72 hrs		20+ days	Backup to DAS storage in Talpan - Significant loss of data possible	Depend on Altel and Apolo - No plans for recovery - also depends on MQ	NT (MAINFRAME IN THE SAME PARTITION AS ALTELL (MEMOFILE USES APCLO) USED BY BRANCHES, RECOVERY BANKING, ETC)	Level 1	7
CREDIT CARD	Visión Plus	Credit Card Processor (Procesador de TDC)	Less than 72 hrs		20+ days +	1 day	Depend on MQ and thus UNIX	MAINFRAME (THIS SYSTEM SUBSTITUTE TOTAL SYSTEMS A YEAR AGO)	Level 1	7
CREDIT CARD	SIAO	CLAIMS System (Sistema de Aclaraciones)	Less than 72 hrs		10 days +	Major loss of data	Tape not moved off-site	NT (Located in the same server of Corporate intranet server)	Level 1	7

FIGURA 1.9: TABLA RESUMEN ANÁLISIS BIA SISTEMAS DE INTERNET Y ADMINISTRACIÓN TARJETAS

Elaborado por:
Salvador Sierra Hernández

Revisado por:
M.I. Jorge Valeriano Assem



Implementación de infraestructura de DRP

Resultado de los Sistemas de Información (DataWareHouse) y ERP (Contabilidad, SAP):

CHANNEL OR BUSINESS AREA	APPLICATIONS	DEFINITION	BUSINESS REQUIREMENTS		GARTNER ASSESSMENT OF RECOVERY CAPABILITY		COMMENT	PLATTFORM	PRIORITY RECOMMENDATION	RANK
			RTO	RPO	RTO	RPO				
INFORMATION SERVICES	SAP	Contabilidad SAP	Less than 72 hrs		20+ days	Potentially can lose 1 week of data		UNIX	Level 1	8
INFORMATION SERVICES	SAP	Presupuesto SAP	Less than 72 hrs		20+ days	Potentially can lose 1 week of data		UNIX	Level 1	8
INFORMATION SERVICES	SAP	Control de Activos SAP	Less than 72 hrs		20+ days	Potentially can lose 1 week of data		UNIX	Level 1	8
INFORMATION SERVICES	SAP	Pago a Proveedores SAP	Less than 72 hrs		20+ days	Potentially can lose 1 week of data		UNIX	Level 1	8
INFORMATION SERVICES	SAP	SAC	Less than 72 hrs		20+ days	Potentially can lose 1 week of data		UNIX	Level 1	8
INFORMATION SERVICES	SAP	CCS	Less than 72 hrs		20+ days	Potentially can lose 1 week of data		UNIX	Level 1	8
INFORMATION SERVICES	SAP	PIICO	Less than 72 hrs		20+ days	Potentially can lose 1 week of data		UNIX	Level 1	8
INFORMATION SERVICES	Datawarehouse	DataWareHouse	Less than 72 hrs		20+ days	Potentially can lose 1 week of data		UNIX	Level 1	9

FIGURA 1.10: TABLA RESUMEN ANÁLISIS BIA SISTEMA DE INFORMACIÓN Y TOMA DECISIONES

Resultado de los Sistemas de Administración de Riesgo y Cartera:

CHANNEL OR BUSINESS AREA	APPLICATIONS	DEFINITION	BUSINESS REQUIREMENTS		GARTNER ASSESSMENT OF RECOVERY CAPABILITY		COMMENT	PLATTFORM	PRIORITY RECOMMENDATION	RANK
			RTO	RPO	RTO	RPO				
RISK	Riesgos de Mercado y de Crédito (servicios de información) - Algorithmics		Less than 72 hrs	PROPIETARY DATABASE	20+ days	Potentially can lose 1 week of data	4 CPU, Proprietary database	UNIX (COMPLEMENTARY OF SCAT SYSTEM)	Level 1	10
RISK	Calificación Internal de Riesgos (CIR)		Less than 72 hrs	SAME MACHINE AS ALGORITHMICS	20+ days	Potentially can lose 1 week of data		UNIX (COMPLEMENTARY OF SCAT SYSTEM)	Level 1	10
RISK	Credit Scoring - Diana		Less than 72 hrs		10+ days	minimal loss of data	6 days of email data - tapes not moved off-site	WINDOWS EXCHANGE	Level 1	10
INSTITUTIONAL SERVICES	Correo Electrónico		Less than 72 hrs	LOCAL BACK-UP	48 hours			WINDOWS EXCHANGE	Level 1	11
FILIALES (FILIALES)	Cyber	Gestion y Cobranza de Cartera adquirida para su recuperacion	Less than 72 hrs		20+ days	Potentially can lose 1 week of data		UNIX	Level 1	12
INSTITUTIONAL SERVICES	Valija de sucursales		Less than 72 hrs		10 days +	Major loss of data - SQL server tapes not moved off-site		WINDOWS (RUNS IN CORPORATE INTRANET)	Level 1	13
DEPOSITS	Atel	Deposits	Less than 72 hrs	0 or minimal loss of data	10 days +	1 day	Atel not covered under Sungard but will be retired soon	MAINFRAME	Level 0	To be retired

FIGURA 1.11: TABLA RESUMEN DE ANÁLISIS BIA SISTEMAS DE RIESGO Y CARTERA

Resultado de los sistemas de Riesgos, Internet nivel 2(Módulos menos críticos):

CHANNEL OR BUSINESS AREA	APPLICATIONS	DEFINITION	BUSINESS REQUIREMENTS		GARTNER ASSESSMENT OF RECOVERY CAPABILITY		COMMENT	PLATTFORM	PRIORITY RECOMMENDATION	RANK
			RTO	RPO	RTO	RPO				
CREDIT CARD	Guardavalores	Envío y custodia de Contratos y pagarés	96 hrs		10 days +	Major loss of data	Tape not moved off-site	NT (Located in the same server of Corporate intranet server) - Branches Intranet	Level 2	14
RISK	Criterios de Aceptación de Riesgos (CAR)		96 hrs	SAME MACHINE AS ALGORITHMICS	20+ days	Potentially can lose 1 week of data		UNIX (COMPLEMENTARY OF SCAT SYSTEM)	Level 2	15
RISK	Mercados Objetivos (MO)		96 hrs	SAME MACHINE AS ALGORITHMICS	20+ days	Potentially can lose 1 week of data		UNIX (COMPLEMENTARY OF SCAT SYSTEM)	Level 2	15
INTERNET	BNET Personal	Bancreer Personal	96 hrs	No data stored in front-end application servers	20+ days	None	BNET will be retired by December 2004 - Access depend on portal	UNIX	Level 2	To be retired
INTERNET	BNET Empresarial	Bancreer Empresarial (Corporate)	96 hrs	No data stored	20+ days	None	BNET will be retired by December 2004 - access depend on Portal	UNIX	Level 2	To be retired

FIGURA 1.12: CONT. RESUMEN BIA SISTEMAS DE RIESGOS, CRÉDITO E INTERNET CRITICIDAD MEDIA



Como resumen de las tablas anteriores simplemente se desprende que todas las áreas consideran que los sistemas no pueden estar más de 72 horas fuera de servicio y consideran altamente riesgoso la pérdida de información. Estos resultados impactarían mucho el diseño de la solución que deberá de cubrir estos requerimientos.

El último paso fue relacionar cada una de las aplicaciones con los canales de entrega para analizar dependencias y en su caso revisar cuales aplicaciones críticas éstas relacionadas entre sí y/o tienen dependencias.

Todos los sistemas están íntimamente relacionados entre sí, el análisis siguiente pretendía determinar que sistemas eran los mínimos a poder restablecer la mayoría de los servicios buscando que la mayor parte de la funcionalidad sea cubierta y tratando de generar un esquema en que la recuperación implique un número menor de infraestructura y dejando fuera aquellos sistemas que no estén ligados.

Aplicaciones Canales de Entrega

			APLICACIONES	Canales					Otro	Tesorería	PRODUCTOS DE CREDITO				
				Internet	Sucursales	Terminal Pto. Venta	Cajero Aut.	Banortel	Admin	Tesorería	TARJETAS DE CREDITO	CREDITOS HIPOTECARIOS	CREDITOS DE AUTO	CREDIOMINA	CREDITIVO
CANALES	Banca por Internet	Internet	BXI	X							X	X	X	X	X
		Consumidor	BNET Personal	X							X	X	X	X	X
		Internet	BEM	X							X	X	X	X	X
		Corporativo	BNET Empresarial	X							X	X	X	X	X
		Payworks	Payworks	X							X	X	X	X	X
		Portal	Portal	X							X	X	X	X	X
	Sucursales (Branches)	Aplicativo de Sucursales	Proteo	Proteo		X					X	X	X	X	X
			CT	CT		X					X	X	X	X	X
			NTF	NTF		X						X	X	X	X
			Módulos Aduanales	Módulos Aduanales		X				X					
	Medios de Pago	ATM	ATM's	ATM's				X			X				
			Base 24	Base 24				X			X				
		POS	Aplicaciones para TPV's	Aplicaciones para TPV's			X					X			
			CMS	CMS			X	X							
	Banortel	Banortel	IVR	IVR					X						
			Bantel	Bantel					X						
			MemoFile	MemoFile					X						
	DEPOSITOS (CAPTACION)	Operaciones Pasivas	Captación y Servicios	Aitell	X	X	?	X			X	X	X	X	X
			Altamira	Altamira	X	X	?	X			X	X	X	X	X

FIGURA 1.13: TABLA ANÁLISIS RELACIONES SISTEMAS DE CANALES DE ENTREGA- SISTEMAS CENTRALES

En resumen la figura 13 muestra del lado izquierdo los canales o medios por los que el negocio gestiona clientes, como son las sucursales, sus sistemas de internet, a su lado la aplicación o el dispositivo final; por ejemplo hay 4 sistemas de internet, uno para clientes, otro para empresas, uno para comercios y el portal de servicios financieros, en otro están los cajeros y las terminales punto de venta (POS). Finalmente al centro de la tabla esta la relación de cada uno de ellos con los 3 servicios más críticos que el negocio considera como vitales para la supervivencia del Banco.

Cada una de las siguientes tablas mostrara el resumen muy consolidado de un análisis detallado por modulo de cada aplicación buscando determinar claramente cuando la criticidad determinada por el usuario es resultado de opiniones personal y no reales, es decir se analizó a detalle las relaciones de los procesos de cada módulo y se validó que efectivamente la operación representaba una afectación contable real a los sistemas centrales.

Con estos análisis se pretende determinar que aplicaciones no son realmente críticas y podría considerarse excluirse del modelo buscado para el DRP y sobre todo ir eliminando posibilidades de que el proyecto suba su costo de implementación.



Aplicaciones de Filiales

CREDITOS (COLOCACION)	APLICACIONES	Canales					Otro	Tesorería	PRODUCTOS DE CREDITO				
		Internet	Sucursales	Terminal Pto. Venta	Cajero Aut.	Banortel	Admin	Tesorería	TARJETAS DE CREDITO	CREDITOS HIPOTECARIOS	CREDITOS DE AUTO	CREDIOMINA	CREDITIVO
CREDITOS (COLOCACION)	Banca de Consumo	Innova		X					?	X	X	X	X
		Apolo	?	X			X		?	X	X	X	X
		Visión Plus	?	?	?	?			X				
		Cargas Masivas		X					X				
		Formalización		X					X				
	Operaciones Activas	SIAO	?	X			X		X				
		Guardavalores		X					X	X	X	X	X
		Cyber		X				X					
		SIBAD						X					
		SGVI						X					
FILIALES	Banco de Recuperación	Gastos Jurídico					X						
		Trámites					X						
		CACIB					X						
		Arrendadora					X						
		Factoraje					X						
	Almacenedora	Almacenedora					X						
		Avalúos		X			X						
		Fiduciario		?			X						
		Jurídico					X						

FIGURA 1.14: TABLA ANÁLISIS RELACIONES SISTEMAS DE FILIALES- SISTEMAS CENTRALES

Aplicaciones de Riesgo

INTERNACIONAL	APLICACIONES	Canales					Otro	Tesorería	PRODUCTOS DE CREDITO				
		Internet	Sucursales	Terminal Pto. Venta	Cajero Aut.	Banortel	Admin	Tesorería	TARJETAS DE CREDITO	CREDITOS HIPOTECARIOS	CREDITOS DE AUTO	CREDIOMINA	CREDITIVO
INTERNACIONAL	Banca Internacional	Módulo Extranjero	X	X			?	?					
		SCC	X	X				?					
		Bank Trade	X	X				?					
		SWIFT	X	X				?					
RIESGOS	Control de Riesgos	Algorithmics		X				X	?	?	?	?	?
		CIR		X				X					
		CAR		X				X					
		MO		X				X					
		Diana		X				X	X	X	X	X	X

FIGURA 1.15: TABLA ANÁLISIS RELACIONES SISTEMAS DE SISTEMAS DE RIESGO- SISTEMAS CENTRALES



Análisis de Impacto al Negocio Productos de Debito

APLICACIONES			PRODUCTOS DE DEBITO E INVERSION																
			Nómina Empresas	Imanort e I	Imanort e II	Suma	Sociedad NORTE AP	Enlace Tradicional (P. Física)	Enlace Tradicional (P. Moral)	Enlace Productiva (P. Moral)	Enlace Dinámica	Enlace Inteligente	Productiva Especial (Cetes)	Productiva Especial (Tiie)	Nómina Empleados Bte				
CANALES	Banca por Internet	Internet Consumidor	BXI	X	X	X	X	X	X	X	X	X	X	X	X	X	X		
			BNET Personal	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
		Internet Corporativo	BEM	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
		Payworks	BNET Empresarial	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
		Portal	Payworks	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
	Sucursales (Branches)	Aplicativo de Sucursales	Portal	Proteo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
				CT	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
				NTF	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
				Módulos Aduanales															
				ATM's	X	?	?	X		X	X	X	X	X	X	X	X	X	X
	Medios de Pago		ATM	Base 24	X	?	?	X		X	X	X	X	X	X	X	X	X	
			POS	Aplicaciones para TPV's	X			X		X	X	X	X	X	X	X	X	X	X
			CMS	CMS	X			X		X	X	X	X	X	X	X	X	X	X
	Banortel	Banortel	IVR																
			Bantel																
	DEPOSITOS (CAPTACION)	Operaciones Pasivas	Captación y Servicios	MemoFile															
			Altell	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
			Altamira	X	X	X	X	X	X	X	X	X	X	X	X	X	X		

FIGURA 1.16: TABLA ANÁLISIS RELACIONES SISTEMAS DE CANALES DE ENTREGA- SISTEMAS DE DEBITO E INVERSIÓN

1.3.4 CONCLUSIONES

Cada una de las tablas fue analizada por un comité en donde se expuso como la interacción de todos los sistemas es muy estrecha y dejar fuera componente solo posibilita la existencia de errores en caso de activar servicios tecnológicos que se interconectan mutuamente.

Se comento el caso de internet en donde la aplicación de clientes tocaba los siguientes sistemas; autenticación, Altamira, SAP, contabilidad, fiscal, riesgos, Clientes, medios de pago y CRM, al ligar estos sistemas se observa que crean nuevas ligas para servicios que en la fase uno fueron eliminados por no considerar críticos.

El resultado de la interpretación de estas tablas y un análisis profundo de las dependencias entre ellos son:

“Todos los sistemas están mutuamente relacionados en parte de sus componentes y esa dependencia obliga a que en un esquema de DRP sean incluidas para asegurar la funcionalidad del sistema, en caso contrario el proceso de recuperación no solo será un proceso de habilitación de servicios sino un enjambre de solución de problemas diversos que se presentarían al comenzar a operar.”

1.3.5 Procesos Críticos Identificados

Como resultado de la priorización antes realizada, se pueden identificar los siguientes como los procesos críticos de las Unidades de Negocio que tendrán mayor impacto en caso de un desastre mayor:

- Sucursales
 - Depósitos / Captación
 - Cajeros Automáticos
- Tesorería



- Tesorería
- Cambios
- Mesa de Dinero
- Mercado de Capitales
- Sociedades de Inversión
- Colocación
 - Tarjeta de Crédito
 - Créditos al Consumo
- Internet
- Transferencias y Liquidaciones Internacionales y Nacionales
- Otros de Soporte y/o Administrativos
 - Banortel
 - Contabilidad
 - DataWarehouse
 - Análisis de Riesgos

1.3.6 Generación de iniciativas (posibles Proyectos)

Basado en la priorización anterior y en los procesos críticos, se recomendó llevar a cabo las siguientes iniciativas a corto plazo:

Iniciativa 1

Confirmar la Estrategia de Recuperación en Caso de desastre y Continuidad de Negocios

Iniciativa: Confirmar la estrategia de BC y DR		Programa: Continuidad de Negocio		Prioridad: Alta										
Objetivos: <ul style="list-style-type: none"> ■ Proporcionar una estrategia formal para la continuidad del negocio en el caso de que se presente un evento identificado en los escenarios de desastre para procesos críticos del negocio: Inversiones, Transacciones (Mercado de Dinero, Fondos Mutuos y Valores), Administración del Portafolio 		Iniciativas de Negocio Relacionadas: <ul style="list-style-type: none"> ■ Estrategia de Almacenamiento 												
		Patrocinador del Negocio: Directores Ejecutivos												
		Dueño del Negocio: Gtes. de Unidades de Negocio												
		Miembros Críticos: Negocio y TI												
Alcance: <ul style="list-style-type: none"> ■ Procesos y aplicaciones críticas del negocio ■ Confirmar métricas de RTO, RPO y disponibilidad para aplicaciones críticas ■ Acuerdos en los escenarios a ser incluidos ■ Finalizar los elementos de Continuidad de Negocios (coordinador, instalaciones alternas, roles y responsabilidades, confirmación de TI con estrategia de DR) 		Unidades de Negocio: All Plan de Alto Nivel: <ul style="list-style-type: none"> ■ Documentar Roles y Responsabilidades para Continuidad de Negocios (BC) y recuperación en Caso de Desastre (DR) ■ Confirmar/Alinar la Estrategia de BC y DR para cada escenario clave ■ Documentar y Publicar la Estrategia 												
Beneficios y Costos: <table border="1" style="width: 100%;"> <tr> <td style="width: 50%;"><u>Proyecto Actual</u></td> <td style="width: 50%;"><u>Seguimiento</u></td> </tr> <tr> <td>Bon: Indirecto</td> <td>Beneficio: Plan de BCP/DR</td> </tr> <tr> <td>Costo: \$20,000 USD</td> <td>Costo:</td> </tr> <tr> <td>Tempo: 4 semanas</td> <td>Tiempo:</td> </tr> <tr> <td>Riesgo: Bajo</td> <td>Riesgo:</td> </tr> </table>		<u>Proyecto Actual</u>	<u>Seguimiento</u>	Bon: Indirecto	Beneficio: Plan de BCP/DR	Costo: \$20,000 USD	Costo:	Tempo: 4 semanas	Tiempo:	Riesgo: Bajo	Riesgo:			
<u>Proyecto Actual</u>	<u>Seguimiento</u>													
Bon: Indirecto	Beneficio: Plan de BCP/DR													
Costo: \$20,000 USD	Costo:													
Tempo: 4 semanas	Tiempo:													
Riesgo: Bajo	Riesgo:													
Métricas: RTO, RPO, Disponibilidad														
¿Origen? Personal Interno														
Factores de Riesgo/Éxito: <ul style="list-style-type: none"> ■ Ninguno 	Actividades Previas: <ul style="list-style-type: none"> ■ Ninguna 	Plan de Contingencia: <ul style="list-style-type: none"> ■ Ninguno 	Acciones de Seguimiento <ul style="list-style-type: none"> ■ Reunión Ejecutiva para finalizar la estrategia 											

FIGURA 1.17: ESQUEMA RESUMEN DE INICIATIVA PRINCIPAL-ESTRATEGIA DEL BR FINAL

La iniciativa uno representa el proyecto destinado al análisis de las posibles opciones, el cumplimiento del RTO y RPO así como los costos asociados a cada posible opción. El capítulo dos del presente documento detalla estas opciones y los costos. De esta iniciativa se desprendieron varios proyectos de infraestructura como la construcción de una fibra oscura entre los dos sitios, la renovación del equipo central y de comunicaciones y la consolidación del almacenamiento central.



Iniciativa 2

Desarrollar los Planes de Continuidad de Negocios

Iniciativa: Develop Business Continuity Plans		Programa: Business Continuity	Prioridad: Alta
Objetivos: <ul style="list-style-type: none"> Desarrollar un plan detallado para la recuperación del negocio en caso de que se presente un evento de desastre. Establecer los mecanismos para mantener los planes actualizados 		Iniciativas de Negocio Relacionadas: <ul style="list-style-type: none"> Estrategia de BC y DR, Plan de TI de DR 	
		Patrocinador del Negocio: Directores Ejecutivos	
		Dueño del Negocio: Gtes. de Unidades de Negocio	
		Miembros Críticos: Negocio y TI	
Alcance: <ul style="list-style-type: none"> Organización de Continuidad de Negocios y recuperación en Caso de Desastres –los roles y responsabilidades (equipo de dirección, equipo de respuesta en emergencia); Plan para cada fase (respuesta inicial, movilización, recuperación, validación, reinicio de operación, procesos temporales, regreso a casa); Pruebas de escritorio y afinación 		Unidades de Negocio: Todas Plan de Alto Nivel: <ul style="list-style-type: none"> Determinar roles y gobierno Establecer el presupuesto y las políticas para el mantenimiento recurrente del plan Contratar a una empresa para el desarrollo del Plan de Continuidad de Negocios Desarrollo del Plan Ejecutar prueba de escritorio para el Plan 	
Beneficios y Costos: <ul style="list-style-type: none"> Costo Interno -\$50,000 Costo Externo -\$125,000 a \$175,000 	Proyecto Actual Ben: Indirecto Costo: \$175 a 225 mil Tiempo: 3-4 meses Riesgo: Bajo Metricas: RTO, RPO, ¿Origen? Asistencia de un Proveedor	Seguimiento Beneficios: Costo: Tiempo: Riesgo:	
Factores de Riesgo/Éxito: <ul style="list-style-type: none"> Retraso en implantación de Planes de Recuperación en Caso de Desastre 	Actividades Previas: <ul style="list-style-type: none"> Iniciativa 1: Implantación de Recuperación en Caso de Desastre en Interlomas 	Plan de Contingencia: <ul style="list-style-type: none"> Continuar con la opción de Interlomas 	Acciones de Seguimiento <ul style="list-style-type: none"> Crear un Capítulo Completo

FIGURA 1.18: LAMINA RESUMEN DE ESTRATEGIA: DESARROLLO DEL PLAN

La iniciativa dos implico fundamentalmente implico el diseño de la solución, partiendo de estrategias y planes de organización de las áreas, revisión y actualización de los planes de contingencia de cada área y hacer pruebas de escritorio de las opciones planteados. El costo represento los servicios de consultoría de una empresa que coordino las reuniones, compromisos de las áreas para describir y escribir sus planes y acciones.

Iniciativa 3

Desarrollar los Planes y Pruebas Detallados de Recuperación en Caso de Desastre

Iniciativa: Desarrollo de planes y pruebas detallados de DR		Programa: Infraestructura	Prioridad: Alta
Objetivos: <ul style="list-style-type: none"> Desarrollo de planes detallados de Recuperación en Caso de desastre (DR) para la recuperación de la infraestructura de TI que soporta los requerimientos del negocio Confirmar que el plan pueda ser ejecutado 		Iniciativas de Negocio Relacionadas: <ul style="list-style-type: none"> Estrategia de Almacenamiento 	
		Patrocinador del Negocio: Directores Ejecutivos	
		Dueño del Negocio: Gtes. de Unidades de Negocio	
		Miembros Críticos: Negocio y TI	
Alcance: <ul style="list-style-type: none"> El Alcance incluye planes detallados para la recuperación de sistemas críticos; computadoras e infraestructura en los sitios de recuperación del negocio; pruebas integrales de Continuidad de Negocios y recuperación en Caso de Desastre; los 4 escenarios; la contratación con un proveedor de servicios de telecomunicaciones para recuperación del conmutador y ACD (equipo de voz y sistemas) 		Unidades de Negocio: All Plan de Alto Nivel: <ul style="list-style-type: none"> Determinar el enfoque del plan (Interno o Externo) Confirmar la estrategia de DR con TI y refinar el costo Establecer las herramientas y metodologías Contratar a un proveedor (si se necesita) Desarrollar el Plande DR Desarrollar los escenarios de prueba y los planes de prueba Conducir las pruebas integrales Actualizar / refinar los Planes 	
Beneficios y Costos: <ul style="list-style-type: none"> Costo Interno – estimado en 10 días por sistema =100 días – 50 a 100 mil Pruebas – 5 días x 5 Personas de TI, 10 Personas del Negocio – 20 mil Asistencia Externa 100 mil 	Current Project Ben: Indirecto Costo: \$175 a \$200 mil Tiempo: 4-6 meses Riesgo: Bajo Metricas: Costos Centro de Computo/DR ¿Origen? Asistencia de un Proveedor	Seguimiento Beneficios: Costo: Tiempo: Riesgo:	
Factores de Riesgo/Éxito: <ul style="list-style-type: none"> TI tiene que proveer servidores y servicios de telecomunicaciones adicionales 	Actividades Previas: <ul style="list-style-type: none"> Iniciativa 1 	Plan de Contingencia: <ul style="list-style-type: none"> Ninguno 	Actividades de Seguimiento: <ul style="list-style-type: none"> Crear un Capítulo Completo

FIGURA 1.19: LAMINA DE ESTRATEGIA Y CONSTRUCCIÓN DE LA SOLUCIÓN.

La iniciativa tres pretendía es establecimiento de los planes adecuándose al esquema de DRP con el que se contaba, sin embargo esta tuvo que ser replanteada ya no como iniciativa si no como el proyecto global del DRP el cual se replanteo totalmente con personal interno. No era posible excluir sistemas, no era posible perder datos, la recuperación no puede esperar más de 24 horas, estos aspectos llevaron al modelo que se explica a detalle a partir del capítulo 2.6



Éstas iniciativas fueron llevadas a cabo bajo el modelo de procesos de la institución financiera y son detallados en el diseño de solución (capítulo 2) de este reporte.

1.3.7 Análisis de Impactos Financieros

- A través de las entrevistas realizadas a las distintas áreas de negocio que pueden ser afectadas directa o indirectamente en un Evento de una Falla Mayor, se identificaron los siguientes procesos / productos que pueden llegar a tener el mayor impacto financiero para el Banco:
 - Tesorería.
 - Operaciones Cambiarias.
 - Productos de Crédito al Consumo.
 - Productos de Débito al Consumo (Depósitos e Inversiones).
 - Sueldos.

- Para llevar a cabo los cálculos de las pérdidas financieras potenciales en caso de un desastre, se tomaron en cuenta las siguientes consideraciones y cálculos:
 - Se identificó que el mayor impacto se tenía principalmente en el margen financiero y en las comisiones:
 - En el caso de Tesorería y Operaciones Cambiarias, el impacto más importante se debe a la pérdida del margen financiero por no poder llevar a cabo sus respectivas operaciones.
 - En los créditos al consumo, el mayor impacto recaería en las comisiones, tanto en las obtenidas en las operaciones diarias como sería el caso de Tarjetas de Crédito, así como en comisiones potenciales a no ganar por no poder colocar los distintos créditos al consumo del banco. Los créditos corporativos no tendrían un impacto financiero de inmediato como en el caso de los de consumo.
 - En el caso de chequeras e inversiones, el impacto financiero es tanto por el margen financiero que generan, así como por las comisiones que se obtienen por la operación y manejo de las mismas.
 - Cada una de las pérdidas potenciales antes mencionadas se calculó en función de los días laborables en los que podría sufrir el impacto. Por ejemplo, en el caso de Tesorería y Operaciones Cambiarias, el impacto sería únicamente en los días hábiles en que no pudieran operar (es decir, 250 días anuales), pero en el caso de tarjetas de crédito, la pérdida potencial de comisiones se tiene sobre todos los días (365 días anuales) en los que no se puedan operar las tarjetas de crédito.

Las siguientes tablas resumen todo el análisis por área de las pérdidas económicas cuantitativas que representaría la posibilidad de una falla mayor, se incluyen solo las nueve principales que representaban mayor impacto económico y de posición respecto de la competencia. El estudio para llegar a estas tablas requirió de 3 meses de trabajo paralelo con consultores fiscales y financieros de la empresa Compass Inc. dedicada al análisis económico de potenciales problemas tecnológicos en una empresa.



Pérdida Potencial en un Evento de Falla Mayor

TESORERIA

- Tesorería puede perder dinero debido la inhabilidad de cargar comisiones al cliente, y por no ganar los márgenes financieros de los montos operados por no tener operaciones normales
- La pérdida estimada diaria de las operaciones de Tesorería en el caso de un desastre es de \$1.996 millones
- Ésta es el área detectada con el mayor impacto financiero del para La institución Financiera en el caso de un desastre

TESORERIA		
Unidades	Total Anual de Transacciones	N/A
Unidades	Promedio Diario de Transacciones	N/A
000's Pesos	Margen Financiero en \$	\$318,816.15
000's Pesos	Márgen Financiero en \$ por Transacción	N/A
000's Pesos	Márgen Financiero en \$ por Transacción	N/A
%	Margen Financiero en %	N/A
000's Pesos	Margen Financiero para TODAS las Transacciones	\$1,275.26
000's Pesos	Comisiones Anuales	\$180,397.10
000's Pesos	Comisiones Diarias para TODAS las Transacciones	\$721.59
000's Pesos	Comisiones Diarias por Crédito	N/A
Unidades	Días Laborables	365
Unidades	Días Laborables	250
000's Pesos	Pérdida POTENCIAL Diaria Comisiones	\$721.59
000's Pesos	Pérdida POTENCIAL Diaria Márgen Financiero	\$1,275.26
000's Pesos	Pérdida POTENCIAL Diaria por Canal	\$1,996.85

FIGURA 1.21: RESUMEN ANÁLISIS PÉRDIDAS OPERATIVAS FALLA GRAVE DE UN SISTEMA

Análisis de Impacto al Negocio

Pérdida Potencial en un Evento de Falla Mayor (cont.)

OPERACIONES CAMBIARIAS

- Operaciones cambiarias pueden perder utilidad y margen financiero debido a la inhabilidad de realizar operaciones de compra y venta de divisas contra Pesos
- Para estimar la utilidad y el margen financiero potencial a perder, se tomaron los siguientes conceptos: Utilidad por la compra - venta de divisas, operaciones de Spot y Forward, valorización de divisas y margen financiero de operaciones cambiarias
- La pérdida diaria estimada para las operaciones cambiarias en el caso de un desastre es de \$1.352 millones de pesos

OPERACIONES CAMBIARIAS (CAMBIOS)		
Unidades	Total Anual de Transacciones	N/A
Unidades	Promedio Diario de Transacciones	N/A
000's Pesos	Utilidad Anual & Margen Financiero en \$	\$338,198.21
000's Pesos	Utilidad Anual & y Márgen Financiero en \$ por Transacc	N/A
000's Pesos	Utilidad Diaria & y Márgen Financiero en \$ por Transacc	N/A
%	Utilidad Promedio Anual & Margen Financiero en %	N/A
000's Pesos	Utilidad Diaria & Margen Financiero para TODAS las	\$1,352.79
000's Pesos	Comisiones Anuales	\$0.00
000's Pesos	Comisiones Diarias para TODAS las Transacciones	\$0.00
000's Pesos	Comisiones Diarias por Crédito	N/A
Unidades	Días Laborables	365
Unidades	Días Laborables	250
000's Pesos	Pérdida POTENCIAL Diaria Comisiones	\$0.00
000's Pesos	Pérdida POTENCIAL Diaria Márgen Financiero	\$1,352.79
000's Pesos	Pérdida POTENCIAL Diaria por Canal	\$1,352.79

FIGURA 1.22: RESUMEN ANÁLISIS PÉRDIDAS OPERATIVAS FALLA GRAVE SISTEMAS DE OPERACIONES CAMBIARIAS



Análisis de Impacto al Negocio Pérdida Potencial en un Evento de Falla Mayor (cont.)

CREDITO AL CONSUMO

- Debido a las operaciones diarias, las Tarjetas de Crédito son el producto de consumo que tendrá un mayor impacto financiero en el caso de un desastre. Se estima una pérdida potencial diaria de \$1M+.
- En Tarjetas de Crédito, como en el resto de los créditos al consumo, los mayores impactos

		TARJETAS DE CREDITO	CREDITOS HIPOTECARIOS	CREDITOS DE AUTO	CRE DINOMINA	CRE DIACTIVO
Unidades	Total Anual Nuevos Créditos	47,940	5,659	43,025	111,556	4,273
Unidades	Promedio Diario Nuevos Créditos	192	23	172	446	17
000's Pesos	Márgen Financiero Anual en \$	\$310,278.42	\$521,403.90	\$282,138.84	\$234,010.35	\$256,669.78
Unidades	Número de Créditos en Diciembre	264,869	76,636	109,195	134,864	12,857
000's Pesos	Márgen Financiero Anual en \$ por Crédito	\$1.17	\$6.80	\$2.58	\$1.74	\$19.96
000's Pesos	Márgen Financiero Diario \$ por Nuevo Crédito	\$0.00	\$0.02	\$0.01	\$0.01	\$0.07
%	Márgen Financiero Promedio Anual en %	13.99%	3.67%	6.17%	26.46%	8.87%
000's Pesos	Márgen Financiero Diario para Nuevos C	\$0.66	\$0.44	\$1.53	\$2.65	\$1.15
000's Pesos	Comisión Anual del Total de Créditos	\$323,899.80	\$72,046.87	\$61,368.33	\$27,187.21	\$53,972.19
000's Pesos	Comisión Promedio Anual por Crédito Nuevo	0.750	14.473	1.474	0.249	12.966
000's Pesos	Comisiones Diarias de TODOS los Crédito	\$1,031.22	\$327.62	\$253.59	\$110.99	\$221.61
Unidades	Días Laborables	365	365	365	365	365
Unidades	Días Laborables	250	250	250	250	250
000's Pesos	Pérdida POTENCIAL Diaria Comisiones	\$1,031.22	\$327.62	\$253.59	\$110.99	\$221.61
000's Pesos	Pérdida POTENCIAL Diaria Márgen Financiero	\$0.66	\$0.44	\$1.53	\$2.65	\$1.15
000's Pesos	Pérdida POTENCIAL diaria para Productos	\$1,031.88	\$328.06	\$255.11	\$113.64	\$222.76

FIGURA 1.23: RESUMEN ANÁLISIS PÉRDIDAS OPERATIVAS FALLA GRAVE SISTEMAS DE CRÉDITO AL CONSUMO

Análisis de Impacto al Negocio Pérdida Potencial en un Evento de Falla Mayor (cont.)

DEBITO AL CONSUMO E INVERSIONES

- El producto principal de cuenta de cheques de La institución Financiera será afectado considerablemente en caso de un desastre, debido la pérdida de nuevas cuentas potenciales que no podrían ser abiertas, así que el Banco no ganaría una cantidad estimada de \$1.159 millones de pesos de comisiones potenciales.

	Nómina Empresas	Imanorte I	Imanorte II	Suma	Sociedad NORTEAP	Enlace Tradicional (P. Física)	Enlace Tradicional (P. Moral)
	CHECKING ACCOUNT	INVESTMENT	INVESTMENT	SAVINGS / DEBIT	MUTUAL FUND	CHECKING ACCOUNT	CHECKING ACCOUNT
Estimado Total Anual Nuevas Cuentas Diciembre - Noviembre	833	9,960	1,908	108,576	3,468	37,536	17,916
Promedio Diario Nuevas Cuentas	3	40	8	434	14	150	72
Márgen Financiero Anual en \$	\$542,711.03	\$318,418.49	\$34,631.50	\$401,335.36	\$0.00	\$406,747.79	\$721,043.59
Número de Créditos en Diciembre	10,249	115,527	5,279	845,723	4,802	306,040	112,593
Márgen Financiero Anual en \$ por Cuenta	\$52.95	\$2.76	\$6.56	\$0.47	\$0.00	\$1.33	\$6.40
Márgen Financiero Diario \$ por Cuenta	\$0.1451	\$0.0076	\$0.0180	\$0.0013	\$0.0000	\$0.0036	\$0.0175
Márgen Financiero Promedio Anual en %	10.93%	2.70%	1.77%	5.85%	0.00%	6.70%	6.68%
Márgen Financiero Diario para TODAS las Cuentas en	\$1,486.88	\$872.38	\$94.88	\$1,099.55	\$0.00	\$1,114.38	\$1,975.46
Comisión Anual de TODAS las Cuentas	\$403,662.86	\$0.00	\$0.00	\$151,987.99	\$30,935.15	\$281,664.13	\$205,743.24
Comisión Promedio Anual por Cuenta	\$39.39	\$0.00	\$0.00	\$0.18	\$6.44	\$0.92	\$1.83
Comisiones Diarias de TODAS las Cuentas	\$1,158.57	\$0.00	\$0.00	\$416.41	\$84.75	\$771.68	\$563.68
Días Laborables	365	365	365	365	365	365	365
Días Laborables	250	250	250	250	250	250	250
Pérdida POTENCIAL Diaria Comisiones	\$1,158.57	\$0.00	\$0.00	\$416.41	\$84.75	\$771.68	\$563.68
Pérdida POTENCIAL Diaria Márgen Financiero	\$0.48	\$0.30	\$0.14	\$0.56	\$0.00	\$0.55	\$1.26
Pérdida POTENCIAL diaria para Cuentas	\$1,159.06	\$0.30	\$0.14	\$416.97	\$84.75	\$772.23	\$564.94

FIGURA 1.24: RESUMEN ANÁLISIS PÉRDIDAS OPERATIVAS FALLA GRAVE SISTEMAS DE DEBITO E INVERSIONES



Análisis de Impacto al Negocio Pérdida Potencial en un Evento de Falla Mayor (cont.)

DEBITO AL CONSUMO E INVERSIONES (cont.)

	Enlace Productiva (P. Moral)	Enlace Dinamica	Enlace Inteligente	Productiva Especiales (Cetes)	Productiva Especiales (Tite)	Nómina Empleados Etc	En Dólares (P. Física)
	CHECKING ACCOUNT	CHECKING ACCOUNT	CHECKING ACCOUNT	CHECKING ACCOUNT	CHECKING ACCOUNT	CHECKING ACCOUNT	CHECKING ACCOUNT
Units	2,448	10,248	1,236	96	-	2,292	1,452
Units	10	41	5	0	0	9	6
000's Peso:	\$353,855.63	\$239,470.78	\$110,258.29	\$31,940.56	\$414.00	\$5,304.04	\$3,732.25
Units	27,403	103,087	28,185	426	3	13,967	9,044
000's Pesos	\$12.91	\$2.32	\$3.91	\$74.98	\$138.00	\$0.38	\$0.41
000's Pesos	\$0.0354	\$0.0064	\$0.0107	\$0.2054	\$0.3781	\$0.0010	\$0.0011
%	5.27%	6.68%	3.28%	1.60%	0.63%	2.39%	0.44%
000's Peso:	\$969.47	\$656.08	\$302.08	\$87.51	\$1.13	\$14.53	\$10.23
000's Peso:	\$69,563.60	\$91,991.48	\$19,026.30	\$1,596.12	\$5.21	\$4,370.79	\$1,541.62
000's Pesos	\$2.54	\$0.89	\$0.68	\$3.75	\$1.74	\$0.31	\$0.17
000's Peso:	\$190.59	\$252.03	\$52.13	\$4.37	\$0.01	\$11.97	\$4.22
Units	365	365	365	365	365	365	365
Units	250	250	250	250	250	250	250
000's Pesos	\$190.59	\$252.03	\$52.13	\$4.37	\$0.01	\$11.97	\$4.22
000's Pesos	\$0.35	\$0.26	\$0.05	\$0.08	\$0.00	\$0.01	\$0.01
000's Pesos	\$190.93	\$252.29	\$52.18	\$4.45	\$0.01	\$11.98	\$4.23

FIGURA 1.25: RESUMEN ANÁLISIS PÉRDIDAS OPERATIVAS FALLA GRAVE SISTEMAS DE DEBITO E INVERSIONES

Análisis de Impacto al Negocio Pérdida Potencial en un Evento de Falla Mayor (cont.)

DEBITO AL CONSUMO E INVERSIONES (cont.)

	En Dólares (P. Moral)	Especial Dólares	Pag 7, 14 y 21 días	Pag 28 días	Pag 91,182 y 366 días	Inversión Creciente (Cedes)	Pag Cayman 6,13 y 29 días
	CHECKING ACCOUNT	CHECKING ACCOUNT	INVESTMENT	INVESTMENT	INVESTMENT	INVESTMENT	INVESTMENT
Estimado Total Anual Nuevas Cuentas Diciembre - Novie	1,164	660	12,180	10,896	3,660	-	1,008
Promedio Diario Nuevas Cuentas	5	3	49	44	15	0	4
Margen Financiero Anual en \$	\$8,281.10	\$8,154.15	\$23,021.29	\$413,396.14	\$5,653.58	\$11.64	\$3,080.22
Número de Créditos en Diciembre	10,213	15,067	21,904	289,214	5,631	6	4,538
Márgen Financiero Anual en \$ por Cuenta	\$0.81	\$0.54	\$1.05	\$1.43	\$1.00	\$1.94	\$0.68
Márgen Financiero Diario \$ por Cuenta	\$0.0022	\$0.0015	\$0.0029	\$0.0039	\$0.0028	\$0.0053	\$0.0019
Márgen Financiero Promedio Anual en %	0.31%	0.44%	4.26%	0.44%	3.28%	2.66%	0.45%
Márgen Financiero Diario para TODAS las Cuentas er	\$22.69	\$22.34	\$63.07	\$1,132.59	\$15.49	\$0.03	\$8.44
Comisión Anual de TODAS las Cuentas	\$6,189.38	\$0.01	\$0.01	\$0.00	\$0.00	\$0.00	\$0.00
Comisión Promedio Anual por Cuenta	\$0.61	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Comisiones Diarias de TODAS las Cuentas	\$16.96	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Días Laborables	365	365	365	365	365	365	365
Días Laborables	250	250	250	250	250	250	250
Pérdida POTENCIAL Diaria Comisiones	\$16.96	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Pérdida POTENCIAL Diaria Márgen Financiero	\$0.01	\$0.00	\$0.14	\$0.17	\$0.04	\$0.00	\$0.01
Pérdida POTENCIAL diaria para Cuentas	\$16.97	\$0.00	\$0.14	\$0.17	\$0.04	\$0.00	\$0.01

FIGURA 1.26: RESUMEN ANÁLISIS PÉRDIDAS OPERATIVAS FALLA GRAVE SISTEMAS DE DEBITO E INVERSIONES CONT.



Análisis de Impacto al Negocio Pérdida Potencial en un Evento de Falla Mayor (cont.)

DEBITO AL CONSUMO E INVERSIONES (cont.)

	Pag Cayman 59 días	Pag Cayman 89 días	Pag Cayman 135 y 180 días	Pag Cayman 225,269,315,3 59 y 450
	INVESTMENT	INVESTMENT	INVESTMENT	INVESTMENT
Estimado Total Anual Nuevas Cuentas Diciembre - Noviembre	228	-	-	708
Promedio Diario Nuevas Cuentas	1	0	0	3
Margen Financiero Anual en \$	\$4,196.27	\$496.39	\$2,709.31	-\$2,857.41
Número de Créditos en Diciembre	5,332	990	4,424	1,773
Margen Financiero Anual en \$ por Cuenta	\$0.79	\$0.50	\$0.61	-\$1.61
Margen Financiero Diario \$ por Cuenta	\$0.0022	\$0.0014	\$0.0017	-\$0.0044
Margen Financiero Promedio Anual en %	0.38%	0.29%	0.25%	-0.47%
Margen Financiero Diario para TODAS las Cuentas	\$11.50	\$1.36	\$7.42	-\$7.83
Comisión Anual de TODAS las Cuentas	\$0.00	\$0.00	\$0.00	\$0.00
Comisión Promedio Anual por Cuenta	\$0.00	\$0.00	\$0.00	\$0.00
Comisiones Diarias de TODAS las Cuentas	\$0.00	\$0.00	\$0.00	\$0.00
Días Laborables	365	365	365	365
Días Laborables	250	250	250	250
Pérdida POTENCIAL Diaria Comisiones	\$0.00	\$0.00	\$0.00	\$0.00
Pérdida POTENCIAL Diaria Margen Financiero	\$0.00	\$0.00	\$0.00	-\$0.01
Pérdida POTENCIAL diaria para Cuentas	\$0.00	\$0.00	\$0.00	-\$0.01

FIGURA 1.27: RESUMEN ANÁLISIS PÉRDIDAS OPERATIVAS FALLA GRAVE SISTEMAS DE DEBITO E INVERSIONES

Análisis de Impacto al Negocio Pérdida Potencial en un Evento de Falla Mayor (cont.)

SUELDOS

- En un caso de un desastre, muchos empleados del Banco no tendrán acceso a sus oficinas o a las herramientas necesarias (como aplicaciones) para trabajar. Por esto, la productividad de la mayoría de los empleados será baja y ésta tendrá un impacto financiero muy importante al Banco.

	CORPORATIVA	COMERCIAL	EMPRESARIAL	GOBIERNO	FOBAPROA	FILIALES	TESORERIA	OTROS FISCALES Y NO BANCARIOS
000's Pesos								
Gastos Anual por Personal	\$40,633.23	\$1,887,077.57	\$88,616.60	\$12,456.39	\$0.00	\$71,608.55	\$28,769.62	\$839,327.30
000's Pesos								
Gastos Diarios por Personal	\$111.32	\$5,170.08	\$242.79	\$34.13	\$0.00	\$196.19	\$78.82	\$2,299.53
Unidades								
Días Laborables	365	365	365	365	365	365	365	365
000's Pesos								
Pérdida POTENCIAL Diaria por Salarios y Beneficios Improductivos	\$111.32	\$5,170.08	\$242.79	\$34.13	\$0.00	\$196.19	\$78.82	\$2,299.53
	\$5,558.31							

FIGURA 1.28: RESUMEN ANÁLISIS PÉRDIDAS OPERATIVAS EN SUELDOS POR FALTA DE PRODUCTIVIDAD



Análisis de Impacto al Negocio Pérdida Potencial en un Evento de Falla Mayor (cont.)

CANALES

- En esta vista del análisis, se incluye el impacto financiero visto en el análisis del crédito al consumo y débito, así que NO se debe considerar como un impacto financiero separado, es únicamente otra vista.
- Esta vista por canal incluye todas las operaciones financieras hechas a través de Sucursales, Cajeros, TPV's, Internet y Callcenter la institución Financiera.
- El impacto financiero del canal de Sucursales no se calculó, debido a la complejidad de la información. El área financiera de La institución Financiera no tiene el desglose de la información para hacer un análisis formal.

		ATM	POS	INTERNET	BANORTEL (CALL CENTER)
Unidades	Total Anual de Transacciones	204,974,774	11,349,515	17,399,646	20,746,487
Unidades	Promedio Diario de Transacciones	561,575	31,095	47,670	56,840
000's Pesos	Margen Financiero en \$	\$19,258.92	\$40,924.86	\$8,334.98	\$0.00
000's Pesos	Margen Financiero en \$ por Transacc	\$0.0001	\$0.0036	\$0.0005	\$0.0000
000's Pesos	Margen Financiero en \$ por Transacc	\$0.0000	\$0.0000	\$0.0000	\$0.0000
%	Margen Financiero en %	6.58%	6.74%	6.63%	0.00%
000's Pesos	Margen Financiero para TODAS las	\$52.76	\$112.12	\$22.84	\$0.00
000's Pesos	Comisiones Anuales	\$495,690.30	\$75,516.97	\$47,434.65	\$62,395.68
000's Pesos	Comisiones Diarias para TODAS las	\$1,358.06	\$302.07	\$189.74	\$249.58
000's Pesos	Comisiones Diarias por Crédito	\$0.00	\$0.00	\$0.00	\$0.00
Unidades	Días Laborables	365	365	365	365
Unidades	Días Laborables	250	250	250	250
000's Pesos	Pérdida POTENCIAL Diaria Comisione:	\$1,358.06	\$302.07	\$189.74	\$249.58
000's Pesos	Pérdida POTENCIAL Diaria Margén Fin	\$52.76	\$112.12	\$22.84	\$0.00
000's Pesos	Pérdida POTENCIAL Diaria por Canal	\$1,410.82	\$414.19	\$212.57	\$249.58

FIGURA 1.29: RESUMEN ANÁLISIS PÉRDIDAS OPERATIVAS FALLA GRAVE SISTEMAS DE CANALES

Análisis de Impacto al Negocio Resumen de Pérdida Potencial Diaria (En Miles de Pesos Mexicanos)

Resumen de la pérdida potencial diaria si toda la infraestructura no estuviera disponible. Dependiendo del tipo de producto, el ingreso no puede perderse, sino retrasarse.

■ Productos de Crédito	■ Volumen (Cantidad)	Pérdida Potencial de Ingresos
Préstamos Automotriz	172	\$255
Préstamos Hipotecarios	23	\$328
Tarjetas de Crédito	192	\$1,032
Credinomina	446	\$114
Crediativo	17	\$223
Total		\$1,951

■ Productos de Débito	■ Volumen (Cantidad)	Pérdida Potencial de Ingresos
Nómina Empresas	3	\$1,159
SUMA	434	\$417
Enlace Tradicional (Personal)	150	\$772
Enlace Tradicional (Corporativo)	72	\$565
Enlace Dinámica	41	\$252
Otros	213	\$366
Total	913	\$3,532

■ Tesorería y Operaciones Cambiarias	■ Volumen (Cantidad)	Pérdida Potencial de Ingresos
Tesorería		\$1,997
Operaciones Cambiarias		\$1,352

\$8,832 ← Miles de Millones

■ Otros	■ Volumen (Cantidad)	Pérdida Potencial de Ingresos	■ Penalizaciones Estimadas
Sueldos		\$5,558	\$1,000

FIGURA 1.30: RESUMEN ANÁLISIS PÉRDIDAS POTENCIALES POR FALLA GRAVE EN LOS SISTEMAS



Impacto Potencial de un Desastre de 10 Días (En Pesos Mexicanos)

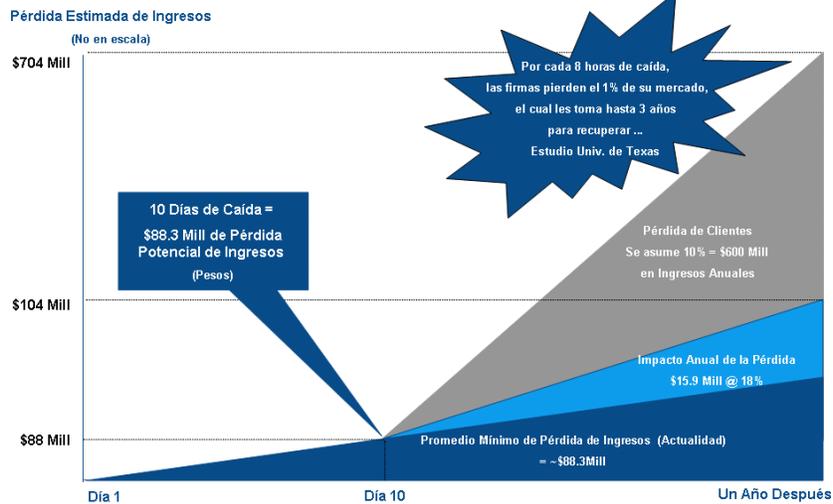


FIGURA 1.31: REPRESENTACIÓN ESQUEMÁTICA DE PÉRDIDAS PARA UN EMPRESA DEL SECTOR FINANCIERO

Gráfica obtenida de un reporte de IDC mediante encuestas a empresas afectadas en eventos graves a nivel mundial de 1992 a 2007.

1.3.8 Revisión de soluciones similares

¿Cómo se comporta la industria?

Gartner llevó a cabo una Encuesta a Empresas de Servicios Financieros en Relación al 11 de Sept.

- De 230 entrevistados, 15 declararon desastres relacionados al evento del 11 de Sept.:
 - 10 ocuparon sitios de recuperación
 - Las estancias se extendieron de 3 a 70 días
 - El promedio de estancia en el sitio de recuperación fue de 28 días

Muchos esperan corregir las debilidades en sus Planes de Continuidad de Negocio debido a Sept. 11 y el resto planea llevar a cabo una variedad de acciones.

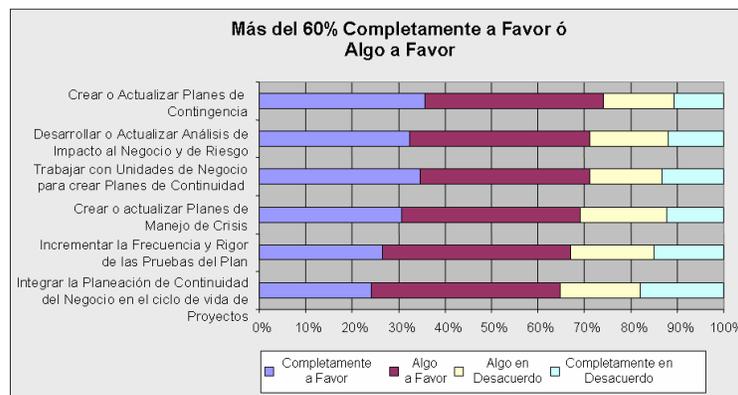


FIGURA 1.32: ESQUEMA DE LA ACEPTACIÓN DE LOS PLANES DE DRP

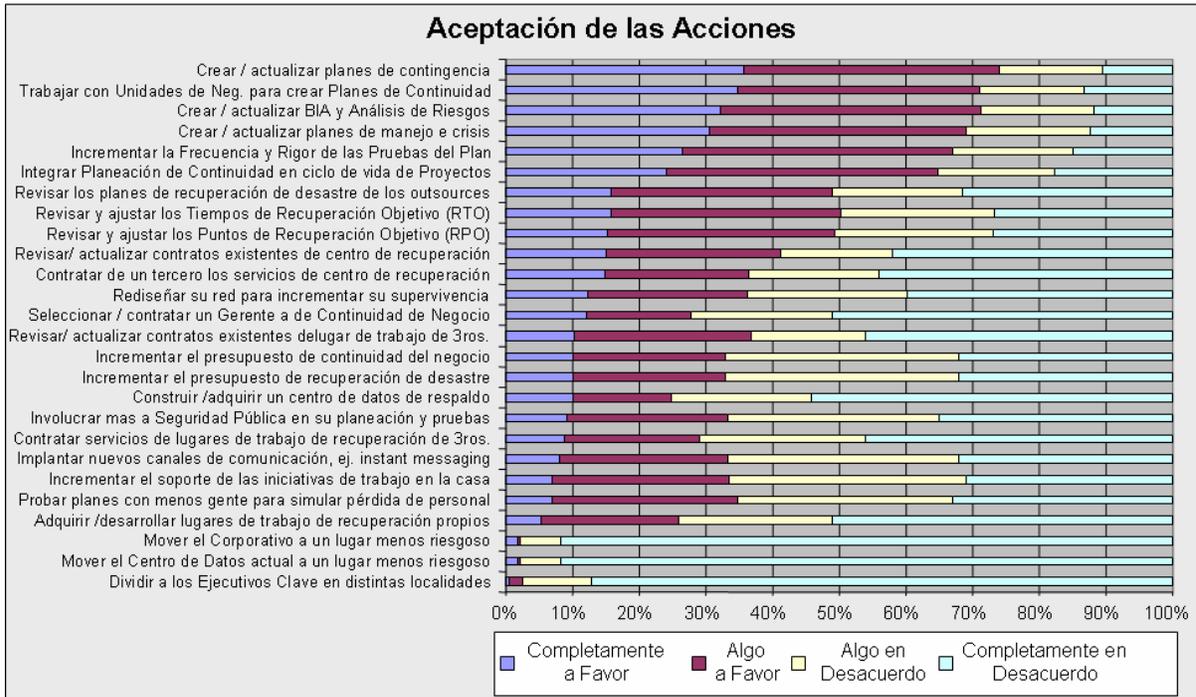


FIGURA 1.33: ESQUEMA LA ACEPTACIÓN DE LOS ESQUEMAS DE DRP

Antes de Sept. 11, los escenarios de Continuidad más cubiertos por los planes, eran para tratamientos diarios; mientras que los escenarios menos cubiertos fueron los más desastrosos de Sept. 11

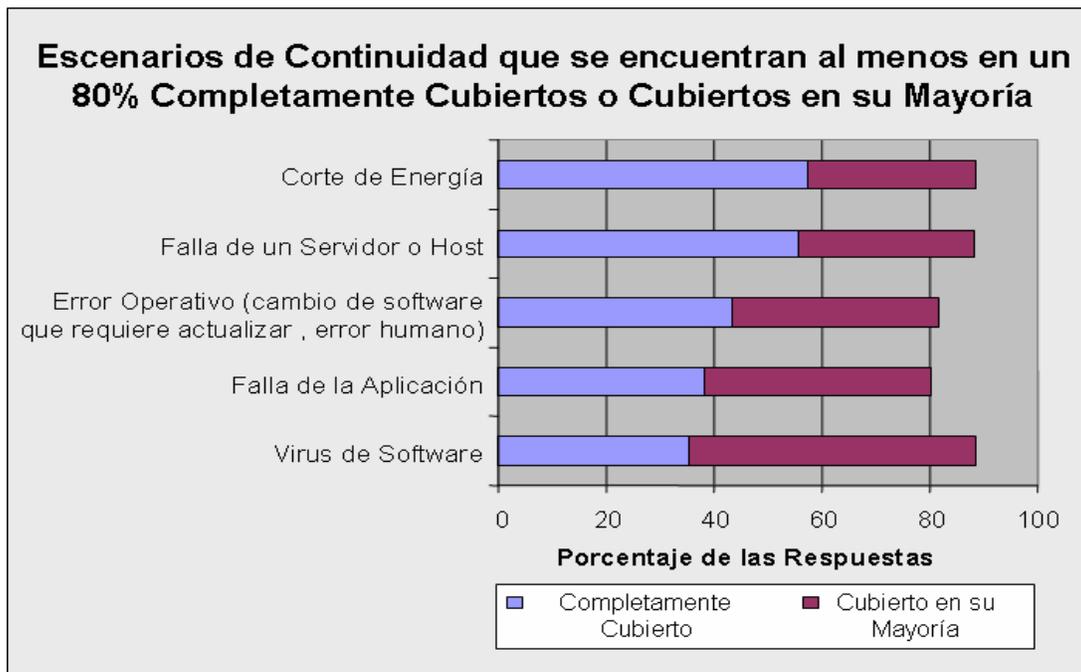


FIGURA 1.34: ESQUEMA DE LA COBERTURA DE ESCENARIOS

Análisis de Gartner presentado como un estudio de 200 a 2006.



Escenarios de Continuidad que se encuentran al menos en un 50% No Cubiertos o Parcialmente Cubiertos

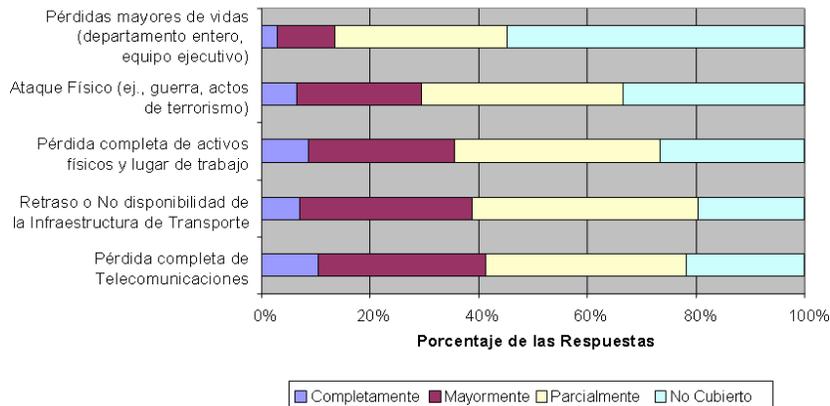


FIGURA35: ESQUEMAS DE ESCENARIOS CUBIERTOS EN UN DESASTRE

Vulnerabilidades Expuestas

- Diversificación geográfica de sitios de respaldo.
- Acceso - falla del plan para la movilización y el transporte.
- Conectividad - fragilidad de las telecomunicaciones y energía, con puntos únicos de falla y sin redes alternativas de rápida activación.
- Puntos de choque - Bolsas de Valores, Firmas de Liquidaciones, Corredores Distribuidores - donde una interrupción puede accionar efectos significativos para el sistema financiero.

Las Deficiencias Más Importantes de los Planes de Continuidad del Negocio

- Ningún espacio de trabajo alternativo, el equipo de trabajo del Centro de Operaciones de Emergencia no sabía dónde juntarse, no se podían comunicar.
- No hay comunicación y no pueden utilizar los respaldos ya que deben transferirse por telecomunicaciones.
- Empleados muertos o incapaces de soportar el impacto emocional.
- Capacidad de respaldo insuficiente - no se había crecido con el negocio.
- Planes demasiado detallados, no llevados a cabo, no mantenidos fuera de sitio, no suficientemente buenos (no contienen nombres alternos, tiempo no realista).
- Problemas con la sincronización de respaldos, o con los mismos respaldos, en parte, como resultado de una prueba inadecuada de las interfaces.
- Etc.

1.4 Conclusiones Principales

- Septiembre 11 introdujo nuevas amenazas que solo pocas personas habían planeado.
- Organizaciones generalmente no están preparadas para continuidad del negocio.
- Planeación de Continuidad del Negocio todavía se ve como una responsabilidad del Área de Sistemas, el cual debe fondearlo y darle seguimiento.
- Carencia de suficientes pruebas de Planes de Continuidad es muy común.
- Septiembre 11 está llevando a una re-evaluación de los Planes de Continuidad existentes, así como de sus premisas y escenarios.
- El énfasis está cambiando a Continuidad del Negocio desde la recuperación en caso de desastre.
- Las mejoras en la planeación de la Continuidad del Negocio se centran en acciones baratas que no aumentarán el presupuesto de TI significativamente.
- Revisión y validación de los planes existentes de continuidad del negocio.



- Incremento del conocimiento, de la compra, de la ayuda, así como del involucramiento de la Alta Dirección.
- Mayores pruebas y ejercicios para todos los planes.
- Enfatizar más la continuidad del negocio en vez de la recuperación en caso de desastres.
- Repensar las premisas y los escenarios sobre los cuales se basan los planes.
- Re-evaluación de los recursos personales.

1.5 **Recomendaciones al BANCO (RESUMEN DEL BIA)**

- Desarrollar una Estrategia de Recuperación de TI que soporte al BIA, los requisitos de negocio de RTO / RPO, todas las plataformas de misión crítica (Mainframe, Tandem, Unix, NT, SUN, HP, etc.) así como las comunicaciones de red adecuadas para efectivamente poder soportar las funciones de negocio de misión crítica en todas las localidades.
 - Priorizar recuperación de funciones de negocio de misión crítica y sus aplicaciones.
- Desarrollar un Plan de Recuperación de Desastres que soporte a los objetivos de negocio y contenga las instrucciones detalladas de lo que tiene que ser ejecutado por el personal no técnico.
 - Probar y validar el Plan de Recuperación de Desastre por lo menos cada seis meses para asegurar que se encuentre conforme a las aplicaciones de misión crítica del negocio.
 - Incluir en las pruebas y validaciones de las aplicaciones de misión crítica, al personal de funciones de negocio, haciéndolos responsables del desarrollo de los criterios de la pruebas, los textos de las pruebas, y la validación de la información recuperada.
- Desarrollar una Estrategia de Continuidad del Negocio y un Plan por unidad crítica de negocio (proceso / área), que proporcione los procedimientos manuales, detalle los textos de recuperación, indique los lugares de trabajo para la recuperación, herramientas, y el personal; defina las funciones de negocio de misión crítica y las estrategias de recuperación priorizadas que apoyen las funciones de negocio.
 - Desarrollar una Estrategia de Recuperación del Lugar de Trabajo que incluya el análisis de casos del negocio de varias alternativas. Una vez que la estrategia sea acordada por las Unidades de Negocio y después financiada e implantada, La Institución Financiera debe documentar esta estrategia en el BCP.
 - Probar y validar el BCP por lo menos una vez al año para asegurar que cumple con los requerimientos del negocio para la continuidad de las operaciones.
 - Establecer una política efectiva de recursos humanos y el procedimiento para permitir al personal adecuado capacitarse para el DR y el BCP, también, implantar un proceso de evaluación anual que incluya las responsabilidades de TODOS los empleados y que defina claramente sus metas y objetivos anuales que serán medidos y recompensados durante el curso del año.



2. DISEÑO DE LA SOLUCION

2.1 Antecedentes.

Con la presentación de BIA en enero del 2006 se autoriza el inicio del proyecto y se solicita la presentación del esquema tecnológico y arquitectónico que cubra con las expectativas requeridas en el BIA buscando cubrir las aplicaciones críticas y sistemas relacionados que aseguren el arranque de un centro de respaldos en el tiempo comprometido y con posibilidades de certificación y pruebas constantes.

Se realizó una investigación de campo utilizando a los proveedores más importantes y solicitándoles visitas a centros de respaldos que consideraran de vanguardia en México. El resultado fue que ninguna solución implementada en los clientes a los que fuimos invitados a la solución cubría un 40% de lo que el BIA requería, los modelos más avanzados basaban su modelo en respaldos y replicas de discos de bases de datos en forma asíncrona, ninguno aseguraba un RTO menor a 24 horas y un RPO de hasta 2 horas de pérdida potencial de datos por la latencia de las replicas asíncronas.

Las fases desarrolladas en el diseño incluyeron:

- Definición de la mejor alternativa para cumplimiento del requerimiento.
- Definir el lugar.
- Definir el modelo de replicación, proveedores e infraestructura.
- Definir el modelo de comunicaciones.
- Definir la primera fase, que aplicaciones y equipos se considerarían.
- Definir los procesos y procedimientos a ejecutar en caso de desastre, las pruebas y certificaciones del modelo construido.

2.2 Análisis- Búsqueda de Opciones.

Se analizaron siete escenarios a fin de cubrir el requerimiento del BCP, el cual nos solicito tener un RTO de 8 horas (máximo) y RPO de 0. (Objetivo planteado para cumplimiento del BIA):

Se documentan y explican siete posibles escenarios y el cumplimiento del objetivo en cada uno.

Escenarios Analizados

Descripción		
E1	Recuperación en Hot Site de Sungard con configuración actual ampliando la capacidad de comunicaciones.	Infraestructura Sungard
E2	Recuperación en Hot Site de Sungard ampliando alcance a dominios críticos y capacidad de telecom.	
E3	Centro de almacenamiento de datos en Palo Alto, Centro Secundario y Recuperación en Monterrey (Esquema propuesto por Gartner).	Infraestructura Procesamiento Propia
E4	Centro Secundario y Recuperación en Monterrey (espacio físico propio)	
E4 ^a	Centro Secundario y Recuperación en Outsourcing en Monterrey (espacio físico en outsourcing)	
E5	Centro Secundario y Recuperación en Palo Alto (espacio propio a menos de 40 KM)	
E5 ^a	Centro Secundario y Recuperación en Outsourcing en Santa Fe (espacio outsourcing a menos de 40 KM)	

FIGURA 2.2: RESUMEN DE ESCENARIOS PRESENTADOS

Alternativas – Evaluación



		Ponderación	E1	E2	E3	E4	E4 ^a	E5	E5 ^a
Riesgo	RPO 0 Min.	0.20	0	0	50	50	50	100	100
	RTO 8 Horas	0.10	0	0	50	50	50	100	100
	Cobertura	0.15	25	65	66	66	66	86	86
Simplicidad	Instalación	0.05	90	70	10	30	60	30	60
	Ejecución	0.15	30	10	10	40	40	90	90
	Costo	0.35	82	72	0	16	20	18	24
		1.00	41.4	40.0	26.9	38.0	40.9	64.3	67.9

Notas:
 • Rango de evaluación de 0 a 100 puntos por cada concepto
 • Evaluación de Costo 100 = costo \$0, 0 = Costo escenario más caro

(-) (+)
Cumple

FIGURA 2.3: RESUMEN DE RESULTADOS Y EVALUACIÓN DE ESCENARIOS VS BIA

La opción que nos aseguraba el cumplimiento del RTO y RPO requerido implicaba un centro alternativo con replicación síncrona.

2.3 Definir el Lugar para el sitio Alterno con opción de replicación síncrona

El primer planteamiento era revisar y asegurar que bajo un efecto natural grave como por ejemplo un terremoto no afectara ambos sitios.

Análisis de Zonas sísmicas Santa Fe y Tlalpan.

En la Ciudad de México se distinguen tres zonas sísmicas de acuerdo al tipo de suelo:

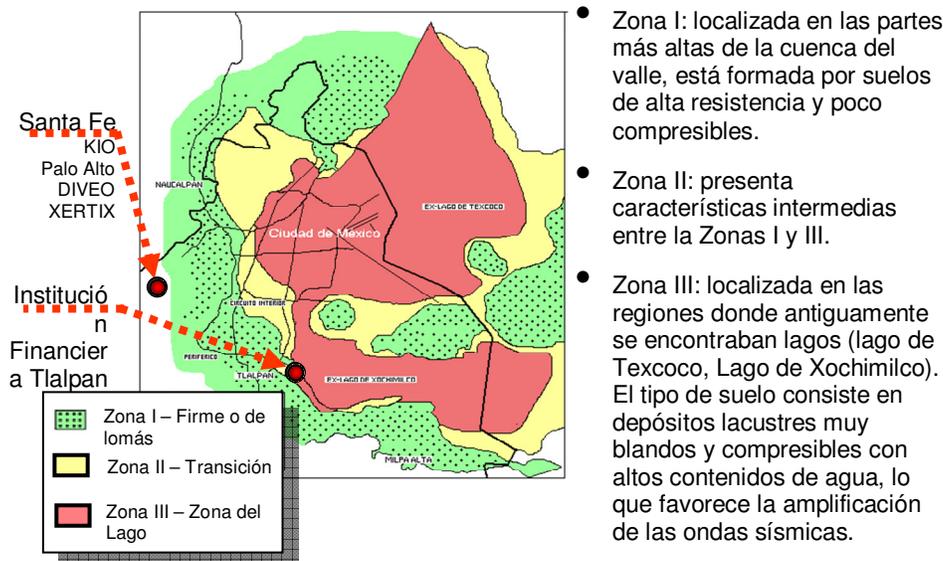


FIGURA 2.4: RESUMEN ANÁLISIS UBICACIÓN CENTRO RESPALDO

La opción E5 pretendía utilizar un edificio propiedad del banco con posibilidad de habilitación de sitio sin embargo los costos de adecuación sobretodo de energía y climatización eran muy elevados así como los permisos ya que la zona era habitacional.

La opción **E5^a** representaba la mejor opción y justo en Santa Fe existen 2 empresas dedicadas a la renta de espacio en un data center bajo la modalidad outsourcing (contrato con externos) y con equipos propios.

El modelo Objetivo se plantea en el siguiente diagrama:

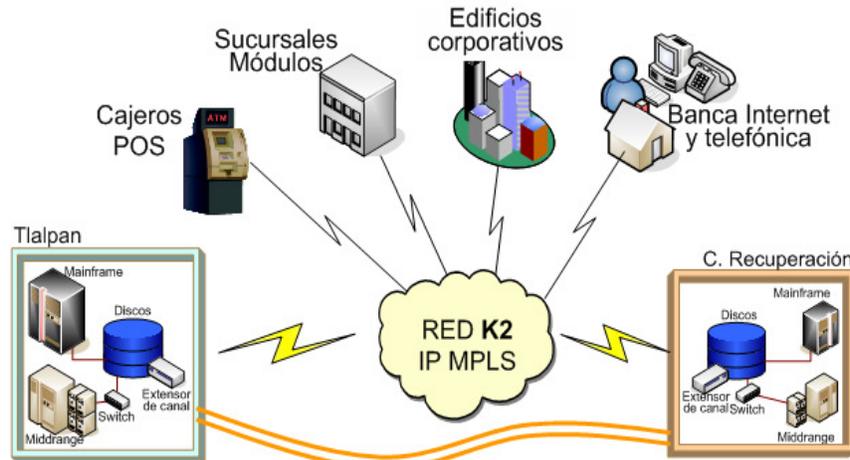


FIGURA 2.5: ESQUEMA CONCEPTUAL DE SOLUCIÓN OBJETIVO

Este modelo representa una de las soluciones más completas en los modelos de recuperación existente:

- Replica síncrona de todos los datos.
- Enlace utilizando fibras oscuras (cables de fibra directos punto a punto sin dispositivos de amplificación o interconexión)
- Iluminación de la fibra con tecnologías de extensores de canal, capaces de iluminar la fibra a velocidades mayores a 10Mbps (10 megabits por segundo) y con la posibilidad de alcanzar 100Mps solo con adición de tarjetas.
- No existe pérdida de datos porque el centro de datos local da por hecho una escritura solo hasta que el remoto envía la confirmación de la operación en el sitio remoto.
- El modelo de interconexión de red debe ser tipo MPLS (Multiprotocol Label Switching) el cual permite transportar diferentes tipos de paquetes, priorizarlos y redirigirlos desde la capa de red a cualquier sitio.
- Con el modelo de red MPLS no es necesario cambiar la IP (Internet Protocol comúnmente identificado con cuatro octetos ejemplo, 192.100.234.1) del dispositivo y con un modelo de priorización de destinos es posible mantener el mismo tipo de red en dos sitios diferentes son colisionar a nivel capa 3 de comunicaciones y poder direccionar desde centrales diferentes al sitio principal
- La recuperación del sitio remoto se limita a el alta o arranque de los equipos.

Este modelo es la respuesta a los objetivos planteados en el BIA llegar a él implica la construcción de la infraestructura en el sitio alterno y la simplificación del principal para no hacerlo una tarea compleja y costosa.

2.4 Definir Centro de Datos - Sitio Alterno

Se tienen tres posibles centros de cómputo en outsourcing, los cuales fueron visitados por las diferentes áreas involucradas en el proyecto (Tecnología, Auditoría, BCP y Compras).

Sites	Distancia de Fibra a Site Tlalpan (Bestel)	Evaluación	Costo por m2 mensual (USD)
KIO Networks	37/43	9.34	\$255.00
XERTIX	37/43	6.00	\$150.00
DIVEO (IBM)	43/47	7.43	\$142.00

FIGURA 2.6: TABLA DE COSTOS DE RENTA DE PISO DE CENTRO DE COMPUTO.



KIO, XERTIX y DIVEO, son las empresas en México dedicadas a comercializar espacio físico de Centro de cómputo para compañías que no cuentan con centro de cómputo propio, los bancos usan este tipo de servicios porque se reducen los costos operativos de energía, edificios, aires acondicionados, centrales de comunicaciones dado que estas empresas comparten estos servicios. En la mayoría de los casos éstos incluyen todo el equipamiento para un DRP en nuestro caso se solicitó solo el tema de Piso falso o lugar físicos, los equipos y las comunicaciones fueron excluidos porque el modelo exige administración total de la infraestructuras en ambos sitios.

En resumen todos los factores evaluados nos determinaron el siguiente resumen mostrado en la tabla siguiente:

		Ponde- ración	KIO	DIVEO	XERTIX
Site Alterno	Distancia	.35	3.5 	3.01 	3.5
	Instalación	.50	5.0 	3.0 	1.0
	Costo	.15	.84 	1.42 	1.5
		1.00	9.34	7.43	6.00

FIGURA 2.6.1: RESUMEN EVALUACIÓN SITIO PARA DRP

La recomendación es la contratación de *DIVEO* con las siguientes áreas de oportunidad a negociar:

- Reducción del área a contratar (RFP 350 m) a 300 m, derivado de la adquisición de equipos más pequeños. Se deberá realizar un diseño físico del nuevo centro de cómputo en conjunto con DIVEO.
- Reducción del costo en el rango del 10 al 15%. Hasta \$195.00 por m2.
- Obtención del área de Business Park (60 puestos) por 20 días al año para pruebas, incluida en el costo.
- Contrato a 5 años.

2.5 Definir Comunicaciones-Fibra Oscura y equipos de Iluminación

Se tienen tres posibles proveedores con la calidad requerida para un proyecto de esta naturaleza.

Proveedores	Ruta Primaria	Ruta Secundaria	% de fibra canalizada /aérea	Evaluación	Pago Único (USD) 60 Meses	Mantenimiento (USD) 60 meses
BESTEL	32.10	43	79-21 59-41	7.73	\$615,850	\$154,00
XERTIX	ND	ND	ND	3.01	\$0	\$480,000
MetroRed	47	37.50	86-14 27-73	7.91	\$585,000	\$210,000

FIGURA 2.7: TABLA RESUMEN COSTO

Para determinar las opciones del tipo de fibra y empresa que debería de construir el resultado del análisis se muestra en la siguiente lamina, destacando la de Bestel con menor distancia y menor atenuación.



Características	BESTEL		MetroRed	
	Opción 1	Opción 2	Opción 1	Opción 2
Fibra	Monomodo Corning SMF-28	Monomodo Corning SMF-28	Monomodo Corning SMF-28	Monomodo Corning SMF-28
Distancia	34 KM	47.7 KM	38 KM	41K
Contrucción				
Enterrada	59.01%	65.83%	80%	75%
Aérea	40.99%	34.17%	20%	25%
Empalmes	12	14	16	17
Atenuación por empalme	NA	NA	0.1 dB	0.1 dB
Atenuación por conector	NA	NA	0.5 dB	0.5dB
db en ruta	9.67	12.6	NA	NA
Nivel de servicio en caso de corte	6 horas	67 horas	6 horas	6 horas
Penalización			Proporcional al tiempo de indisponibilidad	Proporcional al tiempo de indisponibilidad
Costo pago de contado (USD)	\$615,850	\$320,550	\$585,000	\$500,000
Mantenimiento anual pago de contado	\$30,800	\$16,030	\$42,000	\$24,000
Total	\$769,850	\$400,700	\$795,000	\$620,000
Costo en renta mensual (USD)	NA	NA	\$32,500	\$24,000
Total	NA	NA	\$1,950,000	\$1,440,000
Tiempo de contrato (meses)	60	60	60	60

FIGURA 2.8: RESUMEN ANÁLISIS PROVEEDORES DE FIBRA OSCURA

		Ponderación	Bestel	XERTIX	MetroRed
Fibra	Distancia	0.30	3.00	0	2.36
	Canalización	0.10	1.00	0	0.84
	Costo	0.30	2.06	3.00	1.70
	Manto	0.10	0.48	0.01	1.00
	Servicio	0.20	1.20	0.01	2.00
		1.00	7.73	3.01	7.91

FIGURA 2.9: RESUMEN EVALUACIÓN

Para lograr una comunicación Síncrona era necesario contar con equipos y tecnología que permitieran tener un ancho de banda muy grande que asegure la copia de datos síncrona sin impacto en el performance de las aplicaciones. Por redundancia se opto por Bestel y MetroRed.

2.6 Definir Modelo de Replicación: Copia síncrona

Empleo de un esquema de replicación de datos síncrona manejada por la infraestructura de almacenamiento principal.

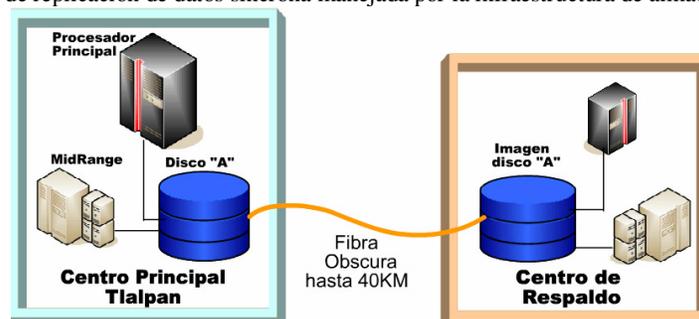


FIGURA 2.10: RESUMEN ESQUEMA CONCEPTUAL REPLICA SÍNCRONA DATOS



- Toda actualización de información realizada en el centro de cómputo principal es automáticamente reflejada en el centro de respaldo.
- Todas las plataformas y aplicaciones contenidas dentro del alcance del DRP direccionan su esquema de almacenamiento a los discos en replicación.

La recomendación final es la contratación de *MetroRed* y *Bestel*. Con el fin de tener la distancia más corta en dos rutas, esto, debido a que es indispensable para la implementación del Parallel Sysplex, restricción de IBM en un GDPS (Global Distance Parallel Sysplex, Cluster de equipos Mainframe IBM) y cumplimiento de las distancias máximas de los equipos de iluminación.

Los equipos de iluminación definidos fueron equipos ADVA con 2 tarjetas y redundancia de 10MB. Se buscó que la administración de estos equipos fuera hecha por el Banco para ser dueños de todo el espectro de luz que puedan manejar los equipos y en un futuro poder tener crecimiento en las velocidades y ancho de banda de este medio.

2.7 Definir modelo de Comunicaciones-Cajeros, Sucursales y Aplicaciones

¿Cuál debería ser el modelo que nos permitiera que todo dispositivo final, PC de sucursal, Cajeros, POS, en un momento dado pudiera conectarse a una red totalmente diferente ubicada en otro sitio sin tener que intervenir el dispositivo?

Se veía complejo ya que el modelo buscado era el de una recuperación total de los sistemas en poco tiempo, el resultado fue aprovechar un proyecto de renovación de la red de sucursales la cual se basaba en comunicación y equipo propietario a un modelo con servicios externos de renta y mantenimiento de medios de comunicación.

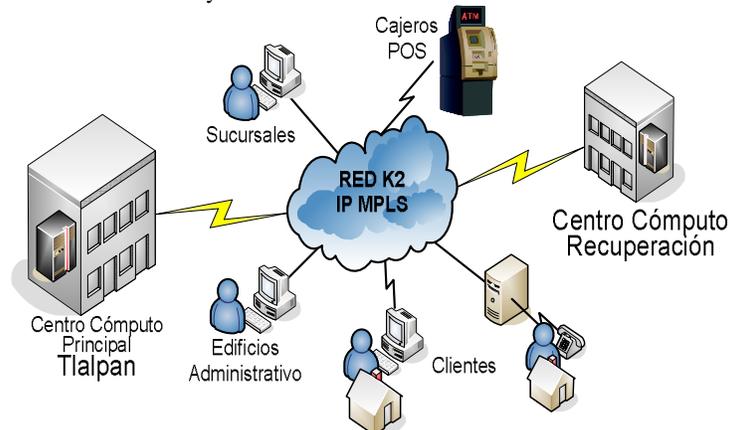


FIGURA 2.11: ESQUEMA CONCEPTUAL MODELO DE COMUNICACIONES MLPS

Internamente se denominó K2 que no era más que cambiar el modelo a un outsourcing de los medios de comunicación con la empresa TELMEX, este proyecto permitió varios temas:

- Incremento del ancho de banda de las sucursales.
- Renovación tecnológica de los equipos de comunicaciones cada 4 años como parte del contrato.
- Integración de Servicio MPLS para manejo de prioridad y calidad en los servicios internos que permiten priorizar el tráfico del sistema de sucursal sobre el correo por ejemplo.
- Integración a los esquemas de monitoreo y soporte.
- Capacidad de movimiento del destino de la red a otro sitio que potencialmente anuncie la misma dirección IP que el dispositivo busca.
- Permitir segmentar la red a sitios diferentes permitiendo hacer pruebas reales de dispositivos específicos apunten al nuevo sitio, esto es una sucursal completa es posible anunciarla en el sitio alternativo sin que ello interrumpa la operación el sitio principal.

Este modelo permitió hacer real la posibilidad de una migración (Switch) total o parcial al sitio de DRP sin tener que ir a tocar el dispositivo final.

Se realiza una evaluación y se establece en el sitio alternativo una red con equipo CISCO mismo que se utiliza en el sitio principal.



2.8 Definición de equipamiento para la fase 1 aplicaciones críticas

La fase uno para aplicaciones críticas determinó que las aplicaciones que debieran ser cubiertas inclúan todo el sistema de sucursales, sistemas de cajeros y puntos de venta, internet y aplicaciones de administración y operaciones (back-office).

Se requirió de inversión para el arrendamiento de equipo central bajo el modelo de ONDEMAND el cual permite tener toda la capacidad requerida para una contingencia pero solo pagando un porcentaje de la misma con derecho a numero finito de pruebas con la capacidad total. Estas inversiones se ajustaran a las renovaciones de los equipos principales de Tlalpan buscando una sinergia entre la negociación y el costo.

2.9 Diseño y construcción.

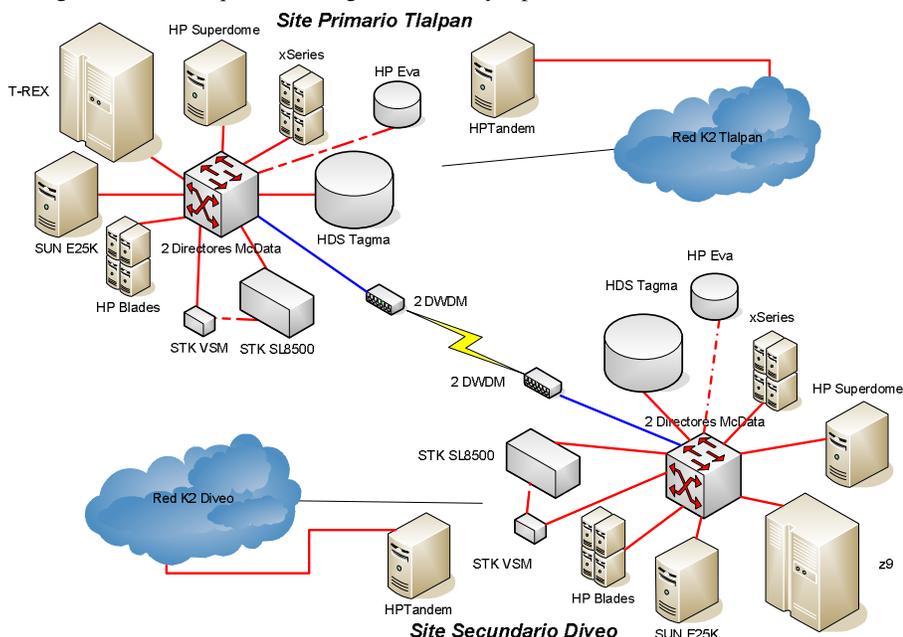
En esta etapa se desarrollo todo el proceso de configuración de los equipos, la negociación análisis de competencia y compra. En esta parte todo el proceso se realizó bajo los lineamientos y normativa de la institución financiera en su apartado de compras.

La siguiente parte, lista todos los equipos, configuración final, no se entro a detalle en cada uno porque son procesos técnicos de muchas hojas que llevaron en varios casos meses de desarrollo desde la energía, cableado, configuración pruebas y migración.

Los equipos adquiridos fueron:

- Equipo Tandem .- Sistema de alta disponibilidad con sistema operativo Guardian HO6.16 y sistema aplicativo BASE24, este sistema administra toda la red de cajeros (3600) y puntos de venta (54,000).
- Equipo Central.- Sistema de procesamiento central con la aplicación bancaria ALTAMIRA basado en sistema operativo OS390, con lenguaje de programación COBOL-CICS.
- Equipos Intel.- Sistemas para ambientes administrativos y departamentales regionales basados en Windows 2000, Windows 2003, más de 245 aplicaciones.
- Equipos UNIX.- Sistemas de procesamiento central basados en Solaris y HPUNIX con aplicaciones administrativas centrales como SAP, Meta4, Portal, Intranets, BEA.
- Almacenamiento.- Sistema de almacenamiento de datos central con arreglo de discos virtuales y software de replicación local y remota.

El diseño final gráfico buscado quedo de la siguiente forma y represento una construcción de casi un año.





2.9.1 Procesadores-Tandem

Se tiene solo una posibilidad ya que es un sistema propietario, HP.

Proveedores	Nivel de cumplimiento del RFP (Escala 1 a 10)	Costo (USD)	Mantenimiento 1ro al 3er año
HP	10	\$1,602,038.00	

FIGURA 2.12: COSTO SOLUCIÓN TANDEM

La recomendación es la contratación de *HP* con las siguientes áreas de oportunidad a negociar:

- El equipo es un upgrade al de desarrollo con suficiente capacidad para soportar cargas en caso de DRP \$78,002 a \$78,008
- Incluir el Soporte durante tres año de 7x24
- No comprometer los mantenimientos de los años 4 y 5, pero limitarlo al importe ofrecido

Centro de computo Tlalpan

Centro computo Xertix



FIGURA 2.14: FOTOS TANDEM CENTRO DE COMPUTO TLALPAN-DIVEO

INFRAESTRUCTURA CENTRAL PLATAFORMA TANDEM

TANDEM HP NON STOP INTEGRITY NS16206

NOMBRE DEL SISTEMA			
\BNORTE			
NUMERO DE SISTEMA			
65431			
CPU TANDEM			
HARDWARE	SISTEMA OPERATIVO	VERSIÓN	MEMORIA POR CPU
6 CPUs N16000	Non-Stop Kernel & OSS	H06.20	8 GB
DISCOS TANDEM			
TIPO	NUMERO	TAMAÑO	ESPEJO
M840072	30	72 GB	SI
APLICACIONES			
PRODUCTOS DE SOFTWARE		VERSION	
XPNET		3.0	
BASE24-ATM		6.0.5	



BASE24-POS	6.0.5
TSS	6.2
JAVA	1.4.2
BASE24-INFOBASE	2.5
PRM	7.1
AO	3.3
KEYMONITOR	3.0

Equipo TANDEM Producción



Equipo Tandem Desa y QA

BLADE

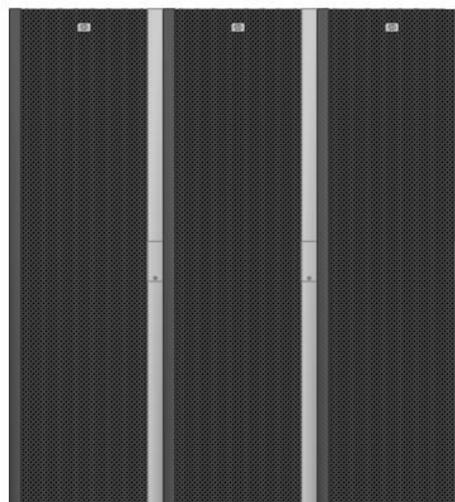


FIGURA 2.15: ESQUEMA TÉCNICO FINAL TANDEM

Servidor Tandem DRP, DESARROLLO Y QA en Xertix
TANDEM HP NON STOP BLADE

NOMBRE DEL SISTEMA			
\BNORTE			
NUMERO DE SISTEMA			
72853			
CPU TANDEM			
HARDWARE	SISTEMA OPERATIVO	VERSIÓN	MEMORIA POR CPU
BLADE NB5000C	Non-Stop Kernel	J06.08	16 GB
DISCOS TANDEM			
TIPO	NUMERO	TAMAÑO	ESPEJO
MSA70	70	72 GB	SI
APLICACIONES			
PRODUCTOS DE SOFTWARE		VERSION	



XPNET	3.0
BASE24-ATM	6.0.5
BASE24-POS	6.0.5
TSS	6.2
JAVA	1.4.2
BASE24-INFOBASE	2.5
PRM	7.1
AO	3.3
KEYMONITOR	3.0

2.9.2 Procesador Central

PROCESADOR CENTRAL PLATAFORMA MAINFRAME

El principal Sistema de Procesamiento Central para la plataforma Mainframe es de la familia z/10 de IBM, cuyas características principales son las siguientes:

IBM z/10 2097 Modelo 611 – Sitio Local (Tlalpan)

- 11 procesadores de 495 MIPs cada uno, 4.4 GHz de velocidad
- Capacidad total 5445 MIPs
- 2 Procesadores zIIP
- 94 GB de Memorial Real
- 36 canales FICON de 8 Gbps y 32 canales ESCON
- 4 procesadores criptográficos
- 5 tarjetas (2 puertos cada una) OSA Exp3 de 10 Gbps
- 2 tarjetas (4 puertos cada una) OSA Exp3 de 1 Gbps
- 1 tarjeta de 2 puertos OSA Exp2 1000 Base-T de 1 Gbps
- Actualmente se tienen 4 particiones lógicas definidas:
 - Producción
 - Preproducción
 - Desarrollo o QA
 - TEST (pruebas de Soporte Técnico)



IBM z/10 2097 Modelo 501 - Sitio Alterno (XERTIX)

- 1 procesador de 462 MIPs, 4.4 GHz de velocidad
- 11 procesadores CBU (Crece en demanda)
- 2 Procesadores zIIP
- 94 GB de Memorial Real
- 36 canales FICON de 8 Gbps y 32 canales ESCON
- 4 procesadores criptográficos
- 5 tarjetas (2 puertos cada una) OSA Exp3 de 10 Gbps
- 2 tarjetas (4 puertos cada una) OSA Exp3 de 1 Gbps
- 1 tarjeta (2 puertos) OSA Exp2 1000 Base-T de 1 Gbps

El equipo de Diveo solo tiene activo un CPU con la posibilidad de activar e igualar la configuración del site principal.



2.9.3 Almacenamiento Central

El almacenamiento central fue uno de los retos principales y de mayor complejidad, el objetivo fue centralizar todo el almacenamiento incluso dispositivos de “boot” de todos los sistemas, con esto el DRP estaría completo al 100%. Cuando un sistema actualizara un dato de configuración en forma prácticamente instantánea esta configuración se activa en el sitio alterno, evitando los riesgos de otros modelos de DRP en donde solo replican datos y están prácticamente cada que se actualiza una configuración o aplicación perdiendo potencialmente la posibilidad de recuperarse.

El principal Sistema de Almacenamiento central para esta plataforma es discos Hitachi, cuyas características principales son las siguientes:

Universal Storage Platform Virtual (USPV) Site Tlalpan

Hardware:

- 40 TB Usable.
- 30 TB para disco primario.
- 10 TB para snapshot para BR Local.
- 24 Canales FICON 4 Gbps.
- 144 GB de Caché.
- 20 GB de Shared Memory.
- Discos de 146 GB.
- Velocidad del disco de 15,000 rpm.

Software:

- Flash Copy para BR Local.
- Compatible Hyper PAV.
- Compatible PAV.
- zHPF.
- Shadow Image.
- True Copy for z/OS R.



Universal Storage Platform Virtual (USPV) Site Remoto (DIVEO)

Hardware:

- 30 TB Usable.
- 30 TB para disco primario.
- 24 Canales FICON 4 Gbps.
- 96 GB de Caché.
- 16 GB de Shared Memory.
- Discos de 146 GB.
- Velocidad del disco de 15,000 rpm.

Software:

- True Copy for z/OS R.



INFRAESTRUCTURA DE ALMACENAMIENTO PLATAFORMA OPEN

El principal Sistema de Almacenamiento central para las plataformas Unix y Windows es discos Hitachi, cuyas características principales son las siguientes:

Universal Storage Platform Virtual (USPV) Site Tlalpan



Hardware:

- 242.5 TB Usables.
- 2.5 TB (400 GB) disco de estado sólido.
- 120 TB para disco primario.
- 120 TB para BR (Shadow Image y Copy On Write).
- 64 Canales Fibre Channel (FC) 8 Gbps.
- 400 GB de Caché.
- 28 GB de Shared Memory.
- Discos de 300 y 600 GB.
- Velocidad del disco de 15,000 rpm.

Software:

- Disaster Recovery Bundle (True Copy).
- Copy On Write (COW).
- Hitachi Dynamic Provisioning (HDP).
- Hitachi Device Manager (HDM).
- Hitachi Tier Storage Manager (HTSM).
- HI Command Tuning Manager.
- Hitachi Storage Service Manager (HSSM).
- Hitachi Dynamic Link Manager (HDLM).



Universal Storage Platform Virtual (USPV) Site Remoto (XERTIX)

Hardware:

- 120 TB Usable.
- 64 Canales Fibre Channel (FC) 8 Gbps.
- 400 GB.
- 28 GB de Shared Memory.
- Discos de 300 y 600 GB.
- Velocidad del disco de 15,000 rpm.

Software:

- Disaster Recovery Bundle (True Copy).
- Hitachi Dynamic Provisioning (HDP).
- Hitachi Device Manager (HDM).
- Hitachi Tier Storage Manager (HTSM).
- HI Command Tuning Manager.
- Hitachi Dynamic Link Manager (HDLM).



2.9.3.1 Infraestructura de Respaldos Mainframe y Open en sitio Local (TLALPAN)

El principal sistema de respaldo en nuestra plataforma Mainframe, está compuesta de un equipo Virtual Storage Manager 5 (VSM5) de la empresa Oracle (Antes SUN) y una librería SL8500. En el caso de los respaldos de Open se basa con el software de respaldos Legato Networker 7.6 y usando la misma librería SL8500, de tal manera que se comparte con la del Mainframe, usando diferentes secciones y drives. Las características principales de estos equipos son las siguientes:

Virtual Storage Manager 5

Hardware:

- 8 GB de Caché.



- 5 TB de disco.

Software:

- Library Station.

Librería SL8500

Hardware:

- 3000 Celdas.
- 6 Drives T10000 para plataforma Mainframe.
- 12 Drives T10000 para plataforma Open.
- 8 Brazos mecánicos, para alta disponibilidad.
- 1 TB de Densidad en la capacidad de los cartuchos en forma nativa.



INFRAESTRUCTURA DE RESPALDOS MAINFRAME Y OPEN EN SITE ALTERNO (XERTIX)

El principal sistema de respaldo en nuestra plataforma Mainframe, está compuesta de un equipo Virtual Storage Manager 5 (VSM5) de la empresa Oracle (Antes SUN) y una librería SL8500. En el caso de los respaldos de Open se basa con el software de respaldos Legato Networker 7.6 y usando la misma librería SL8500, de tal manera que se comparte con la del Mainframe, usando diferentes secciones y drives. Las características principales de estos equipos son las siguientes:

Virtual Storage Manager 5

Hardware:

- 8 GB de Caché.
- 5 TB de disco.

Software:

- Library Station.

Librería SL8500

Hardware:

- 3000 Celdas.
- 6 Drives T10000 para plataforma Mainframe.
- 10 Drives T10000 para plataforma Open.
- 8 Brazos mecánicos, para alta disponibilidad.
- 1 TB de Densidad en la capacidad de los cartuchos en forma nativa.



Para lograr la conectividad se requirió de crear una red de fibra de almacenamiento (SAN-Storage Area Network) con interfaces de 4GB, en todos los equipos adquiridos fue considerado en forma estratégica que cada equipo siempre en su configuración básica contuviera 2 interfaces HBA (Host Bus Adapter) de Fibra 4-8 GB, 4 puertos Ethernet 10,100,1000 Mbps y 2 Puertos de fibra (FC Fiber Channel) de 10Gbits.

El proceso se realizó primero en el sitio de Tlalpan, en los sistemas Unix se realizó mediante sistema operativo anexando los discos requeridos al Volumen Grupo y con el software de Veritas definen el disco espejo en el nuevo disco, el sistema operativo termina y simplemente se suspenden los discos del equipo anterior, se hace un Split del volumen. En los equipos Intel se utilizaron herramientas propias de los discos los cuales virtualizaron las zonas entre el disco y el equipo y simplemente cuando el disco final tuvo el control se eliminaban los discos internos o arreglos externos a que apuntaban los Intel.

2.9.4 Infraestructura Computo Central

La siguiente infraestructura corresponde a la plataforma UNIX, Solaris y HP, esta infraestructura fue renovada durante el proceso de consolidación. En el sitio de DRP se colocó un equipo con menos capacidad solo para los ambientes productivos, se excluyeron los equipos de desarrollo, calidad.



Estos equipos se adquieren bajo el modelo de arrendamiento a 3 años en \$2, 000,000 USD, que representa un flujo de gasto de 55,000 USD mensuales.

INFRAESTRUCTURA CENTRAL PLATAFORMA UNIX

TLALPAN

SUN M9000-64

Hardware:

- 16 CMU's con 4 CPU Quad Core, 256 Cores Total.
 - SPARC64 VII: 2.8GHZ.
- 3 Tb de Ram.
- 128 Interfaces de red.
- 96 puertos de fibra para SAN.
- Solaris 10.



SUN M9000-32

Hardware:

- 8 CMU's con 4 CPU Quad Core, 128 Cores Total.
 - SPARC64 VII: 2.8GHZ.
- 1 Tb de Ram.
- 64 Interfaces de red.
- 48 puertos de fibra para SAN.
- Solaris 10.



Aplicaciones:

BD: Oracle 10g, 11i, 40 Instancias, 130 bases de datos productivas

- | | |
|-----------------------------------|---------------------------|
| ◦ SAP Netweaver | ◦ Reuters |
| ◦ Remedy | ◦ Portal Internet |
| ◦ SAS | ◦ Cyber |
| ◦ ALERT (riesgos) | ◦ Portal Movil |
| ◦ BD Intranet | ◦ Casa de Bolsa: Murex, |
| ◦ Legato Networker | Charles River, Kondor, |
| ◦ Contro-SA | T24 |
| ◦ Data Ware House | ◦ Control-D |
| ◦ ACE Server | ◦ Ambientes de Desarrollo |
| ◦ Payworks | y QA |
| ◦ Oblix | |
| ◦ OAM | |
| ◦ CREa | |
| ◦ Staffware | |
| ◦ Content Manager | |
| ◦ SAP, BI Portal | |
| ◦ Experian | |
| ◦ ACI PRM | |
| ◦ Genesys | |
| ◦ SPEI | |
| ◦ Genesys | |
| ◦ Ldap | |
| ◦ CC-Harvest | |
| ◦ Tracker | |
| ◦ Power Borker | |
| ◦ DNS | |
| ◦ PRM (Proactive Risk Management) | |
| ◦ PEM | |
| ◦ Swift | |
| ◦ Zabbix | |



2.9.5 Unix HPUX

TLALPAN

HP Superdome

Hardware:

- 8 celdas con 4 CPUs, 32 cores total
 - PA-Risc 8900 @ 1.1 GHz.
- 164 Gb de Ram.
- 32 Interfaces de red.
- 32 puertos de fibra para SAN.
- HP-UH 11.11.

Aplicaciones:

BD: 10g, 5 instancias, 12 bases de datos productivas

- SAP R3
- Transferencias terceros
- SACBUR
- SCAT
- Custodia de Valores
- Meta4
- Firmás
- Reflection Web
- Ambientes de Desarrollo



2.9.6 Configuración DRP Solaris

SUN M9000-32

Hardware:

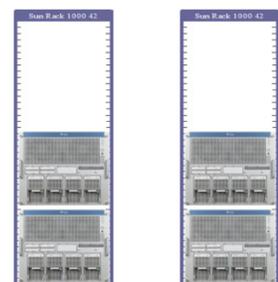
- 6 CMU's con 4 CPU Quad Core, 96 Cores Total
 - SPARC64 VII: 2.8GHZ.
- 768 Gb de Ram.
- 48 Interfaces de red.
- 48 puertos de fibra para SAN.
- Solaris 10.



SUN M5000 (4)

Hardware:

- 8 CMU's con 4 CPU Quad Core, 128 Cores Total
 - SPARC64 VII: 2.8GHZ.
- 1.5 Tb de Ram.
- 48 Interfaces de red.
- 32 puertos de fibra para SAN.
- Solaris 10.





BD: Oracle 10g, 11i, 40 Instancias, 130 bases de datos productivas, todas las aplicaciones de Producción replicadas.

2.9.7 Configuración DRP HPUX

DRP

HP Superdome

Hardware:

- 3 celdas con 4 CPUs, 12 cores total
 - PA-Risc 8900 @ 1.1 GHz.
- 96 Gb de Ram.
- 12 Interfaces de red.
- 12 puertos de fibra para SAN.
- HP-UH 11.11.

BD: 10g, 5 instancias, 12 bases de datos productivas

- SAP R3.
- Transferencias terceros.
- SACBUR.
- SCAT.
- Custodia de Valores.
- Meta4.
- Firmás.
- Reflection Web.



2.9.7.1 WINDOWS

INFRAESTRUCTURA CENTRAL PLATAFORMA INTEL

Infraestructura Vmware & Windows

- ✚ 42 Servidores x86 centrales IBM 3850 X5 8 core
- ✚ Alto nivel de virtualización VMWare Vsphere 4.1, 98% de los servidores son virtuales.
- ✚ Aplicaciones:
 - Banca por internet/movil, Intranets, Correo, Software de Red (Active directory/DNS/DHCP/etc), colaboración (Sharepoint)
 - Bases de datos departamentales / Intranets
 - Aplicaciones de casa de bolsa
 - Aplicaciones de Call Center



3. IMPLEMENTACIÓN FINAL

3.1 Modelo de Infraestructura Final, Consolidada y Virtualizada

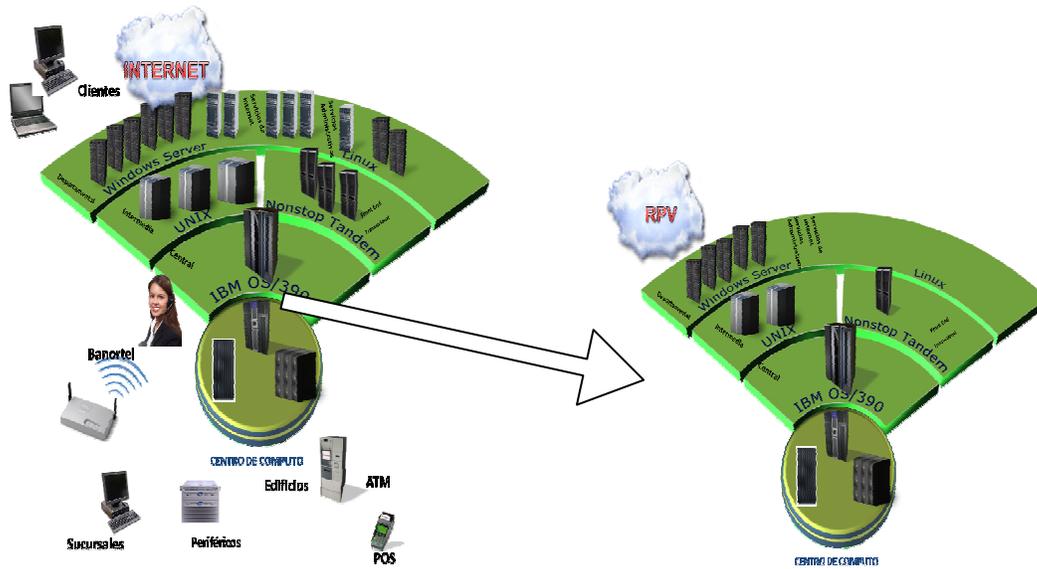


FIGURA 3.1: ESQUEMA TÉCNICO FINAL CENTRO DE COMPUTO TLALPAN-DIVEO

En la fase uno en el sitio de Diveo se implementó la infraestructura necesaria para cubrir las aplicaciones más críticas determinadas en el BIA con replicación síncrona.

3.2 Presupuestos y Base del análisis de Costos y Viabilidad.

Presupuesto DRP					
Tradicional	Descripción	2003	2004	2005	
Gasto	Renta de Enlace Filadelfia	450,000	480,000	530,000	
	Renta de DRP Filadelfia	1,800,000	1,926,000	2,051,190	
	Pago de 3 Pruebas, asistencia	180,000	180,000	180,000	
	Actualización de la capacidad	212,000	195,000	322,000	
TOTAL ANUAL		\$2,642,000	\$2,781,000	\$3,083,190	

FIGURA3.2: RESUMEN COSTO GASTO SIN PROYECTO MILLONES USD



Proyección Proyecto Nuevo	Descripción	2006	2007	2008	2009	2010
Gasto	Renta de Fibras	300,000	300,000	300,000	300,000	300,000
	Arrendamiento Equipos Centrales	2,100,000	2,100,000	2,100,000	2,100,000	2,100,000
	Arrendamiento Equipos DWDM	260,000	260,000	260,000	260,000	260,000
	Renta de Piso.	309,120	309,120	309,120	309,120	309,120
Inversión	Equipo Comunicaciones	740,000				
TOTAL ANUAL		\$3,709,120	\$2,969,120	\$2,969,120	\$2,969,120	\$2,969,120

FIGURA3.3: RESUMEN COSTO REALIZAR PROYECTO MILLONES USD

En este escenario se eliminan las inversiones de los equipos en el centro de datos de Tlalpan ya que la renovación de esos equipos era propia de la operación normal de los sistemas del Banco y solo considera las inversiones en Diveo y compara con los gastos del DRP anterior.

La viabilidad financiera del proyecto es aceptada ya que en un año logra una disminución del flujo de gasto+ inversión y en el primer año solo se solicita un 23% adicional al gasto del primer año del proyecto. Pero con este nuevo modelo el DRP da un giro de más de 180 grados y se vuelve 100% funcional y cumple con el 100% de los requerimientos solicitados en el BIA para la Fase 1.

4. CONSTRUCCION

4.1 Fases

La fase de construcción se dividió en 3 grandes bloques:

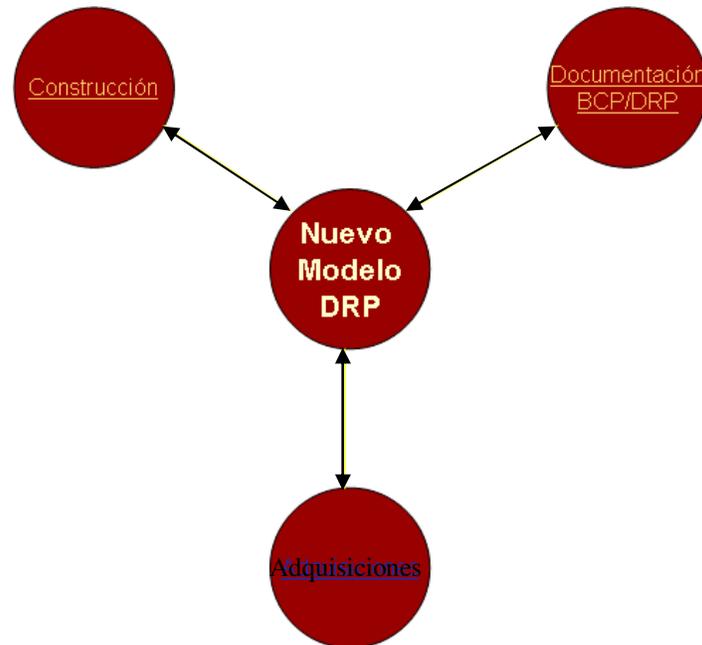


FIGURA 4.1: ESQUEMA FASES DE CONSTRUCCIÓN Y DOCUMENTACIÓN

La parte de adquisiciones fue muy simple porque en el mismo proceso de análisis se realizaron los procesos para realizar la comparación técnica y económica de las diferentes soluciones y proveedores, a este proceso se le denominó RFP (Request For Proposal) y se realizó para cada una de las adquisiciones, en donde ya se definía claramente las configuraciones detalladas de cada uno de los equipos requeridos. En el RFP se mezclaba la adquisición del equipo del edificio principal y el de DRP buscando una sinergia mayor con el proveedor y logrando mayores reducciones en los costos.

En el RFP básicamente se planteaban los siguientes elementos descriptivos:

- Objetivo.
- Descripción del componente.
- Descripción de los servicios de instalación y migración.
- Diagrama de la solución.
- Fecha de entrega de Propuesta.
- Fecha de Decisión de Ganador.

Como siguiente paso se realizó la fase de evaluación y dependiendo del caso se realizaron pruebas de laboratorio en donde los ingenieros validan las características de funcionalidad y desempeño del equipo propuesto.

A continuación en la tabla 4.2 se presenta un ejemplo de la valoración por el RFP en donde se califican las características más importantes de la solución y se dan pesos específicos a cada una de ellas.

En el llenado de esta tabla participan las áreas de compras, auditoría y tecnología para cubrir todos los aspectos de control normativo que una adquisición requiere.



Implementación de infraestructura de DRP

HARDWARE	Solicitud Banorte		HITACHI		Calif	Peso	EMC/Dell		Calif	Peso
	TLALPAN	XERTIX	TLALPAN	XERTIX			TLALPAN	XERTIX		
Equipo	Propuesto por Proveedor	Propuesto por Proveedor	VSP	VSP			VMAX 4	VMAX 4		
Capacidad Total	144 TB	84 TB	149.38TB	86.65 TB			144 TB	84 TB		
Capacidad en disco Primario	60 TB	--	60 TB	--	100		60 TB	--	100	
Capacidad SSD	4 TB	4 TB	4.7 TB	4.7	100		4 TB	4 TB	100	
Capacidad Disco BR Local	60 TB	--	62.7 TB	--	100		60 TB	--	100	
Capacidad Disco Copia Remota	--	60 TB	--	60.9 TB	100		--	60 TB	100	
Capacidad SnpaShot	20 TB	20 TB	20.9 TB	20.9 TB	100		20 TB	20 TB	100	
Cache ambos controladores	512 GB	512 GB	512 GB	512 GB	100		512 GB	512 GB	100	
Memoria de Control Ambos Controladores	572 GB	572 GB	32 GB	32 GB	100		No usian		80	
Tamaño y Velocidad Disco	De mayor desempeño	De mayor desempeño	300 GB SAS 10K rpm	300 GB SAS 10K rpm	90		300 GB 15K rpm	300 GB 15K rpm	100	
Num. Canales FC	24	24	16 FC/32 FICON	16 FC / 32 FICON	100		16 FC / 24 FICON	16 FC / 24 FICON	100	
Velocidad Tarjetas de Canal	8 Gbps	8 Gbps	8 Gbps	8 Gbps	100		8 Gbps	8 Gbps	100	
Cableado ambos Sites	Cableado del Disco al panel de Parcheo	Cableado del Disco al panel de Parcheo	SI	SI	100	79.5	SI	SI	100	80.6
SOFTWARE										
Compatible FlashCopy/Shadowmage for z/OS	SI	SI	SI	SI	100		SI	SI	100	
True Copy for z/OS o HUR	SI	SI	SI (60 TB)	SI (60 TB)	100		SI	SI	100	
Basic HyperSwap	SI	SI	SI	SI	100		SI	SI	100	
GDPS 3.5	SI	SI	SI	SI	100		SI	SI	100	
Dynamic Provisioning	SI	SI	NO (*)	NO (*)	80		SI	SI	100	
Dynamic Tiering	SI	SI	NO (*)	NO (*)	80		SI	SI	100	
Compatible Hyper PAV	SI	SI	SI	SI	100		SI	SI	100	
Compatible PAV	SI	SI	SI (165 TB)	SI (100 TB)	100		SI	SI	100	
z High Performance Ficon (HPF)	SI	SI	SI	SI	100		SI	SI	100	
Tunning Manager	SI	SI	SI (170 TB)	SI (100 TB)	100		SI	SI	100	
Tier Storage Manager	SI	SI	SI (170 TB)	SI (100 TB)	100		SI	SI	100	
					93.4783				94.7826	
CAPACITACION										
En todo el SW requerido y Hardware	Capacitación en los nuevos equipos y en el SW solicitado durante los 3 años de garantía del equipo		Hitachi considera a 4 personas		100		Dell considera a 1 persona para su capacitación		75	
RESIDENTE										
Duración del residente	3 años		3 años		100		3 años		100	
Horario de 9 a 6 pm y en horarios de fin de semana	Independencia en los horarios de trabajo		SI		100		SI		100	
SERVICIO DE SOPORTE										
Nivel de Conocimiento	Capacidad para conocer sus propios equipos		Muy Bueno		95		Bueno		90	
	Retroalimentación de áreas internas		Muy buena		90		Buena		85	
	Retroalimentación de Clientes		Muy Buena		90	14.6	Buena		85	13
VENTAJAS										
Tecnología reconocida e instalada en Max Madurez de Banorte en la Tecnología de Almacenamiento propuesta por los proveedores	Capacidad instalada en otros clientes de México Lo que busca Banorte es tener la facilidad y la experiencia en el dominio de los productos a administrar para facilitar la migración y mitigar el riesgo en el manejo de los datos productivos		Muy Buena en Open y Mainframe Con Hitachi se tiene la experiencia de 15 años administrando sus productos de almacenamiento en disco y 5 años en el manejo de herramientas de replica que facilitan la migración sobre sus propios discos		95		En Open muy buena y en Mainframe muy poco Con EMC no se tiene la experiencia ni en usar su tecnología ni en el conocimiento de sus productos, por lo que la curva de aprendizaje sería mayor y esto pudiera ser un punto de riesgo tanto en la migración como en la propia operación. Realmente nos llevaría tiempo el		85	
					100				50	
NIVELES DE SERVICIO PROBLEMAS										
Disponibilidad en caso de problemas	2 Horas en sitio en caso de contingencia y 4 horas para solución		SI		100		SI		100	
Involucramiento en la solución de problemas aunque no sean suyos	Colaboración con proveedores en el que comparten una solución		Excelente		100		Muy Buena		95	
					97	94			86.5	93
					HITACHI 94		EMC/DELL		93	

FIGURA 4.2: TABLA DE VALORACIÓN POR RFP (CONCURSO)

Los resultados son revisados por un área de arquitectura que con base en los resultados compara contra la documentación en internet o de analistas y en los casos en los que las tecnologías son líderes y cubren funcionalmente todos los requerimientos, se toman en consideración los costos y calidad de los servicios en caso de ser proveedor actual. Un proveedor actual debe ser constantemente valorado en su calidad de servicio ya que sus niveles de soporte, actitud y atención pueden ser considerados y den un peso adicional a las decisiones en la elección del proveedor de la solución, es decir aquel proveedor que a pesar de tener buen producto pero su servicio es de mala calidad y no busca la mejora constante es desvalorado en la evaluación y pudiera causar que salga bajo en la calificación global.

Al seleccionar el proveedor el modelo de pago usado fue el de arrendamiento, en donde nuevamente se realiza una evaluación para buscar el mejor factor de arrendamiento en pesos dentro del mercado, esta evaluación correspondió a las áreas administrativas y de rentabilidad.

4.2 Fases de implantación

Se determina trabajar en 5 fases de implementación que fueron divididas por criticidad del servicio, quedando en primer lugar servicios a cliente en sucursales con los sistemas de administración y control asociados, en segundo lugar los sistemas de tesorería y casa de bolsa, en tercero los sistemas de cajeros e internet, en cuarto los sistemas de riesgos, prevención de lavado, control operativo, finalmente sistemas de callcenter (centro de contacto para atención telefónica a clientes) y toma de decisiones.

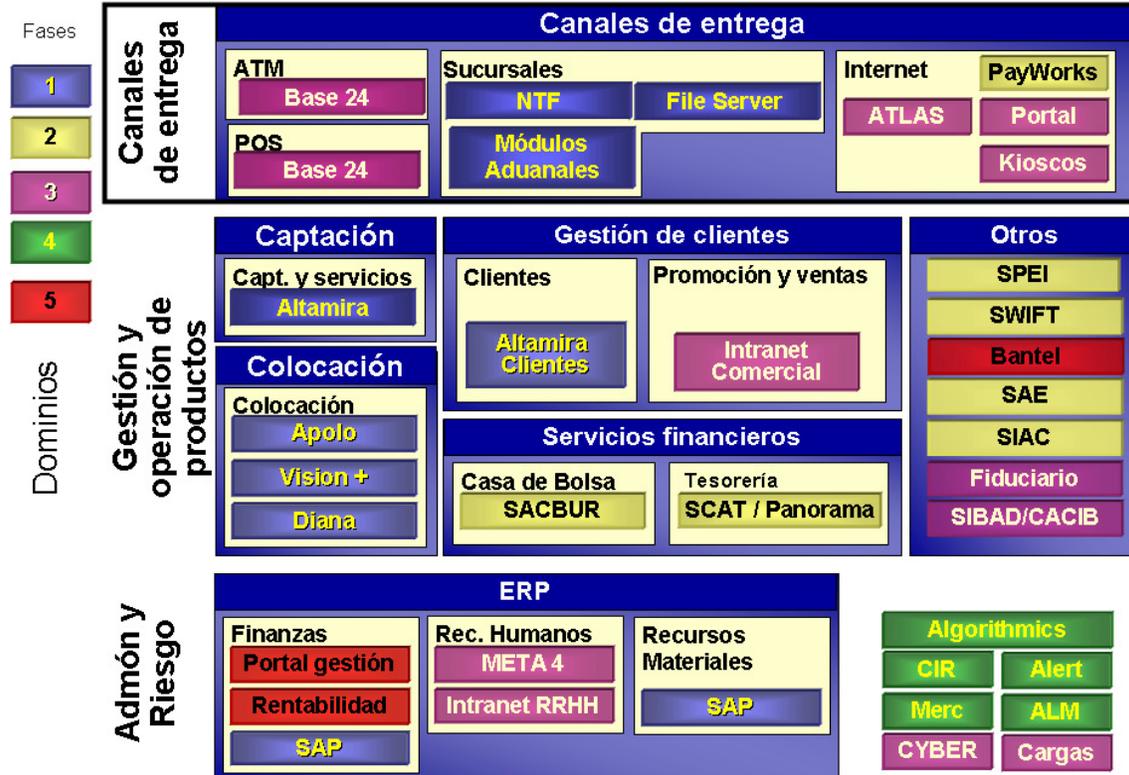


FIGURA 4.3: ESQUEMA DE FASES DE MIGRACIÓN POR APLICACIÓN

En la primera fase se integran en forma física los servidores y servicios requeridos para activar las plataformas en donde corre la operación de sucursales, en este caso el sistema de sucursales opera el 99% sobre la plataforma mainframe.

El proceso de implementación se divide en dos partes; la construcción en un ambiente local, con pruebas y la migración al sitio remoto con el esquema local ya validado.

4.3 Fases de Pruebas

Prueba local.- En esta etapa se instalaron los directores de fibra para construir la red de fibra para el almacenamiento y se realizó una interconexión entre los discos del equipos central y el disco central nuevo en donde se realizaría la réplica, estos directores de fibra se interconectaron al sitio remoto a través de equipos atenuadores de fibra que simulaban 40 km de distancia y la latencia que más o menos se experimentaría, se realizaron pruebas y ajustes a parámetros tanto en la parte de los puertos de 10GB como en el numero de procesos que se requerían para mantener la copia sin afectación a los servicios locales. Este proceso fue el más difícil y como las pruebas eran síncronas se tuvieron varios problemas durante la construcción y entendimiento del proceso, el resultado fue construir un sistema de monitoreo que bloquee los puertos de copia en caso de un mal funcionamiento o error en el disco remoto o las comunicaciones ya que de no hacerlo así en caso de un problema el sistema local sufre una fuerte degradación.

Traslado a Diveo.- Ya con pruebas locales de monitoreo se levantaron sistemas de pruebas en forma local y acceso local con éxito, se desarmo la infraestructura, se elimino el equipo de atenuación y se conectaron al dwdm los discos. En diveo se creó la nueva SAN, se creó la conectividad con los discos y las fibras del DWDM (Dense wavelength Division Multiplexing, equipo que se usa para iluminar fibras oscuras con velocidades de transmisión superiores a los 10gbs) fueron unidas.

Prueba Remota.- En esta primera prueba se copiaron solo discos de la partición de pruebas la cual no tenia carga transaccional se realizaron pruebas de volumen y se realizaron ajustes en los extensores de canal (DWDMs) y numero de procesos en el disco para el proceso de copia. Se incremento el cache en los discos remotos para asegurar la disminución del tiempo de latencia en la escritura remota.



Prueba DRP.- Durante 2 semanas solo se mantuvo la réplica síncrona total de la partición de producción sin ningún otro equipo, en resumen estaban sincronizados de manera concurrente y con operación en el centro principal 37,400 discos con varios tamaños, resultando exitoso el proceso de réplica de datos. Para la prueba de DRP solo fue necesario suspender la copia, cambiar los discos de modo copia a modo open y activar la producción de Producción en DIVEO, la prueba fue exitosa desde el primer momento y los problemas a resolver no fueron de datos, todos fueron de conectividad y configuración asociada al sitio remoto en donde las posiciones de las tarjetas eran diferente. Con esta prueba se estableció como único que la estructura de tarjetas y direccionamiento de dispositivos tiene que ser respetada en ambos sitios.

Estrategia de Implantación del DRP del sistema Central

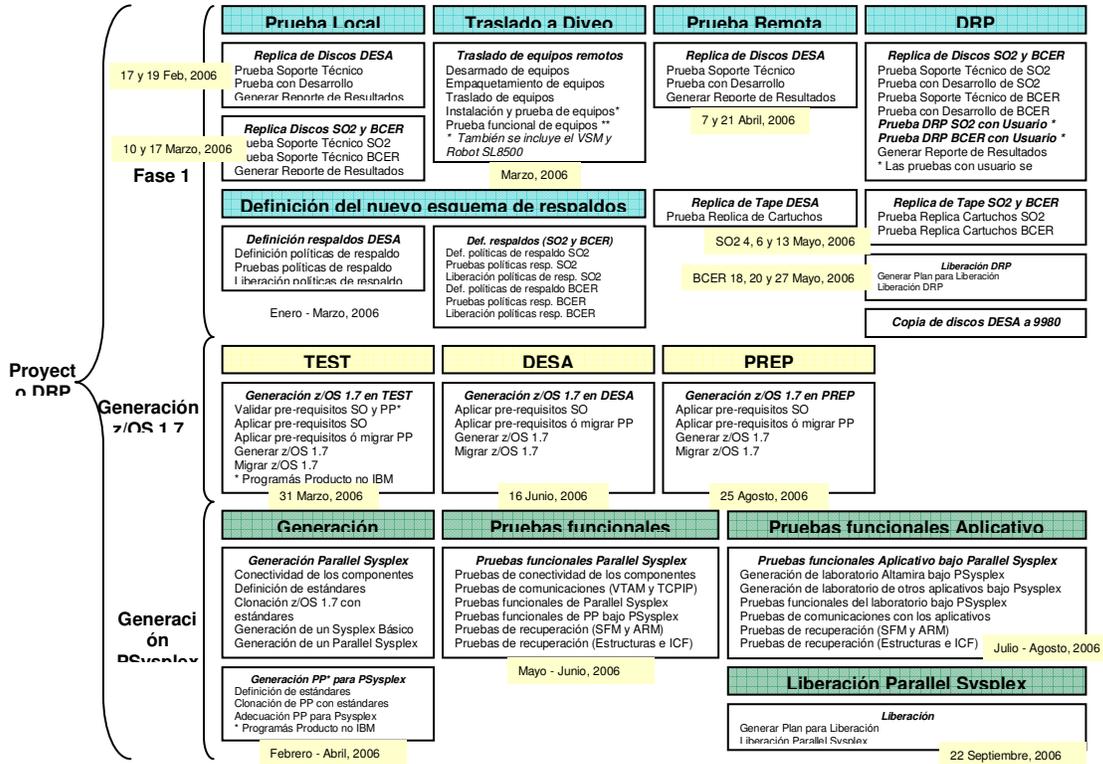


FIGURA 4.4: ESQUEMA MODELO DE PRUEBAS EN SISTEMA CENTRAL

Este es el diagrama físico de la configuración del equipo central mainframe con el esquema físico de conectividad a directores y DWDM's.

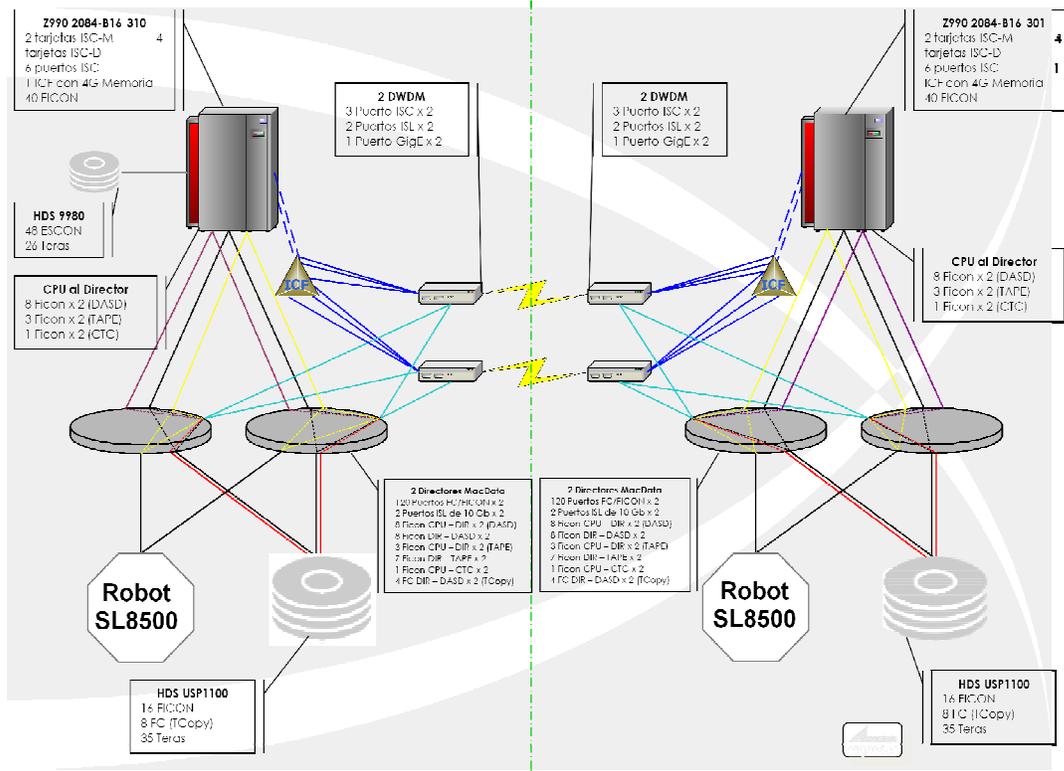


FIGURA 4.5: ESQUEMA TÉCNICO DE MAINFRAME DRP

El proceso completo de construcción e implementación fue de 11 meses a partir de contar con todos los equipos, el proceso y metodología utilizada aseguraron la continuidad total durante todo el proceso de construcción y pruebas.

El equipo dedicado a esta construcción era el mismo de soporte día a día y esto se determinó así para lograr que el mismo equipo realizara los ajustes locales y analizara los cambios de comportamiento al integrar la nueva solución principalmente en los aspectos de tiempo de respuesta al disco, ya que en sistema de este tipo son de los elementos más críticos con los que se cuenta.

Calendario Fase 1

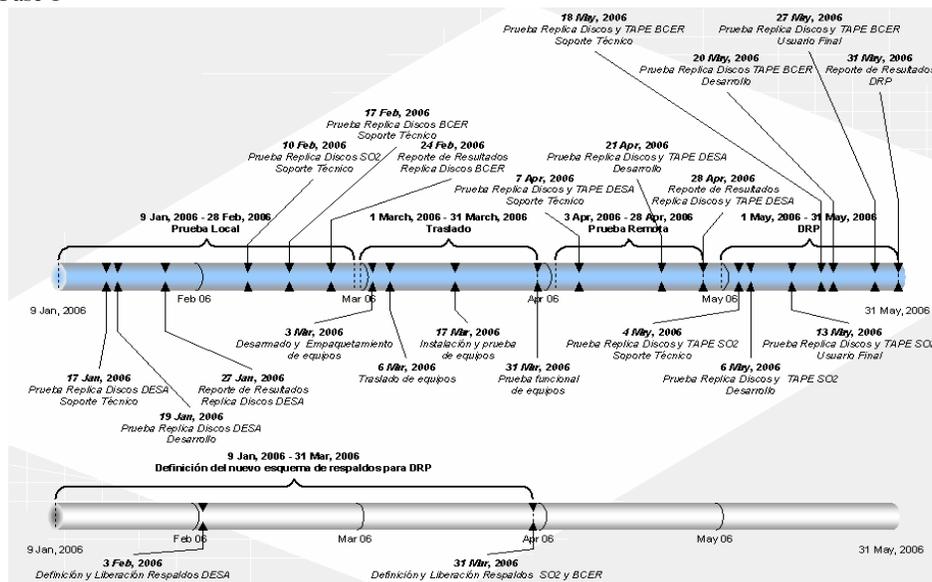


FIGURA 4.6: ESQUEMA PLAN DE FECHAS DE PRUEBAS MAINFRAME

Elaborado por:
Salvador Sierra Hernández

Revisado por:
M.I. Jorge Valeriano Assem



4.4 Fases de Construcción (En diagrama Etapas 3,4,5 Construcción del resto de las plataformas)

Para las siguientes fases lo que se observó es que al realizar las construcción y procesos de pruebas de replicación local de equipos UNIX y Windows centrales, varias de las aplicaciones consideradas en otras fases de aplicaciones no críticas quedaron cubiertas al re sincronizar los discos de esos equipos.

Ejemplo:

Equipo M9000 contenía más de 75 aplicaciones entre ellas sistemas de las fases 2,3,4 y 5 el esfuerzo de conectar el equipo completo a la red SAN y discos nuevos fue uno solo e implicó que en la misma fase de pruebas todas éstas aplicaciones fueron evaluadas al mismo tiempo.

Se realizó el mismo ejercicio para el resto de plataformas logrando un esquema simplificado de infraestructura con virtualización básica en ambientes UNIX y WINDOWS.

Este es un esquema final de la consolidación lograda en el edificio principal.

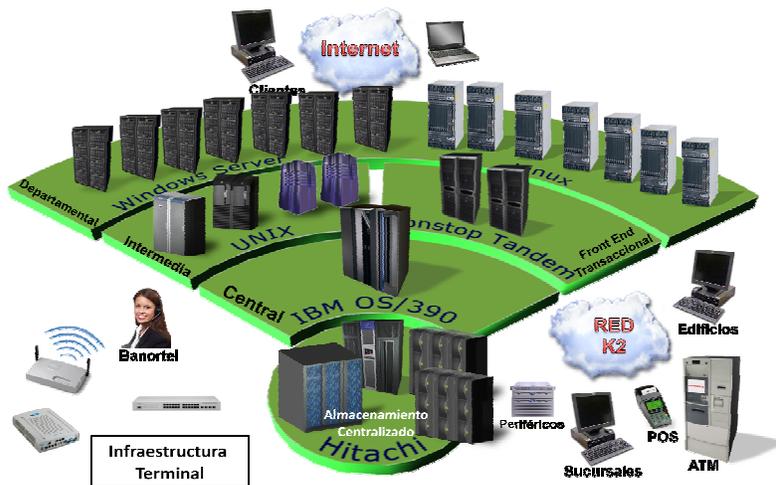


FIGURA 4.7: ESQUEMA TÉCNICO DE CONSOLIDACIÓN TLAPAN

La centralización del almacenamiento permitió crear el esquema idóneo de replicación que no solo cubriera los aspectos de la recuperación del DRP si no de la recuperación local (BSP) mediante el uso del mismo tipo de tecnología.

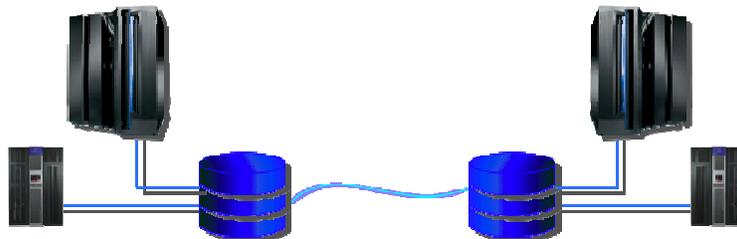


FIGURA 4.8: ESQUEMA TÉCNICO DE COPIA SÍNCRONA

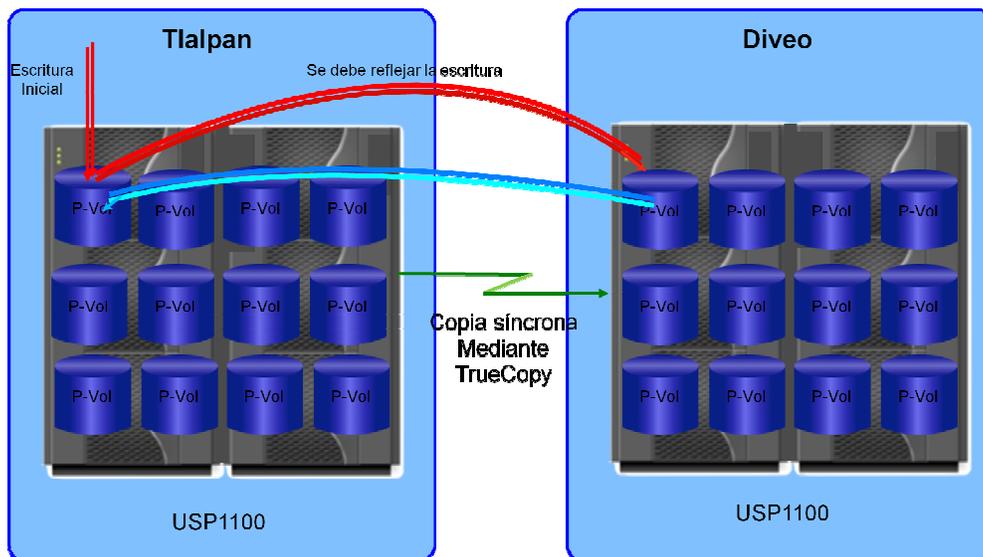


FIGURA 4.9: ESQUEMA GRAFICO REPLICACIÓN SÍNCRONA

Implementación de un esquema de recuperación Local

La habilitación de las pruebas en los diferentes ambientes y el validar la posibilidad de una recuperación total, permitió que con la implementación de esta tecnología se creara un mecanismo muy simple de recuperación local por ejemplo en caso de problemas de en un disco o una falla humana que derive en pérdida de información, corrupción de datos, análisis de problemas, caída de equipos. Se habilito un sistema que permitiera copias de volúmenes de discos en la infraestructura local; esto permite la habilitación casi inmediata de la recuperación de un sistema completo en forma integral. En el pasado el uso de recuperación de datos con base encintas podía resultar en una catástrofe ya sea por el tiempo mismo de la recuperación o por fallas en las cintas requeridas.

Gráficamente el modelo opera como sigue:

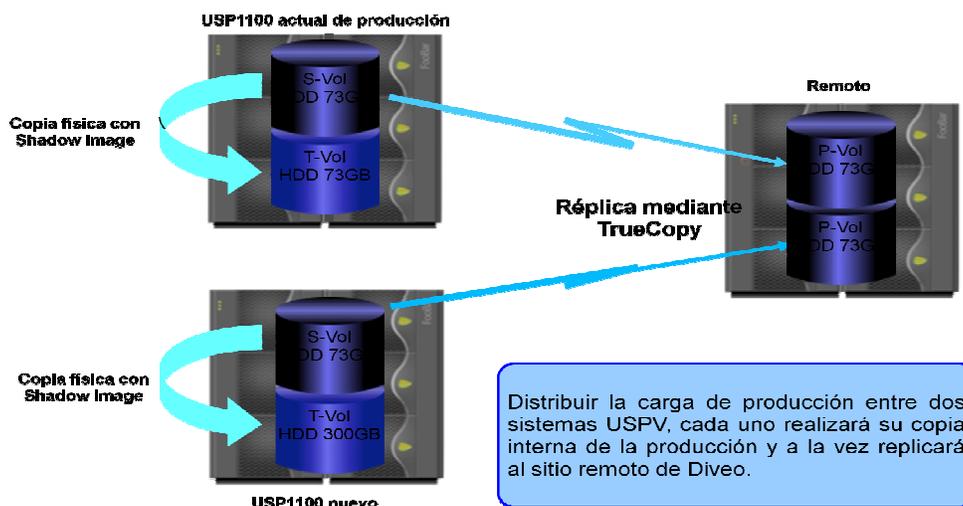


FIGURA 4.10: ESQUEMA GRAFICO REPLICACIÓN LOCAL CON DISCOS MARCA HITACHI MODELO USPV

5. DOCUMENTACION

5.1 Elaboración de Planes de Continuidad

5.1.1 Antecedentes

Un paso fundamental después la construcción y pruebas es la organización de la documentación que se generó durante el proyecto, así mismo los mecanismos de actualización y consulta, se realizan una serie de acciones para desarrollar esta importante etapa:

- Se adquiere Software LDRPS para Elaboración de Planes de Continuidad del BCP-DRP en Marzo del 2006 a la Compañía STROHL Systems. Este software de manera estructurada permite almacenar toda la documentación de los procesos de arranque del DRP.
- Se da Capacitación en Mayo 2006 a las Áreas de Tecnología y Usuarios.
- Se inicia y finaliza la captura de Planes y Fases del DRP de Tesorería Derivados.
- Se inicia la captura de Plan y Fases de Casa Bolsa Derivados.
- Capacitar a personal de Infraestructura-Febrero 2006.
- Alinear la documentación vs. Plan Construcción y BIA.
- Elaboración de Planes de Soporte Técnico Central, Comunicaciones, Regionales, Centro de Crisis, Desarrollo para el DRP.- Junio 2006.

Se realiza un documento que represente el proceso que debe seguir el personal y los sistemas en caso de un desastre y se utiliza la siguiente metodología para crearlo.

5.1.2 Organización de fases: Metodología

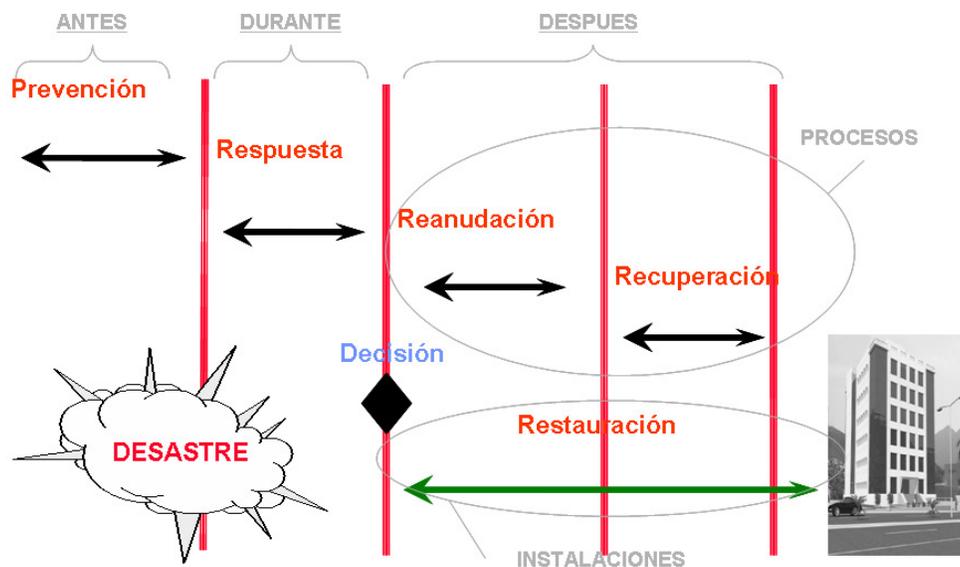


FIGURA 5.1: ESQUEMA CONCEPTUAL FASE DE INVOCACIÓN DRP

5.1.3 Estructura de Fases y Planes

Después de definir las fases se crean con base en la herramienta los planes detallados para cada área fundamentados en el documento Principal denominado Con el nombre de la institución Financiera donde se indica que durante un tiempo específico todas las áreas deben declarar la contingencia y esperar a que los sistemas del DRP sean activados y validados, en el documento se detalla el proceso y por cada aplicación una visión muy rápida que asegure su correcta operación.

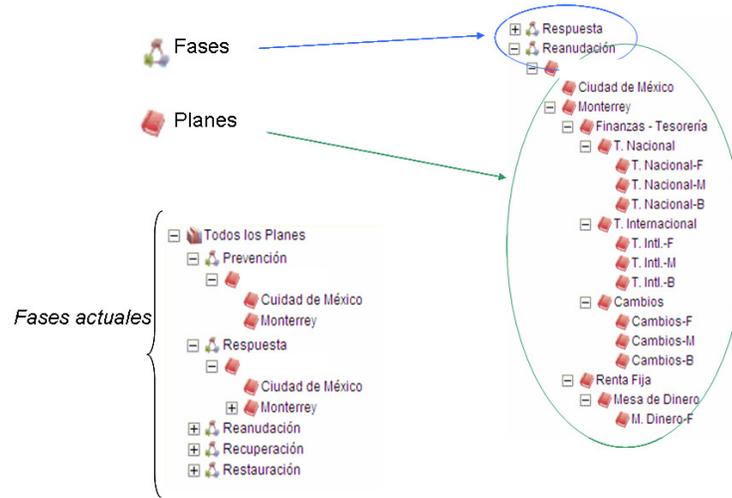


FIGURA 5.2: ESTRUCTURA DE DOCUMENTACIÓN DE FASES DE ACTIVACIÓN DRP

5.1.4 Organización de los Planes / Recursos

Cada uno de los planes se agrupa en los siguientes grandes rubros en los cuales se detalla información de personal, teléfonos, equipos, activos, etc. Y finalmente se ligan a los procesos, los cuales a su vez se separan por áreas de control.

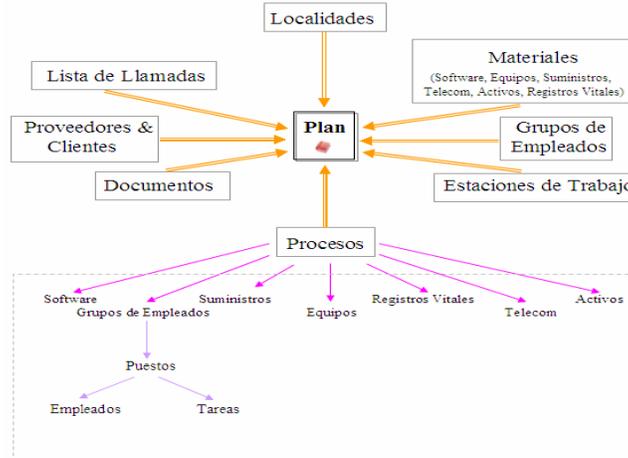


FIGURA 5.3: ESQUEMA DETALLE DE INSUMOS EN LA INVOCACIÓN

5.1.5 Organización de los Planes / Recursos

La organización para la localización detallada de la documentación es a nivel área y es organizada en forma jerárquica para su fácil entendimiento. La herramienta genera esta organización y tiene los flujos para su revisión y seguimiento.

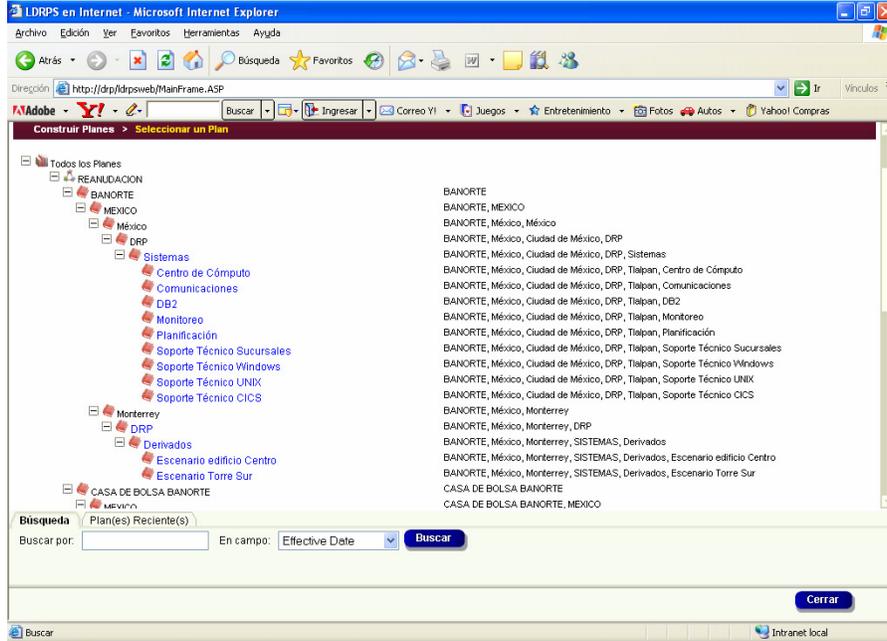


FIGURA 5.4: PANTALLA SISTEMA DOCUMENTAL DRP

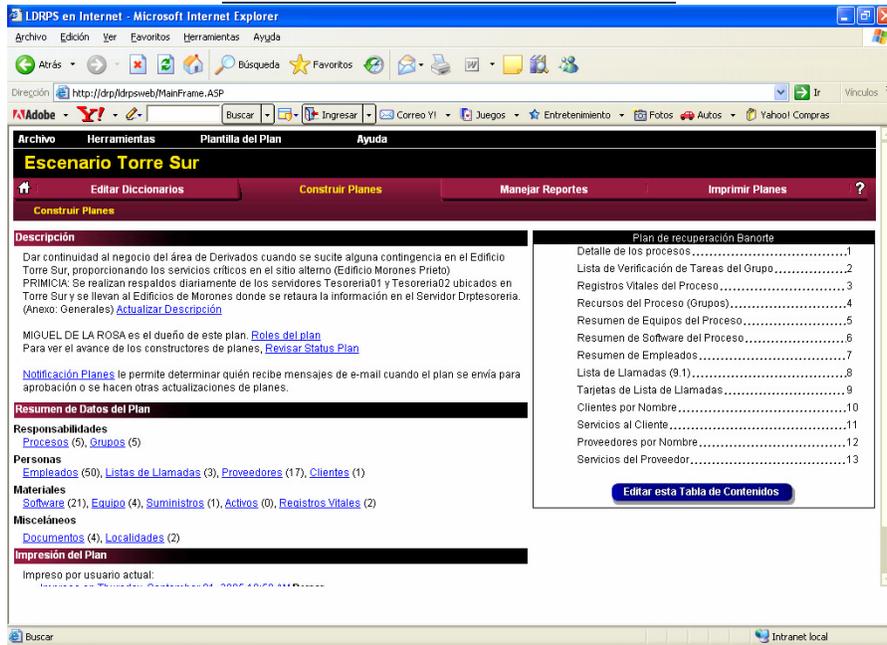


FIGURA 5.5: ORGANIZACIÓN DOCUMENTAL

5.1.6 Organización de los Planes / Recursos

Dentro de la planificación de los recursos hay una apartado especial asociado a los edificios corporativos en donde se detalla las acciones que cada edificio debe tomar en caso de un desastre, el mismo proyecto creó un sub-proyecto para la creación de áreas especiales en el centro de computo principal que pudieran albergar a personal y utilizarlo como centro temporal de emergencias. Este centro temporal ha tenido mucho éxito debido a que varias veces ha sido usado por problemas en el acceso a otros edificios corporativos.

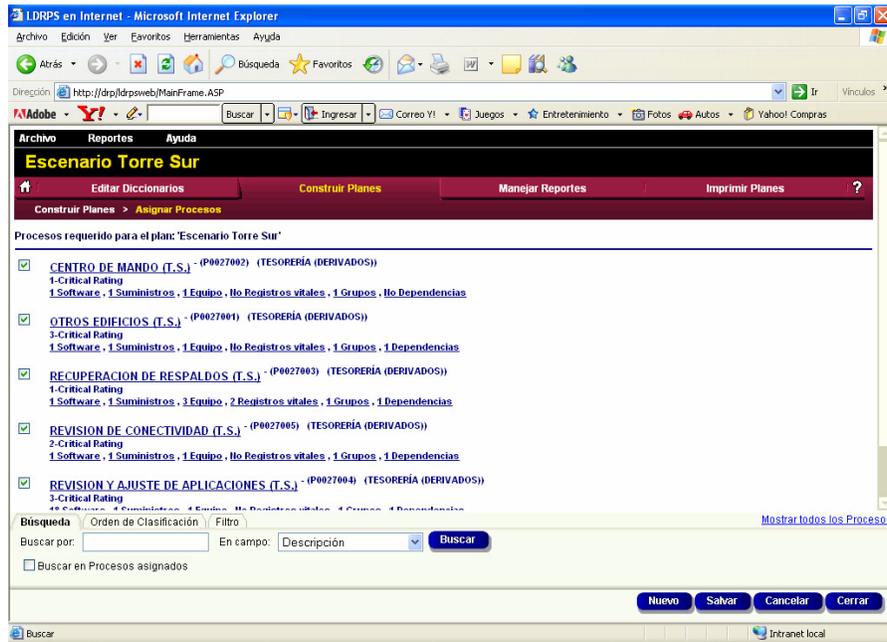


FIGURA 5.6: EJEMPLO DE PÁGINA DE ACCESO A DOCUMENTACIÓN DE PROCESOS



6. CONCLUSIONES

El plan de continuidad del Negocio es el procedimiento principal que contiene no solo los aspectos técnicos sino los humanos, operativos, comerciales, etc., es decir es el plan que todo empleado debe seguir en caso de la contingencia, este plan es muy amplio y da todos los lineamientos para reemprender la operación de un centro de datos y del negocio en una forma expedita, sin riesgos y lo más importante con toda la información.

Un punto dentro del BRP(Plan de continuidad del Negocio) es el DRP el DRP que nos compete es el tecnológico que implica como afrontaremos tecnológicamente la recuperación de los sistemas en caso de un desastre, y en ese caso se presentó el proceso de evaluación que nos permitió revisar varias propuestas que consideraban desde, casos de recuperación usando cintas y posible pérdida de días de datos a otras propuestas más avanzada como la copia de datos asíncrona, que implica levantar en días pero con menor pérdida de datos, y la propuesta final que se diseño, propuso y construyo basada en sincronía de datos, que implica levantar en horas y pérdida de datos mínima.

Este proyecto genero una de las soluciones de DRP más avanzadas de la industria.

- ✚ Proyecto realizado para garantizar la recuperación de los servicios críticos e información ante un incidente grave que afecte su infraestructura principal.
- ✚ Objetivo: mitigar efectos negativos que una disrupción grave pueda generar a los clientes y a la misma institución
- ✚ Más que nunca el centro de Datos del Banco Mexicano más importante lo distingue como institución segura y confiable.

“La información es textualmente el patrimonio de los clientes”

En este contexto, podemos señalar que el centro de Datos de este Banco cuenta hoy con una de las soluciones de recuperación de su plataforma informática más avanzada dentro de su industria a nivel internacional, lo que lo convierte en conjunto con otros avances tecnológicos emprendidos (Virtualización), en una de las instituciones financieras más seguras y confiables en el mercado de nuestro país. Esta afirmación se fundamenta en publicaciones en internet, casos de referencia de Gartner Consulting Group en donde se hace amplia referencia a este caso.

El proyecto de Recuperación en Caso de Desastre de la Infraestructura principal fue desarrollado para que en caso de que acontezca un incidente grave se garantice el funcionamiento de los servicios, y más importante, la integridad y disponibilidad inmediata de la información de usuarios de estos sistemas ya sean internos (empleados) o externos (clientes, empresas).

Este proyecto fue una estrategia que el área de tecnología del banco emprendió para abordar una de las iniciativas institucionales más relevantes, el plan de continuidad de negocio o BCP (Business Continuity Plan) que persigue mitigar los efectos negativos que una disrupción grave en los sistemas pudiera generar a sus clientes y al mismo banco, afectando el logro de planes estratégicos, su reputación, las operaciones, liquidez, calidad crediticia, posición de mercado y cumplimiento con las leyes y normativas vigentes.

El objetivo buscado es asegurar a los clientes, usuarios y accionistas la seguridad de que ante un incidente grave, el banco continuará sus operaciones brindando el servicio asegurando la continuidad y protegiendo los datos.

El desarrollo del proyecto se siguió bajo las bases de las metodologías estándares de proyectos (ISO100006) que siguen siendo vigentes y ampliamente usadas desde las revisadas en clase de ingeniería en computación en la UNAM, hasta las que usan grandes firmas de consultoría para la implementación de proyectos de tecnología simples y complejos. En el siguiente diagrama esquematizó en forma muy resumida el modelo que seguimos en este proyecto.

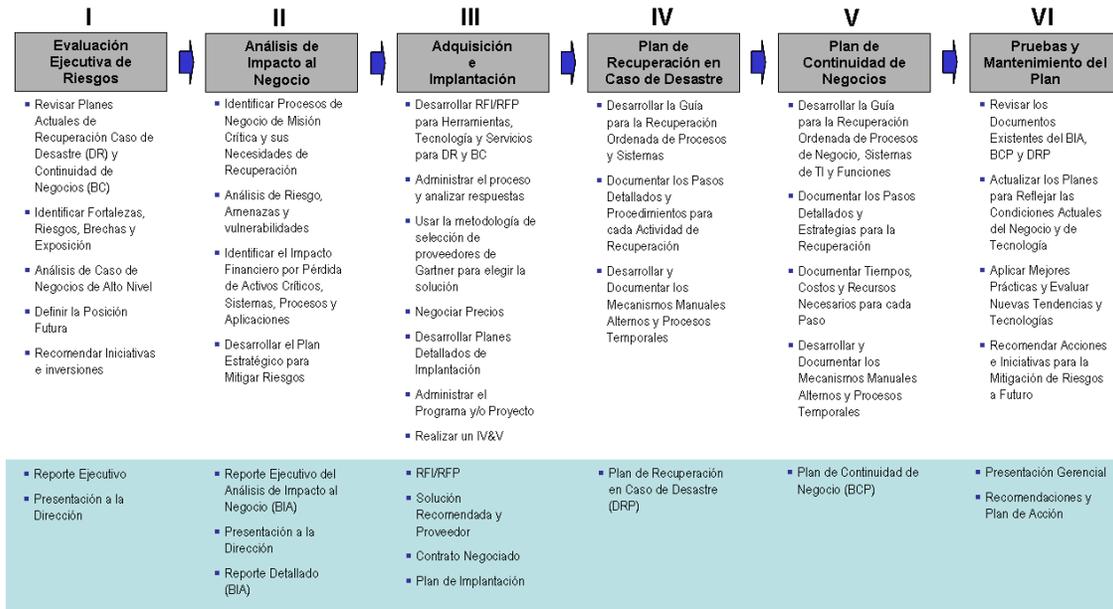


FIGURA 6.1: RESUMEN ESQUEMÁTICO DE TODOS LOS PROCESOS SEGUIDOS EN EL PROYECTOS

6.1 Características finales del Proyecto.

En el proyecto se aprovecharon todas las ventajas de la tecnología actual más avanzada en los temas de HW, almacenamiento, redes de datos y de fibra y finalmente la consolidación; sacando partido al máximo de:

- la experiencia acumulada durante los últimos años
 - Lo que se debe hacer, y lo que no.
- el empleo de las tecnologías más avanzadas disponibles
 - Almacenamiento.
 - Procesamiento.
 - Transmisión.

El proyecto cubrió alcances y requerimientos sumamente exigentes:

- Tiempo de recuperación (RTO – Recovery Time Objective): 4 horas máximo.
- SIN PÉRDIDA ALGUNA DE INFORMACION (RPO – Recovery Point Objective) : 0 min.
- De fácil operación.
- Siempre vigente y de simple mantenimiento.

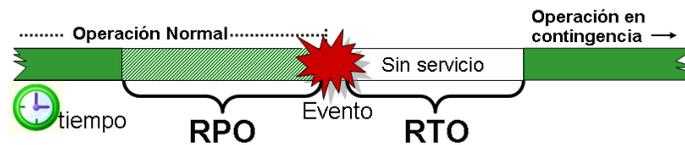


FIGURA 6.2: REQUERIMIENTO DE RPI Y RTO FINAL

En conjunto con proveedores líderes en el mercado en cada una de las tecnologías (IBM; HP, Hitachi, CISCO, EMC, ORACLE, TELMEX), se diseñó y construyó un esquema de recuperación innovador de los servicios informáticos centrales aprovechando las tecnologías más avanzadas de almacenamiento, procesamiento y transmisión de información existentes y buscando cubrir con los parámetros más exigentes:



Un tiempo de recuperación de 4 horas máximo una vez puesto en marcha el mecanismo de recuperación.

Sin pérdida alguna de información.

6.2 Habilitación de un centro de cómputo de recuperación espejo (hot site)

- Ubicado en zona a no más de 40 Km de distancia del centro principal:
 - Infraestructura de suministro eléctrico y de telecomunicaciones diferente.
 - En zona de baja sismicidad.
 - Cuidando que los circuitos de suministro eléctrico y centrales de comunicaciones no tengan dependencia o relación alguna con los que dan servicio al centro de cómputo principal.

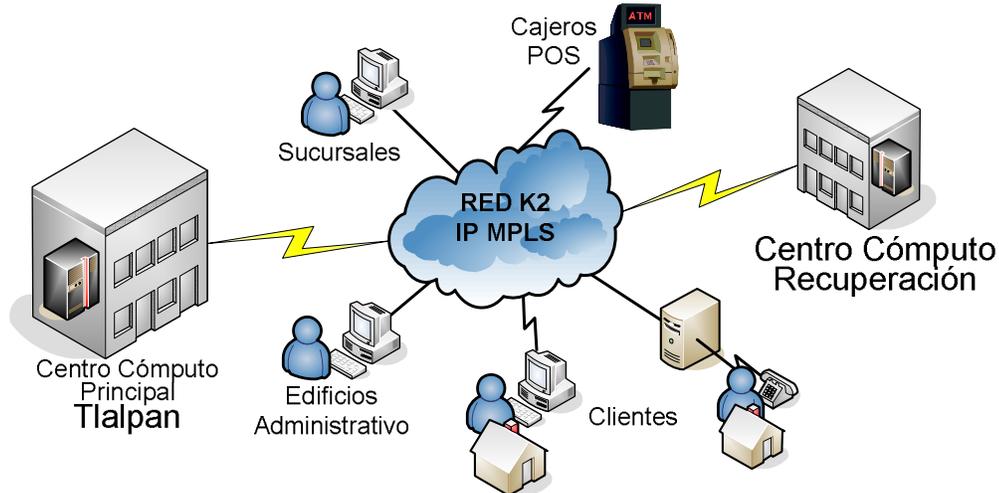


FIGURA 6.3: ESQUEMA DE DRP CON SITIO ESPEJO, REPLICA SÍNCRONA

6.3 Consolidación de la información en un sistema de almacenamiento único

- Aprovechando las excelentes facilidades de virtualización de almacenamiento existentes.
- Todas las plataformas incluidas:
 - Mainframe, UNIX, Windows, Linux.
- Incluyendo:
 - Información (archivos, bases de datos, etc.).
 - Sistemas operativos.
 - Aplicaciones.
- Mejoras en la velocidad de acceso (paso de 1gb a 8gb) y disponibilidad (Se crearon cluster de Alta Disponibilidad que incrementan a 99,9 la disponibilidad del equipo).

Se realizó la consolidación de la totalidad de la información contenida en cada plataforma existente en el banco y sus filiales en un mismo sistema de almacenamiento (HITACHI), esto gracias a las capacidades de virtualización de los equipos de tecnología reciente, que además cuentan con avanzadas características de seguridad, disponibilidad, confiabilidad y velocidad de acceso.

Esto no solo incluye la información como archivos y bases de datos, sino también los sistemas operativos y las aplicaciones.

6.4 Cada dato actualizado es reflejado en la infraestructura de almacenamiento en ambos centros al mismo tiempo (replica síncrona)

- Día y noche, durante el servicio en línea y el batch

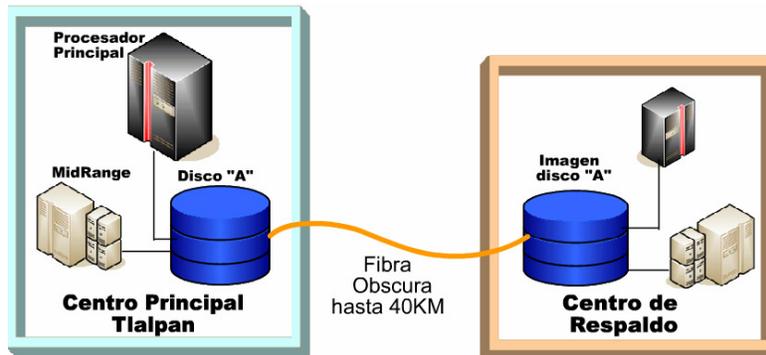


FIGURA 6.4: ESQUEMA REPLICACIÓN SÍNCRONA CONTINUA

Lo que distingue a esta solución de recuperación como una de las más efectivas y modernas de la industria financiera, fue la simplificación administrativa técnica que se gestionó al reducir la cantidad de equipos y sistemas a administrar (en el comité de la Comisión Nacional Bancaria y de Valores se presentó el modelo y se valoró como la mejor implementación de DRP en la banca mexicana), toda actualización efectuada a la información contenida en el sistema de almacenamiento central, es reflejada de forma automática y en milisegundos en una configuración similar instalada en el nuevo centro de cómputo de respaldo de la institución Financiera. A esto se le conoce como “replica síncrona”, la cual sólo es posible mediante la integración y articulación de las más modernas tecnologías de procesamiento y comunicación de datos, además del uso de fibra óptica dedicada para resolver así el inmenso ancho de banda que requiere la actualización de información de millones de transacciones que esta institución Financiera opera durante su jornada diaria.

Así, garantizamos que en una remota eventualidad cuyo desenlace represente la inhabilitación del centro de cómputo principal, toda la información hasta el último segundo esté actualizada y lista para ser usada en el centro de cómputo de respaldo, incluida también la contenida en cartuchos magnéticos producida en el transcurso de los procesos de actualización nocturna (SUN).

Como ventaja adicional, este mecanismo de replicación simplifica las actividades de mantenimiento del esquema de recuperación ya que también la actualización de nuestras aplicaciones que se realiza frecuentemente para proveer a la clientela de servicios innovadores, es reflejada de igual forma en la infraestructura de respaldo manteniéndose siempre lista y actualizada.

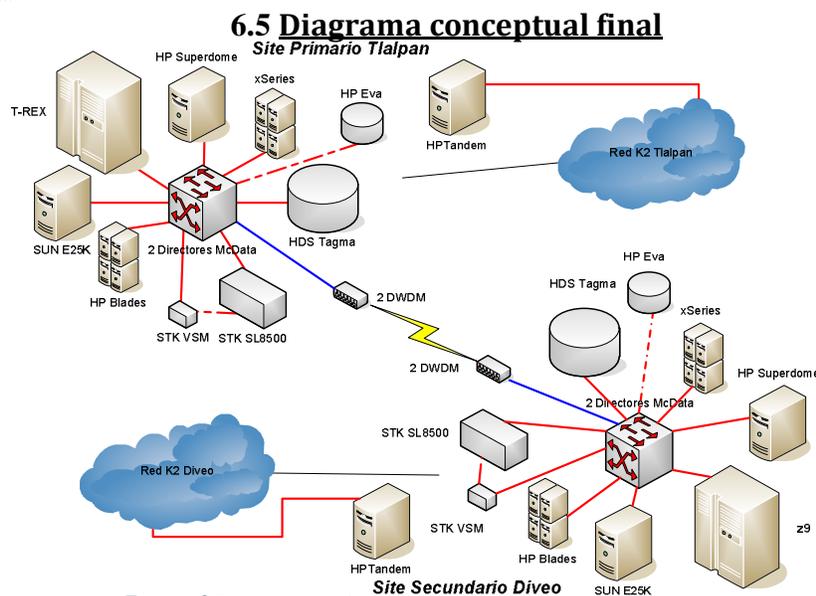


FIGURA 6.5: ESQUEMA TÉCNICO SOLUCIÓN SITIO ALTERNO REPLICA



Ventajas

- ✦ No hay pérdidas de información al momento de un incidente.
- ✦ La información es consistente al través de todas las plataformas; no es necesario articular complejos puntos de sincronía entre ellas.
- ✦ Las aplicaciones y sistemas están siempre actualizados en el centro de respaldo:
 - Mantenimiento simple del esquema.
- ✦ Para extender el esquema de respaldo a nuevos servicios basta con:
 - incluirlos en el sistema de almacenamiento.
 - Proveer la capacidad de procesamiento de respaldo.

6.6 Todos los edificios y sucursales enlazados a través de red IP con los centro de cómputo

- ✦ Conmutación automática de la red conforme se anuncian las mismas direcciones IP desde el Centro de Cómputo de respaldo

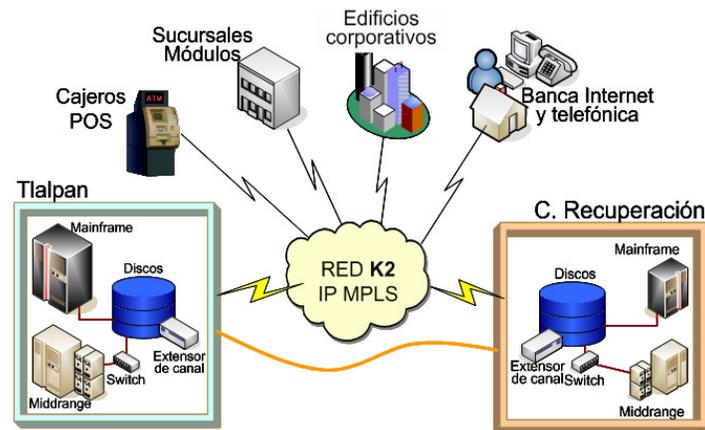


FIGURA 6.7

El banco cuenta con una red de comunicaciones que conecta la totalidad de sus sucursales y edificios corporativos incluyendo al centro de cómputo principal. Esta está basada en una red privada virtual (Telmex) que maneja protocolo IP y esquemas de manejo de calidad de servicio sobre MPLS.

El centro de respaldo es un nodo más, posibilitando así que al momento de ser necesario toda la comunicación del Banco sea conmutada dinámicamente de forma transparente y automática a esté sin la necesidad de realizar cambios en la infraestructura de telecomunicaciones de cada edificio u oficina.

Al momento de requerirse, las direcciones de los servidores en el centro de cómputo principal, de un momento a otro se anuncian desde el centro de respaldo conforme éste se activa lo que construye dinámicamente las nuevas rutas de comunicación.

6.7 Aprovechamiento de los esquemas de contratación y licenciamiento basados en capacidad bajo demanda

- ✦ Instalación de equipos con la capacidad de procesamiento total pero con una fracción de la capacidad activa.
 - Reduce notablemente el costo de construcción del esquema de recuperación:
 - Costo de Hardware.
 - Licenciamiento de software.
 - Capacidad activa dedicada a cargas de los ambientes de desarrollo y calidad.
 - La capacidad total se activa en minutos a través de una llave de micro código.



A través de los nuevos esquemas de contratación de crecimiento bajo demanda, se ha hecho posible el instalar equipos con la capacidad de procesamiento total pero con una fracción de la capacidad activa lo que reduce notablemente el costo de construcción del nuevo esquema de recuperación. Al momento de ser requerida, la potencia de los equipos de respaldo es incrementada hasta cubrir la equivalente a la capacidad normal en producción simplemente con la activación de una llave de micro código aplicada al momento.

6.8 Uso de tecnologías de virtualización de procesamiento

- ✚ Independencia el tipo de servidor
 - Mitigar la problemática relacionada con la diversidad de servidores para Windows
 - Elemental para mantener la compatibilidad de la infraestructura de ambos centros
- ✚ Mejor aprovechamiento del hardware de procesamiento
 - Es posible ir incluyendo servidores virtuales a un equipo físico mientras la capacidad de cómputo y memoria lo permitan, en el pasado si un sistema de poca demanda usaba un equipo la capacidad ociosa no era factible reutilizar.

ESTATUS ACTUAL

El proyecto finaliza en 2006 en su totalidad con la inclusión de todas las aplicaciones y equipos.

En todos los casos los equipos fueron adquiridos bajo el esquema de arrendamiento puro, lo que permitió que en 2010 se volviera a presentar un proyecto de renovación tecnológica con inversión adicional de \$0 pesos y una ligera reducción del flujo en el gasto, con un incremento de más del doble de la capacidad de cómputo.

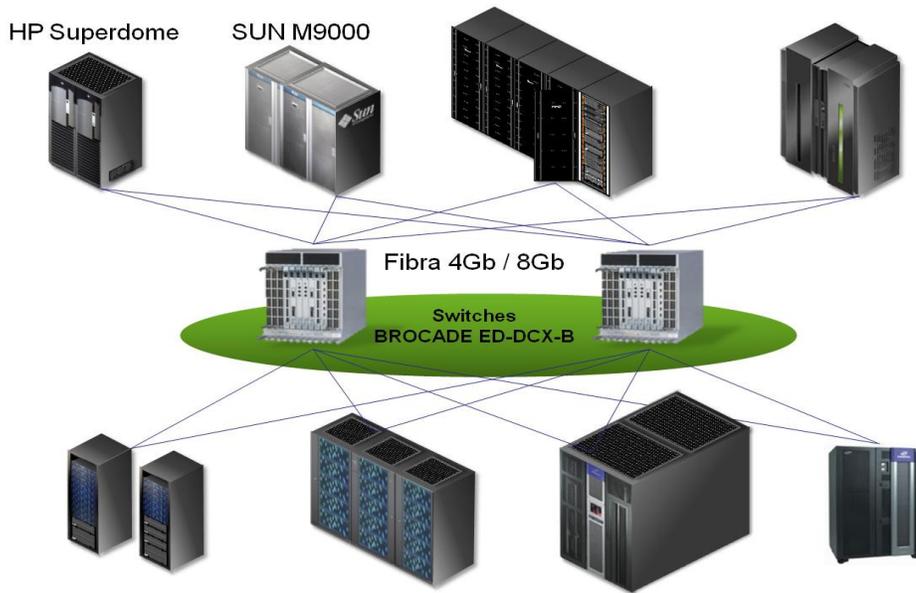
En este proyecto simplemente se planteo continuar con los mismos flujos de gastos de arrendamiento pero buscar el cambio tecnológico de las siguientes infraestructuras buscando una capacidad del 100% superior a lo que hoy se tenía con la idea de soportar 4 años.

- Almacenamiento Central pasa de 120TB a 240TB.
- Equipos Intel pasan de 900 Cores a 1792 Cores (Pero se reduce de más de 100 servidores a 56).
- Equipos UNIX M9000 pasan de 3 a 2.
- Directores de 516 Puertos.
- DWDM's con 8 lamdas 40GB.
- Equipo Central de Z9 a Z10.
- Equipos de respaldos de AMS1000 100TB a AMS2500 260TB.

En muchos de los casos los flujos fueron reducidos hasta en 10%(caso Intel), y se obtiene un crecimiento de capacidad para los próximos 4 años (no se considera nuevos proyectos).

- ✚ Gracias al aprovechamiento de las tecnologías recientes de almacenamiento y otras, se hace posible para la institución Financiera logre una reducción en el RTO:
 - RTO = 3 horas.
 - RPO = 0 información pérdida.
 - Sistemas y aplicaciones siempre actualizadas en el centro de recuperación.
 - Se mantiene el esquema de fácil mantenimiento y crecimiento.
 - Esquema de recuperación local.

Finalmente agradecer sin lugar a duda toda la enseñanza recibida durante mi educación universitaria que me ha permitido en estos años de trabajo ir utilizando todas las herramientas y conceptos aprendidos los cuales son validos 100% en cualquier ambiente tecnológico.



A continuación se presenta un esquema gráfico de cómo se logra una evolución tecnológica total de toda la infraestructura aprovechando proyectos de renovación y crecimiento de infraestructura y que nos ayudo a asegurar la continuidad de los servicios de la empresa donde laboro. El reto continúa y todos los días trato de mejorar y aportar para lograr convertirlo en una empresa tecnológicamente reconocida en México y el mundo.



- 56 RACKS Intel
- 1,406 m2 Área de centro de cómputo (Incluye Operadores y Cintoteca)
- 1 Equipos SUN 15K
- 2 Equipos HP Superdome, 27 Equipos SUN varios Modelos, 52 Equipos HP V, K, L, R
- 2 Tandems
- 1 Equipo Central, 2 Discos Centrales, 1 STK Respaldos
- 12 Modulos de discos centrales, fibra, NAS, SAN, Direct Atach.

FIGURA 6.8: ESTRUCTURA E INVENTARIO DE INFRAESTRUCTURA 2004

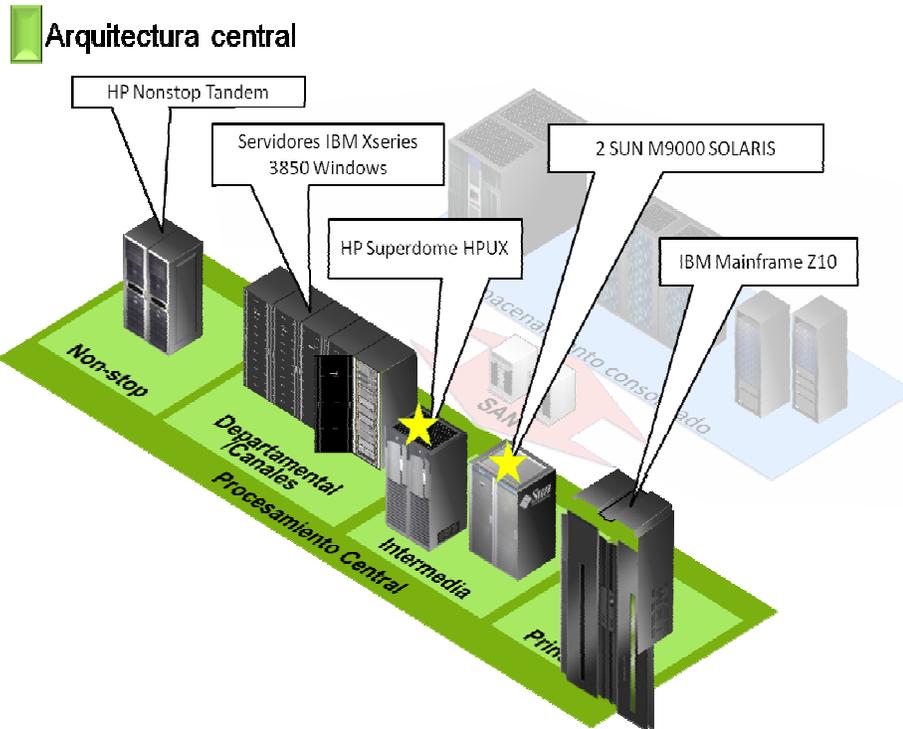


FIGURA 6.10: INVENTARIO DE EQUIPO EN EL SITIO PRINCIPAL 2011

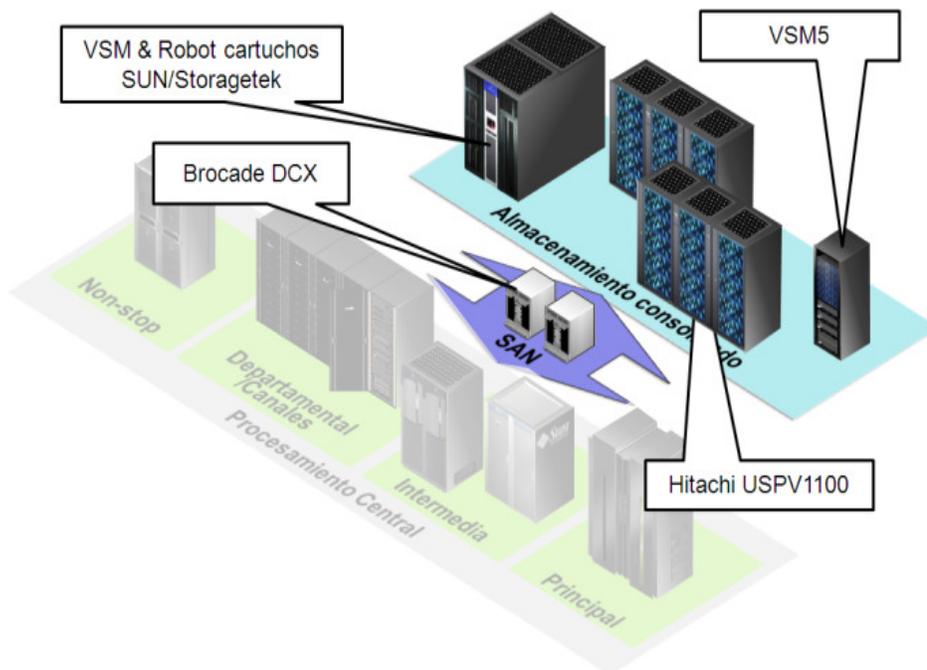


FIGURA 6.11: INVENTARIO DE ALMACENAMIENTO CENTRAL ACTUALIZADO



Reconocimientos y Menciones del Proyecto:

26 March 2007

Roberta J. Witty Kristen Noakes-Fry

Banorte implemented and tested a comprehensive disaster recovery strategy that limits disruptions to the business units. Enterprises in Latin America and elsewhere can learn from Banorte's success.

Marzo 2011

Virtualización EX5, la nueva forma de virtualizar y hacer más eficientes los datos - Salvador Sierra
<http://www.industrytrendforum.com/presentaciones/?did=36>

Referencias:

Pink Elephant Consultant, ITIL Fundamentos de la administración de Servicios de TI, Ed.2007.

Gartner Inc., Document DRP Fundamental and Analysis Houston Summit 2003

OGC, Service Strategy ,ITIL – IT Service Management, 2007

Van Bon J and Hoving W. SAME – the Strategic Alignment Model Enhanced. ITSM PORTAL, 2007.

Van der Hoven DJ, Hegger G, van Bon J. 'BII: Beheer van de interne informatievoorziening'. In: IT Beheer Jaarboek 1998, Ten Hagen and Stam, 1998.

Wijers G, Seligmann PS and Sol HG. The Structure of IS Development Methods: a Framework of Understanding. SERC and Delft University of Technology, 1992

Kendall Kenneth ,Análisis y diseño de sistemas Ed 1991

Jeffrey L Whitten, Análisis y diseño de sistemas de Informacion Ed. 1993

Gartner, Evaluación de Riesgo de TI, Análisis de Impacto al Negocio y Estrategia de Recuperación en Caso de Desastre, Reporte 2008 Institución Financiera.

Maggie Keneller, The Benefits of ITIL,2010

Hitachi Data Systems,HotBusiness Continuity and the Hitachi Tagmástore, 2009

Hitachi Data Systems Universal Storage Platform Hitachi Data Systems red paper WHP-163 2010.

Hitachi Data Systems, Hitachi Universal Replicator Advanced Technology.

Addressing Federal Government Disaster Recovery Requirements with Hitachi Freedom Storage

Jon William Toigo, Disaster Recovery Planning (3rd Edition) by Jon William Toigo ISBN

Andrew Hiles, Business Continuity: Best Practices (2nd Edition) by ISBN

Web Sites

Contingency Planning and Management <http://www.contingencyplanning.com/>

Continuity Central <http://www.continuitycentral.com/>

Disaster Recovery Journal <http://www.drj.com/>

DRI International (Disaster Recovery Institute) <http://www.drii.org/>