UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERIA INDUSTRIAL Y SISTEMAS

"CENTRO DE COMPUTO ALTERNO EN LA BANCA COMO BASE PRINCIPAL DEL PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)"

INFORME DE SUFICIENCIA PARA OBTENER EL

TITULO PROFESIONAL DE

INGENIERO DE SISTEMAS

VICTOR RAUL SEDAMANO AMAO

LIMA – PERU

2004

DEDICATORIA:

El presente trabajo es dedicado a mis padres que me dieron todo su apoyo y confianza para seguir mis estudios superiores en esta Universidad y finalmente lograr su cometido, ser un profesional del nivel de esta casa de estudios.

AGRADECIMIENTO:

Un agradecimiento a mi Centro de Trabajo por el apoyo incondicional en el desarrollo de mi carrera profesional así como a mis colaboradores en llevar adelante este proyecto y en forma muy especial a las personas que me apoyaron a seguir adelante con el desarrollo del presente trabajo con su apoyo, asesoría, consejos y correcciones.

INDICE GENERAL

DESCRIPTOTES TEMATICOS

CCA

Centro de Computo Alterno

PCN

Plan de Continuidad de Negocios

PCI

Plan de Continuidad Informático

Recuperación de Desastres

Data Center

Computador Central

Servidores

Replicación

Riesgos

Auditoria

Contingencia Informática.

Infraestructura.

RESUMEN EJECUTIVO

El Banco del Dinero tienen en cuenta que el entorno bancario en el que se desenvuelve es cada vez mas cambiante y competitivo lo cual se ve a través de la sofisticación de los productos ofrecidos, la calidad de servicio a los clientes, la alta competitividad, los márgenes de ingresos mas reducidos, la globalización, las nuevas tecnologías, los riesgos, fraudes, amenazas y otros factores mas, hace que este tipo de negocio sea mas complejo y vulnerable; es por esto que para tener los servicios ofrecidos siempre disponibles y confiables hace que la recuperación y continuidad operativa de sus operaciones sea un punto esencial para la protección del negocio.

Adicional a los factores descritos anteriormente hoy en la actualidad hay una normativa dada por la entidad gubernamental que supervisa a los Bancos, la Superintendecia de Banca y Seguros, quien a emitido la Resolución SBS Nro. 006-2002 y la Circular Nro. G-105-2002, donde su objetivo es propender a que las empresas supervisadas cuenten con un sistema de control de riesgos que les permita identificar, medir, controlar y reportar los riesgos que enfrentan con la finalidad de proteger los intereses del público o clientes quienes son la razón de ser del negocio bancario. Entre los riesgos que se describen y enfrentan las empresas

supervisadas en el desarrollo de sus actividades se encuentran los riesgos de operación, los cuales pueden generarse por deficiencias o fallas en la Tecnología de la Información (TI), que actualmente se a convertido para los bancos el centro principal de su información, procesos y sistemas de atención hacia los clientes. Finalmente la SBS trata de establecer criterios mínimos prudenciales para que las empresas supervisadas realicen de manera adecuada la gestión de dichos riesgos en forma obligatoria y siguiendo un marco basado en las normas internacionales muy similares a la que describe la norma ISO17799.

En tal sentido el Banco del Dinero sensible a esta realidad decidió desarrollar su plan de Recuperación de Desastres (Disaster Recovery), implementando su Centro de Computo Alterno en una ubicación especializada para este tipo de implementaciones (Data Center), la cual esta en una ubicación remota , a suficiente distancia para no verse comprometida ante un daño o desastre en el centro principal de procesamiento.

Describiendo brevemente un poco de historia en el proceso de contingencia del computador central, se puede decir que el Banco desde hace muchos años atrás, conciente de la importancia de brindar un servicio de alta disponibilidad a sus clientes y usuarios, decidió adquirir un computador de respaldo o contingencia con iguales características al computador principal ubicado en el mismo Centro de Computo del Banco. Dos años mas tarde se dio cuenta que se necesitaba tener la data replicada al instante que ocurrían las operaciones y/o transacciones en el

computador central así como tener un menor tiempo de recuperación. Para ello adquirió un software de replicación en línea de las transacciones o ocurrencias del computador principal al computador de respaldo. Este contingencia implementada funcionó en varias oportunidades para el Banco. El siguiente paso a esta contingencia era tener un Centro de Computo Alterno remoto y ya se tenia las primeras intenciones dentro del Plan Estratégico del Banco, pero dado el avance tecnológico y crecimiento de las aplicaciones y sistemas ya no era simplemente el computador central sino que ya se contaba con Servidores críticos para el negocio.

Es por esto que dado avance tecnológico y el crecimiento de la plataforma tecnológica, los riesgos y normativas era necesario y mandatario que se implemente un centro de computo alterno tanto para el computador central y los servidores principales donde se ejecutan sistemas de negocio importantes para el Banco, esto implico el desarrollo de un proyecto de mediana magnitud pero de alto costo debido a los equipos involucrados, procesos, líneas y equipos de comunicación, medidas y políticas de seguridad, replicaciones o procedimientos de backups mas rigurosos.

El Banco para ello realizo una serie e visitas a proveedores y evaluaciones de propuestas para llevar a delante este proyecto, dada la evaluación y condiciones favorables para el Banco se eligió el Data Center de IBM como Centro de Computo Alterno para el Banco.

Este proyecto fue tomado por la alta dirección ejecutiva del banco en conjunto con el Comité ejecutivo de Riesgo y definió como primera etapa de la implementación del Centro de Computo alterno a los servicios mas imprescindibles para el negocio que involucra el Computador Central y Servidores críticos. Al ser este un primer paso en este esquema de contingencia, en el futuro pueden ser cambiados adicionando mas elementos críticos para que el Banco vaya considerando en sus evaluaciones constantes de riesgo y de esta forma garantizar una alta disponibilidad en los servicios que el Banco brinda a sus clientes.

INTRODUCCIÓN

El Banco cuenta con sistemas de negocio automatizados y para ello tiene un centro de procesamiento de información en su sede principal en la cual se encuentra el computador central que es el corazón de la información y de los sistemas que la procesan, siendo además el punto de integración de otros computadores o equipos de procesamiento, llámese estos servidores multipropósito para diversos servicios o sistemas que usa el Banco tanto para atender a sus clientes como para sus procesos internos. Todas las áreas estratégicas del Banco dependen de los sistemas de este procesador central, así mismo los diversos canales de venta o atención a clientes, como la red de agencias (llámese ventanillas), call center, banca por Internet, la red de cajeros automáticos, tarjeta de crédito así como las conexiones con terceros como la red Visa, la red Telebanco, Aduanas, Bolsa de Valores, Cámara de Compensación Electrónica, Banco Central de Reserva, Cavali, Certicom, Superintendencia de Bancos y Seguros, Sucursales del exterior, conexiones con proveedores de servicio como las compañías de Telecomunicaciones, servicios básicos y muchas otras conexiones dentro de la complejidad de servicios que brinda el Banco a sus Clientes.

Dado el nivel de importancia y complejidad del centro de computo descrito, el Banco cuenta con equipos en redundancia ubicadas dentro de la misma oficina principal, políticas estrictas de backup, software de replicación en línea y una serie de medidas de seguridad física, lógica, procedimientos y políticas necesarias para salvaguardar este centro de Procesamiento.

Por otro lado la alta Dirección del Banco al desarrollar su plan estratégico tiene como uno de sus grandes objetivos y tareas el de la Evaluación de Riesgos de Operaciones dentro del cual se encuentra el Riesgo de Tecnológico y para identificar, analizar y mitigar estos riesgos nace el Plan de Continuidad del Negocio (PCN), que contiene al Plan de Continuidad de Informática (PCI), cuya acción principal es reducir el riesgo del Centro de Computo y dada las medidas actuales es necesario implementar un Centro de Computo Alterno (CCA) en una ubicación remota como estrategia de recuperación, de tal manera que si ocurriera un desastre (incendio, inundación, vandalismo, terremoto, etc.), en el centro de procesamiento actual, se active en el menor tiempo posible el Centro de Computo Alterno, para continuar las operaciones del Banco atendiendo a los clientes, usuarios internos del Banco, Canales de Venta y/o empresas que tienen relación de negocios y supervisión con el Banco.

Por ello el presente trabajo tiene como objetivo desarrollar el proyecto de Implementación del Centro de Computo alterno, para lo cual se describirá mas adelante la metodología de Gerencia de Proyectos Informáticos que se uso para

llegar a buen termino de los objetivos y metas establecidas dentro de su marco conceptual y diseño.

Dentro del desarrollo se describirán las salvaguardas que se consideraron luego de una evaluación de riesgos donde se consideraron los siguiente pasos básicos, Identificar los activos de TI, Evaluar las Amenazas, Evaluar la Vulnerabilidades, Calcular el Riesgo, Determinar el Impacto, Seleccionar las salvaguardas y Documentar el riesgo residual.

Al lograrse la implementación de este Centro de Computo Alterno, el Banco adquiere un alto valor ante los frentes externos, como las clasificadoras de riesgos, tener una imagen de confianza, las aseguradoras y los accionistas extranjeros. De igual modo se cumple con la normativa dada por la entidad supervisora de los Bancos, la Superintendecia de Banca y Seguros, que se encuentra en la Resolución SBS Nro. 006-2002 (anexo 1) y la Circular Nro. G-105-2002 (anexo 2), cuyo objetivo es propender a que las empresas supervisadas cuenten con un sistema de control de riesgos que les permita identificar, medir, controlar y reportar los riesgos que enfrentan con la finalidad de proteger los intereses del público o clientes quienes son la razón de ser del negocio bancario.

CAPITULO I

ANTECEDENTES

En esta etapa es importante llegar a conocer al Banco del Dinero en análisis para lo cual se hará una descripción en forma breve y precisa de tal forma que nos podamos familiarizar con la organización y tener un buen punto de vista del alcance de la solución planteada con este proyecto.

1.1 DIAGNOSTICO ESTRATÉGICO.

1.1.1 Breve descripción.

El Banco del Dinero, pertenece al sector bancario de nuestro país. Cuenta con 32 modernos centros de negocios en la ciudad de Lima, los cuales están perfectamente acondicionados para servir a los clientes con comodidad y agilidad, gracias a la consolidación de las inversiones realizadas en los últimos años en infraestructura y en sistemas informáticos de punta. Cuenta además con una Sucursal en la Republica de Panamá, internacionalizando mas aun las operaciones del banco, atendiendo los requerimientos de clientes privados y comerciales a través de servicios bancarios de primer nivel y apuntando

a la diversificación del fondeo. El Banco desde sus inicios se dirigió principalmente a los niveles o segmentos socioeconómicos A y B. Actualmente se encuentra en busca de nuevos mercados, por lo cual se esta incursionando en el segmento C. Tiene mas de 10 años en el sector bancario y es regulada por la Superintendencia de Bancos y Seguros.

El Banco como parte indispensable de su desarrollo, cuenta con Personal altamente capacitado y centrado en la adecuada, oportuna y eficiente satisfacción de las necesidades de sus clientes. En este sentido, resalta la creciente calificación del Banco del Dinero dentro de las 25 mejores empresas para trabajar en el Perú, hecho que ratifica el compromiso e identificación del personal con el Banco y con su responsabilidad de servicio hacia sus clientes.

El Banco del Dinero esta asociado con un banco extranjero de nivel internacional con presencia en mas de 50 países. Esta alianza estratégica es un compromiso de largo plazo y significa para sus clientes un sólido respaldo.

En suma, el Banco del Dinero ostenta los factores claves para el éxito, los cuales le permiten enfrentar al mercado competitivo en forma consolidada y con el claro objetivo de convertirse en un gran banco en cuanto a solidez, rentabilidad y liderazgo en servicio y en calidad de

activos, gracias al compromiso de sus accionistas y de su personal, así como de la confianza de sus clientes y bancos corresponsales en su diaria interrelación con el Banco.

1.1.2 Su enfoque : Rentabilidad y Eficiencia, buscado la Especialización

Lo cual significa básicamente :

Dirigirse a los negocios rentables en los que se puede tener una ventaja competitiva (no hay espacio para negocios que no son rentables).

Trabajar con eficiencia a todo nivel buen uso de los recursos con resultados positivos.

Ofrecer alta calidad de servicio : buen trato personal y agilidad en la atención y respuestas.

1.1.3 Elemento Diferenciador : La Calidad de su Servicio.

Basado básicamente en acciones simples y concretas

Buen trato personal.

Agilidad y rapidez en la atención (alta disponibilidad de los servicios).

Resolución efectiva de reclamos.

Buena y oportuna información.

1.1.4 Visión.

Ser el mejor banco para los clientes y un gran lugar de trabajo para su gente.

Esta visión simple y concreta enfocada en atraer y retener a los mejores clientes creando valor y lealtad, todo esto con ayuda de personal altamente comprometido con la visión.

1.1.5 Misión.

Ser un banco eficiente y rentable, enfocado en las personas y sus empresas, que se diferencia por su agilidad, la calidad de su servicio y el profesionalismo de su gente.

Como se puede apreciar la misión tiene un horizonte de planeamiento definido con carácter retador con orientaron a futuro.

1.1.6 Valores.

Definidos puntualmente en los siguientes

- Integridad
- Profesionalismo
- Equipo Humano
- Calidad de Servicio
- Eficiencia.

1.1.7 Objetivos.

Estos apuntan a :

- Mejorar la rentabilidad incrementando los ingresos.
- Incrementar el numero de clientes personales.
- Mejorar la clasificación de riesgo del Banco.
- Elevar el nivel de Eficiencia.
- Reducir la morosidad
- Mejorar la satisfacción de servicio al cliente y clima interno del banco.

1.1.8 Estrategias.

Lo que se a denominado las 7 estrategias capitales :

- Disciplinado enfoque estratégico
- Agresividad en ventas
- Estricto control de riesgos.
- Calidad humana
- Pasión por el servicio
- Procesos ágiles y modernos.
- Obsesión por la eficiencia.

A continuación con lo descrito en los puntos anteriores pasaremos a Formular el análisis del entrono tanto en el ámbito interno como externo para el Banco usando el análisis FORD.

1.1.9 Fortalezas.

- Buena calidad de cartera de clientes
- Accionariado conformado por un grupo sólido
- Socio Estratégico
- Buena imagen y prestigio entre los clientes y el entorno de estos
- Buen nivel de automatización
- Amplia capacidad de procesamiento
- Bajos costos operativos
- Personal gerencial y ejecutivo capacitado y con experiencia en banca
- Trato amable y cortesía con el cliente
- Personal identificado con el banco
- Gente joven y adaptable
- Buena clasificación de riesgo

1.1.10 Debilidades

- Red de agencias insuficiente
- Limitación en canales de distribución (Banca Electrónica)
- Estructura organizacional con tendencia a burocratizarse y jerarquizarse
- Falta de banca de inversión
- Sistema de Información Gerencial básico.
- Escasa delegación de autoridad para decisiones de riesgo

- ❖ Mitigar los riesgos develados del estudio de Riesgo Operacional.
- ❖Falta de divulgación y conocimiento de productos del banco por clientes y empleados
- ❖ Insuficiente percepción de procesos integrales
- ❖ Falta mayor trabajo en equipo
- ❖ Fuerza de ventas básico y tradicional.

1.1.11 Oportunidades

- ❖ Captación de clientes insatisfechos de la gran banca
- ❖ Desarrollo del Segmento de la Microempresa y PYMES
- ❖ Desarrollo de Comercio Exterior
- ❖ Desarrollo de Mercado de Capitales
- ❖ Desarrollo de Banca Personal y Privada
- ❖ Desarrollo del Cash Management para empresas
- ❖ Mayor acceso a tecnología de punta
- ❖ Desarrollo del mercado de MIVIVIENDA
- ❖ Integración a la red del Banco extranjero socio.
- ❖ Know How del Banco Socio con experiencia de mas de 150 años.
- ❖ Clientes que trabajan con un solo banco
- ❖ Firma del Tratado del APTA
- ❖ Explotación del Gas de Camisea
- ❖ Continuar comprando cartera de Bancos que están reduciendo su accionar en el mercado bancario peruano.

- Explotar la buena e imagen y calificación como Banco en el entorno de negocios.
- Diversos proveedores de Data Centers locales.

1.1.12 Riesgos

- Sobre exposición a devaluación dada por la dolarización de la cartera
- Incremento de Banca Extranjera
- Descalce de Activos y Pasivos
- Volatilidad de mercados internacionales
- Crisis Económicas de mercados externos como: Brasil y Argentina
- Falta de un Centro de Computo Alterno para caso de desastres.
- Regulaciones del Ejecutivo – Tributarias
- Regulaciones de la entidad supervisora (SBS)

1.2 DIAGNOSTICO FUNCIONAL

1.2.1 Productos.

Brevemente pasaremos a enumerar los productos y servicios :

- Banca Minorista :
  - Tarjeta de Crédito
  - Financiamiento Pequeña Empresa
  - Productos Pasivos
  - Pagos y Cambios

- Créditos Hipotecarios
- Banca Seguros

❖ Banca Comercial :

- Financiamiento de Ventas.
- Leasing
- Financiamiento Inmobiliario.
- Comercio Exterior
- Cambios
- Programa para Proveedores

❖ Banca Transaccional

- Agencias
- Cash Management (Pagos, Cobranza e Información)
- Cambios
- Comercio Exterior
- Servicios Varios

❖ Otros:

- Mesa de Distribución.
- Banca Privada
- Servicios Fiduciarios.

1.2.2 Clientes

Los clientes están segmentados en los siguientes mercados objetivos:

- ❖ Banca Personal : Personas del nivel socioeconómico Ay B con fuerte tendencia a entrar al nivel socioeconómico C.
- ❖ Pequeña Empresa : Empresas y negocios con ventas anuales de $50 m hasta $1mm.
- ❖ Banca Empresarial : Empresas con ventas anuales de $1mm hasta los $20mm.
- ❖ Tesorerita : Corporaciones, Instituciones, Empresas, Personas.
- ❖ Banca Transaccional : Corporaciones, Institución, Empresas, Personas.

1.2.3 Proveedores

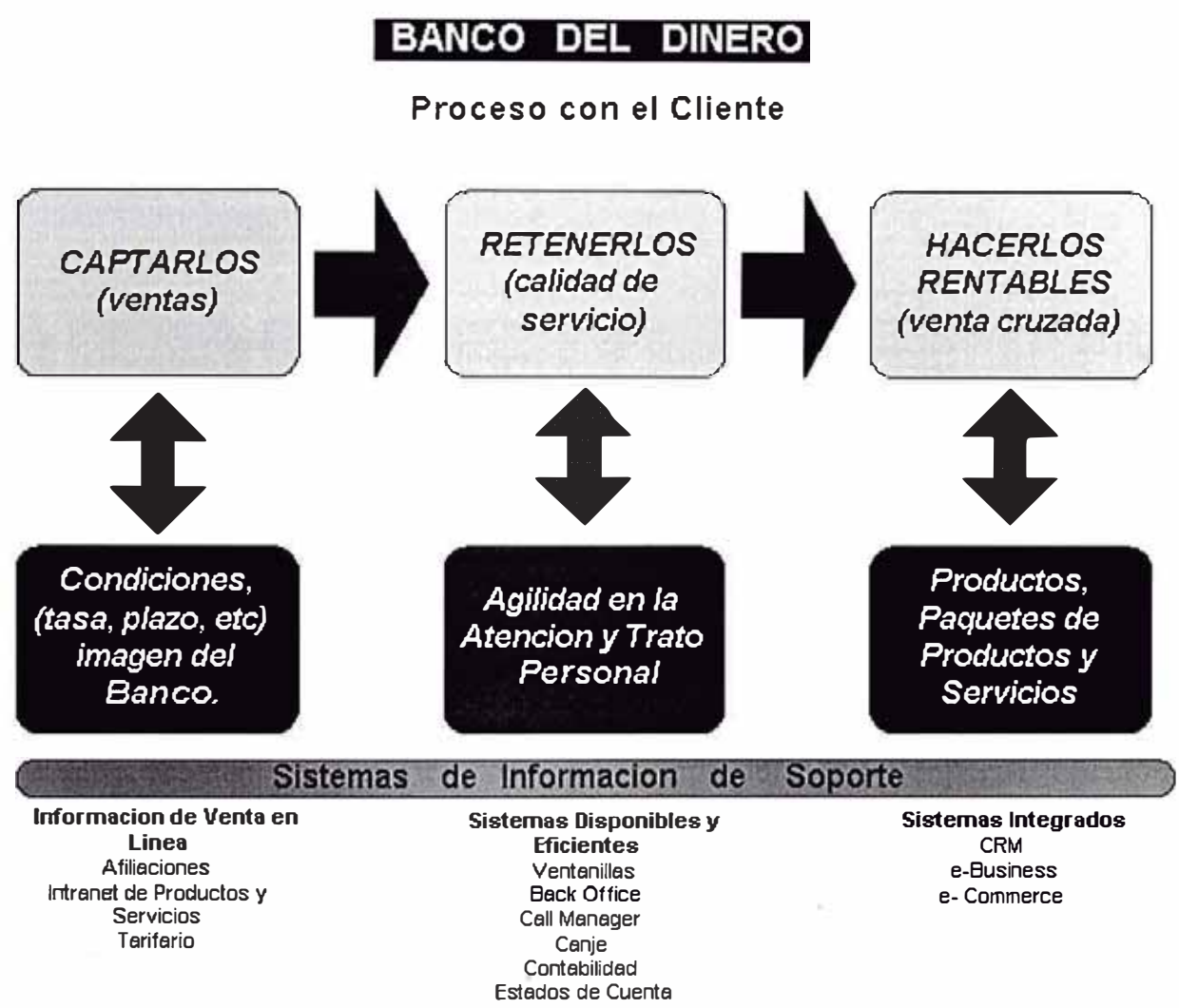
El Banco como empresa de tamaño medio tiene una serie de proveedores de todo Tipo y tamaños, se nombraran algunos de ellos :

- AT&T
- Banco de Crédito
- Computer Associates
- CosapiData
- CosapiSoft
- Enlace courier.
- Enotria
- Estudios de Abogados
- Hermes

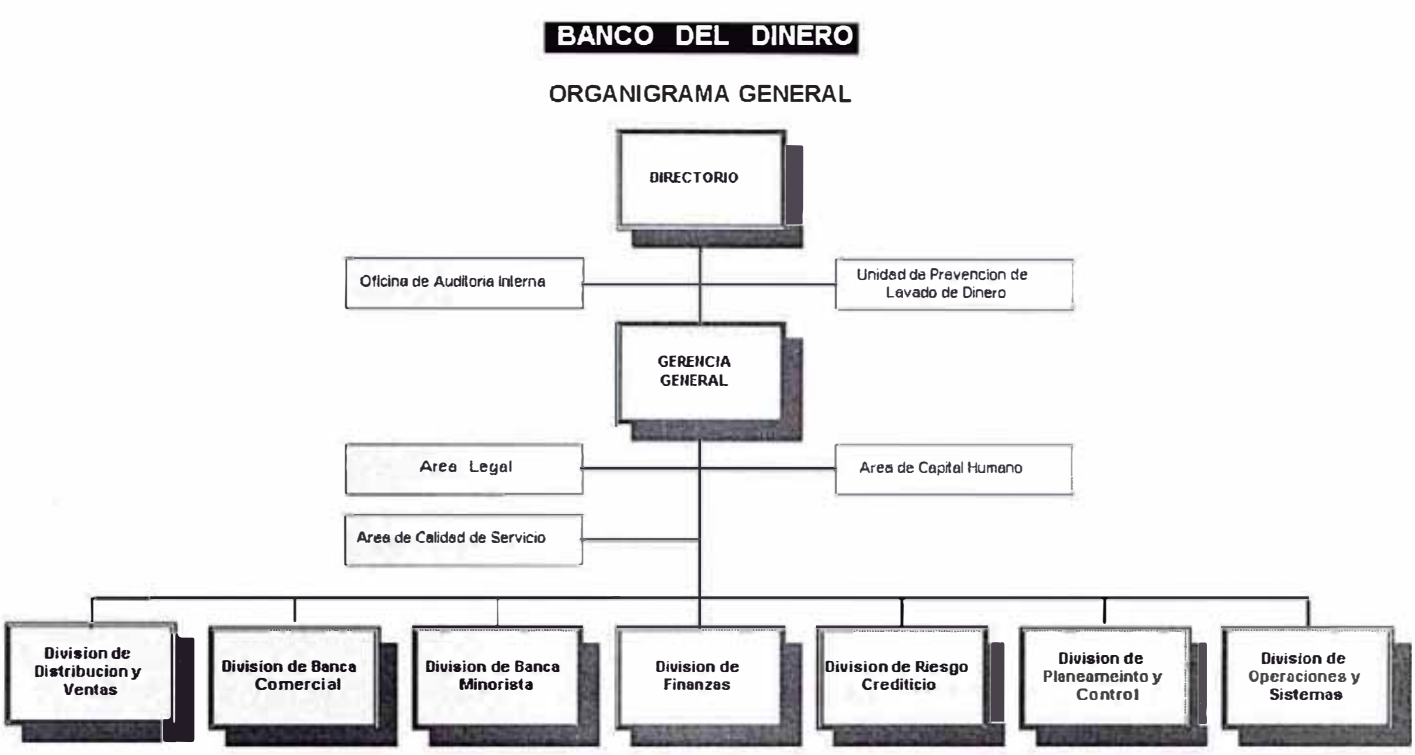
- IBM
- JEvans y Asociados
- Microsoft
- Novatronic
- Olivetti
- Prosegur
- Suplacor (productos de oficina en línea)
- System Support & Service
- Telefónica del Perú
- TIM
- Unibanca
- Unisys
- Verisign
- Xerox

1.2.4 Proceso

A continuación se describirá gráficamente el proceso simple y mas importante para el Banco como un resumen de lo descrito en el acápite del diagnostico estratégico , el proceso con el CLIENTE:



1.2.5 Organigrama del Banco del Dinero.



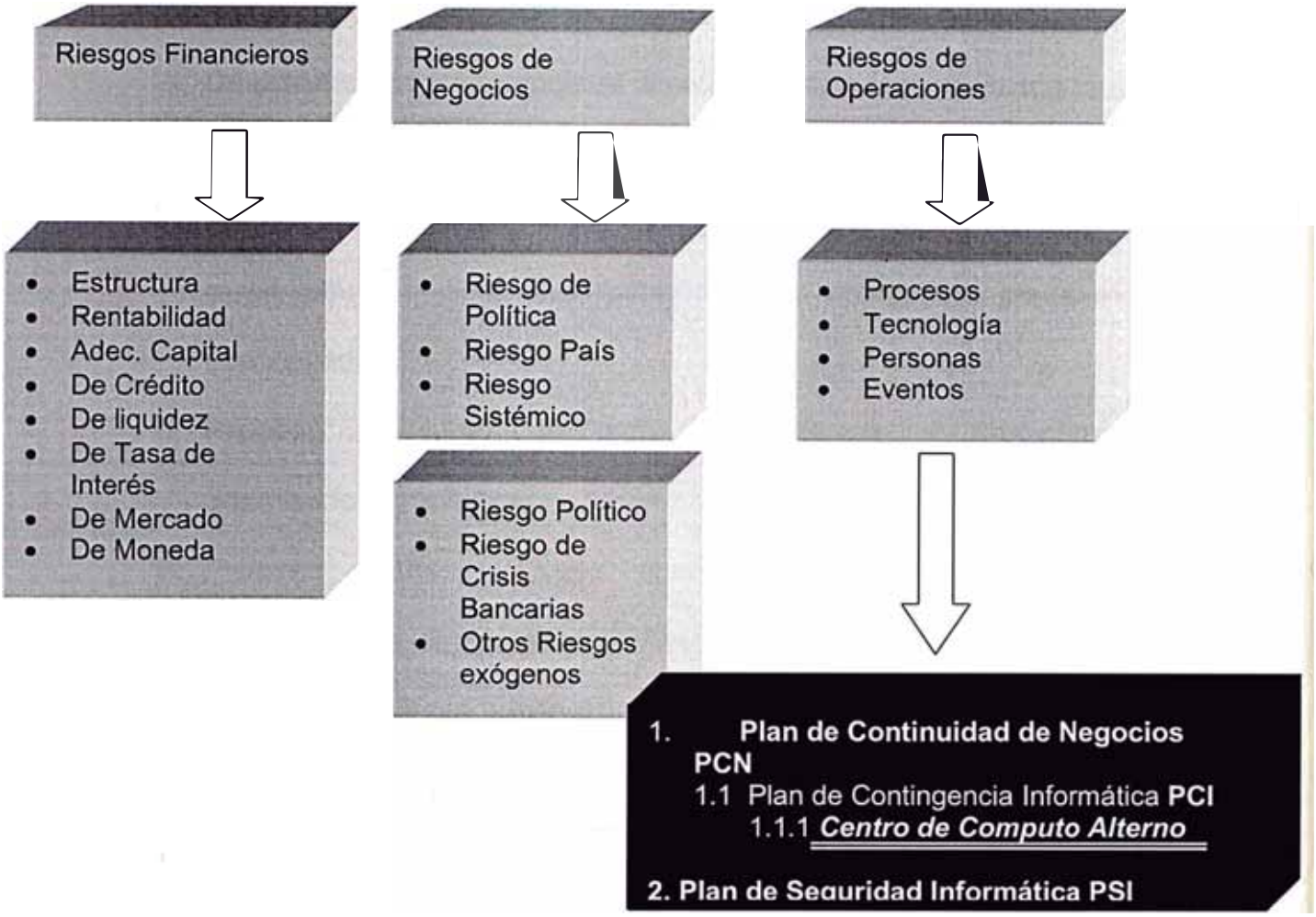
- En el anexo 3 se puede apreciar las áreas que están debajo de cada División en el anexo 4 se pude apreciar con mas detalle el area de sistemas que esta debajo de la Division de Operaciones y Sistemas.

CAPITULO II

MARCO TEORICO

El desarrollo del presente trabajo esta comprendido dentro del desarrollo de todo Plan de Contingencia Informática (PCI) ; que se ocupa de identificar, controlar y ejecutar procedimientos que minimicen los riesgos asociados a los recursos tecnológicos; y este a su vez esta comprendido dentro del Plan de Continuidad de Negocios (PCN), que es el plan macro que se ocupa de identificar y controlar los riesgos asociados a la continuidad operativa del negocio bancario. La estrategia del Centro de Computo Alterno esta directamente relacionada con los procesos definidos como críticos dentro del PCN y que colocan en alto riesgo la continuidad del negocio bancario.

Como se muestra en el grafico siguiente las primeras regulaciones tienen que ver con el manejo financiero de los Bancos, luego se enfatiza los riegos relacionados con eventos externos o del entorno del negocio, para finalmente evaluar los riesgos asociados con los procesos operativos propios del negocio dentro de los cuales se encuentran los riesgos de Tecnología.



El tema a desarrollar es específicamente el que esta relacionado a la implementación de un Centro de Computo Alterno como estrategia de mitigación de riesgos relacionados a los recursos tecnológicos.

2.1 DEFINICIONES.

Para continuar con el desarrollo del presente trabajo creemos que es importante y necesario proporcionar algunas definiciones de terminologías que nos ayudaran a entender mejor el contenido del presente trabajo.

a. **Administración de Riesgos:** Proceso que consiste en identificar, medir, controlar y reportar los riesgos que la empresa enfrenta.
b. **Directorio:** Toda referencia al directorio, entiéndase realizada también a cualquier órgano equivalente.
c. **Información**: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.
d. **Proceso**: Conjunto de actividades, tareas y procedimientos organizados y repetibles.
e. **Proceso crítico**: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la empresa.
f. **Reglamento del Sistema de Control Interno**: Reglamento del Sistema de Control Interno aprobado mediante la Resolución SBS Nº 1040-99 del 26 de noviembre de 1999.
g. **Servicios críticos provistos por terceros**: Servicios relacionados a procesos críticos provistos por terceros y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la empresa.
h. **Superintendencia**: Superintendencia de Banca y Seguros.
i. **Tecnología de información**: Incluye los sistemas informáticos y la tecnología asociada a dichos sistemas.

2.2 TEMAS BASICOS SOBRE RIESGOS DE OPERACIÓN.

A continuación se describirán los temas básicos sobre Riesgos de Operación que dan origen al Plan de Continuidad de Negocio (PCN), del cual se desprende el Plan de Contingencia Informática que contiene como uno de sus puntos importante el Centro de Computo Alterno que es el objetivo del presente trabajo.

2.2.1 Breve descripción.

Las empresas deben administrar adecuadamente los riesgos de operación que enfrentan. Entiéndase por riesgos de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos.

2.2.2 Responsabilidad del Directorio y la Gerencia

El Directorio es responsable del establecimiento de políticas y procedimientos generales para identificar, medir, controlar y reportar apropiadamente los riesgos de operación. Asimismo, será también su responsabilidad el velar por el cumplimiento de las referidas políticas y procedimientos y de las disposiciones contenidas en el presente Reglamento. Corresponderá a la Gerencia General la implementación de las políticas y procedimientos generales establecidos por el Directorio.

2.2.3 Unidad de riesgos

La Unidad de Riesgos será la encargada de la administración de los riesgos de operación que enfrenta la empresa, pudiendo comprender a alguna unidad especializada para la evaluación de dicho riesgo.

Asimismo, para dicho fin, la unidad de riesgos o, de ser el caso, la unidad especializada, deberá contar con la infraestructura adecuada, así como con los recursos humanos, técnicos y logísticos que le permitan el apropiado cumplimiento de sus funciones, de acuerdo a la dimensión y estructura de la empresa, la naturaleza de sus operaciones y servicios y la complejidad de los mismos.

Entre las funciones de la referida unidad responsable se incluirán por lo menos las siguientes:

a. Preparación y evaluación de políticas para la administración de los riesgos de operación.
b. Desarrollo de metodologías para la evaluación cuantitativa y/o cualitativa de los riesgos de operación.
c. Evaluación de los riesgos de operación, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.

d. Consolidación y desarrollo de reportes e informes sobre la administración de los riesgos de operación por proceso, o unidades de negocio y apoyo.

e. Identificación de las necesidades de capacitación y difusión para una adecuada administración de los riesgos de operación.

f. Otras necesarias para el desarrollo de su función.

2.2.4 Manual de organización y funciones

La empresa deberá disponer de una estructura organizacional y administrativa que le permita una adecuada administración de los riesgos de operación. Dicha estructura deberá establecerse de manera que exista independencia entre la unidad de riesgos y aquellas otras unidades de negocio, así como una clara delimitación de funciones, responsabilidades y perfil de puestos en todos sus niveles. Estos aspectos deberán encontrarse recogidos en el manual de organización y funciones de la empresa.

2.2.5 Manuales de políticas y procedimientos

Las políticas y procedimientos establecidos para la administración de los riesgos de operación deberán estar claramente definidos en los manuales de políticas y procedimientos; asimismo, deberán ser consistentes con el tamaño y naturaleza de la empresa y con la complejidad de sus operaciones y servicios.

2.2.6 Manual de control de riesgos

El manual de control de riesgos deberá contener una sección especial sobre los riesgos de operación. Dicha sección deberá contemplar por lo menos los siguientes aspectos:

g. Políticas para la administración de los riesgos de operación.
h. Funciones y responsabilidades de las unidades de negocio y de apoyo en la administración de los riesgos de operación.
i. Descripción de la metodología aplicada para la medición y evaluación de los riesgos de operación.
j. La forma y periodicidad con la que se deberá informar al Directorio y a la Gerencia General, entre otros, sobre la exposición a los riesgos de operación de la empresa y de cada unidad de negocio.
k. El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

2.2.7 Procesos Internos.

Las empresas deberán administrar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, de tal forma que se minimice la

posibilidad de pérdidas financieras relacionadas al diseño inapropiado de los procesos críticos, o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y costos planeados.

Las empresas deberán administrar apropiadamente los riesgos asociados a la tecnología de información, de tal modo que se minimice la posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas informáticos y tecnologías relacionadas a ellos, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información.

Para este fin, las empresas podrán considerar los riesgos vinculados a las fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, así como las fallas en la adecuación a los objetivos del negocio, entre otros aspectos.

2.2.8 Personas

Las empresas deben administrar apropiadamente los riesgos asociados a las personas de la empresa, de tal modo que se minimice la posibilidad de pérdidas financieras asociadas a inadecuada capacitación del personal, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero y similares.

2.2.9 Eventos externos.

Las empresas deberán considerar en la administración de los riesgos de operación la posibilidad de pérdidas derivada de la ocurrencia de eventos ajenos al control de la empresa que pudiesen alterar el desarrollo de sus actividades. En tal sentido, entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia

de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros.

2.2.10 Auditoria Interna

La Unidad de Auditoria Interna deberá evaluar el cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación. Asimismo, la Unidad de Auditoria Interna deberá incluir la referida evaluación en las actividades permanentes del Plan Anual y deberá realizar los informes y recomendaciones que se deriven de la misma.

2.2.11 Auditoria Externa

Las sociedades de auditoría externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la administración de los riesgos de operación.

2.2.12 Empresas Clasificadoras de Riesgo

Las empresas clasificadoras de riesgo deberán tener en cuenta las políticas y procedimientos establecidos por la empresa para la administración de los riesgos de operación en el proceso de clasificación de las empresas supervisadas.

2.3 PLAN DE CONTINUIDAD DE NEGOCIOS (PCN)

En esta sección queremos brindar un resumen de los conceptos que enmarcar un Plan de Continuidad de Negocios, ya que no es el objetivo del presente trabajo realizar un desarrollo del mismo, pero ayudaran a entender de donde provienen los requerimientos que nos llevan a la implementación de un Centro de Computo Alterno como estrategia para afrontar interrupciones no programadas de los recursos tecnológicos.

2.3.1 Objetivo del PCN.

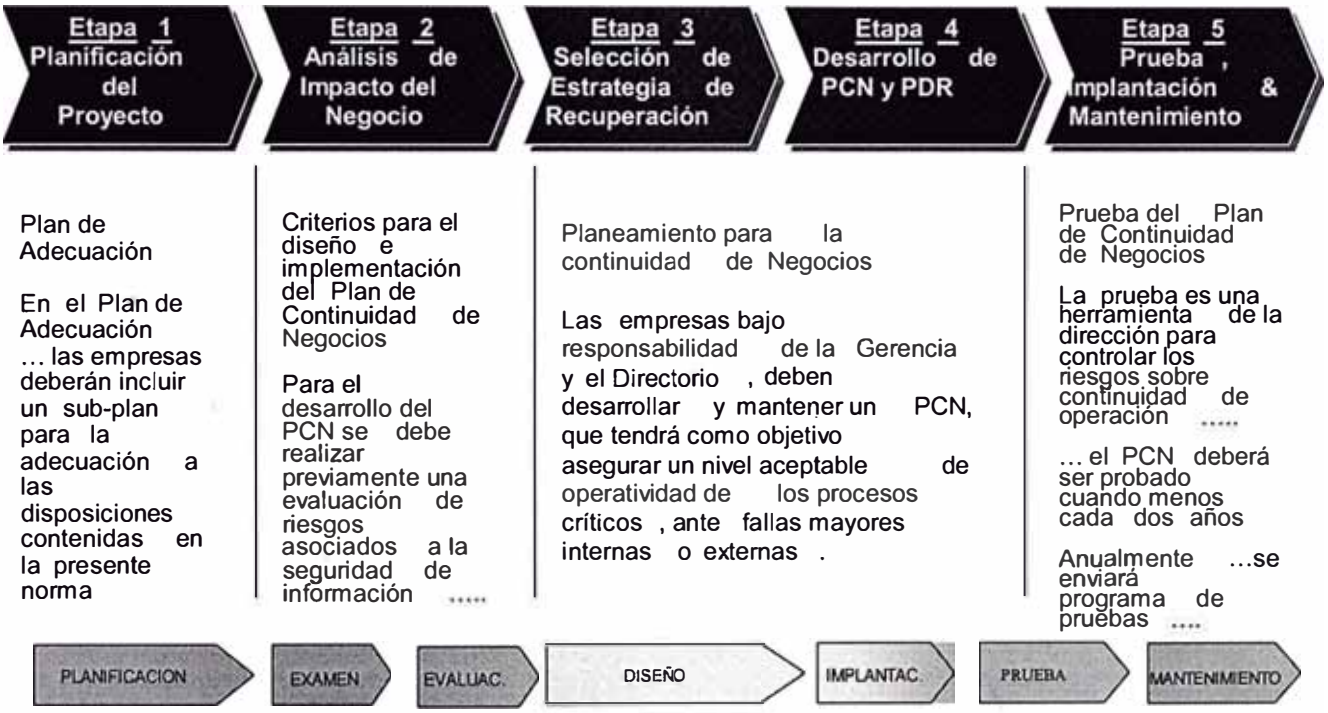
Reducir interrupciones de las actividades del negocio y proteger procesos críticos del negocio de los efectos de los desastres graves.

El proyecto para desarrollar el Plan de Continuidad de Negocios, en adelante PCN, comprende un esfuerzo coordinado, centrado en la administración, desarrollo, integración y mantenimiento de estrategias efectivas en costo, para minimizar el impacto de fallas en el Banco y la atención a sus clientes, permitiendo una rápida y efectiva evaluación, recuperación y continuidad de las operaciones durante una crisis o desastre

La regulaciones actuales de la Superintendencia define la necesidad de contar con un Plan de Continuidad de Negocios, elaborarlo en base a un análisis de impacto al negocio previo y elaborar procedimientos para

su constante mantenimiento y prueba. Asimismo, establece la necesidad de realizar pruebas integrales del plan cada dos años e informar anualmente a la Superintendencia.

El grafico siguiente muestra las etapas en las cuales se desarrolla un PCN:



Una breve descripción de estas etapas del PCN se encuentran en el anexo 5.

2.4 PLAN DE CONTINUIDAD INFORMATICO (PCI)

El Plan de Contingencia Informático es un sub plan dentro del Plan de Continuidad de Negocios (PCN), en esta etapa los procesos críticos ya han sido identificados, analizados y hechas las mediciones de impacto; y todo el esfuerzo de este plan esta abocado en hacer que esos procesos críticos no sufran interrupciones o en todo caso sean mínimas con tiempos de para aceptables para el negocio.

2.4.1 Objetivo.

- Brindar un nivel aceptable de operatividad a los procesos calificados como críticos en la evaluación realizada en el Plan de Continuidad de Negocios y que tienen un alto componente tecnológico.

- El presente Plan tiene por finalidad señalar las acciones a seguir, antes, durante y después de los diferentes eventos que ocurran durante una situación de Contingencia, estableciendo las responsabilidades del personal de la Institución ante una emergencia.

- Facilitar la coordinación, definiendo las líneas de comunicación entre todos los niveles, reduciendo la duplicidad de esfuerzos, confusión e incertidumbre en el manejo de las actividades en una contingencia.

- En resumen, establecer las bases de un sólido y efectivo sistema de reacción ante las contingencias que pudieran presentarse, minimizando el impacto financiero, preservando la imagen institucional y asegurando una rápida y transparente normalización de los servicios.

2.4.2 Alcances.

- El Plan de Contingencia para el Área Informática contempla el centro de computo central y todos los locales de la institución que mantengan equipos informáticos o participen de alguna manera en la cadena tecnológica, considera además la falla de suministros y/o recursos y los eventos producidos tanto en la cadena tecnológica como en los procesos catalogados como críticos por la organización.

- Los eventos provocados por fallas en suministros, equipos y proveedores son:

  a) Problemas en la Integridad de las Bases de Datos
  b) Falla en el software central
  c) Falla en el hardware de los equipos tecnológicos calificados como críticos
  d) Falla en el suministro de energía.

e) Falla en el suministro de servicio del circuito de comunicaciones.

- Este Plan de Contingencia Informático se complementa con el Plan de Continuidad de Negocios en el caso que el Centro de Cómputo Principal del Banco quede inoperativo afectado por un siniestro.

2.4.3 Definiciones Generales, Contingencias, Plan y Niveles.

- Contingencia.- Es una ocurrencia, evento o conjunto de eventos que afecta a uno o varios de los componentes de los sistemas del Banco y que puede generar una falla o suspensión no planeada de la atención al público, ya sea por falla de equipos o software, falla de servicios, acción de la naturaleza o del hombre

- Plan de Contingencia.- Es la descripción y documentación del conjunto de procedimientos y acciones que permiten reducir el nivel de riesgo y restaurar los servicios de las operaciones críticas de la organización como consecuencia de una interrupción no planeada a efectos de mantener la continuidad operativa, preservando la imagen institucional y minimizando las pérdidas financieras.

- Centro de Computo Alterno (CCA).- Es un ambiente debidamente acondicionado con todos los recursos tecnológicos necesarios

(comunicación, hardware, software, etc) que permitan afrontar con éxito casos de desastres en el centro de computo principal.

- Niveles de Contingencia.- Están basados en el impacto que puede producir la paralización de los procesos de la empresa. Para calificar el nivel de impacto de una contingencia en la Cadena Tecnológica es necesario evaluar si la interrupción nos impide operar plenamente los procesos de rutina o los catalogados como Críticos y si los eventos de esta interrupción nos permitirá operar en condiciones normales en corto, mediano o largo plazo. Esta evaluación nos permitirá conocer las restricciones de los procesos y el tipo de procedimiento alterno con las acciones más apropiadas a implantar a fin de obtener la recuperación más inmediata de las operaciones de la Institución.

- Los niveles considerados son:

  - **Bajo Grado.**

    Son interrupciones que se producen por un mal funcionamiento de los sistemas en general o por fallas originadas por los equipos y medios del entorno informático.

En esta clasificación el impacto en las operaciones de la empresa no es significativo. La recuperación del evento es sencilla; de bajo costo y corto tiempo

- **Mediano Grado.**

  Las interrupciones corresponden a paralizaciones parciales del sistema y/o de los equipos de Procesamiento o de Comunicaciones.

  En este nivel de gravedad, la operación de los servicios o procesos críticos se efectúan en forma restringida, utilizando medios alternos o a través de procedimientos manuales y/o combinados, software sustituto para algunas funciones, empleo de PC´s y programas especiales de emergencia, etc.

  Debe actuarse en forma rápida para la recuperación plena del estado normal de atención.

- **Alto Grado.**

  Son Contingencias mayores como consecuencia de una paralización de los procesos por fallas graves de los sistemas o de los equipos, así como por la destrucción parcial o total de las instalaciones, equipos y/o sistemas principales que opera el Centro de Cómputo.

Puede requerirse de métodos de recuperación de la data de respaldo, reemplazo o arreglo de equipos, restablecimiento de medios o de ambientes y locales alternos para el procesamiento de las operaciones.

El tiempo en recuperar las instalaciones o sistemas anteriores es eventualmente largo y costoso.

2.4.4 Organigrama para afrontar una Contingencia.

- **Comité de Contingencia (CC)**

  Es el máximo Organismo en una situación de Contingencia, conformado por la Alta Dirección (principales gerencias de la organización) y presidido por la Gerencia General.

- **Central de Monitoreo de Contingencia (CMC)**

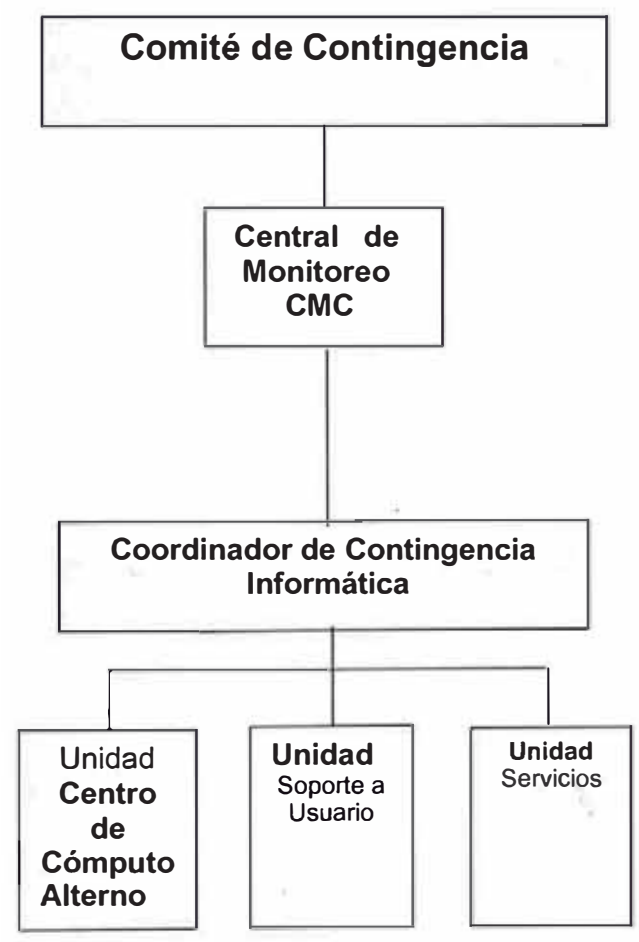
  Órgano de apoyo al Comité de Contingencia, conformado por especialistas en diferentes temas, quienes centralizan las comunicaciones y dan instrucciones de cómo resolver los eventos que originan la contingencia.

- **Coordinador de Contingencia Informática**

  Es el jefe operativo a cargo de las Unidades Informáticas y reporta al Jefe de la Central de Monitoreo de Contingencia CMC

- **Unidades de Contingencia**

  Personal operativo que hace frente a una contingencia, encargados de resolver las diferentes situaciones que se presenten antes, durante o después una contingencia informática.



2.5 CENTRO DE COMPUTO ALTERNO (CCA)

Es un ambiente debidamente acondicionado con todos los recursos tecnológicos necesarios (comunicaciones, hardware, software, operación, seguridad, etc.), para dar un servicio de continuidad de operación del negocio, que permitan afrontar con éxito considerando un escenario que afecte las instalaciones del Centro de Procesamiento de Datos principal del Banco.

Para lograr el éxito es importante la reducción de tiempos de recuperación de sistemas al replicar los datos y contar con los servidores, previamente calificados críticos, dedicados con software pre-cargado.

Para la implementación de esta estrategia existen varias alternativas; algunos optan por implementarlo en sus locales propios y otros por contratar los servicios de empresas especializadas en brindar servicios de Sites Externos, y una tercera alternativa podría ser una intermedia donde parte de los servicios estén en un Site Externo de una empresa especializada y otros en locales propios de la empresa. Para la decisión final siempre se tomara en cuenta aspectos de costos, disponibilidad y regulaciones vigentes.

Todo CCA deberá contener los siguientes componentes:

- Implementación de la infraestructura y servicios de un CCA.
- Disponibilidad de la infraestructura de un Centro de Cómputo Alterno.

- Disponibilidad de capacidad de procesamiento de servidores
- Software de replicación de datos
- Equipos de comunicaciones.
- Servicios de operación.
- Plan de pruebas periódicas de verificación de la recuperación, asistencia durante su ejecución y documentación del resultado de las mismas.

Los elementos que integran este proyecto son:

2.5.1 Infraestructura.

La infraestructura de Centro de Cómputo debe contar con sistemas de detección y extinción de incendios, piso y falso techo, cableado de sitio, control de acceso, paredes y vidrios externos blindados y reforzados. Asimismo, el Centro de Cómputo debe contar con equipos de UPS, Grupo Electrógeno y Aire Acondicionado.

El local deberá contar con un servicio de seguridad que opera las 24 horas y que tiene, entre otras funciones, realizar un monitoreo constante a través del Circuito Cerrado de Televisión. El acceso debe ser controlado fuera y dentro del local, las áreas son clasificadas y controladas para evitar el acceso a áreas no autorizadas.

2.5.2 Capacidad de Procesamiento.

Este es un aspecto que no se debe descuidar ya que las capacidades de procesamiento deben ser semejantes y/o deben soportar la operativa normal del negocio. Esto debe estar debidamente medido y probado.

Ejemplo de Capacidades para un servidor AS/400:

- Capacidad Batch : 950 CPWs
- Capacidad Interactiva : 150 CPWs
- Memoria RAM : 4 GB
- Disco Duro : 150 GB
- Tarjeta de red Ethernet de 10/100 Mbps
- Lectora de CD, etc

Ejemplo de Capacidades para un servidores Intel:

- Server 1 : 2 procesadores de 2.4 Ghz, 1 GB de RAM y 1 x 40 GB
- Server 2 : 2 procesadores de 2.4 Ghz, 1 GB de RAM y 1 x 40 GB
- Server Base de Datos : 2 procesadores de 2.4 Ghz, 1 GB de RAM y 2 discos duros de 73.4 GB cada uno.
- Servidor de Dominio (PDC+DNS-WINS-DHCP) Procesador 2.4 Ghz, 2 GB de RAM y 2 discos de 40 GB cada uno.

- Estos servidores y/o particiones Intel deberán contar con una (1) tarjeta de red Ethernet de 10/100 Mbps y una (1) lectora de CD.

Dispositivos adicionales como:

- Unidad de tape backup LTO 3581 y Tivoli Storage Manager.
- Unidad de tape 3590.
- Impresora 6412 de 1200 LPM.
- Una unidad de Tape Backup externa DDS-4.

2.5.3 Sala de Usuarios.

El CCA deberá disponer de una sala de usuarios equipada con puestos de trabajo, anexos telefónicos, fax, impresoras láser, PCs . Estas facilidades deben estar disponibles en caso de contingencia, o para realizar las pruebas.

2.5.4 Equipo de Telecomunicaciones.

Para la comunicación entre el Centro de Cómputo y la sede central del Banco, se deberá disponer de toda la infraestructura necesaria que garantice la comunicación, adicionalmente se deben mantener lineas de comunicación de contingencia en caso de fallas.

Se deberá contar con equipos de comunicación como:

- routers.
- switches, etc

2.5.5 Software de Replicación en Línea.

Para la optima replicación de datos entre la sede principal y el CCA se deberá contar con un software de Alta de Disponibilidad, ya que esta replicación deberá ser hecha en línea, esto es imprescindible para un negocio bancario donde la data es actualizada constantemente; otros negocios no bancarios quizás no lo necesiten; en todo caso deberá ser un requerimiento del PCN.

2.5.6 Operación del CCA.

Consiste en la ejecución de actividades periódicas que permitan el correcto funcionamiento del Centro de Computo Alterno.

La operación debe ser en forma permanente 24 horas al día, 7 días a la semana, 365 días al año. Estos pueden ser :

- Monitoreo de Sistema Operativo
- Monitoreo de los archivos de bitácoras (log) del sistema operativo para la verificación del correcto funcionamiento de los componentes de software (Sistema Operativo) y Hardware de manera preventiva y correctiva.
- Monitoreo del Proceso de Replicación
- Monitoreo de la herramienta de replicación de datos, revisando que el proceso de replicación se encuentre operativo y revisión de archivos de bitácoras (log) para la verificación del correcto funcionamiento.

- Monitoreo de Redes
- Monitoreo de la disponibilidad y desempeño del enlace de comunicaciones, que permita un correcto acceso y operatividad del proceso de replicación de datos.

2.5.7 Mantenimiento del Hardware.

Contempla la ejecución de mantenimientos preventivos y correctivos de los servidores

2.5.8 Soporte de Software.

Contempla los servicios de soporte técnico relacionados al sistema operativo, que incluye mantenimientos, actualizaciones y aplicaciones de Services packs o Hot Fixes publicadas por los fabricantes los cuales son básicamente para corregir algún error reportado o cerrar brechas de seguridad descubiertas.

2.5.9 Registro de Eventos en Bitácora.

Consiste en la documentación de los eventos dentro del CCA en un archivo de bitácora. Se incluyen eventos, fecha de eventos, estado del evento, especialistas involucrados.

2.6 PRUEBAS DEL PLAN DE CONTINGENCIA.

Con el objeto de poder verificar el funcionamiento del Plan de Contingencia, se deberán realizar pruebas en forma periódica estas pueden ser programadas y coordinadas con las areas usuarias de acuerdo a lo descrito en el PCN.

2.7 ROLES Y RESPONSABILIDADES.

Para el presente proyecto se han definidos los siguientes roles y sus respectivas responsabilidades

- **Gerente de Proyecto :** Ejecutivo designado como dueño o responsable del proyecto. Dicho ejecutivo y sus delegados tendrán la suficiente autoridad y atribución para resolver los conflictos que puedan poner en riesgo los objetivos, metas o resultados del proyecto.

- **Coordinador de Proyecto** : Es la persona a cargo de la administración permanente de la infraestructura y recursos provistos y que forman parte del proyecto. Asimismo, es el responsable de coordinar las labores de implementación, producción y pruebas de contingencia.

- **Operadores** : Personas con conocimiento técnico sobre labores de operación y cuya responsabilidad es apoyar al Coordinador del Proyecto en todas las gestiones y labores que él considere pertinente realizar.

- **Especialistas de Soporte Técnico :** Son los responsables de realizar las labores de mantenimiento preventivo y correctivo de los componentes del CCA.

- **Especialista de Comunicaciones y Seguridad:** Son los responsables de la configuración de los equipos de comunicación, firewalls y proxies.

Mas detalle se puede apreciar en el Anexo 10.

CAPITULO III

PROCESO DE TOMA DE DECISIONES

3.1 PLANTEAMIENTO DEL PROBLEMA.

Habiendo ya descrito ampliamente al negocio en los puntos anteriores, la alta Dirección del Banco concientes de los resultados de la evaluación del Riesgo de Operaciones toma como acción analizar cada problema para definir las estrategias para llevar a cabo las soluciones que conlleven a minimizar los riesgo y con el objetivo de contrarrestar las interrupciones a las actividades del negocio y proteger los procesos críticos de los efectos de los principales desastres.

Dentro de los riesgos principales se plantea el problema de no contar como parte de su continuidad operacional del negocio con un Centro de Computo Alterno en un lugar lo suficientemente distante al Centro de Computo principal, de tal manera que si ocurriera un desastre (incendio, inundación, vandalismo, falla de seguridad, terremoto, etc.), en el centro de computo principal, se active en el menor tiempo posible el Centro de Computo Alterno, de tal manera de continuar las operaciones y procesos de negocios del

Banco con el objetivo principal de continuar atendiendo a los clientes, usuarios internos del Banco, Canales de Venta y/o empresas que tienen relación de negocios acordadas con el Banco.

Dentro de esta problemática vista como parte de la continuidad operacional de las operaciones del Banco para atender principalmente a los clientes, se presentan problemas colaterales como son : la imagen de confianza y buen servicio (refiriéndose en reducir al mínimo de interrupciones la atención al cliente), contar con buen resultado frente a las clasificadoras de riesgos que es muy importante como evaluación de Negocios en el mundo empresarial, mejorar la negociación de las prima de seguro con las aseguradoras, cumplir estándares de los accionistas extranjeros, cumplir con la normativa dada por la entidad supervisora de los Bancos, la Superintendecia de Banca y Seguros, y así mismo cumplir con las revisiones anuales de las compañías auditoras externas.

Es necesario mencionar que en el contexto de resolver el problema planteado, nace el Plan de Continuidad del Negocio (PCN), que contiene al Plan de Continuidad de Informática (PCI), cuya acción principal es reducir el riesgo del Centro de Computo y se plantea la necesidad de implementar un Centro de Computo Alterno (CCA) en una ubicación remota como estrategia de recuperación.

Luego de los procesos antes analizados, el presente trabajo plantea resolver el problema que representa la falta de disponibilidad de los sistemas de información considerados críticos, luego de una análisis exhaustivo de todos los procesos del negocio bancario del Banco del Dinero. Básicamente lo que se trata es de implementar toda la arquitectura Tecnológica (Hardware, Software de Base, Software Aplicativo, redes LAN y Wan, configuraciones, comunicaciones,), así como los, procedimientos, políticas, niveles de servicio, pruebas periódicas, revisiones no avisadas, etc. , en este Centro de Computo Alterno de tal manera que estén disponible los sistemas Informáticos definidos como críticos dentro del proceso del negocio que fueron seleccionados por el Comité Ejecutivo de Riesgos.

El Banco para llegar a definir cuales eran los procesos críticos a replicar en el Centro de Computo Alterno se baso en la metodología BIA (Business Impact Analisys), Análisis de Impacto en el Negocio el cual se realizo dentro de toda la organización para determinar las funciones, proceso de negocio e infraestructura de soporte que son críticos para la continuidad o viabilidad del Banco. Este Análisis exhaustivo que se realizo en toda la organización con la participación de los involucrados en los procesos de negocio se puede ver en el anexo 6.

Es necesario mencionar que como parte del problema de la implementación de este CCA, era evaluar los costos a incurrir en este proyecto debido a los

altos costos de los componentes tecnológicos y procesos a incluir, como hardware, licencias de software base y software aplicativo, líneas de comunicación, servicio de operación y monitoreo, etc. lo cual mereció una ardua evaluación buscando el mejor costo beneficio tomando en cuenta todos los servicios ofrecidos así como el valor agregado que se pudiera encontrar entre las propuesta de los diferente proveedores del mercado local y estas a su vez comparándola con la posibilidad de una implementación desarrollada por el mismo Banco.

Como podemos percibir con lo descrito anteriormente podemos concluir que la solución a plantear se encuentra alineado a los planes estratégicos del Banco que a su vez involucra un estudio de todos los procesos de negocio de la organización.

3.2ALTERNATIVAS DE SOLUCION.

Antes de plantear las alternativas de solución evaluadas es importante mencionar que luego de la evaluación de Riesgos de Operaciones llevada en el Banco por la Gerencia de Riesgos, el Comité Ejecutivo de Riesgos encargo llevar la evaluación de Alternativas del Centro de Computo Alterno a la Gerencia de División de Operaciones y Sistemas, quien en conjunto con sus áreas de Tecnología y Seguridad llevaron a cabo la búsqueda de alternativas de solución para finalmente llevar el planteamiento final a al Comité de Gerencia.

Para el problema planteado a la División de Operaciones y Sistemas se definen tres alternativas de solución que son en base a al estudio de mercado nacional de proveedores de Data Centers y de que es lo que han adoptado como solución el Sistema Bancario de nuestro país; a partir de ello definimos tres alternativas de solución, que se describen a continuación:

3.2.1. CENTRO DE COMPUTO ALTERNO PROPIO.

Esta solución lo que se propone es la implementación del centro de computo alterno propio, es decir ubicar dentro los diversos locales propios del banco uno que se adecue para la construcción o adecuación de un ambiente idóneo para un Centro de Computo, para ello definiremos los recursos necesarios para su implementación

como: costos de construcción, personal, equipamiento de hardware, software, etc. Ver Anexo 7.

Ventajas:

- No dependencia con el proveedor de servicios
- Las políticas de Seguridad serian las propias
- Independencia para realizar cambios en la infraestructura

Desventaja:

- Alto costo para su implementación
- Falta de un local propio con disponibilidad, se tendría que adquirir
- Obsolescencia de equipos de computo
- Falta de personal para la operación del CCA
- Contratación de líneas de comunicación para proporcionar servicios, encarecen la alternativa.
- Se requiere de mayor tiempo para su implementación

3.2.2. CENTRO DE COMPUTO ALTERNO TERCERIZADO

Aquí analizamos la alternativa de contratar los servicios de una empresa especializada en brindar estos servicios, analizaremos las ofertas existentes en el mercado. En esta solución existen dos sub-tipos de implementación:

- **Housing :**

  Donde el Banco es propietario de los equipos de computo, y solo se contrata el espacio físico adecuado con energía eléctrica estabilizada, aire acondicionado, seguridad física, accesibilidad y la infraestructura de comunicación. Normalmente estos los Data Center de Clase mundial que ofrecen el servicio de DR (Disaster Recovery), tienen la filosofía de n+1 en los equipos de posible falla, es decir equipos con redundancia.

- **Hosting :**

  Aquí la empresa proveedora brinda el servicio de integración de hardware de servidores, dispositivos de almacenamiento, software de base, subsistemas de administración asociados, utilitarios y herramientas de acceso remoto a través de vínculos de comunicación a la medida del cliente en forma dedicada o compartida, con servicios de respaldo de la información

Ventajas:

- Alta especialización de los proveedores de servicios en brindar Sites de Contingencias.
- Para la alternativa del hosting se elimina el riesgo de obsolescencia de equipos, ya que el proveedor debe proporcionar los equipos con las características necesarias.
- El proveedor asume el costo de mantenimiento de los equipos.

- Los proveedores ya cuentan con la infraestructura de comunicaciones, y están enlazados a la mayoría de servicios bancarios. (Bancared)
- La implementación se haría en menor tiempo
- Los Sites de los proveedores, cuentan con las reglamentaciones que la SBS solicita, y están certificados por empresas aseguradoras y/o certificadotas.
- Al tratarse de servicios que son brindados a varias empresas, el costo del servicio se diluye, ya que se comparten los costes.
- Al ser propietarios de los equipos los costos son menores y así mismo pueden dar el servicio en forma dedicada o compartida.

Desventajas:

- Alta dependencia con el proveedor
- Riesgo Controlado de perdida de información (bajo contrato)
- Cambios tecnológicos (hardware y software) que pueden obligar al Centro de Computo de la empresa ha realizarlos por temas de compatibilidad.

3.2.3. CENTRO DE COMPUTO ALTERNO MIXTO

Esta solución es una combinación de las dos anteriores, es decir parte de los servicios del centro de computo se colocaran en locales acondicionados propios del banco y otros servicios se tercerizarán.

De lo que se trata es de minimizar los costos para la implementación del CCA, tratando de utilizar locales propios del Banco para albergar servidores medianos y se pueda brindar algunos servicios. Solo el servidor grande (HOST AS/400) donde reside el core bancario y los servidores que proporcionan atención a las agencias (Sistema de Ventanillas) estarían alojadas en el Site de Contingencia.

3.3 METODOLOGÍA DE SOLUCION

El proyecto a desarrollarse no es del tipo clásico de desarrollo de software, sino mas bien de la implementación de un Centro de Computo Alterno, y por ende usaremos la metodología IDEA relacionado a la gerencia de proyectos informáticos de tipo Soporte Tecnológico.

Como es conocido la metodología IDEA contiene 4 fases principales para la gerencia de proyectos:

3.3.1 INICIO

En esta etapa se deberán aprobar los parámetros básicos del proyecto; así como la firma de contratos a los que hubiera lugar respetando las definiciones mencionadas en el documento Informe de Definición del Proyecto.

Formulación del Proyecto, aquí se definirán los alcances, plazos, costos, participantes y riesgos.

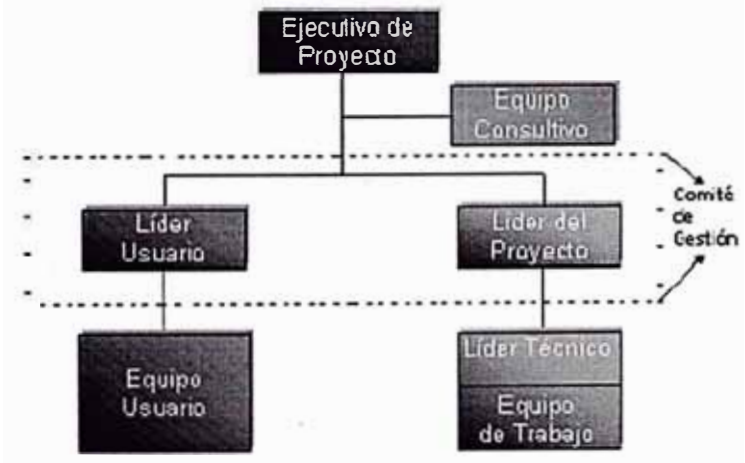
Informe de Definición, aquí las actividades mas importantes son: Modelamiento de Objetivos; tomados de la definición de procesos críticos propuestos en el Plan de Continuidad de Negocios, conformación del equipo de trabajo, la elaboración de los respectivos informes y el lanzamiento oficial del proyecto.

Plan de trabajo – Cronograma de Actividades, se elaborara el respectivo cronograma para la aprobación de todos los miembros del equipo de trabajo.

En el punto 3.5.3 se muestra un resumen del cronograma de trabajo y en el anexo 8 se encuentra el detalle del mismo.

No se debe dejar de lado la importancia de los Roles que jugara cada miembro del equipo de trabajo, el grafico siguiente muestra como se formaran los respectivos equipos:

Una vez definido los participantes en un proyecto se les asigna un ROL (definición que agrupa actividades afines) a desempeñar. Se puede asignar a una persona más de un rol a la vez, dependiendo del tamaño del proyecto y de las características de la misma.



Ver el detalle en el Anexo 9

3.3.2 DESARROLLO

Para esta etapa debemos tener una visión de la solución física y funcional lo mas próxima a como quedara en su implementación final, y la aceptación de la misma por parte del usuario, en este proyecto debe ser a entera satisfacción del Banco ya que el servicio del CCA lo esta dando un tercero.

3.3.2.1 Arquitectura Funcional.

Aquí esbozaremos el diagrama para la puesta en operación en el Centro de Computo Alterno, de los procesos que se definieron como críticos en el Plan de Continuidad de Negocios; de tal forma que no dejemos de incluir a ninguno.

3.3.2.2 Arquitectura Tecnológica.

Esta es la parte mas compleja dentro de esta etapa; ya que se tendrá que construir toda la solución en hardware, software, comunicaciones, configuración y procedimientos de operación del nuevo Centro de Computo Alterno.

3.3.2.3 Pruebas Integrales.

En esta actividad se involucra al usuario del proyecto, quien deberá liderar las pruebas con los demás usuarios, al tratarse de pruebas que tienen que ver con la interrupción de los servicios

del banco, se debe tener especial cuidado y medir los riesgos que esto pudiera implicar. Estas pruebas serán programadas y cada participante tendrá su manual de procedimientos para los casos de contingencia de acuerdo a la definición del PCN.

3.3.2.4 Certificación.

El usuario conjuntamente con el personal de sistemas certificaran el buen funcionamiento del Centro de Computo Alterno, para lo cual se suscribirá el documento de aceptación del proyecto.

3.3.2.5 Capacitación.

Esta es la actividad mas importante, ya que al tratarse de eventos de desastres (el no contar con el centro de computo ha sido catalogado como un desastre de grado alto) todo el personal del banco debe estar en conocimiento del proyecto y saber el rol que le toca en caso de suceder, todo esto esta en mas detalle en el documento del PCN.

El rol del personal de sistemas también es importante ya que varias las actividades de recuperación van a estar en manos del personal de IT, para lo cual se requiere capacitación y entrenamiento constante. Debido a las actualizaciones de versiones y cambios que puedan suceder en el tiempo de

acuerdo a los acuerdos registrados en el control de cambios. Ver anexo 10.

3.3.2.6 Implantación.

Es la actividad final del proyecto, y debe ser difundida a todo el personal. Luego de esta etapa de implantación, entra en vigencia la operación continua del CCA llevada a cabo por el proveedor del servicio conjuntamente con el personal del Banco de acuerdo a las definiciones previas.

3.3.3 ESTABILIZACIÓN

Luego de la etapa del desarrollo, debemos obtener la versión de la solución planteada inicialmente habiendo cumplido con los objetivos propuestos en la primera etapa.

3.3.3.1 Mejoras no previstas.

Al tratarse de un proyecto de tipo Soporte Técnico las mejoras se obtendrán como resultado de las pruebas que se realicen, las cuales deben ser documentadas e incluidas en los respectivos documentos.

3.3.3.2 Corrección de Errores.

Esto deberá ser superado en las diversas pruebas de esfuerzo que se realicen.

3.3.3.3 Capacitación.

Se volverá a capacitar sobre las mejoras que fueron implementadas y los errores en los que se incurrieron.

3.3.3.4 Control de Cambio.

Cualquier requerimiento que implique cambios en las funciones y/o características de los servicios definidos previamente en el Contrato, será tratado según lo establecido en el procedimiento, denominado "Procedimiento de Control de Cambios".Que incluye:

- Solicitud de Cambio
- Calificación del Cambio, que puede clasificarse en:
    - "MEJORA"
    - "CAMBIO"
    - "MODIFICACIÓN"
- Procedimiento para cada caso:

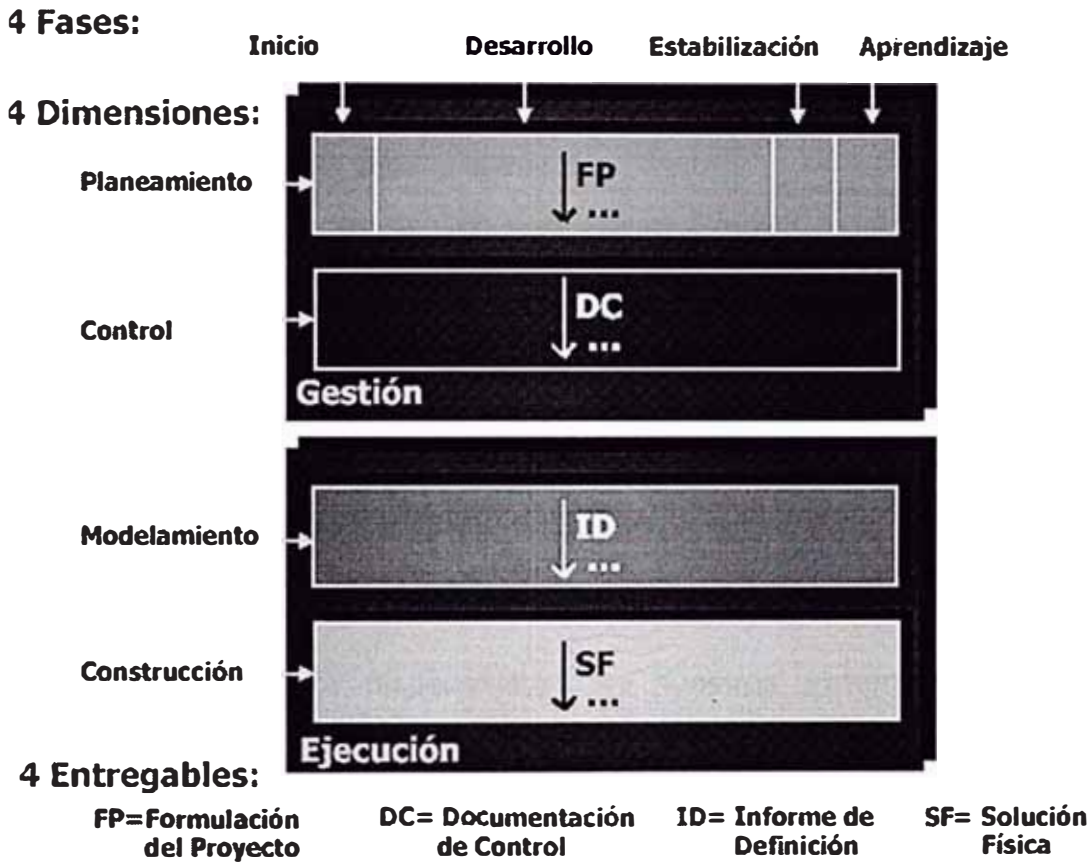
Mas detalle ver el anexo 10

3.3.4 APRENDIZAJE

En esta etapa las pruebas serán el mejor método de aprendizaje, mientras mas pruebas se realicen mejor será la calidad del proyecto.

Aquí existirá un equipo de trabajo permanente evaluando el resultado de las pruebas dada la envergadura de la misma al involucrar a todo el personal y los riesgos que esto involucra. Así mismo en este aprendizaje continuo se documentaran los cambios y mejoras que ocurran a lo largo del tiempo.

En el siguiente grafico se muestran las 4 fases en sus 4 dimensiones de la Metodología IDEA, descritas anteriormente para la implementación del proyecto del Centro de Computo Alterno para el Banco del Dinero.



3.4 TOMA DE DECISIONES.

En esta sección del informe nos centraremos en seleccionar la alternativa que más se ajuste a los requerimientos del Banco para la implementación del CCA.

La sección 3.2 "Alternativas de solución" será nuestro marco de referencia.

A continuación las alternativas y su identificación:

Alternativa I : Centro de Computo Alterno Propio

Alternativa II : Centro de Computo Alterno Tercerizado

Alternativa III : Centro de Computo Alterno Mixto

No debemos olvidar los objetivos mas importantes de la implementación del CCA:

- Garantizar alta disponibilidad en nuestros sistemas centrales, que permitan que el Banco nunca deje de operar con sus servicios.
- Garantizar la seguridad de la información que se almacena en nuestros Computadores centrales ante cualquier siniestro.

"Las caídas de sistemas ocasionan grandes perdidas económicas a las empresas"

Cabe resaltar que como parte del análisis que en parte ayudo a la toma de decisiones es hacer un estudio de mercado de las empresas financieras en

nuestro y recabar información sobre que soluciones dentro de las alternativas posibles habían optado así como consultar las experiencias obtenidas con la solución. A continuación se muestra dicho grafico y un breve análisis.

Entidades Financieras	CUENTA CON CCA	CCA PROPIO		CCA TERCERIZADO					
		PROPIO - LIMA	PROPIO EXTRANJERO	IBM	TELEFONICA	GMD	AT&T	IMPSAT	UNISYS
BANCO DE CREDITO	Si	X							
BANCO WIESE SUDAMERIS	Si	X							
BANCO STANDARD CHARTERED	Si			X					
BANCO FINANCIERO	Si				X				
BANCO DE COMERCIO	Si				X				
BIF	Si	X							
BANCO DEL DINERO	No								
INTERBANK	Si	X							
BANCO DEL TRABAJO	Si	X							
BBVA BANCO CONTINENTAL	Si		X						
CITIBANK	Si		X						
M IBANCO	Si	X							X
BANKBOSTON	Si		X						
FINANCIERA CORDILLERA	Si			X					
FINANCIERA CMR	Sin Inf								
BNP PARIBAS	Si		X						
BANCO DE LA NACIÓN	Si			X					
AGROBAN	Si			X					
Totales	18	6	4	4	2				1

Bancos con CCA	16
Bancos sin CCA	2
Bancos con CCA Propio	10
Bancos con CCA Tercerizado	7

Como muestra el cuadro, los bancos extranjeros cuentan con CCA propio (4) localizados en Sites externos propios de sus respectivas corporaciones y estos obedecen a estándares que son hechos en sus casas matrices. De los Bancos con capital nacional y con Sites propios tenemos a los bancos mas grandes (Credito, Wiese, Interbank) que generalmente tienen locales acondicionados y con una infraestructura mayor que les permite tener su CCA en sus propios locales.

De los bancos medianos, caso Financiero, Comercio, estos han elegido la opción de la tercerizacion con estrategia. El Banco del Dinero se encuentra en este grupo por su tamaño y la complejidad de sus sistemas; lo cual nos lleva a señalar que al parecer es la estrategia mas viable para este tipo de banca.

Luego del análisis anterior para la elección de la mejor alternativa emplearemos un cuadro de evaluación, donde cada item tendrá una ponderación que nos ayudara a decidir por la alternativa mas acorde a las necesidades del banco.

3.4.1. Evaluación de la mejor Alternativa.

El siguiente cuadro muestra las rubros a tomar en cuenta para esta evaluación así como el puntaje dada a cada uno de ellos. En la leyenda se explica el significado de los valores numéricos de calificación.

Ponderaciones	Alternativa I	Alternativa II	Alternativa III
Costos	4	2	3
Seguridad	4	1	3
Disponibilidad	3	2	2
Reglamentación SBS	3	2	2
Total	**14**	**7**	**10**

1= Excelente 2= Bueno 3= Regular 4= Malo

- **Costos:** La Alternativa II manejo mejor el tema de costos ya que al tratarse de una tercerizacion de servicios, se comparten los costos de infraestructura, las demás alternativas al tratarse de implementar algo propio (estamos suponiendo que el Banco del Dinero no cuenta con local para este fin) siempre el costo de la construcción y el mantenimiento hace que sea mas costosa.

- **Seguridad:** La Alternativa II, al tratarse de un Data Center especializado y construido para estos fines cuenta con un

sistema de seguridad certificado por entidades externas. Para las otras alternativas se tendría que hacer todo el proceso de certificación y una vez obtenido, se tendría que hacer el mantenimiento y las actualizaciones ; tarea operativa que incrementaría las funciones del banco.

- **Disponibilidad:** La Alternativa II la disponibilidad es inmediata, para las demás se tendría que esperar a concluir con el proceso de construcción.

- **Reglamentación SBS y otros:** Los Sites de los proveedores de este tipo de servicio han tomado en cuenta toda la reglamentación que sugiere la SBS y las entidades auditoras externas para su funcionamiento.

Como observamos en el cuadro anterior la opción que mejor se ajusta a los requerimientos del Banco es la Alternativa II Centro de Computo Alterno Tercerizado.

Una vez elegida la mejor alternativa nos centraremos en elegir al mejor proveedor de servicios disponible en el mercado, para ellos hemos convocado a todos los proveedores conocidos que tienen como clientes a bancos, a continuación un resumen de sus propuestas considerando costos, ventajas y desventajas:

Telefónica Data.: TDP
Pago Unico: $7,000
Pago Mensual: $6,900
Ventajas: Buena infraestructura con certificación internacional, incluye servidores.
Desventaja: Tiempo de respuesta no es la mejor, no ofrece valor agregado

AT&T:
Pago Unico: $1,185
Pago Mensual: $1000+1030=2,030
Ventaja: Tiempo de respuesta aceptable, bajo costo
Desventaja: Su local no es tan seguro como lo que requerimos, solo ofrece housing.

IBM:
Pago Unico: $10,000 (incluye consultoria de migración de Aplicativos).
Pago Mensual: $5,400
Ventaja: Fabricante de nuestro equipo As/400, alta especialización en manejo de hardware y software para estos equipos, valor agregado con periféricos (dispositivos de backup para AS/400 y Servidores, impresoras, lectoras, etc), ofrece Housing y Hosting y operación diaria.
Desventaja: Contrato forzoso a 5 años

GMD:
Pago Mensual: $495+1030= 1,525
Pago Unico: $1,015
Ventaja: Cliente importante para ellos, Independencia de las líneas de comunicación, Bajo Costo
Desventaja: Su cercania, menos de 2 millas. No incluye equipos ni equipos perifericos para los backup compatibles con lo que usa el banco.

IMPSAT:
Pago Mensual: $7,000
Pago Unico: $4,000
Ventaja: Data Center de Calidad Mundial, tiene clientes corporativos, buena llegada de lineas de comunicación, multicarrier.
Desventaja: Alto Costo, solo opción de Housing, no tiene ningun equipamiento de los que necesita el Banco.

3.4.2. Metodología para la decisión final.

	GMD	TDT	IBM	AT&T	IMPSAT
1. Costo	2	4	2	2	4
2. Distancia al CC	4	2	2	2	2
3. Seguridad	3	2	2	3	2
4. Servicio y Valor Agregado	3	3	2	3	3
5. Solidez Empresa	3	2	1	4	3
6. Experiencia en el producto	3	2	1	3	4
7. Infraestructura del Site	3	2	2	3	1
8. Tiempo de Implementación	2	2	2	2	2
PUNTAJE TOTAL :	**23**	**19**	**14**	**22**	**21**
1=Excelente, 2=Bueno, 3=Regular, 4=Malo					

* En el tema de Costos se puede mencionar que IBM del Perú incluía en su oferta un AS/400, 8 Servidores IBM y los periféricos compatibles a los equipos que posee el Banco. Asi mismo la consultoria para migrar aplicativos que usan conexión SNA a TCP/IP por actualizacion de Sistema Operativo.

Como resultado de la evaluación se recomienda contratar los servicios de IBM del Perú bajo la modalidad Hosting para la implementación del centro de computo alterno.

3.5 ESTRATEGIA ADOPTADA

Luego de la toma de decisión se pasara a describir el detalle del contenido de la estrategia adoptada para dar solución al problema presentado por el Banco. Estas estrategias fueron adoptadas de acuerdo a la metodología descrita en el punto 3.3.

3.5.1 FORMULACION DEL PROYECTO.

Se decidió contratar el Data Center con IBM (que de acá en adelante lo nombraremos como el Proveedor), y desarrollar el proyecto en conjunto.

3.5.1.1 Objetivos:

- El objetivo principal de este proyecto es desarrollar un conjunto de servicios que permita mantener la operación de los procesos críticos de negocio ante interrupciones prolongadas y llegar en el menor tiempo posible a restablecer los sistemas informáticos del Banco. En el Anexo 11 se describen los tiempos de recuperación estimados.
- Disponer de facilidades de centro de cómputo alterno para la implementación del plan de contingencia de sistemas.
- Tener la operación del CCA en manos de expertos en los equipos del mismo fabricante y un Data Center adecuado para una contingencia.

- Ahorro de costos frente a la opción de implantar y mantener por su cuenta la infraestructura y operación de un centro de cómputo de respaldo.
- Cumplir con los requerimientos de la Superintendencia de Banca y Seguros (SBS) con respecto al centro de cómputo de respaldo.

3.5.1.2 Alcances:

Producto del análisis de procesos críticos definidos por el negocio se decidió que el CCA debería proporcionar los siguiente servicios en caso de contingencia:

- Computador Principal replicándose en línea.
- Servidores que atienden el sistema de ventanillas de las agencias del Banco. Para el caso de contingencia se ha considerado activar casi de inmediato 11 agencias definidas por el área de negocios, el local principal y la segunda sede mas importante del Banco.
- Servidor que atiende el sistema de la Mesa de Dinero de Tesorería.
- Servidor que atiende el agente de Bolsa del Banco
- Servidor Macrofiche para tener los listados de consulta en línea.
- Servidor para la Administrador de usuarios de Red, para que puedan identificarse y conectarse a los equipos de la red.

- Servidor que atiende el sistema de Front Office de las agencias. Se ha contratado a AT&T como proveedor para las líneas de conexión para 11 agencias y 2 sedes principales del Banco. El cambio de las 11 agencias al centro de computo alterno será en forma automática.

3.5.1.3 Duración del proyecto

La duración del proyecto es de 17 meses, a continuación se muestra el cronograma de trabajo. Para mas detalle referirse al Anexo 8.

		Nombre de tarea	Duración	Inicio	Fin	Recurso
1		**PLAN DE CONTINUIDAD DE NEGOCIO**	4 mss	19/08/02	06/12/02	
2						
3		**PLAN DE CONTINGENCIA INFORMTICA (PCI)**	3 mss	19/11/02	10/02/03	
4						
5	✓	**⊟ CENTRO DE COMPUTO ALTERNO**	**202 días?**	**11/02/03**	**20/11/03**	
6	✓	**⊞ Analisis de Mercado**	**50 días**	**11/02/03**	**21/04/03**	
10	✓	**⊞ Plan de Respaldo**	**152 días**	**22/04/03**	**20/11/03**	
13	✓	**⊞ Analisis de cotizaciones**	**67 días?**	**08/05/03**	**08/08/03**	
18	✓	**⊞ Coordinaciones con el Proveedor**	**30 días**	**11/08/03**	**19/09/03**	
21						
22		**⊟ Servicio de contingencia para el Banco del Dinero (CCA)**	**132,5 días**	**17/09/03**	**25/03/04**	
23		**⊟ Etapa 1 - Implantación del proyecto**	**97,5 días**	**17/09/03**	**05/02/04**	
24	✓	Kickoff	1 día	23/09/03	23/09/03	IBM;BD
25	✓	Entrega de relación de personal del IBM asignada al proyecto	3 días	24/09/03	26/09/03	IBM
26	✓	Entrega de relación de personal de Bco Dinero asignado al proy	3 días	29/09/03	01/10/03	BD
27		Definición de plan de reuniones de control del proyecto	3 días	02/10/03	06/10/03	IBM;BS
28	✓	Firma del acta de inicio del servicio	0 días	23/09/03	23/09/03	IBM;BD
29		**⊞ Habilitación de facilidades de HW**	**43 días**	**24/09/03**	**24/11/03**	
43		**⊞ Instalación de SO y aplicativos en servidores Intel**	**2 días**	**28/10/03**	**29/10/03**	**BD**
46		**⊞ Instalacion del BDC (Backup Domain Controller Dom_**	**5 días**	**29/10/03**	**04/11/03**	**BD**
53		**⊞ Instalacion de Dinero Bolsa (Dedicado)**	**4 días**	**04/11/03**	**07/11/03**	
59		**⊞ Instalacion del Macrofiche (Compartido)**	**4 días**	**10/11/03**	**13/11/03**	**BD**
65		**⊞ Instalacion del SIG-Bussiness Object (Compartido)**	**4 días**	**14/11/03**	**19/11/03**	**BD**
71		**⊞ Servidores de Ventanilla (Dedicados)**	**19 días**	**29/10/03**	**24/11/03**	**BD**
92		Instalacion de las 5 PCs entregadas por IBM	2 días	07/11/03	10/11/03	BD
93		Pruebas de aplicativos Business Object, Macrofiche, Banktrade	2 días	26/12/03	29/12/03	
94		**⊟ Habilitación de facilidades de SW**	**79 días**	**17/09/03**	**09/01/04**	
95		**⊞ SW de replicación MIMIX**	**73 días**	**24/09/03**	**08/01/04**	

95		⊞ **SW de replicación MIMIX**	**73 días**	**24/09/03**	**08/01/04**	
103	✓	Adquisición de licencia BRMS	25 días	17/09/03	22/10/03	IBM
104		⊞ Instalación y configutación de BRMS	6 días	23/10/03	30/10/03	
109		Instalación y configuración de sistemas de Bco en iSeries**	1 día	20/11/03	20/11/03	BD
110		Full backup de servidor iSeries	1 día	09/01/04	09/01/04	IBM
111		⊟ **Habilitación de Comunicaciones**	**68,25 días**	**09/10/03**	**16/01/04**	
112	✓	⊞ **Coordinación**	**5 días**	**09/10/03**	**15/10/03**	
118		⊞ **Implantación**	**63,25 días**	**16/10/03**	**16/01/04**	
128		⊟ **Tareas Paralelas de Migración**	**82 días**	**17/09/03**	**14/01/04**	
129		⊞ **Migración aplicativo Comercio Exterior**	**25 días**	**17/09/03**	**22/10/03**	
138		⊞ **Migración aplicativo Bandinero**	**65 días**	**03/10/03**	**07/01/04**	
165		Migración a SO 5.1 y App servidor desarrollo BS	5 días	30/12/03	07/01/04	IBM, BD
166		Migración a SO 5.1 servidor producción BS	2 días	06/01/04	07/01/04	IBM, BD
167		Configuración de herramientas de control de cambios	1 día	07/01/04	07/01/04	BD
168		Definición de esquema de seguridad con TCP/IP	10 días	10/11/03	21/11/03	IBM, BD
169		Implantación de esquema de seguridad	5 días	08/01/04	14/01/04	BD
170		⊟ **Definición Inicial de Procedimientos del servicio**	**67 días**	**06/10/03**	**12/01/04**	
171		Entrega de procedimientos de Centro de Computo Alterno d	1 día	07/10/03	07/10/03	IBM
172		⊞ **De Operación**	**30 días**	**13/10/03**	**21/11/03**	
188		⊞ **Administrativos**	**20 días**	**13/10/03**	**07/11/03**	
191		Prueba de procedimientos	3 días	08/01/04	12/01/04	
192		Definición de proc de recuperación en contingencia DRP	15 días	06/10/03	27/10/03	BD
193		⊟ **Prueba unitaria del servicio (sin usuarios)**	**18,5 días**	**12/01/04**	**05/02/04**	
194		⊞ **Planeamiento**	**6 días**	**12/01/04**	**19/01/04**	
198		⊞ **Desarrollo**	**9 días**	**20/01/04**	**30/01/04**	
203		Entrega de informe de las actividades ejecutadas por IBM	0,5 días	27/01/04	27/01/04	IBM
204		Aprobación de informe	7 días	27/01/04	05/02/04	BD
205		Firma del Acta de Conformidad de la Etapa I	0 días	05/02/04	05/02/04	IBM;BD

3.5.1.4 Equipo de Proyecto

El detalle del equipo de trabajo y sus roles para llevar adelante el proyecto se describen en el siguiente cuadro:

ROL	DESCRIPCIÓN
Ejecutivo del Proyecto o Gerente de Unidad	Ejecutivo de cargo gerencial quien se mantendrá informado del proyecto y a quien se escalará los temas relacionados al proyecto. Existe un Ejecutivo a Nivel Gerencial por parte del Banco y su par parte del Proveedor. Participaran de las reuniones ejecutivas para evaluar el avance del proyecto y tomar decisiones si existieran actividades que puedan poner en riesgo el proyecto o en todo caso barreras que se presenten que afecten los tiempos o costos.
Gerentes o líder del Proyecto	Ejecutivo designado como dueño o responsable del proyecto. Dicho ejecutivo y sus delegados tendrán la suficiente autoridad y atribución para resolver los conflictos que puedan poner en riesgo los objetivos, metas o resultados del Proyecto. Existe un Gerente por parte del Banco y un por parte del Proveedor del servicio, quienes tendrán sus reuniones periódicas (semanales y quincenales), para evaluar el avance del proyecto y las acciones a tomar por tareas que se puedan atrasar o por las tareas siguientes a la reunión.

ROL	DESCRIPCIÓN
Líder Usuario	Ejecutivo del Banco designado como responsable para llevar a cabo las actividades necesarias con los usuarios de las diversas áreas del Banco para cumplir con las pruebas periódicas del Centro de Computo Alterno. Responsable de la capacitación de los procedimientos al personal involucrado de acuerdo a lo establecido en el Plan de Continuidad Informático.
Líder Técnico	Ejecutivo responsable del diseño de la arquitectura tecnológica de la solución para el problema planteado. Llevara a cabo la implementación del CCA con el equipo de especialistas tecnológicos tanto del Banco como del proveedor.
Especialistas en Aplicativos de Negocios que funcionen AS/400 e Intel	Personas con conocimientos técnicos sobre la plataforma AS/400 e Intel y los aplicativos del Banco que corran sobre los mismos. Quienes montaran los Sistemas de Negocios del Banco y los dejaran funcionando de acuerdo a lo establecido para un desastre en el Centro de Computo Principal.
Especialistas de SW especializado y Comunicaciones	Personas con conocimiento técnico sobre software de base (Sistemas operativos y afines), replicación, backup, Redes y Seguridad, quienes instaran y configuraran dichos aplicativos de acuerdo a los estándares del Banco.
Especialistas Técnicos para la operación.	Especialistas encargados del mantenimiento y soporte de servidores y comunicaciones durante la operación en el CCA por parte del proveedor.
Operadores	Personas con conocimiento técnico sobre labores de operación de sistemas y cuya responsabilidad es apoyar al Coordinador del Proyecto en todas las gestiones y labores que él considere pertinente realizar

3.5.1.5 Beneficios del Proyecto

Los beneficios potenciales que se alcanzaran con la implantación del presente proyecto son los siguientes:

- Ahorro, al compartir los costos de infraestructura de un centro de cómputo.
- Alternativa eficiente, al utilizar recursos que pueden ser compartidos con otros clientes (*) para el caso en que la recuperación sea mayor a 4 horas.
- Contar con especialistas en hardware y software del proveedor como recursos de soporte para el Centro de Cómputo Alterno.
- Concentrar el tiempo de sus recursos del área de Tecnología de Información en la puesta en marcha de otros proyectos asociados al negocio.
- Costos fijos, presupuestables de acuerdo a una tarifa mensual acordada para un periodo de sesenta (60) meses.

3.5.1.6 Riesgos del Proyecto

- Los riesgos mas relevantes son:
- Al tratarse de un servicio tercerizado, existe el riesgo de que el proveedor suspenda el servicio por decisiones corporativas; es decir ya no ofrecer mas servicios de ese tipo.
- Siendo un proyecto que no traerá ingresos financieros para el banco, existe la posibilidad de que no se le asigne la prioridad del caso y se deje de lado para continuar con otros proyectos que si representen ingresos sustanciales.
- Un cambio en la estrategia de TI también podría hacer que este proyecto se detenga o en todo caso se modifiquen los términos del servicio y sus condiciones.

3.5.2 INFORME DE DEFINICION.

Las principales definiciones del proyecto son:

- Implementación del servicio.
- Consultaría para la Migración de Sistema Operativo del Computador Central.
- Disponibilidad de la infraestructura de un Centro de Cómputo Alterno.
- Disponibilidad de capacidad de procesamiento de un servidor AS/400 en calidad de "Capacidad Principal Dedicada", mas adelante se definirá las características del equipo ofrecido.*

- Licencias del Software de replicación de datos MIMIX para el computador de replica en el CCA.
- Disponibilidad de capacidad de procesamiento en la plataforma Intel, en las modalidades de “Capacidad Complementaria Dedicada”, y “Capacidad Complementaria Compartida”, mas adelante se detalla la configuración ofrecida.(*)
- Equipos de comunicaciones por el lado del proveedor. Mas adelante se detallara la configuración ofrecida.
- Servicios de operación 24 x 7 x 365.
- Plan de pruebas periódicas de verificación de la recuperación, asistencia durante su ejecución y documentación del resultado de las mismas.

3.5.3 ETAPAS DEL PROYECTO.

El presente proyecto será implantado en 2 etapas, las cuales se iniciarán a la firma del Contrato. La primera etapa corresponde a la implementación y la segunda a la operación mensual del servicio.

A continuación se describe cada una de estas etapas:

3.5.3.1 Implementación del Proyecto

Esta etapa se iniciará a la firma del “Acta de Inicio de Proyecto”, máximo a los quince (15) días de firmado el contrato. Una vez firmada el acta, el proveedor notificará por escrito al Banco la

relación del personal asignado al proyecto, debiendo también el Banco notificar al Proveedor la relación de su personal asignado al proyecto. Ambas partes deberán remitir dichas comunicaciones dentro de los 10 días calendario de firmada el acta. Durante la semana siguiente a la firma del acta, los coordinadores de ambas partes se reunirán para definir el cronograma definitivo de implantación del proyecto. Se debe considerar que las particiones estarán disponibles a los 35 días calendario de firmada el acta. Se definirán fechas definitivas para las siguientes actividades, las mismas que deberán llevarse a cabo durante esta etapa:

- Habilitación de las particiones y/o servidores provistos por el Proveedor (Responsabilidad del Proveedor).
- Instalación y configuración del sistema operativo y del software de replicación MIMIX en el lado del Proveedor (Responsabilidad del Proveedor).
- Instalación y configuración de otros productos de software, programas, bases de datos y aplicaciones en general (Responsabilidad del Ciente).
- Habilitación de las comunicaciones (Responsabilidad del Banco y del Proveedor).
- Habilitación de la replicación de datos (Responsabilidad del Banco y del Proveedor).

- Habilitación del software BRMS (Responsabilidad del Cliente)
- Entrega de procedimientos del Centro de Cómputo
- Alterno del Proveedor (Responsabilidad del Proveedor)
- Definición de procedimientos de operación y reportes del servicio (Responsabilidad del Banco y del Proveedor).

Entregable :

El proveedor entregará al Banco un informe sobre la ejecución de las actividades bajo su responsabilidad ejecutadas.

Criterio de Aceptación :

Esta etapa se considerará aceptada una vez que el entregable sea revisado y aceptado por el Coordinador del Proyecto del Banco. Una vez entregado, se procederá a suscribir el Acta de Conformidad del Proyecto entre el Banco y el proveedor.

El acta deberá levantarse y ser suscrita por las partes a más tardar dentro de los siete (7) días calendario siguientes a la fecha de entrega de la documentación. Una vez transcurrido este plazo, sin que el Banco haya realizado observaciones, el acta y el entregable correspondiente se considerarán aceptados tácitamente.

Consideraciones:

1. El Banco deberá ejecutar sus labores dentro de los 30 días calendario siguientes a la fecha señalada en el Acta de

Inicio del Proyecto. Cualquier cambio deberá ser manejado mediante el Procedimiento de Control de Cambios.

2. Durante este periodo se requiera la participación intensiva de los recursos del Banco, entre los que deben estar :
   - Un (1) Gerente de Proyecto.
   - Un (1) Especialista de AS/400 y de las aplicaciones que funcionan sobre esta plataforma en el ambiente de producción del Banco.
   - Un (1) Especialista de Intel y de las aplicaciones que funcionan sobre esta plataforma en el ambiente de producción del Banco.
   - Un (1) Especialista de MIMIX.
   - Un (1) Especialista de Redes.
   - Un (1) Especialista de Seguridad.
   - Un (1) Especialista de BRMS.
3. En caso que el Banco no proceda a ejecutar y terminar las actividades bajo su responsabilidad, dentro de los 15 días calendario siguientes a la fecha planeada, las actividades listadas con anterioridad y los costos fijos del servicio (utilización de particiones y/o servidores, equipos de comunicaciones y espacio de Centro de Cómputo) serán facturadas directamente al Banco, salvo que el Banco presente una carta justificatoria por el retraso y la misma

luego de ser evaluada por el Proveedor sea considerada a criterio del Proveedor como una excepción.

4. En caso que el proveedor no proceda a ejecutar y terminar las actividades bajo su responsabilidad, dentro de los 15 días calendario siguientes a la fecha planeada se otorgará a favor del Banco el equivalente a N días adicionales de servicio, siendo N la cantidad de días útiles de retraso. Esto aplica siempre y cuando el proveedor no presente una carta justificatoria por el retraso, la cual luego de ser evaluada por el Banco sea considerada, a criterio del Banco, como una excepción.
5. .Durante esta etapa, los Gerentes de Proyecto o las personas que ellos designen se reunirán una vez por semana como mínimo o cuando lo estimen conveniente, previo acuerdo entre ambas Partes, para revisar el desarrollo del servicio y los posibles cambios del mismo.
6. Se deberán firmar Actas para controlar el avance del servicio cada dos (2) semanas.

3.5.3.2 Operación del Centro de Computo Alterno.

Esta segunda etapa del proyecto comenzará una vez concluida la etapa anterior.

Se ejecutarán las actividades relacionadas a la verificación de la disponibilidad del servicio y toma de backups señaladas en la sección "Desarrollo del Servicio"

Los Coordinadores se reunirán al menos una vez por mes o cuando lo estimen conveniente, previo acuerdo entre ambas partes, para revisar el desarrollo del servicio y los posibles cambios del mismo.

Adicionalmente, los Coordinadores del Proyecto del Banco y el proveedor deberán coordinar la ejecución de una (1) prueba del plan de contingencia por semestre.

Entregable

- El proveedor entregará al Banco un reporte mensual que contiene información sobre los eventos ocurridos durante la operación del servicio (ver Anexo 17).
- El proveedor entregará al Banco un informe al final de las pruebas de contingencia en base a la encuesta de evaluación de la prueba de contingencia (Anexo 15). Las pruebas de contingencia podrán ejecutarse una (2) veces al año.

Criterio de Aceptación

Esta etapa se considerará aceptada una vez que el entregable sea entregado y aceptado por Cliente.

El acta deberá levantarse y ser suscrita por las Partes a más tardar dentro de los siete (7) días calendario siguientes a la fecha de entrega de la documentación. Una vez transcurrido este plazo, sin que el Banco haya realizado observaciones, el acta y el entregable correspondiente se considerarán aceptados tácitamente.

3.5.4 RESPONSABILIDADES DEL BANCO.

Las principales responsabilidades son:

1. Asignar los recursos requeridos para la prestación del servicio, señalados en párrafos anteriores.
2. Asignar un Gerente de Proyecto, quien deberá ser el punto de contacto frente al Proveedor para los asuntos relacionados a la prestación del servicio.
3. Proveer los enlaces de comunicaciones necesarios tanto para la replicación de los datos como para acceso de los usuarios. El proveedor brindará las configuraciones requeridas para replicación de datos.
4. Proveer los equipos de comunicaciones requeridos en las oficinas del Banco.

5. Instalar, configurar, mantener y dar soporte al software requerido, excepto al sistema operativo.
6. Brindar soporte de software de Replicación para el computador Central.
7. Mantener el convenio de soporte de la solución del software de replicación de los computadores principales con el proveedor de este servicio.
8. Implementar y dar soporte al software BRMS.
9. Contar con un plan y procedimientos de recuperación actualizados
10. Ejecutar pruebas del plan de recuperación.
11. Ejecutar las tareas de recuperación.
12. Operar los equipos de recuperación durante una situación de contingencia o durante las pruebas.
13. El Banco es responsable por el traslado de los cartuchos de backup desde y hacia el Centro de Servicios Integrados del Proveedor.
14. Generar cartuchos de backup de los servidores Intel en sus oficinas.
15. Identificar los cartuchos para toma de respaldos de acuerdo con los procedimientos entregados al Proveedor.
16. Informar los cambios que se requieran en la configuración de respaldo mediante el Procedimiento de Control de Cambios.

17. Proporcionar suministros (papel para impresora, cartuchos, etc.), materiales y medios de almacenamiento que sean necesarias para la adecuada ejecución del servicio.
18. Informar al Proveedor los datos de los recursos que requieren ingresar y las fechas y horas requeridas (simultáneamente, máximo el número de usuarios contratados). Esto es válido tanto para recursos internos del Banco como para aquellos externos que ingresan a nombre del Banco, como por ejemplo los proveedores.
19. Aceptar los cargos ocasionados por llamadas salientes desde el Centro de Cómputo en cualquiera de las líneas de comunicación asignadas. El proveedor habilitará un punto de red para un teléfono IP que se configurará sólo para pruebas de contingencia y/o casos de contingencia real.
20. Designar un punto único de contacto para el manejo del servicio y definir dos (2) personas de nivel ejecutivo; como las autorizadas para hacer la declaración oficial de la contingencia ante el Proveedor.
21. Dirigir y responder por el adecuado desarrollo del Proceso para Control de Cambios al servicio, manteniendo al día la documentación de los cambios y garantizando que la configuración contratada sea acorde a los requerimientos del negocio.

22. Seguir los procedimientos que el proveedor especifique para el proyecto de Centro de Cómputo Alterno. Estos procedimientos serán entregados al Banco al inicio del servicio por el coordinador designado por el Proveedor (como referencia ver Anexo16).
23. Acusar recibo y dar respuesta por el mismo medio a las comunicaciones que así lo requieran dentro de los cinco (5) días calendario siguientes a su recibo.
24. Operar sus conexiones con el Proveedor de comunicaciones. El proveedor del CCA brindará las configuraciones requeridas para replicación de datos.
25. Mantener los niveles de seguridad que requiera la información y su manejo.
26. Participar en reuniones periódicas de seguimiento y control del proyecto.

3.5.5 DESARROLLO DEL PROYECTO.

Para lograr la solución del problema planteado se debe desarrollar el proyecto que como resultado nos de un CCA planteado, para ello es necesario definir un conjunto de servicios que busquen mantener la operación de los procesos críticos de negocio ante interrupciones prolongadas y llegar en el menor tiempo.(ver Anexo 11), "Tiempos de Recuperación") , a restablecer los sistemas informáticos del Banco.

A continuación se definen los servicio, premisas y responsabilidades que se definen entre el Banco y el Proveedor:

3.5.5.1 Alcance del Proyecto.

El alcance de este proyecto es la recuperación del ambiente de producción que se ejecuta en el entorno AS/400 e Intel, ante la posibilidad de una contingencia que impida la utilización de los sistemas del Banco.

3.5.5.2 Características del Proyecto.

3.5.5.2.1 Centro de Cómputo Alterno

La infraestructura de Centro de Cómputo cuenta con sistemas de detección y extinción de incendios, piso y falso techo, cableado de sitio, control de acceso, paredes y vidrios externos blindados y reforzados. Asimismo, el Centro de

Cómputo cuenta con equipos de UPS, Grupo Electrógeno y Aire Acondicionado. El detalle de la infraestructura actual del Centro de Cómputo se presenta en el Anexo 12 .

El local del Proveedor tiene un servicio de seguridad que opera las 24 horas y que tiene, entre otras funciones, realizar un monitoreo constante a través del Circuito Cerrado de Televisión. El acceso al local es controlado y dentro del local, las áreas son clasificadas y controladas para evitar el acceso a áreas no autorizadas.

El Centro de Cómputo estará disponible de Lunes a Domingo, las 24 horas del día, los 365 días del año.

Hasta este Centro de Computo llegarán los enlaces de comunicaciones del Banco.

El Banco puede realizar visitas de inspección al Centro de Cómputo del Proveedor, siguiendo las siguientes pautas:

- Las visitas se deben coordinar con el Proveedor con una (1) semana de anticipación, como mínimo.
- Las visitas se pueden realizar de Lunes a Viernes, en horas de 9:00 AM a 5:30 PM..
- Las visitas tienen una duración de una (1) hora como máximo y siempre deben conducirse en compañía de un representante del Proveedor.

- El Coordinador de Proyecto del Banco debe enviar al Proveedor la lista de personas autorizadas por el Banco para realizar las visitas.
- El máximo de personas es tres (3), sin embargo, en casos de excepción y previo acuerdo mutuo, podrán asistir más personas.
- El Banco podrá realizar hasta dos (2) visitas no programadas al año al Proveedor. Estas visitas deberán ser solicitadas con un plazo no menor a cuatro (4) horas de anticipación y no deberán coincidir con las labores programadas del Proveedor, las cuales son notificadas con por lo menos dos (2) semanas de anticipación.
- En caso el Banco requiera llevar personal de terceros al Centro de Cómputo del Proveedor, podrá hacerlo siempre y cuando cuente con la autorización previa del Proveedor. Para esto, el Banco deberá enviar al Proveedor una carta explicando la necesidad de la visita. El proveedor evaluará caso por caso y podrá autorizar o denegar el acceso. En este último caso, el Proveedor enviará una carta al Banco explicando las razones.

3.5.5.2.2 Capacidad de Procesamiento

El proveedor pondrá a disposición del Banco la capacidad de procesamiento que se describe a continuación:

Capacidad Principal Dedicada

El Banco podrá hacer uso de la siguiente capacidad de procesamiento de un servidor AS/400, para ser usada en replicación de datos, pruebas de contingencia y/o los casos de contingencia:

- Capacidad Batch : 950 CPWs
- Capacidad Interactiva : 150 CPWs
- Memoria RAM : 4 GB
- Disco Duro : 150 GB
- Tarjeta de red Ethernet de 10/100 Mbps
- Lectora de CD

Adicionalmente, el Banco podrá hacer uso de esta capacidad para ejecutar algún reproceso que crea conveniente. En caso se den algún reproceso, el proveedor es responsable de ejecutar las tareas de operación asociadas a la colación de cintas y al control del proceso. Es responsabilidad del Banco que no se vea afectado el funcionamiento de la replicación de

datos y el desempeño del servidor debido a la ejecución de reproceso.

Capacidad Complementaria Dedicada

El Banco podrá hacer uso de la siguiente capacidad de procesamiento Intel para ser usada en pruebas de contingencia y/o casos de contingencia:

- Servidor de Agencias 1 : 2 procesadores de 2.4 Ghz, 1 GB de RAM y 1 disco de 40 GB.
- Servidor de Agencias 2: 2 procesadores de 2.4 Ghz, 1 GB de RAM y 1 disco de 40 GB.
- Servidor de Base de Datos : 2 procesadores de 2.4 Ghz, 1 GB de RAM y 2 discos duros de 73.4 GB c/u.
- Servidor para Mesa de Dinero: 2.4 Ghz, 1 GB de RAM y 1 Disco duro de 40 GB.
- Servidor que atiende al Agente de Bolsa: 2.4 Ghz, 1 GB de RAM y 1 disco de 40 GB.
- Servidor BDC+DNS-WINS-DHCP: 2.4 Ghz, 2 GB de RAM y 2 discos de 40 GB c/u.

El Banco podrá dejar sus programas pre configurados en los servidores. Estos servidores y/o particiones Intel cuentan con

una (1) tarjeta de red Ethernet de 10/100 Mbps y una (1) lectora de CD.

Capacidad Complementaria Compartida

El Banco podrá hacer uso de la siguiente capacidad de procesamiento y/o herramientas de backup para ser usadas en pruebas de contingencia y/o casos de contingencia:

- Servidor Macrofiche : 1.26 Ghz, 1 GB de RAM. 1 disco de 36 GB y 1 disco de 18 GB.
- Servidor del Sistema de Información Gerencial: 1.26 Ghz, 1 GB de RAM y 2 discos de 73 GB c/u.
- Unidad de tape backup LTO 3581 y Tivoli Storage Manager.
- Unidad de tape 3590.
- Impresora 6412 de 1200 LPM.
- Una unidad de Tape Backup externa DDS-4.
- La unidad de tape backup LTO 3581 será homologada por el Proveedor para que pueda leer la información del TSM del Banco.

3.5.5.2.3 Sala de Usuarios.

El Banco dispondrá de una sala de usuarios equipada con cinco (5) puestos de trabajo, cinco (5) anexos telefónicos, un

(1) fax, una (1) impresora láser de 24 ppm y cinco (5) PCs con la siguiente configuración: PIII de 450 MHz, 128 MB de memoria RAM y 10 GB de disco duro, conexión Ethernet 10/100 Mbps, teclado, mouse y sistema operativo Windows XP. Estas facilidades estarán disponibles en caso de contingencia, o para realizar las pruebas.

En caso de contingencia y/o pruebas, las PCs tendrán comunicación con la LAN de contingencia del Banco, ubicada en el Centro de Cómputo Alterno del Proveedor. El Banco podrá instalar software Windows NT o Windows 2000 de su propiedad en las PCs de la Sala de Usuarios en caso de contingencia o pruebas. El Banco es responsable por las licencias de estos productos.

3.5.5.2.4 Equipo de Telecomunicaciones.

Para la comunicación entre el Centro de Cómputo del Proveedor y la oficina principal del Banco, se hará uso de la Red de Multiservicio del Proveedor, la cual está constituida por diversos equipos que permiten la conexión a diversos proveedores de comunicaciones y a los servicios internos del Proveedor. La configuración de la Red de Multiservicio incluye un Router Cisco de la familia 7200, con el sistema operativo

Cisco IOS que soporta funcionalidades avanzadas y firewall, y un Switch Cisco Catalyst de la familia 4006, con la capacidad de soportar enlaces Ethernet, Fast Ethernet y Gigabit Ethernet.

Este servicio ofrece funcionalidades de Firewall (Ver Anexo 13), las cuales protegerán al Banco de accesos no autorizados por parte del personal del Proveedor y de personal de otros clientes.

Adicionalmente, este servicio también brinda protección al Proveedor y a otros clientes de accesos no autorizados de personal del Banco.

Como parte de las facilidades ofrecidas en la presente propuesta, el Proveedor habilitará

- Un puerto de router con capacidad de 4 Mbps donde llegará en enlace de replicación de datos contratado por el Banco.
- Catorce (14) puntos de switch para la conexión entre los servidores y las PCs de la sala de usuarios (ver sección "Sala de Usuarios").
- El proveedor dará las facilidades al Banco, realizando las configuraciones necesarias en la Red Multiservicio, para que:
  - ✓ Los servidores Intel instalados en el Proveedor puedan replicar datos y programas con los

servidores Intel instalados en las oficinas del Banco. El Bancos es responsable por la implementación y administración de la replicación. Igualmente, el Banco es responsable por el impacto que tengan estas replicaciones en el desempeño del enlace de telecomunicaciones.

- ✓ Los servidores Intel asignados al Banco puedan conectarse a Internet, a través de la conexión a Internet del Banco, y realizar upgrades en línea.

- El Proveedor del que desarrolle el proyecto enviará un reporte mensual al Banco que contiene los hechos relevantes del servicio. Este reporte incluye instalación de parches de seguridad del firewall IOS, los cuales se ejecutarán cada vez que sea necesario, y los eventos que afecten la disponibilidad del servicio.
- El Banco podrá configurar 2 Subredes IP y 1 SNA en el ambiente de contingencia provisto por el Proveedor, utilizando para tal fin, los equipos de telecomunicaciones provistos por el Proveedor.
- El Banco podrá solicitar cambios en la configuración de los equipos de comunicaciones del Proveedor una (1) vez por trimestre, siempre y cuando no se exceda el

número de puertos físicos 10/100 estipulados en el contrato.

- En caso el Banco requiera cambios en las capacidades ofrecidas o cambios en la configuración podrá solicitarlos al Proveedor, quien evaluará caso por caso. Estos cambios deben ser manejados mediante el Procedimiento de Control de Cambios (ver Anexo 10).
- En el Anexo 14 se muestra el diagrama de red del Banco.

3.5.5.2.5 Sistema Operativo del Computador Central.

La partición del servidor AS/400 provista por el Proveedor cuenta con sistema operativo OS/400 V5.1.

Este producto será instalado por el Proveedor con el último nivel de PTF disponible al momento de la instalación.

Adicionalmente, este producto contará con mantenimiento preventivo y correctivo a través de paquetes acumulativos de PTFs y/o PTFs individuales, cuya aplicación será de responsabilidad del Proveedor, previo acuerdo con el Banco.

En caso el Banco migre de versión de sistema operativo, el Proveedor instalará en el servidor de contingencia la misma versión del Banco. Estos cambios se podrán dar hasta dos (2)

veces el primer año, y a partir del segundo año una (1) vez por año.

3.5.5.2.6 Software de Replicación en Línea

El proveedor adquirirá e instalará el software de replicación de los AS/400 en sus equipos. Esto implicara un ahorro de costo para el Banco ya que solo tendrá que costear el que use en su Centro de Computo.

3.5.5.2.7 Instalación del Software Aplicativo.

Esta propuesta incluye la instalación de las bibliotecas de acuerdo con los requerimientos de replicación especificados a partir de los datos provistos oportunamente por el Banco.

Asimismo, se incluye la activación de la journalización de datos y objetos a ser replicados, comprobación de replicación de los datos, objetos y la ejecución del switch de procesos hacia el equipo target, bajo una condición equivalente a una contingencia.

3.5.5.2.8 Operación

Consiste en la ejecución de actividades periódicas que permitan el correcto funcionamiento del servicio del presente proyecto.

Este servicio será brindado en forma permanente durante la vigencia del contrato, 24 horas al día, 7 días a la semana, 365 días al año.

A continuación se describen las actividades de operación:

Monitoreo de Sistema Operativo

Monitoreo de los archivos de bitácoras (log) del sistema operativo para la verificación del correcto funcionamiento de los componentes de software (Sistema Operativo) y Hardware de manera preventiva y correctiva. Dicho monitoreo se efectuará de manera automática cada 15 minutos con la Herramienta de Gestión del Centro de Cómputo.

Monitoreo del Proceso de Replicación

Monitoreo de la herramienta de replicación de datos, revisando que el proceso de replicación se encuentre operativo y revisión de archivos de bitácoras (log) para la verificación del correcto funcionamiento. Dicho monitoreo se efectuará cada 2 horas.

Se definirán en conjunto con el Banco y el proveedor los procedimientos claros de monitoreo, determinación de problemas y escalamiento relacionados con el software de Replica. Estos procedimientos será ejecutados por el Proveedor.

Monitoreo de Redes

Monitoreo de la disponibilidad y desempeño del enlace de comunicaciones, que permita un correcto acceso y operatividad del proceso de replicación de datos. Dicho monitoreo se efectuará de manera automática cada 30 segundos con la Herramienta de Gestión del Centro de Cómputo.

Toma Periódica de Respaldos

Contempla la ejecución de backups del servidor AS400, con frecuencia diaria, de la siguiente forma:

- Un (1) backup al inicio del cierre diario de las operaciones del Banco.
- Un (1) backup, en dos (2) copias al final del cierre diario. Las políticas de backup se definirán al inicio del proyecto en forma conjunta con el Banco.

El almacenamiento de las cintas ya grabadas se realizará en forma inmediata a la finalización de la grabación, en un ambiente especial ubicado en el Centro de Cómputo del Proveedor.

Mantenimiento de Hardware

Contempla la ejecución de mantenimientos preventivos y correctivos de las particiones y/o servidores provistos por el Proveedor.

El Proveedor es responsable de reparar las fallas, de presentarse. Esto puede implicar la reinstalación y pruebas del aplicativo. En caso de ocurrir fallas de hardware, el Proveedor comunicará al Banco tal ocurrencia lo antes posible para que el Banco pueda programar y efectuar las labores de instalación, actualización y pruebas del aplicativo.

Soporte de Software

Contempla los servicios de soporte técnico relacionados al sistema operativo OS/400 provisto por el Proveedor.

- El soporte de otros programas, como por ejemplo, el sistema operativo Windows que se instale en los servidores Intel es responsabilidad del Banco.
- En caso el Banco necesite realizar upgrades de software en los servidores Intel en linea via Internet el Proveedor efectuará configuraciones en la Red Multservicio, para que los servidores Intel del Proveedor puedan conectarse a Internet, a través de la conexión a Internet

del Banco, y realizar los upgrades. En otro caso será con la presencia física de los Técnicos del Banco en el CCA.

Registro de Eventos en Bitácora

Es la documentación de los eventos del servicio en un archivo de bitácora dedicado al Banco. Se incluyen eventos, fecha de eventos, estado del evento, especialistas involucrados.

En el reporte mensual al Banco se le enviará los casos relevantes para su información y acciones del caso.

Escalamiento de Problemas

Consiste en notificar e involucrar diferentes niveles dentro de la organización del Proveedor y del Banco para resolución de problemas.

Almacenamiento de Registros Vitales

El Proveedor dispondrá un área para uso del Banco donde se almacenarán los cartuchos correspondientes a sus registros vitales. El Proveedor asignará al Banco 2 lockers con las siguientes dimensiones cada uno: 30 cm de ancho x 40 cm de largo y 35 cm de profundidad, y se encontrará ubicado en el interior del Centro de Cómputo del Proveedor, cumpliendo con los requerimientos de seguridad y de medio ambiente. El

Banco es responsable por el traslado de cintas. El horario en envío y/o recojo de cintas podrá realizarse de Lunes a Domingo, las 24 horas del día. La frecuencia y horarios habituales serán definidos al inicio del proyecto, en forma conjunta, entre el Banco y el Proveedor.

Observaciones:

- En relación a los servicios de backup del Proveedor, la configuración del Tivoli es responsabilidad del Proveedor.
- Los backups del Banco efectuados con Tivoli y LTO podrán ser leídos por los equipos del Centro de Cómputo Alterno del Proveedor.

3.5.5.3 Uso del Centro de Cómputo en Casos de Contingencia

El proveedor tendrá disponible la capacidad dedicada en forma inmediata a la declaración oficial de contingencia; y la capacidad compartida dentro de las dos (2) horas, con un máximo de cuatro (4) horas, siguientes a la declaración oficial de contingencia.

Las instalaciones del Centro de Cómputo Alterno del Proveedor están operativas las 24 (veinticuatro) horas del día durante los 7 (siete) días de la semana.

El Banco deberá proveer el personal apropiado, los suministros, los programas y los procedimientos de recuperación,

compatibles con el equipamiento del Centro de Cómputo del Proveedor. Los detalles serán revisados durante la fase de Implementación Inicial del Proyecto.

La comunicación inicial del Banco al Proveedor de una Situación de Contingencia, puede ser en forma oral pero debe ser seguida por una notificación escrita dentro de las veinticuatro 24 (veinticuatro) horas siguientes a la comunicación inicial.

Si el Banco sufriera una Situación de Desastre y en consecuencia, utilizara las instalaciones del Centro de Cómputo del Proveedor, deberá informar al Proveedor, por razones de planeamiento, el lapso durante el cual estima hacer uso de las instalaciones.

El Banco tendrá derecho a usar las facilidades de uso compartido del Centro de Cómputo durante un periodo de hasta 30 días al año en casos de contingencia. Cuando el Período de Recuperación haya vencido, el Banco deberá enviar una nueva notificación de Situación de Desastre al Proveedor para continuar haciendo uso de las facilidades de uso compartido del Centro de Cómputo, en cuyo caso aplicará el cargo adicional señalado en la sección “Condiciones Comerciales”. El Banco, para obtener un nuevo período, deberá probar que fueron realizadas todas las acciones necesarias para restablecer los

recursos que originariamente fueron afectados por la Situación de Desastre en sus instalaciones de procesamiento de datos. Sin embargo, en caso de que otro Cliente suscrito sufriera una Situación de Desastre durante el período de extensión, este último tendrá prioridad sobre el uso de las instalaciones del Centro de Cómputo.

3.5.5.4 Pruebas del Plan de Contingencia

Con el objeto de poder verificar el funcionamiento del Plan de Contingencia, el Banco podrá solicitar al Proveedor la realización de una prueba cada ocho (8) meses durante el periodo de vigencia del Contrato. Para tal efecto deberá comunicar por escrito al Proveedor, con quince (15) días de anticipación, la fecha requerida para la realización de las pruebas. El tiempo que tomen las pruebas, no deberá exceder las veinticuatros (24) horas efectivas. Las pruebas podrán ser pospuestas por el Proveedor si una notificación de contingencia de otro Cliente es recibida; en este caso, el Proveedor re programará el tiempo de prueba, lo cual será notificado oportunamente al Banco.

El detalle del procedimiento del Plan de Pruebas se encuentra en el Anexo 16.

Observaciones:

- Las pruebas podrán ser realizadas en fines de semana.
- En caso el Banco requiera tiempo adicional para realizar pruebas y esto implique un consumo adicional de los recursos e infraestructura provistos por el Proveedor para la ejecución de las mismas, aplicará el cargo por uso adicional estipulado en la sección “Condiciones Comerciales”.
- El Banco podrá realizar hasta una (1) prueba no programada al año. La primera prueba no programada deberá realizarse despues de efectuada la primera prueba programada. Las pruebas no programadas no deberán coincidir con las labores programadas del Proveedor, las cuales son notificadas con por lo menos dos (2) semanas de anticipación. Estas pruebas se efectuarán en adición a las pruebas programadas.

3.5.5.5 Plan de Pruebas para el Proyecto

A los efectos de obtener una recuperación controlada, en el marco del servicio propuesto, este proyecto incluye la realización de ocho (8) pruebas del plan de contingencia, con una duración de cuarenta y ocho (48) horas efectivas cada una para las dos (2) primeras y veinticuatro (24) horas efectivas para cada una de las seis (6) siguientes. Las pruebas deben realizarse cada ocho

(8) meses. Las pruebas de contingencia se realizarán de acuerdo al horario establecido entre ambas Partes.

La metodología utilizada tiene por objeto ajustar los procedimientos utilizados en cada una de las pruebas y permite conducir gradualmente al usuario hacia mayores niveles de complejidad en la recuperación.

3.5.5.5.1 Método para el desarrollo de las pruebas

Para el desarrollo de las pruebas se realizarán las siguientes tareas :

- Antes de la ejecución de cada prueba se realizará la planificación con el objeto de fijar las pautas a lograr para poder medir el grado de aceptación
- Durante la ejecución de la prueba, personal altamente entrenado en las tareas de recuperación, acompañará al personal del Banco llevando registro de las actividades que se desarrollan.
- Concluida la ejecución de la prueba, se realizará la reunión de evaluación, donde se criticarán las desviaciones de lo planificado con lo logrado en forma efectiva.
- La información emergente de la reunión de crítica será entregada al Banco. Con esta información, el Banco podrá hacer ajustes en el Plan.

Entregable: Un (1) informe por prueba que contendrá la planificación, la configuración utilizada y las actividades llevadas a cabo en el ámbito del Centro de Cómputo Alterno.

3.5.5.5.2 Responsabilidades del Banco

Para cada una de las verificaciones que el Banco lleve a cabo en las instalaciones del Centro de Cómputo Alterno del Proveedor, deberán estar a su cargo las siguientes tareas:

- Coordinar con el Proveedor la oportunidad para la realización de las pruebas
- Proveer soporte magnético con copia de los datos de comprobación y copias de las aplicaciones compatibles con el equipamiento a utilizar en el sitio de recuperación, adicionales a los replicados.
- Proveer suministros (formularios, soportes magnéticos, etc.) y bibliografía de los sistemas Bases usados en la implementacion del CCA.
- Disponer de personal para la ejecución de las tareas de implementación y producción en el sitio de recuperación.

3.5.5.6 Roles de las Brigadas de Contingencia

Una vez declarada la contingencia se activaran las brigadas de contingencia, la integran personas claves de la empresa, cuya principal función será ejecutar los procedimientos respectivos en el CCA. Detalles de sus roles y funciones se describen en el Anexo 18.

3.5.5.7 Inspecciones por Auditorias

El proveedor mantendrá a disposición del Banco, así como de la Superintendencia de Banca y Seguros y/o de los Auditores Externos que éstos designen, la información y documentación que establezca la citada Superintendencia, y que se encuentre relacionada con los servicios prestados. Esta información se pone a disposición con la finalidad de dar cumplimiento a lo establecido por la Resolución 006-2002 de la Superintendencia de Banca y Seguros, y por la Circular G-105-2002, y a las normas que posteriormente las modifiquen.

Asimismo y dentro del marco de las citadas normas, el proveedor se compromete a otorgar al Banco, a la Superintendencia de Banca y Seguros o a los terceros que éstos designen, las facilidades necesarias para realizar una adecuada revisión de los servicios prestados al Banco.

Para los efectos de lo establecido en los párrafos anteriores, el banco deberá informar al Proveedor con no menos de 3 días de anticipación, plazo que podrá ser extendido hasta por 5 días, de la visita de sus auditores, de los funcionarios de la Superintendencia de Banca y Seguros o los terceros que aquellas indiquen, así como también los requerimientos de información o documentación.

CAPITULO IV

EVALUACION DE RESULTADOS

En esta etapa evaluaremos los resultados obtenidos del proyecto luego de haber tomado la decisión.

- ✓ Tener un Centro de Computo Alterno como salvaguarda ante un desastre del Centro de procesamiento principal.

- ✓ Tener un computador adicional dedicado a la contingencia, liberando el computador de desarrollo para otros procesos de negocio.

- ✓ Eliminar costos de operación dedicados a mantener otro centro de procesamiento propio, haciendo economía de escala con el proveedor.

- ✓ Evitar costos adicionales por compras de periféricos adicionales como equipos de backup e impresoras, al compartirlos los que proveedor tiene en su Data Center.

- ✓ Reducir costos de licenciamiento de software al ser asumidos por el proveedor fabricante del computador principal.
- ✓ Crear un comité de trabajo responsable del Plan de Continuidad de Negocio que a su vez coordina con los usuarios para la capacitación y pruebas del CCA.
- ✓ El costo financiero del proyecto se ha respetado al negociar un proyecto con un costo fijo por 5 años.

- ✓ Lograr la participación de todas las áreas de negocio para definir los sistemas críticos del Banco.

- ✓ Tener un nivel de servicio de Calidad Mundial que deben tener los Centros de Computo al contar con un proveedor estratégico en este rubro por tener el know how corporativo y la experiencia mundial en este tipo de servicios.

- ✓ Mejorar nuestra imagen frente a las calificadoras de riesgo que luego se traslada a los clientes en especial empresas.

- ✓ Cumplir las recomendaciones del socio estratégico del Banco

- ✓ Cumplir la normativa del ente supervisor de los Bancos.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

Dentro de las principales conclusiones y recomendaciones más importantes tenemos:

5.1 CONCLUSIONES.

- ✓ La elección de la estrategia de contar con un Centro de Computo Alterno debe ir alineado con las estrategias de TI del negocio y el Plan de Continuidad de Negocios, donde se definen los procesos críticos que deben tener medidas de contingencia.

- ✓ El apoyo de la alta gerencia es imprescindible en este tipo de proyectos que nos son vistos por los usuarios como generadores de ingresos o no toman conciencia de la importancia de tenerlo como garantía de la continuidad del negocio.

- ✓ Es importante la asignación de un presupuesto para el cumplimiento de los objetivos.

- ✓ La evaluación de costo/beneficio de este tipo de proyectos es difícilmente cuantificable por no generar ingresos tangibles al negocio, mas bien se debe medir en términos de cuanto se dejaría de ganar si no se contara con un CCA en el caso de un desastre.

- ✓ Al elegir la alternativa de tercerizar el servicio de Centro de Computo Alterno la forma de contratación cobra significativa importancia, ya que el contrato de servicio debe estipular cláusulas muy claras en temas de seguridad y SLA (Service Level Agreement).

- ✓ Hoy en día existen varias empresas especializadas en proveer este tipo de servicios, lo cual otorga al cliente (Banco) cierto poder de negociación (mayor valor agregado).

- ✓ Al tercerizar el CCA se esta delegando la operación y/o servicio pero la responsabilidad sigue siendo del Banco en especial del área de TI,

- ✓ Con la implementación de este proyecto se satisface dos de las características mas importantes de la información que es la "disponibilidad" y la "integridad"; aspectos importantes tratándose de una entidad financiera.

- ✓ Es importante tener los procedimientos documentados por roles y funciones para que el Centro de Computo Alterno cumpla su objetivo de continuidad del negocio en el tiempo previsto.

- ✓ El éxito del proyecto dependen de la difusión, capacitación, compromiso y pruebas de los usuarios

- ✓ La evaluación del proveedor del servicio es muy importante, ya que mas allá de un simple proveedor debe ser considerado un socio tecnológico estratégico para la retroalimentación del conocimiento que se pueda lograr con su experiencia que pudieran tener al ser expertos en este tipo de servicios, además de contar con infraestructura de hardware, software y comunicaciones similar a la del Banco.

- ✓ Es importante resaltar que el nivel de negociación con el proveedor de servicios debe llegar al mayor detalle para que no deje ambigüedades que luego afecten los costos del proyecto.

- ✓ La definición de detalle de las tareas del proyecto debe realizarse a nivel de los especialistas e involucrados en cada de una de ellas para tener las mejores estimaciones de tiempos en el cronograma de trabajo.

- ✓ Como conclusión final del proyecto se puede observar que existen otros procesos de negocios que deberían ser incluidos en el CCA en las siguientes etapas de evaluación de riesgos, esto debido a que ya se tiene la infraestructura tecnológica implementada (lo mas costoso), que permite una vez definido y documentado los procesos implementarlos sin mayor costo alguno.

5.2 RECOMENDACIONES.

- ✓ Es altamente recomendable y necesario hacer un análisis detallado de la propuesta inicial durante las negociaciones, haciendo énfasis en el equipamiento de la infraestructura tecnológica ofrecida, el equipamiento tanto de Hardware como de Software, las tareas involucradas en los servicios y las configuraciones adecuadas para el Banco, con la finalidad de minimizar el control de cambios durante la implementación y puesta en marcha del proyecto, ya que estos podrían impactar en los costos, dada la magnitud del proyecto en tiempos y costos.

- ✓ Tener la aprobación del la alta gerencia para llevar a cabo proyectos de esta magnitud en costos y tiempos pero que para el día a día no involucra rentabilidad cuantificable para los funcionarios del Banco,

que no están dentro de sus metas de captaciones y colocaciones a cumplir.

- ✓ Hacer una evaluación periódica en la operación del servicio con respecto a la confidencialidad de la información que se manipula, ya que al tratarse de un servicio tercerizado, el tema de la confidencialidad es un tema critico, por tratarse de la información mas importante del Banco.

- ✓ Difundir periódicamente dentro de la institución, los roles de cada persona involucrada en la activación de la contingencia operativa y la activación del Centro de Computo Alterno como Centro de Procesamiento ante una contingencia, con la finalidad de que los miembros involucrados tomen conocimiento del tema, antes los cambios internos del personal y organizacional del Banco.

- ✓ Documentar los procedimientos y responsabilidades de acuerdo a la implantación del proyecto, que puede diferir o estar en mas detalle que en el momento de la concepción del proyecto. Así mismo mantener actualizado por los cambios naturales tanto en la evolución tecnológica como de la organización del Banco.

- ✓ Altamente recomendable es que se cumplan los planes de prueba de este servicio de acuerdo a lo exigido y acordado por la entidad supervisora de la Banca, Seguros y AFPs.

- ✓ Evaluar en un tiempo prudencial de un año que otros servicios criticos para la operación del Banco pueden incorporarse como parte adicional del presente proyecto aprovechando la infraestructura proporcionada y la capacidad ociosa.

GLOSARIO DE TERMINOS

SBS :
Superintendicia de Banca y Seguros. Entidad gubernamental reguladora de las empresas Financieras y de Seguros.

CCA :
Centro de Computo Alterno. Lugar, separado del centro de computo a una distancia considerable, que tiene la infraestructura tecnología tantos de equipos y software, para operar los sistemas mas importantes de una empresa.

MIMIX:
El nombre del fabricante de un software del mismo nombre que sirve para replicar datos y programas en tiempo real para equipos AS/400 o iSeries de IBM

TI :
Tecnología de la Información, que incluye los sistemas informáticos y la tecnología asociada a dichos sistemas.

BIBLIOGRAFÍA

1. Norma sobre Riesgos de Tecnología de Información para la Banca.
   Incluido en el Anexo 2.

2. Manual del Plan de Continuidad del Negocios (PCN).
   Incluido en el Anexo 5.

3. Servicios IBM en seguridad.
   www.ibm.com/services/security

4. Replica en equipos IBM AS/400 y/o iSeries.
   Managed Avaliability – Conepts and Facilities de Mimix en
   http://www.mimix.com/

5. Replica de Domain Controller en Site Remotos para contingencia.
   http://www.microsoft.com/serviceproviders/columns/config_ipsec_P63623.asp

6. La Norma ISO - 17799.
   http://www.iso-17799.com/

7. Bibliografía entregada en el PTAC VI por los profesores..

ANEXOS

A continuación se detallan cada uno de los anexos que se indican el presente trabajo, para un mejor seguimiento y lectura estos están con su propio Índice.

INDICE DE ANEXOS

Anexo 1

Resolución S.B.S.No 006 –2002

Resolución S.B.S. No 006 –2002
El Superintendente de Banca y Seguros

CONSIDERANDO:

Que, es objetivo de esta Superintendencia propender a que las empresas supervisadas cuenten con un sistema de control de riesgos que les permita identificar, medir, controlar y reportar los riesgos que enfrentan con la finalidad de proteger los intereses del público de acuerdo a lo señalado en el artículo 347º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley Nº 26702, y sus modificatorias, en adelante Ley General;

Que, entre los riesgos que enfrentan las empresas supervisadas en el desarrollo de sus actividades se encuentran los riesgos de operación, los cuales pueden generarse por deficiencias o fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos;

Que, resulta necesario establecer criterios mínimos prudenciales para que las empresas supervisadas realicen de manera adecuada la gestión de dichos riesgos;

Estando a lo opinado por las Superintendencias Adjuntas de Banca, Seguros y Asesoría Jurídica; y,

En uso de las atribuciones conferidas por los numerales 7 y 9 del artículo 349º de la Ley General y por la Resolución SBS N° 1028-2001 del 27 de diciembre de 2001;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento para la Administración de los Riesgos de Operación, que forma parte integrante de la presente Resolución.

Artículo Segundo. - La presente Resolución entra en vigencia al día siguiente de su publicación en el Diario Oficial ¨ El Peruano".

Regístrese, comuníquese y publíquese,

SOCORRO HEYSEN ZEGARRA
Superintendente de Banca y Seguros (e)

REGLAMENTO PARA LA ADMINISTRACION DE LOS RIESGOS DE OPERACION

CAPITULO I
DISPOSICIONES GENERALES

Alcance
Artículo 1º.- Las disposiciones de la presente norma son aplicables a las empresas señaladas en los artículos 16° y 17° de la Ley General, al Banco Agropecuario, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco de la Nación, a la Fundación Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI) y a las derramas y cajas de beneficios que se encuentren bajo la supervisión de esta Superintendencia, en adelante empresas.

Definiciones
Artículo 2º.- Para los efectos de la presente norma deben considerarse los siguientes términos:

a. Administración de riesgos: Proceso que consiste en identificar, medir, controlar y reportar los riesgos que la empresa enfrenta.
b. Directorio: Toda referencia al directorio, entiéndase realizada también a cualquier órgano equivalente.
c. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.
d. Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles.
e. Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la empresa.
f. Reglamento del Sistema de Control Interno: Reglamento del Sistema de Control Interno aprobado mediante la Resolución SBS Nº 1040-99 del 26 de noviembre de 1999.
g. Servicios críticos provistos por terceros: Servicios relacionados a procesos críticos provistos por terceros y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la empresa.
h. Superintendencia: Superintendencia de Banca y Seguros.
i. Tecnología de información: Incluye los sistemas informáticos y la tecnología asociada a dichos sistemas.

Riesgos de operación
Artículo 3º.- Las empresas deben administrar adecuadamente los riesgos de operación que enfrentan. Entiéndase por riesgos de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos.

Responsabilidad del Directorio y la Gerencia

Artículo 4º.- El Directorio es responsable del establecimiento de políticas y procedimientos generales para identificar, medir, controlar y reportar apropiadamente los riesgos de operación. Asimismo, será también su responsabilidad el velar por el cumplimiento de las referidas políticas y procedimientos y de las disposiciones contenidas en el presente Reglamento. Corresponderá a la Gerencia General la implementación de las políticas y procedimientos generales establecidos por el Directorio.

Unidad de riesgos

Artículo 5º.- De conformidad con lo dispuesto en el Reglamento del Sistema de Control Interno, la Unidad de Riesgos será la encargada de la administración de los riesgos de operación que enfrenta la empresa, pudiendo comprender a alguna unidad especializada para la evaluación de dicho riesgo.

Asimismo, para dicho fin, la unidad de riesgos o, de ser el caso, la unidad especializada, deberá contar con la infraestructura adecuada, así como con los recursos humanos, técnicos y logísticos que le permitan el apropiado cumplimiento de sus funciones, de acuerdo a la dimensión y estructura de la empresa, la naturaleza de sus operaciones y servicios y la complejidad de los mismos.

Entre las funciones de la referida unidad responsable se incluirán por lo menos las siguientes:

a. Preparación y evaluación de políticas para la administración de los riesgos de operación.
b. Desarrollo de metodologías para la evaluación cuantitativa y/o cualitativa de los riesgos de operación.
c. Evaluación de los riesgos de operación, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.
d. Consolidación y desarrollo de reportes e informes sobre la administración de los riesgos de operación por proceso, o unidades de negocio y apoyo.
e. Identificación de las necesidades de capacitación y difusión para una adecuada administración de los riesgos de operación.
f. Otras necesarias para el desarrollo de su función.

Manual de organización y funciones

Artículo 6º.- De conformidad con las disposiciones contenidas en la presente norma y en el Reglamento del Sistema de Control Interno, la empresa deberá disponer de una estructura organizacional y administrativa que le permita una adecuada administración de los riesgos de operación. Dicha estructura deberá establecerse de manera que exista independencia entre la unidad de riesgos y aquellas otras unidades de negocio, así como una clara delimitación de funciones,

responsabilidades y perfil de puestos en todos sus niveles. Estos aspectos deberán encontrarse recogidos en el manual de organización y funciones de la empresa.

Manuales de políticas y procedimientos

Artículo 7º.- Las políticas y procedimientos establecidos para la administración de los riesgos de operación deberán estar claramente definidos en los manuales de políticas y procedimientos; asimismo, deberán ser consistentes con el tamaño y naturaleza de la empresa y con la complejidad de sus operaciones y servicios.

Manual de control de riesgos

Artículo 8º.- El manual de control de riesgos deberá contener una sección especial sobre los riesgos de operación. Dicha sección deberá contemplar por lo menos los siguientes aspectos:

a. Políticas para la administración de los riesgos de operación.
b. Funciones y responsabilidades de las unidades de negocio y de apoyo en la administración de los riesgos de operación.
c. Descripción de la metodología aplicada para la medición y evaluación de los riesgos de operación.
d. La forma y periodicidad con la que se deberá informar al Directorio y a la Gerencia General, entre otros, sobre la exposición a los riesgos de operación de la empresa y de cada unidad de negocio.
e. El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

CAPITULO II
ADMINISTRACION DE LOS ASPECTOS QUE ORIGINAN LOS RIESGOS DE OPERACION

Procesos internos

Artículo 9º.- Las empresas deberán administrar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, de tal forma que se minimice la posibilidad de pérdidas financieras relacionadas al diseño inapropiado de los procesos críticos, o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada

documentación de transacciones, así como el incumplimiento de plazos y costos planeados.

Tecnología de información
Artículo 10º.- Las empresas deberán administrar apropiadamente los riesgos asociados a la tecnología de información, de tal modo que se minimice la posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas informáticos y tecnologías relacionadas a ellos, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información.

Para este fin, las empresas podrán considerar los riesgos vinculados a las fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, así como las fallas en la adecuación a los objetivos del negocio, entre otros aspectos.

Personas
Artículo 11º.- Las empresas deben administrar apropiadamente los riesgos asociados a las personas de la empresa, de tal modo que se minimice la posibilidad de pérdidas financieras asociadas a inadecuada capacitación del personal, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero y similares.

Eventos externos
Artículo 12º.- Las empresas deberán considerar en la administración de los riesgos de operación la posibilidad de pérdidas derivada de la ocurrencia de eventos ajenos al control de la empresa que pudiesen alterar el desarrollo de sus actividades, afectando los aspectos que dan origen a los riesgos de operación referidos en los artículos 9º, 10º y 11º del presente Reglamento. En tal sentido, entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros.

CAPITULO III
REQUERIMIENTOS DE INFORMACION

Informe anual a la Superintendencia
Artículo 13º.- Las empresas deberán presentar a la Superintendencia, dentro de los noventa (90) días calendario siguientes al cierre de cada ejercicio anual, un informe referido a la evaluación de los riesgos de operación que enfrenta la empresa por proceso o unidad de negocio y apoyo. Dicho informe deberá contemplar por lo menos los siguientes aspectos:

a. Metodología empleada para la administración de los riesgos de operación.

b. Identificación de los riesgos de operación por proceso o unidad de negocio y apoyo.
c. Evaluación de los riesgos de operación identificados.
d. Medidas adoptadas para administrar los riesgos de operación materiales identificados y plazos para su aplicación. Dichas medidas podrán ser, entre otras:
   Evitar el riesgo
   Reducir su probabilidad de ocurrencia
   Reducir las consecuencias
   Transferir el riesgo
   Retener el riesgo
e. Funcionarios responsables de las actividades de control de riesgo identificadas.
f. Plan de actividades de la Unidad de Riesgos en lo referente a la administración de los riesgos de operación.

Información adicional
Artículo 14º.- La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de los riesgos de operación de la empresa.

Asimismo, la empresa deberá tener a disposición de esta Superintendencia todos los documentos a que hace mención el presente Reglamento, así como la información de auditoría o revisiones realizadas por la casa matriz en caso de las empresas cuya matriz no se encuentre en el país.

CAPITULO IV
COLABORADORES EXTERNOS

Auditoría Interna
Artículo 15º.- La Unidad de Auditoría Interna deberá evaluar el cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación, así como de lo dispuesto en el presente Reglamento. Asimismo, la Unidad de Auditoría Interna deberá incluir la referida evaluación en las actividades permanentes del Plan Anual y deberá realizar los informes y recomendaciones que se deriven de la misma.

Auditoría Externa

Artículo 16º.- Las sociedades de auditoría externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la administración de los riesgos de operación, considerando el cumplimiento de lo dispuesto en el presente Reglamento.

Empresas Clasificadoras de Riesgo
Artículo 17º.- Las empresas clasificadoras de riesgo deberán tener en cuenta las políticas y procedimientos establecidos por la empresa para la administración de los riesgos de operación en el proceso de clasificación de las empresas supervisadas.

DISPOSICIONES FINALES Y TRANSITORIAS

Servicios provistos por terceros
Primera.- Las empresas son responsables de asegurar el cumplimiento de la normatividad emitida por la Superintendencia, aun en aquellos casos en que ciertas funciones sean realizadas por terceros. En este sentido, además del cumplimiento de lo dispuesto en la presente Resolución, las empresas deberán asegurarse de que los contratos suscritos con proveedores de servicios críticos a la empresa, incluyan cláusulas que faciliten una adecuada revisión de la respectiva prestación, por parte de las empresas, la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa, así como por parte de la Superintendencia o la persona que ésta designe.

Medidas adicionales
Segunda.- La Superintendencia podrá disponer la adopción de medidas adicionales a las previstas en el presente Reglamento con el propósito de atenuar la exposición a los riesgos de operación que enfrentan las empresas.

Sanciones
Tercera.- En caso de incumplimiento de las disposiciones contenidas en el presente Reglamento la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Plazo y Plan de Adecuación
Cuarta.- Las empresas contarán con un plazo de adecuación a las disposiciones de la presente norma que vencerá el 30 de junio de 2003. A dicha fecha las empresas deberán tener a disposición de este organismo de control los Manuales de Políticas y Procedimientos, el Manual de Organización y Funciones, el Manual de Control de Riesgos y los contratos de servicios críticos provistos por terceros a que se refiere la primera disposición final y transitoria del presente reglamento, adecuados a las disposiciones comprendidas en el mismo.

Para el ejercicio 2002 las empresas no se encuentran obligadas a presentar el informe anual a que se refiere el artículo 13º del presente reglamento. Sin embargo, en un plazo que no excederá del 30 de junio de 2002 deberán remitir a este organismo de control un plan de adecuación a las disposiciones contenidas en la presente norma. Dicho plan deberá incluir un diagnóstico preliminar de la situación existente en la empresa, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Reglamento de Auditoria Interna
Quinta.- Toda referencia realizada al término riesgo informático en el Reglamento de Auditoria Interna, aprobado mediante la Resolución SBS Nº 1041-99, deberá ser entendida como referida a los riesgos de operación, de acuerdo con lo dispuesto en la presente norma.

Anexo 2

CIRCULAR Nº G - 105 - 2002

Ref.: Riesgos de tecnología de información

Lima, 22 de febrero de 2002

CIRCULAR Nº G - 105 - 2002

Ref.: Riesgos de tecnología de información

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 26702 y sus modificatorias, en adelante Ley General, y por la Resolución SBS N° 1028-2001 del 27 de diciembre de 2001, con la finalidad de establecer criterios mínimos para la identificación y administración de los riesgos asociados a la tecnología de información, a que se refiere el artículo 10º del Reglamento para la Administración de los Riesgos de Operación, aprobado mediante la Resolución SBS Nº 006-2002 del 4 de enero de 2002, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones:

Alcance

Artículo 1º.- Las disposiciones de la presente norma son aplicables a las empresas señaladas en los artículos 16° y 17° de la Ley General, al Banco Agropecuario, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco de la Nación, a la Fundación Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI) y a las derramas y cajas de beneficios que se encuentren bajo la supervisión de esta Superintendencia, en adelante empresas.

Definiciones

Artículo 2º .- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.
b. Ley General: Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.

c. Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la empresa.

d. Reglamento: Reglamento para la Administración de los Riesgos de Operación aprobado por Resolución SBS N° 006-2002 del 4 de enero de 2002.

e. Riesgos de operación: Entiéndase por riesgos de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos.

f. Riesgos de tecnología de información: Los riesgos de operación asociados a los sistemas informáticos y a la tecnología relacionada a dichos sistemas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información, entre otros criterios.

g. Seguridad de la información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.

h. Objetivo de control: Una declaración del propósito o resultado deseado mediante la implementación de controles apropiados en una actividad de tecnología de información particular.

Responsabilidad de la empresa

Artículo 3°.- Las empresas deben establecer e implementar las políticas y procedimientos necesarios para administrar de manera adecuada y prudente los riesgos de tecnología de información, incidiendo en los procesos críticos asociados a dicho riesgo, considerando las disposiciones contenidas en la presente norma, en el Reglamento, y en el Reglamento del Sistema de Control Interno aprobado mediante la Resolución SBS Nº 1040-99 del 26 de noviembre de 1999.

La administración de dicho riesgo debe permitir el adecuado cumplimiento de los siguientes criterios de control interno:

i. **Eficacia**. La información debe ser relevante y pertinente para los objetivos de negocio y ser entregada en una forma adecuada y oportuna conforme las necesidades de los diferentes niveles de decisión y operación de la empresa.

ii. **Eficiencia.** La información debe ser producida y entregada de forma productiva y económica.
iii. **Confidencialidad.** La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
iv. **Integridad**. La información debe ser completa, exacta y válida.
v. **Disponibilidad.** La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.
vi. **Cumplimiento normativo.** La información debe cumplir con los criterios y estándares internos de la empresa, las regulaciones definidas externamente por el marco legal aplicable y las correspondientes entidades reguladoras, así como los contenidos de los contratos pertinentes.

Estructura organizacional y procedimientos
Artículo 4°.- Las empresas deben definir y mantener una estructura organizacional y procedimientos que les permita administrar adecuadamente los riesgos asociados a la tecnología de información, consistente con su tamaño y naturaleza, así como con la complejidad de las operaciones que realizan.

Administración de la seguridad de información
Artículo 5º.- Las empresas deberán establecer, mantener y documentar un sistema de administración de la seguridad de la información, en adelante "Plan de Seguridad de la información **- (PSI)".** El PSI debe incluir los activos de tecnología que deben ser protegidos, la metodología usada, los objetivos de control y controles, así como el grado de seguridad requerido.

Las actividades mínimas que deben desarrollarse para implementar el PSI, son las siguientes:

a. Definición de una política de seguridad.
b. Evaluación de riesgos de seguridad a los que está expuesta la información
c. Selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados, indicando las razones de su inclusión o exclusión.
d. Plan de implementación de los controles y procedimientos de revisión periódicos.
e. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Las empresas bancarias y las empresas de operaciones múltiples

que accedan al módulo 3 de operaciones a que se refiere el artículo 290º de la Ley General deberán contar con una función de seguridad a dedicación exclusiva.

Subcontratación (outsourcing)

Artículo 6º.- La empresa es responsable y debe verificar que se mantengan las características de seguridad de la información contempladas en la presente norma, incluso cuando ciertas funciones o procesos críticos puedan ser objeto de una subcontratación. Para ello se tendrá en cuenta lo dispuesto en la Primera Disposición Final y Transitoria del Reglamento. Asimismo, la empresa debe asegurarse y verificar que el proveedor del servicio sea capaz de aislar el procesamiento y la información objeto de la subcontratación, en todo momento y bajo cualquier circunstancia.

En caso que las empresas deseen realizar su procesamiento principal en el exterior, requerirán de la autorización previa y expresa de esta Superintendencia. Las empresas que a la fecha de vigencia de la presente norma se encontrasen en la situación antes señalada, deberán solicitar la autorización correspondiente. Para la evaluación de estas autorizaciones, las empresas deberán presentar documentación que sustente lo siguiente:

a) La forma en que la empresa asegurará el cumplimiento de la presente circular y la Primera Disposición Final y Transitoria del Reglamento.
b) La empresa, así como los representantes de quienes brindarán el servicio de procesamiento en el exterior, deberán asegurar adecuado acceso a la información con fines de supervisión, en tiempos razonables y a solo requerimiento.

Aspectos de la seguridad de información

Artículo 7°.- Para la administración de la seguridad de la información, las empresas deberán tomar en consideración los siguientes aspectos:

7.1 Seguridad lógica

Las empresas deben definir una política para el control de accesos, que incluya los criterios para la concesión y administración de los accesos a los sistemas de información, redes y sistemas operativos, así como los derechos y atributos que se confieren.

Entre otros aspectos, debe contemplarse lo siguiente:

a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios. Revisiones periódicas deben efectuarse sobre los derechos concedidos a los usuarios.
b) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.
c) Controles especiales sobre utilidades del sistema y

herramientas de auditoría.

d) Seguimiento sobre el acceso y uso de los sistemas y otras instalaciones físicas, para detectar actividades no autorizadas.
e) Usuarios remotos y computación móvil.
f)

7.2 Seguridad de personal

Las empresas deben definir procedimientos para reducir los riesgos asociados al error humano , robo, fraude o mal uso de activos, vinculados al riesgo de tecnología de información. Al establecer estos procedimientos, deberá tomarse en consideración, entre otros aspectos, la definición de roles y responsabilidades establecidos sobre la seguridad de información, verificación de antecedentes, políticas de rotación y vacaciones, y entrenamiento.

7.3 Seguridad física y ambiental

Las empresas deben definir controles físicos al acceso, daño o interceptación de información. El alcance incluirá las instalaciones físicas, áreas de trabajo, equipamiento, cableado, entre otros bienes físicos susceptibles a riesgos de seguridad.

Se definirán medidas adicionales para las áreas de trabajo con necesidades especiales de seguridad, como los centros de procesamiento, entre otras zonas en que se maneje información que requiera de alto nivel de protección.

7.4 Clasificación de seguridad

Las empresas deben realizar un inventario periódico de activos asociados a la tecnología de información que tenga por objetivo proveer la base para una posterior clasificación de seguridad de dichos activos. Esta clasificación debe indicar el nivel de riesgo existente para la empresa en caso de falla sobre la seguridad, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

Administración de las operaciones y comunicaciones

Artículo 8º.- Las empresas deben establecer medidas de administración de las operaciones y comunicaciones que entre otros aspectos contendrán lo siguiente:

Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.
- Control sobre los cambios del ambiente de desarrollo al de producción.
- Separación de funciones para reducir el riesgo de error o fraude.
- Separación del ambiente de producción y el de desarrollo.
- Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.

Seguridad sobre las redes, medios de almacenamiento y

documentación de sistemas.
- Seguridad sobre correo electrónico.
- Seguridad sobre banca electrónica.

Desarrollo y mantenimiento de sistemas informáticos - Requerimientos de seguridad

Artículo 9º.- Para la administración de la seguridad en el desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.
b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.
c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.
d) Controlar el acceso a las librerías de programas fuente.
e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.

Procedimientos de respaldo

Artículo 10º.- Las empresas deben establecer procedimientos de respaldo regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con lo requerido en el Plan de Continuidad.

La empresa debe conservar la información de respaldo y los procedimientos de restauración en una ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro principal de procesamiento.

Planeamiento para la continuidad de negocios

Artículo 11º.- Las empresas, bajo responsabilidad de la Gerencia y el Directorio, deben desarrollar y mantener un "Plan de Continuidad de Negocios" (PCN), que tendrá como objetivo asegurar un nivel aceptable de operatividad de los procesos críticos, ante fallas mayores internas o externas.

Criterios para el diseño e implementación del Plan de Continuidad de Negocios

Artículo 12º.- Para el desarrollo del PCN se debe realizar previamente una evaluación de riesgos asociados a la seguridad de la información. Culminada la evaluación, se desarrollarán sub-planes específicos para mantener o recuperar los procesos críticos de negocios ante fallas en sus activos, causadas por eventos internos (virus, errores no esperados en la implementación, otros), o externos (falla en las comunicaciones o energía, incendio, terremoto, proveedores, otros).

Prueba del Plan de Continuidad de Negocios

Artículo 13º.- La prueba del PCN es una herramienta de la dirección para controlar los riesgos sobre la continuidad de operación y sobre la disponibilidad de la información, por lo que la secuencia, frecuencia y profundidad de la prueba del PCN, deberá responder a la evaluación formal y prudente que sobre dicho riesgo realice cada empresa.

En todos los casos, mediante una única prueba o una secuencia de ellas, según lo considere adecuado cada empresa de acuerdo a su evaluación de riesgos, los principales aspectos del PCN deberán ser probados cuando menos cada dos años.

Anualmente, dentro del primer mes del ejercicio, se enviará a la Superintendencia el programa de pruebas correspondiente, en que se indicará las actividades a realizar durante el ciclo de 2 años y una descripción de los objetivos a alcanzar en el año que se inicia.

Cumplimiento formativo

Artículo 14º.- La empresa deberá asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

Privacidad de la información

Artículo 15º .- Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme la normatividad vigente sobre la materia.

Auditoría Interna y Externa

Artículo 16º.- La Unidad de Auditoría Interna deberá incorporar en su Plan Anual de Trabajo la evaluación del cumplimiento de lo dispuesto en la presente norma.

Asimismo, las Sociedades de Auditoría Externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la administración de los riesgos de tecnología de información, considerando asimismo, el cumplimiento de lo dispuesto en la presente norma.

Auditoría de sistemas

Artículo 17º.- Las empresas bancarias y aquellas empresas autorizadas a operar en el Módulo 3 conforme lo señalado en el artículo 290° de la Ley General, deberán contar con un servicio permanente de auditoría de sistemas, que colaborará con la Auditoría interna en la verificación del cumplimiento de los criterios de control interno para las tecnologías de información, así como en el desarrollo del Plan de Auditoría.

El citado servicio de auditoría de sistemas tomará en cuenta, cuando parte del procesamiento u otras funciones sean realizadas por terceros, que es necesario conducir su revisión con los mismos estándares exigidos a la empresa, por lo que tomará en cuenta las disposiciones indicadas en la Primera Disposición Final y Transitoria

del Reglamento.
Las empresas autorizadas para operar en otros módulos, para la verificación del cumplimiento antes señalado, deberán asegurar una combinación apropiada de auditoría interna y/o externa, compatible con el nivel de complejidad y perfil de riesgo de la empresa. La Superintendencia dispondrá un tratamiento similar a las empresas pertenecientes al módulo 3, cuando a su criterio la complejidad de sus sistemas informáticos y su perfil de riesgo así lo amerite.

Información a la Superintendencia
Artículo 18°.- El informe anual que las empresas deben presentar a la Superintendencia, según lo dispuesto en el Artículo 13° del Reglamento, deberá incluir los riesgos de operación asociados a la tecnología de información, como parte integral de dicha evaluación, para lo cual se sujetará a lo dispuesto en dicho Reglamento y a lo establecido en la presente norma.

Sanciones
Artículo 19°.- En caso de incumplimiento de las disposiciones contenidas en la presente norma, la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Plan de adecuación
Artículo 20°.- En el Plan de Adecuación señalado en el segundo párrafo de la Cuarta Disposición Final y Transitoria del Reglamento, las empresas deberán incluir un sub-plan para la adecuación a las disposiciones contenidas en la presente norma.

Plazo de adecuación
Artículo 21°.- Las empresas contarán con un plazo de adecuación a las disposiciones de la presente norma que vence el 30 de junio de 2003

Atentamente,

SOCORRO HEYSEN ZEGARRA
Superintendente de Banca y Seguros (e)

Anexo 3

ORGANIZACIOND GENERAL DEL BANCO DEL DINERO

Organización General del Banco del Dinero

La Organización general del banco ha sido revisada por las gerencias respectivas y aprobada en sesion de Directorio.

El Banco esta organizado funcionalmente y cuenta con los siguientes niveles en su estructura:

- Directorio
- Gerencia General
- División
- Area
- Departamento
- Sección
- Unidad

Se han establecido los siguientes comités:

- Comité Ejecutivo
- Comité de Riesgos
- Comité de Activos y Pasivos
- Comité de Auditoria

Como órgano de control tiene a la **Oficina de Auditoria Interna** que le reporta al Directorio.

Cuenta además con las siguientes áreas de asesoría y apoyo con nivel de reporte a la Gerencia General:

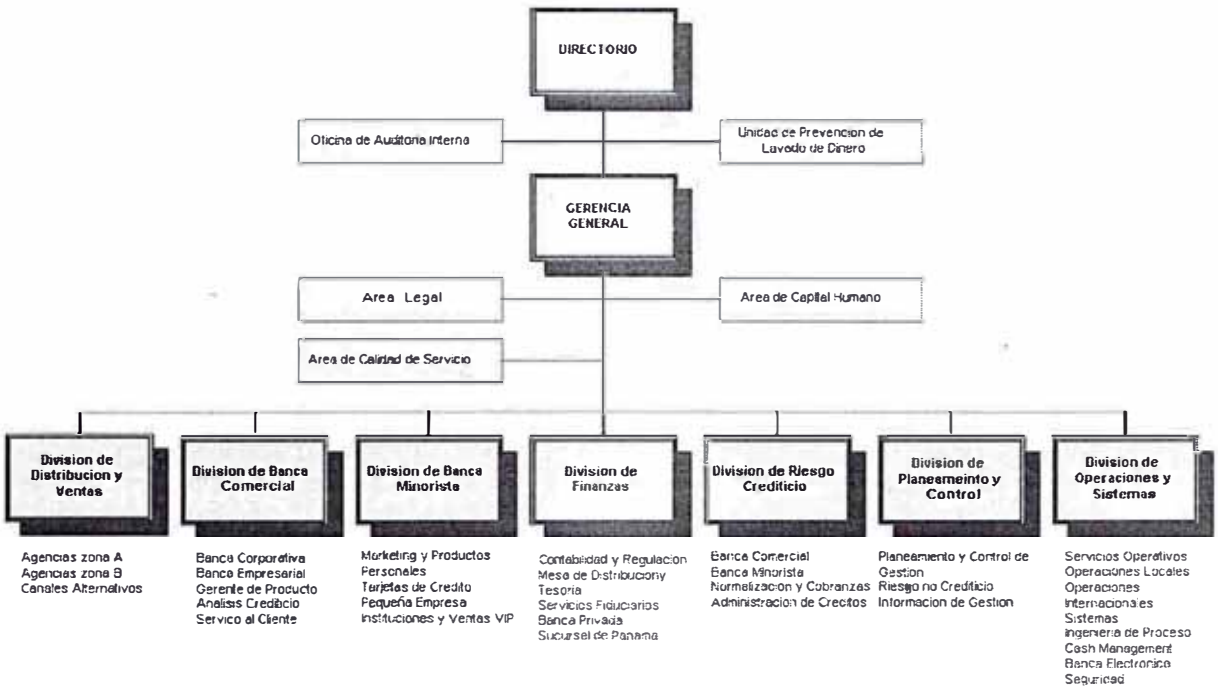
- Area Legal
- Area de Capital Humano
- Area de Calidad de Servicio

Como órganos de línea que dependen de la Gerencia general, cuenta con las siguientes divisiones:

- División de Operaciones y Sistemas
- División de Planeamiento y Control
- División de Riesgo Crediticio
- División de Banca Comercial
- División de Banca Minorista
- División de Finanzas
- División de Distribución y Ventas

BANCO DEL DINERO

ORGANIGRAMA GENERAL

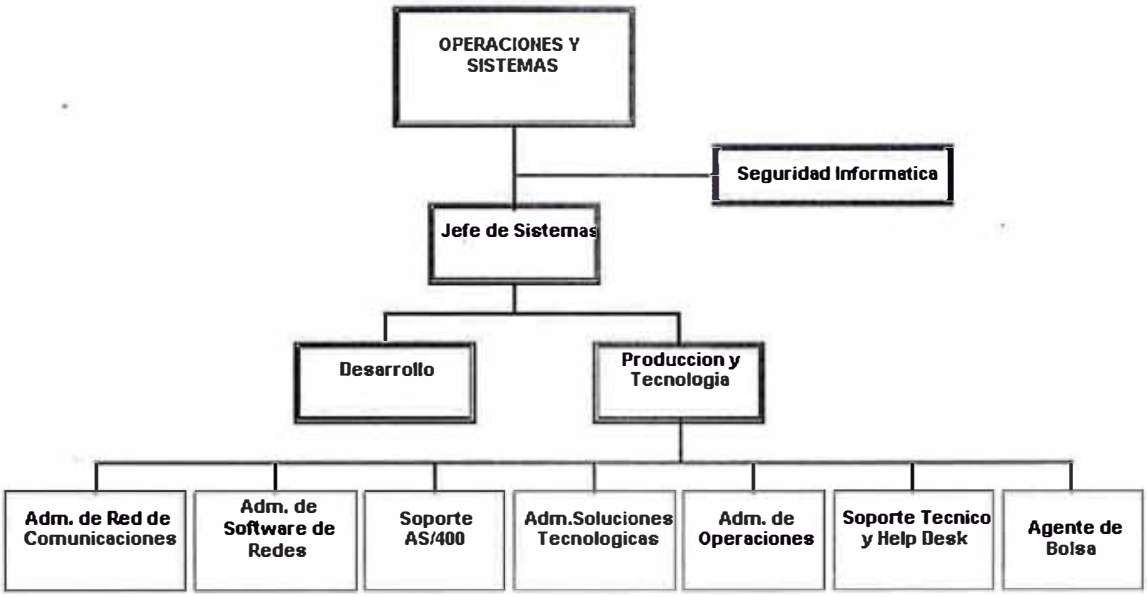


Anexo 4

ORGANIGRAMA DEL AREA DE SISTEMAS

BANCO DEL DINERO

Organigrama del Area de Sistemas que esta bajo la Gerencia Central de Operaciones y Sistemas



(Actualizado al 17 de Setiembre del 2003)

Anexo 5

BREVE DESCRIPCION DE LAS ETAPAS DEL PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)

Resumen del Plan de Continuidad de Negocios PCN

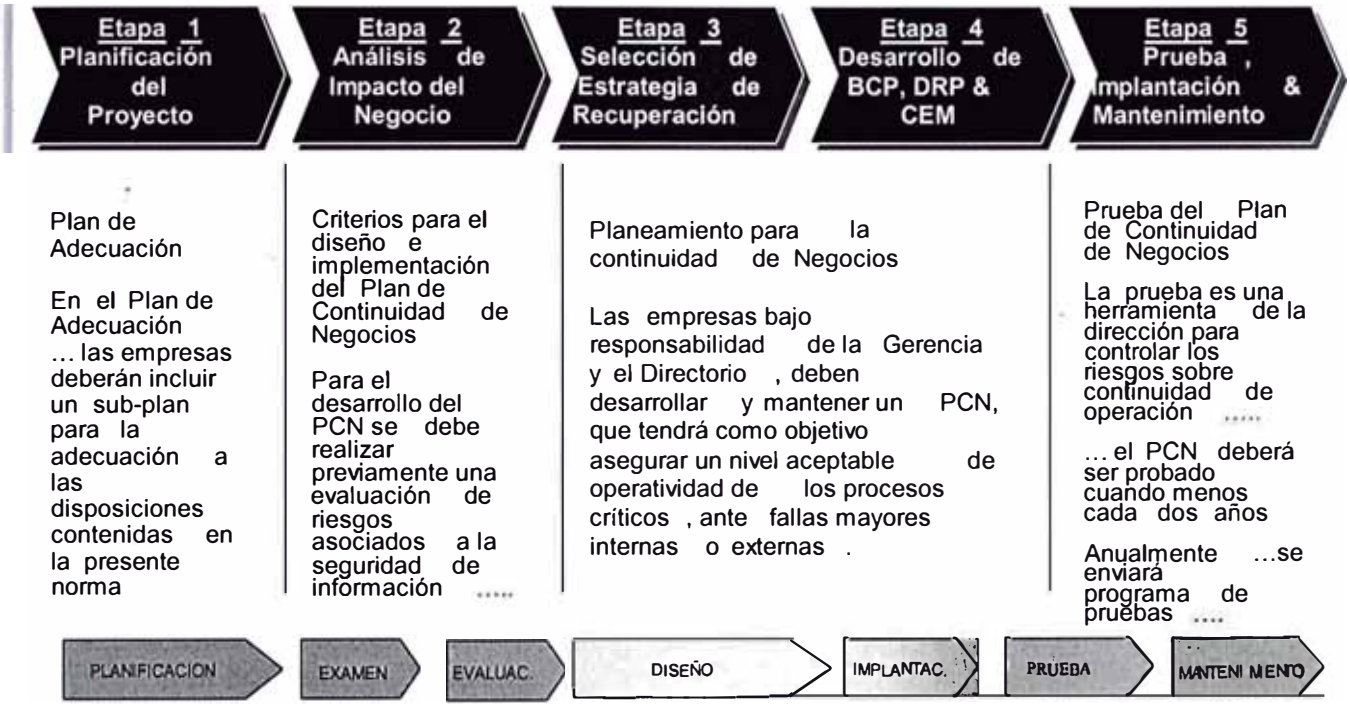
Objetivo del PCN:

Reducir interrupciones de las actividades del negocio y proteger procesos críticos del negocio de los efectos de los desastres graves.

El proyecto para desarrollar el Plan de Continuidad de Negocios, en adelante PCN, comprende un esfuerzo coordinado, centrado en la administración, desarrollo, integración y mantenimiento de estrategias efectivas en costo, para minimizar el impacto de fallas en el Banco y la atención a sus clientes, permitiendo una rápida y efectiva evaluación, recuperación y continuidad de las operaciones durante una crisis o desastre

La regulaciones actuales de la Superintendencia define la necesidad de contar con un Plan de Continuidad de Negocios, elaborarlo en base a un análisis de impacto previo y elaborar procedimientos para su constante mantenimiento y prueba. Asimismo, establece la necesidad de realizar pruebas integrales del plan cada dos años e informar anualmente a la Superintendencia.

El grafico siguiente muestra las etapas en las cuales se desarrolla un PCN:



Etapa 1 – Planificación

El proyecto comienza con una etapa de planificación para validar objetivos y alcances, establecer responsables y confirmar las tareas de las diversas etapas del proyecto. Asimismo, de un mecanismo para el monitoreo de avance del mismo.

Planificación del Proyecto.

Objetivo

La primera tarea es la de crear la estructura necesaria para la ejecución del proyecto PCN. Realizar la planificación del proyecto, programas detallados de trabajo, cronogramas, hitos de control, estimados de tiempos, priorizaciones de actividades y entregables.

- Estructura del Proyecto
- Roles y responsabilidades
- Actividades de trabajo detalladas
- Cronogramas de Ejecución

Etapa 2 – Análisis de impacto

El proyecto comienza con un Análisis de Impacto del negocio, donde se identifican los procesos de negocio críticos para la continuidad y supervivencia de las operaciones del Banco.

El trabajo realizado en esta etapa incluye una evaluación detallada de los efectos financieros y operacionales ante una pérdida parcial o total de las instalaciones de cómputo. Una vez identificado los procesos críticos del negocio, se completa una evaluación de riesgo.

Identificar procesos críticos del negocio

Objetivo

Definir los procesos críticos y necesarios del negocio, para definir la lista de procesos críticos y necesarios del negocio.

Discontinuidad del Negocio

Objetivo

Identificar y evaluar la importancia de cualquier amenaza a los procesos críticos y necesarios del Banco.

Habiendo identificado los procesos y funciones claves del Banco, es necesario identificar y evaluar las amenazas hacia su operación continua.

Entendemos como amenaza a toda persona o cosa considerada peligrosa, podríamos mencionar como ejemplos de amenazas: fuego, daño malicioso, robo, fallas de servicios críticos o básicos, entre otros.

En esta fase las tareas que se llevan a cabo son:

- Identificar y evaluar amenazas
- Cuantificar posibles discontinuidades
- Identificar medidas para la reducción del riesgo
- Preparar evaluación de amenaza y discontinuidad

Objetivo de tiempo de recuperación

Objetivo

Determinar los objetivos de tiempo para la recuperación (o tiempo de inoperancia aceptada) de cada proceso crítico y necesario del Banco, en el evento de una emergencia.

Como parte de la evaluación de los procesos críticos y necesarios del Banco, es necesario considerar el tiempo máximo que el Banco puede mantenerse sin algún proceso crítico, antes que los efectos del desastre se sientan, por ejemplo, el tiempo máximo antes de que un proceso crítico deba ser restaurado. Estos tiempos son definidos como los tiempos objetivos de recuperación.

Cuando se estiman los tiempos objetivos de recuperación en el evento de un desastre regional, es necesario reconocer que todo lo demás en el área también estará fuera del negocio por un tiempo.

Los tiempos objetivos de recuperación para los procesos críticos y necesarios relacionados con computadoras y los no relacionados con computadoras están considerados por separado dado que las tareas envueltas son significativamente diferentes.

Las tareas que se llevan a cabo en esta fase son:

- Determinar los tiempos objetivos de la recuperación de procesos basados en computadora
- Determinar los tiempos objetivos de la recuperación de procesos no basados en computadora
- Estimar el impacto financiero /económico de la recuperación

Hallazgos y conclusiones

Objetivo

Preparar un entregable de la evaluación del análisis del impacto del negocio, y que sirva como base para la selección de la estrategia.

El documento de análisis del impacto contiene una evaluación de la situación actual del Banco con relación a la discontinuidad de las operaciones normales del negocio.

El énfasis mayor del entregable del análisis del impacto del negocio es el costo potencial y el impacto para el Banco de la discontinuidad de sus operaciones normales de los procesos críticos y necesarios.

En esta etapa se realizan las siguientes tareas:

- Planificar tareas pendientes
- Preparar entregable del análisis del impacto del negocio

Entregable

Análisis de Impacto del Negocio.

Etapa 3 – Selección de Estrategia

La selección de la estrategia se encuentra enfocada en la elección de la más apropiada opción de back-up y recuperación de desastre considerando las opciones disponibles, para ello se debe:

- Definir requerimientos mínimos para la operación de todos los procesos de negocio críticos y necesarios, previamente identificados.
- Investigar todas las opciones disponibles de back-up
- Investigar todas las opciones disponibles de recuperación
- Identificar futuras medidas para reducir el riesgo de interrupción del negocio; y
- Seleccionar la mas apropiada estrategia de recuperación

La selección de la estrategia involucra la recolección de información relacionada a la recuperación de procesos críticos y necesarios identificados en la etapa de análisis de impacto. Esta información será usada para documentar detalles de las operaciones existentes, revisar objetivos definidos durante la etapa de análisis de impacto y finalmente seleccionar una estrategia de recuperación de desastres integrada y comprensiva.

El entregable para esta etapa documenta los requerimientos mínimos para los procesos críticos y necesarios; y después de la discusión con la gerencia, recomienda una estrategia de recuperación de desastres.

Fase : Recursos de recuperación mínimos para procesos de negocio computarizados

Objetivo

Identificar en detalle los recursos requeridos para operar los procesos críticos y necesarios soportados por aplicaciones de sistemas bajo condiciones de recuperación.

Cada proceso computarizado tiene un número de requerimientos de recursos. En esta fase, se completa una investigación detallada de los requerimientos de los procesos críticos y necesarios soportados por aplicaciones de sistemas. Para cada uno de estos procesos, se identifican recursos esenciales requeridos durante operaciones bajo condiciones de recuperación.

Esta fase cuenta con las siguientes tareas:

- Recolectar datos existentes
- Determinar los requerimientos de recursos del software de aplicación
- Determinar los requerimientos de recursos de comunicación
- Determinar los requerimientos de recursos de software de sistemas
- Determinar los requerimientos de suministros
- Determinar los requerimientos de recurso de registros vitales
- Determinar los requerimientos de los recursos de equipos

- Determinar los requerimientos de los recursos del personal
- Determinar los requerimientos de los servicios básicos
- Determinar los requerimientos de área de oficina/industria
- Preparar la declaración de los requerimientos mínimos

Recursos de recuperación mínimos para procesos de negocio no computarizados

Objetivo

Identificar en detalle los recursos requeridos para operar los procesos críticos y necesarios no basados en computadoras bajo condiciones de recuperación.

Cada proceso de negocio no basado en computadoras tiene un número de requerimientos de recursos. En esta fase se completa una investigación detallada de los requerimientos de los procesos críticos y necesarios. Para cada proceso crítico y necesario no basado en computadoras se identifican todos los recursos necesarios bajo condiciones de recuperación. Luego, son determinados los recursos requeridos para operaciones de emergencia.

Un proceso crítico y necesario no basado en computadoras puede no requerir de una recuperación total del proceso hasta el mismo nivel como en las operaciones normales.

Este concepto de sólo recuperar partes de los procesos no basados en computadoras resulta en una configuración mínima. La configuración mínima puede ser bastante reducida a comparación de la configuración requerida para la operación completa del proceso completo de negocio. Esto puede resultar en significativamente menor cantidad de recursos requeridos para la configuración mínima.

Para cada proceso crítico y necesario no computarizado se tiene un número de requerimientos a ser considerados incluyendo:

- Suministros
- Registros vitales, incluyendo información basada en computadoras y bases de datos
- Equipos, incluyendo configuración y transportes
- Personal, incluyendo las funciones de cada uno
- Transporte requerido para cada recurso
- Servicios básicos
- Area de oficina

Se debe mantener la seguridad durante operaciones bajo condiciones de recuperación. Esto incluye controles de acceso físicos, implementación de medidas preventivas de desastre o de reducción de riesgo y controles de tipo de auditoría como la segregación de funciones.

Una vez que la información se recolecta, debe de ser detallada en un documento de requerimientos mínimos de los recursos de la recuperación o, si la información existe en otros documentos, se debe de preparar un documento resumen que incorpore referencias específicas a la documentación existente.

Estrategias de Respaldo

Objetivo

- Considerar las estrategias alternativas para el respaldo de la información en distintos medios
- Seleccionar facilidades off-site de almacenamiento
- Determinar la frecuencia y el contenido de las copias de respaldo

La llave para una recuperación exitosa de las operaciones del Banco depende de la manutención adecuada de copias de la información relevante y segura, programas de computadora y documentación. Pese a cuán sofisticada sea la estrategia actual de recuperación, si el Banco no puede reconstruir su información y los ambientes de operación en el momento del desastre, la recuperación fracasará.

A pesar de que el tema de realizar copias de respaldo es mayormente técnico, el Coordinador de la recuperación del negocio debe comprender que es lo que será respaldado, por ejemplo las funciones de negocio. Los procesos críticos y

necesarios fueron identificados en la etapa de análisis del impacto del negocio y las salidas y entradas fueron identificados en las Fases G y H – Recursos de recuperación mínimos. Los requerimientos mínimos de los recursos de recuperación son a los que se necesita realizar copias de respaldo, o en caso de suministros, debe de guardarse un stock en un sitio alternativo.

La selección de una estrategia de copias de respaldo incorpora los temas del almacenamiento in-house y off-site, frecuencia de copias, número de las copias requeridas, responsabilidad de las copias y el mantenimiento de la documentación adecuada de la realización de las copias de respaldo.

Se debe considerar que el tiempo en que la información debe ser retenida puede ser dictado por una regulación legal, estándares de industria o requerimientos del Banco. Estas deberán ser investigadas antes de seleccionar la estrategias de respaldo. El numero de copias realizadas así como el tiempo de retención, pueden también ser influenciada por la importancia y el costo para el Banco. En esta face se debe definir:

- Estrategia de respaldo
- Acuerdos formales de almacenamiento off-site
- Procedimientos de revisión de almacenamiento.

Fase : Lugares de Recuperación

Objetivo

- Identificar todas las opciones de la recuperación del Centro de Computo
- Seleccionar las ubicaciones primarias y secundarias de reunión
- Identificar ubicaciones de centro de comando
- Identificar sitios de recuperación de usuario

Las ubicaciones para la reunión del personal, el control de las operaciones de la recuperación y el procesamiento de las condiciones de recuperación son identificados, evaluados y seleccionados. Un desastre puede tener cualquier alcance, usualmente clasificado en desastres de unidad, local y regionales. Para cada tipo de sitio, se identifican las ubicaciones primarias y alternativas.

Las ubicaciones primarias de recuperación deben de ser adecuadas para las operaciones en el evento que ocurra un desastre local de grandes proporciones, donde un otro sitio es requerido para continuar el procesamiento. Los sitios alternativos deben de ser para los desastres regionales o de unidad. La selección del tipo de sitio de recuperación será influenciado por el tiempo máximo de inoperancia de los procesos de negocio y por el costo de las facilidades del sitio de recuperación.

Curso de Acción

Objetivo

- Formular un número de estrategias alternativas de plan de recuperación de desastres y luego de evaluarlas, seleccionar la más apropiada.
- Obtener un acuerdo para proceder a la etapa de preparación, mantenimiento y prueba del Plan.

Se debe desarrollar un número de estrategias factibles de plan de recuperación de desastres, basadas en los requerimientos de la recuperación, estrategias de copia de respaldo y ubicaciones de recuperación son seleccionadas.

Las selecciones son revisadas de acuerdo a los tiempos objetivos de recuperación y las prioridades establecidas en la etapa anterior.

Las medidas de reducción del riesgo son evaluadas y se recomienda cualquier medida apropiada adicional. Luego de la evaluación de las estrategias factibles de la recuperación de desastre, se escoge la estrategia más adecuada. En la selección de la estrategia de recuperación de desastre, debe de tenerse en mente que el nivel de las copias de respaldo y los arreglos de la recuperación deben de reflejar el valor de los recursos que están siendo protegidos.

Etapa 4 – Elaboración de planes de emergencia, respaldo y recuperación

En esta etapa, se elabora y prueba el PCN. La preparación del plan de continuidad de negocios requiere de la participación substancial del propio personal del Banco, para asegurar la confianza que este funcionará cuando se presente la necesidad.

El plan entonces es sometido a una serie de pruebas y de funcionamientos de ensayo para asegurarse de que está en una forma completamente realizable y eficiente.

El PCN debe contener un mecanismo que asegure su actualización, mediante revisiones regulares y procedimientos de mantenimiento. También, se debe de nombrar a la persona quien será el encargado y obtendrá la responsabilidad de mantener el plan actualizado y probado.

Fase : Preparación del Plan de Continuidad de Negocios

Objetivo

Preparar el borrador del plan de continuidad de negocios, reuniendo información previamente recopilada y preparando procedimientos específicos de recuperación de desastre

Un PCN debe contener toda la información necesaria para recuperar los procesos críticos y necesarios del negocio de una organización de un desastre.

Luego de recuperar los procesos críticos y necesarios del Banco, la organización querrá retomar eventualmente a sus operaciones normales, lo que incluye la recuperación de los procesos opcionales del negocio. Sin embargo, como los procesos opcionales del negocio por definición, no son críticos, los procedimientos de recuperación de estos no son desarrollados como parte del PCN (salvo el registro de las copias de respaldo relevante) sino en el momento en que son requeridos.

Una copia maestra del plan conteniendo toda la información debe de ser guardada en otro sitio. Una copia entera la guarda el Coordinador de recuperación de negocios y otros miembros del Equipo de recuperación de negocio, si se considera apropiado. Otras copias del PCN distribuidas pueden excluir secciones cuya información no sea apropiada para el receptor.

Una vez que el plan de prueba se complete en la siguiente fase son incorporados los procedimientos relacionados a la prueba y mantenimiento continuo del plan.

Etapa 5 – Prueba y mantenimiento de los planes de emergencia, respaldo y recuperación

Prueba y mantenimiento del Plan

Objetivo

Verificar que el PCN pueda ser usado para recuperar las funciones críticas y necesarias del Banco luego que estas sean interrumpidas.

Los objetivos generales de la fase de prueba y mantenimiento del plan son de descubrir y arreglar cualquier error en el plan y de producir procedimientos de prueba y mantenimiento para su uso continuo.

Responsables

El líder de recuperación de desastre debe ser alguien con autoridad que tenga una visión integral del Banco y mantenga la calma bajo presión.

Anexo 6

ANÁLISIS DE IMPACTO DEL NEGOCIO

(BIA – BUSINESS IMPACT ANALISIS)

ANALISIS DE IMPACTO EN EL NEGOCIO

(BIA – BUSINESS IMPACT ANALISIS)

INTRODUCCION

Los desastres causados por un evento natural o humano, pueden ocurrir, en cualquier parte, hora y negocio. Existen distintos tipos de contingencias, como por ejemplo:

- Riesgos naturales, tales como mal tiempo y terremotos;
- Riesgos tecnológicos, tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte;
- Riesgos sociales como actos terroristas y desórdenes.

Pequeñas contingencias podrían provocar un impacto significativo en la habilidad del negocio para conducir operaciones y entregar sus productos y servicios.

El Plan de Continuidad de Negocios del Banco Del Dinero, tiene como objetivo reducir el impacto operacional y financiero de un eventual desastre a un nivel aceptable.

Como base para el desarrollo de los Planes de Recuperación de TI y de Continuidad del Negocio, es necesario realizar un análisis del tiempo de reacción adecuado para la recuperación de las principales aplicaciones que soportan los procesos críticos del negocio. Para esto, se realizó un estudio de Análisis de Impacto en el Negocio (BIA: Business Impact Analisis) en el cual se evaluó la criticidad de los procesos de acuerdo a los siguientes aspectos:

- Máximo tiempo de interrupción aceptado
- Impactos tangibles, que corresponden al costo financiero causado por interrupción del proceso
- Impactos intangibles, que indica los efectos de la interrupción del proceso en: pérdida de la productividad, deterioro de la imagen, pérdida de ventaja competitiva, deterioro servicio al cliente, deterioro de relaciones con entidades

relacionadas, incumplimiento de regulaciones legales y stress / moral de los empleados.

ANÁLISIS DE IMPAACTO EN EL NEGOCIO ("BIA")

Objetivo Principal

El objetivo principal del BIA es determinar las funciones, procesos de negocios e infraestructura de soporte que son críticos para la continuidad o viabilidad del Banco.

Objetivos Específicos

Para lograr el objetivo principal del BIA, se definieron los siguientes objetivos específicos:

- Examinar y comprender los procesos de negocios del Banco e identificar las áreas críticas en el caso de que se produzca una contingencia.
- Identificar las preocupaciones y prioridades de la Dirección del Banco en el caso de que exista una indisponibilidad de los Sistemas de Información producida por una Contingencia.
- Identificar el máximo tiempo en el que un proceso crítico del Banco deberá ser restaurado para su normal y eficiente continuidad
- Identificar el impacto en las aplicaciones que soportan los procesos críticos del Banco
- Proporcionar las bases de una estrategia para la continuidad del negocio en caso de un desastre

Alcance y consideraciones

El BIA busca comprender, a un alto nivel, las unidades de negocio del Banco, sus interdependencias y los tipos de recursos que se necesitan para asegurar la continuidad de los procesos críticos del negocio.

Para el desarrollo de este análisis, se consideraron los siguientes aspectos:

- Situaciones límite, actuando bajo la suposición de que ha ocurrido un desastre, tanto natural, tecnológico como humano.
- En la determinación de los tiempos de recuperación se tuvieron en cuenta la disponibilidad y capacidades del personal del Banco, una vez que el desastre haya ocurrido.
- Las personas entrevistadas en la fase BIA tienen el conocimiento sobre las funciones / procesos de negocio del que son responsables.

METODOLOGÍA DE TRABAJO

El Análisis de Impacto en el Negocio tiene como objetivo determinar los procesos críticos del Banco y las aplicaciones que los soportan con el fin de proporcionar las bases a los Planes de Recuperación TI y de Continuidad del Negocio (PCN).

A lo largo de esta fase se llevaron a cabo las siguientes actividades:

a) Entrevistas a diferentes empleados responsables de los Departamentos que conforman el Banco. A continuación se indican los cargos de las personas entrevistadas:

Cargo
Jefe Zonal Banca Persona
Jefe de Análisis Crediticio
Gerente de Capital Humano
Gerente Central de Planeamiento y Control
Gerente Central de Riesgo de Crédito
Gerente de Legal
Gerente Central de Operaciones y Siste
Gerente de Auditoría Interna
Gerente de Finanzas
Gerente de Calidad de Servicios
Jefe de Administración de Riesgos

En esta actividad se obtuvieron los siguientes logros:

- Conocimiento de la estructura de cada Departamento con el fin de identificar las principales funciones y la relación con los Sistemas de Información del Banco

- Identificación de las principales preocupaciones que se tienen ante una indisponibilidad de los Sistemas de Información en el Banco por causa de una contingencia.

b) Caracterización de los procesos de cada línea de negocio. En esta actividad cada responsable identificó para su línea de negocio los siguientes antecedentes:

i. Macroprocesos

ii. Procesos

iii. Subprocesos

iv. Críticidad asociada a cada subproceso

Críticidad	Simbología
Muy crítico	4
Crítico	3
Medianamente crítico	2
No crítico	1

v. Aplicaciones que soportan cada unos de los procesos del Banco

vi. Máximo tiempo de interrupción en que el subproceso puede estar interrumpido en horas.

vii. Dependencias funcionales de entrada y salida con otros sub-procesos del Banco.

viii. Impactos tangibles: impactos financieros por pérdida del Banco durante los periodos de tiempo de 3 horas, 1 día, 3 días, 1 semana, 2 semanas y 1 mes en los siguientes rangos:

Rango (US$)	Simbología
0-10M	A
10M-50M	B
50M-100M	C
100M-1MM	D
Mayor a 1MM	F

ix. Impactos intangibles clasificados de 1 a 5, siendo 1 el menor impacto y 5 el mayor impacto para los siguientes ámbitos:

Ámbito
Pérdida de la productividad
Deterioro de la imagen
Pérdida de venta competitiva
Deterioro del servicio al cliente
Deterioro de relaciones con entidades relacionadas
Incumplimiento regulaciones legales
Stress / moral de los empleados

c) Validación de la críticidad por proceso

Para efectuar esta validación se efectuó un taller con los gerentes de las Líneas de Negocio, en el que se revisó la críticidad asociada a los subprocesos cuyo tiempo máximo de interrupción definido es menor a 24 horas.

En este taller se llegó a consenso entre los asistentes sobre la criticidad de los sub-procesos y cuyo resultado, unido a los restantes sub-procesos se muestra en este informe.

EVALUACIÓN DE RIESGOS

Para el desarrollo de un proceso BIA es de vital importancia anticiparse y obtener una visión de los posibles riesgos que podrían provocar una crisis de continuidad en las operaciones del negocio. En este sentido, el presente plan se ha enfocado principalmente hacia la mitigación de los riesgos que pudieran conducir a:

- Falla en el proceso del negocio
- Pérdida de activos
- Incumplimiento de Obligaciones regulatorias
- Daño en la imagen y reputación del Banco

El proceso de evaluación de riesgos que se llevó a cabo consistió en identificar los diferentes tipos de amenazas, para luego analizar cualitativamente sus posibles impactos, medidas preventivas y probabilidad de ocurrencia (Alta, Media o Baja). En el anexo 1 se adjunta la matriz de evaluación de riesgos utilizada.

Para llevar a cabo el proceso de identificación de amenazas fue fundamental la comprensión y análisis de los riesgos asociados con aspectos tales como:

- ✓ Industrias especificas: Relacionadas sobretodo con industrias con componentes de infraestructura crítica que están enfrentadas a mayor riesgo, que son más independientes y que tiene mayor impacto.
- ✓ Regiones Geográficas Específicas: Países, estados y ciudades en las cuales el negocio de la organización conduce un alto o bajo riesgo. Los factores incluyen: países que son políticamente inestables; áreas más susceptibles al tiempo y desastres naturales o infraestructuras débiles (ejemplo: energía, telecomunicaciones, leyes nacionales o locales y regulaciones); ciudades con alta concentración de industrias.
- ✓ Instalaciones: Ubicación, condición y configuración de las funciones críticas de negocio conducen a un alto riesgo.
- ✓ Dependencias críticas. El nivel de dependencia de un negocio afecta en riesgo a terceros.

- ✓ Personas: Toda organización confía en su personal para conducir su negocio. Pero algunas organizaciones son mucho más dependientes que otras en cuanto a su productividad, movilización y recursos humanos.

- ✓ Sistemas de Información: Centros de información, negocios transaccionales se ven afectados con mayor frecuencia por interrupciones del proceso.

Las amenazas identificadas que podrían afectar y activar los planes de continuidad del Banco fueron las siguientes:

- Terremoto
- Incendio
- Fuga / Daño por agua
- Explosiones / Atentados
- Fallas de Hw / SO
- Fallas de Sw
- Errores del personal
- Pérdida de energía eléctrica
- Falla en las comunicaciones
- Virus/ Ataque de Hackers
- Asalto / Toma de rehenes
- Disturbios civiles / huelgas

Una vez evaluados los riesgos e identificados aquellos de mayor exposicion, se definieron los escenarios de contingencia asociados, en base a los cuales se desarrollaron las estrategias de continuidad descritas en los planes de Recuperación de Tecnología de Información y de Continuidad de Negocios.

Los escenarios considerados para el desarrollo del Plan de Continuidad de negocios fueron los siguientes:

a. Indisponibilidad de una Agencia o Sucursal del Banco
   Se considera que la Agencia se encuentra imposibilitada para realizar sus funciones normalmente, ya sea por que no cuenta con el soporte necesario de los Sistemas de Información o por que sus condiciones físicas no están funcionando en forma apropiada o requerida.

b. Indisponibilidad del Edificio Alide
Considera la discontinuidad operacional de los procesos de negocio que se llevan a cabo en este edificio, ya sea por destrucción física total o parcial de estas dependencias, o por que no cuentan con el soporte de Sistemas de Información apropiado.

c. Indisponibilidad de la Oficina Principal (excluida la Agencia y el Centro de Cómputo).

Contempla que la Oficina Principal del Banco ha interrumpido sus operaciones, ya sea porque no cuentan con el soporte de Tecnologías de la Información o por que han sufrido un daño físico total o parcial.

d. Indisponibilidad del Centro de Cómputo
En esta situación se ha considerado que se pierde la total funcionalidad del Centro de Cómputo.

La evaluación y administración de estos riesgos han permitido al Banco:

- Desarrollar estrategias de recuperación y respaldo de las decisiones operacionales, tecnológicas y humanas.
- Diseñar e implementar sistemas de información seguros con una alta disponibilidad para la continuidad de los negocios.
- Identificar los controles existentes y los nuevos controles a implementar para minimizar riesgos, evaluando el costo / beneficio de dichos controles.
- Planificar la seguridad de la información y el bienestar del personal.
- Determinar la cobertura de los seguros para los casos que se requiera de una recuperación de pérdidas.

ANÁLISIS DE LA CRITICIDAD DE LOS PROCESOS DE NEGOCIO.

El presente Análisis muestra el análisis realizado sobre los procesos críticos del Banco y las aplicaciones que soportan estos procesos.

A continuación se presenta una lista de los macro-procesos y sus procesos de negocio identificados.

Macro-Procesos y Procesos de Negocio Identificados por Linea de Negocio

En el BIA se analizaron los efectos resultantes de una catástrofe o desastre en los siguientes Procesos de negocio clasificados por Macro-Proceso.

LINEA DE NEGOCIO	MACROPROCESOS	PROCESOS DE NEGOCIO
ADMINISTRACIÓN DE ACTIVOS	ADMINISTRACION DE ACTIVOS	❑ Adquisición ❑ Contabilidad y Reporte ❑ Logística y Servicios ❑ Seguros ❑ Tasación ❑ Venta
BANCA COMERCIAL	BANCA COMERCIAL-COLOCACIONES	❑ Contabilidad y Reporte ❑ Post- Venta ❑ Pre-venta ❑ Venta
BANCA MINORISTA	BANCA PRIVADA-COLOCACIONES	❑ Contabilidad y Reporte ❑ Post-Venta ❑ Pre-venta ❑ Venta
	BANCA PRIVADA-CAPTACIONES	❑ Contabilidad y Reporte ❑ Pre-venta ❑ Post-Venta ❑ Venta
	BANCA PERSONAL-COLOCACIONES	❑ Contabilidad y Reporte ❑ Pre-Venta ❑ Post-Venta ❑ Venta
	BANCA COMERCIAL-PERSONAL CAPTACIONES	❑ Contabilidad y Reporte ❑ Pre-Venta ❑ Post-Venta ❑ Venta

LINEA DE NEGOCIO	MACROPROCESOS	PROCESOS DE NEGOCIO
FINANZAS CORPORATIVAS	REP. OBLIGACIONISTAS	❑ Post-venta ❑ Pre-venta ❑ Venta
	NORMAS Y PROCESOS	❑ Elaboración de Normativa ❑ Rediseño de Procesos
	MERCADEO Y PRODUCTOS	❑ Mercadeo y productos
	FIDEICOMISO	❑ Post-venta ❑ Pre-venta ❑ Venta
	ESTRUCTURACION DE EMISIONES	❑ Contabilidad y Reporte ❑ Post-venta ❑ Pre-venta ❑ Venta
	CONTROL DE CREDITOS	❑ Control de créditos
	CONTROL	❑ Control
	CONTABILIDAD	❑ Cierre contable
	AUDITORIA	❑ Auditoría
	ASEORIA Y APOYO EN LA GESTION	❑ Administración de riesgos ❑ Planeamiento y control de gestión
	ASESORIA LEGAL	❑ Asesoría Legal

LINEA DE NEGOCIO	MACROPROCESOS	PROCESOS DE NEGOCIO
	ADMINISTRACIÓN DE SISTEMAS	❑ Administración de equipos de computo ❑ Administración de la infraestructura de networking ❑ Administración de seguridad ❑ Administración de software especializado ❑ Desarrollo de proyectos de sistemas ❑ Ingeniería y configuración de equipo de computo ❑ Licenciamiento ❑ Mantenimiento de equipos de computo ❑ Mantenimiento de sistemas ❑ Soporte técnico a usuarios ❑ Soporte y mantención de equipos de computo ❑ Soporte y mantención de software base
	ADMINISTRACIÓN DE RECURSOS DEL BANCO	❑ Logística y servicios ❑ Proyectos y Mantenimiento
	ADMINISTRACIÓN DE RECURSOS HUMANOS	❑ Administración de Recursos Humanos
LIQUIDACION Y PAGOS	TRANSFERENCIA DE FONDOS	❑ Envío / recepción ❑ Post-venta
	SERVICIOS EMPRESARIALES	❑ Contabilidad y Reporte ❑ Post-venta ❑ Pre-venta ❑ Venta
NEGOCIACIÓN Y VENTAS	TRADING Y VENTAS	❑ Contabilidad y reporte ❑ Post-venta ❑ Pre-venta ❑ Venta

LINEA DE NEGOCIO	MACROPROCESOS	PROCESOS DE NEGOCIO
SERVICIOS DE AGENCIAS	SERVICIOS	❑ Cheques viajeros gerencia-giros ❑ Contabilidad y reporte ❑ Post-venta ❑ Moneda extranjera ❑ Valores ❑ Varios

A continuación presentamos un resumen de los sub-procesos críticos de negocio por línea de negocio según el criterio acordado en el workshop realizado con la gerencia del Banco para evaluar aspectos referentes a la críticidad de los sub-procesos y aquellos con tiempo de interrupción menor a 24 horas.

Línea de Negocio: Banca Minorista

N°	Macroproceso	Proceso	Sub-proceso	Tiempo máximo de Interrupción (Horas)
1.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Bloqueo de cuenta	0,5
2.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Pago de cheques	0,5
3.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retención de Fondos	0,5
4.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retiros de cuenta	0,5
5.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Suspensión de cheques	0,5
6.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Transferencia de fondos	0,5

N°	Macroproceso	Proceso	Sub-proceso	Tiempo máximo de Interrupción (Horas)
7.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Pago de cuotas / cancelación de créditos	0,5
8.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retiro de libre disponibilidad de cuentas CTS	0,5
9.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Bloqueo de tarjeta efectivo	0.5
10.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Revocatoria y anulación de cheques MB	0.5
11.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Canje de Entrada	1
12.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Canje de Salida	1
13.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Rechazo Canje de Entrada	1
14.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Rechazo Canje de Salida	1
15.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Depósitos en cuenta	1
16.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Liberación de Fondos	1
17.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Pago a cuenta de tarjeta de crédito	1

N°	Macroproceso	Proceso	Sub-proceso	Tiempo máximo de Interrupción (Horas)
18.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Cargos en cuentas de ahorro / corrientes /únicas	3
19.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Abonos en cuentas de ahorros / corrientes /únicas	3
20.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Protesto (letras) - Garantías	3
21.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Ejecución (carta fianza)- Garantías	3

Línea de Negocio: Liquidación y Pagos

	Macroproceso	Proceso	Sub-proceso	Tiempo máximo de Interrupción (Horas)
22.	TRANSFERENCIA DE FONDOS	ENVIO / RECEPCION	Transferencia a/de bancos locales (BCR)	1
23.	TRANSFERENCIA DE FONDOS	POST-VENTA	Retiros de efectivos bóveda BCR	1
24.	TRANSFERENCIA DE FONDOS	POST-VENTA	Depósito de efectivos bóveda BCR	1
25.	TRANSFERENCIA DE FONDOS	POST-VENTA	Retiro de fondos del BCR	1
26.	SERVICIOS EMPRESARIALES	POST-VENTA	Abono de planillas - haberes	3

Línea de Negocio: Negociación y Ventas

	Macroproceso	Proceso	Sub-proceso	Tiempo máximo de Interrupción (Horas)
27.	TRADING Y VENTAS	POST-VENTA	Ingreso / retiro de custodia	0,5
28.	TRADING Y VENTAS	POST-VENTA	Liquidación	0,5
29.	TRADING Y VENTAS	POST-VENTA	Pago	0,5
30.	TRADING Y VENTAS	POST-VENTA	Verificación y Confirmación Op.	0,5

Línea de Negocio: Servicios de Agencias

	Macroproceso	Proceso	Sub-proceso	Tiempo máximo de Interrupción (Horas)
31.	SERVICIOS	POST-VENTA	Inicio de operaciones de promotor servicios	0,5
32.	SERVICIOS	CHEQUES VIAJEROS GERENCIA - GIROS	Anulación de valorados emitidos	0,5
33.	SERVICIOS	CHEQUES VIAJEROS GERENCIA - GIROS	Pago de cheque (Giros, Gerencia)	0,5
34.	SERVICIOS	POST-VENTA	Habilitación de efectivo a las agencias	1
35.	SERVICIOS	POST-VENTA	Remesas de excedentes de agencias	1
36.	SERVICIOS	POST-VENTA	Cierre de operaciones de promotor servicios	1

En la siguiente tabla, se indican las aplicaciones que soportan a cada uno de los procesos críticos.

Línea de Negocio: Banca Minorista

N°	Macroproceso	Proceso	Sub-proceso	Aplicaciones
1.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Bloqueo de cuenta	Transactor
2.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Pago de cheques	Transactor
3.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retención de Fondos	Transactor
4.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retiros de cuenta	Transactor
5.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Suspensión de cheques	Transactor
6.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Transferencia de fondos	Transactor
7.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Pago de cuotas / cancelación de créditos	Transactor, Bansud
8.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retiro de libre disponibilidad de cuentas CTS	Transactor
9.	BCA	POST-VENTA	Bloqueo de tarjeta	Bansud

N°	Macroproceso	Proceso	Sub-proceso	Aplicaciones
	COMERCIAL-PERSONAL CAPTACIONES		efectivo	
10.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Revocatoria y anulación de cheques MB	Transactor
11.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Canje de Entrada	Bansud
12.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Canje de Salida	Bansud
13.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Rechazo Canje de Entrada	Bansud
14.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Rechazo Canje de Salida	Bansud
15.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Depósitos en cuenta	Transactor
16.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Liberación de Fondos	Transactor
17.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Pago a cuenta de tarjeta de crédito	Transactor
18.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Cargos en cuentas de ahorro / corrientes /únicas	Transactor, SIAF

N°	Macroproceso	Proceso	Sub-proceso	Aplicaciones
19.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Abonos en cuentas de ahorros / corrientes /únicas	Transactor, SIAF
20.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Protesto (letras) - Garantías	Transactor, Bansud
21.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Ejecución (carta fianza)- Garantías	Transactor, Bansud

Línea de Negocio: Liquidación y Pagos

	Macroproceso	Proceso	Sub-proceso	Aplicaciones
22.	TRANSFERENCIA DE FONDOS	ENVIO / RECEPCION	Transferencia a/de bancos locales (BCR)	SIAF, BACTRADER
23.	TRANSFERENCIA DE FONDOS	POST-VENTA	Retiros de efectivos bóveda BCR	SIAF, BACTRADER
24.	TRANSFERENCIA DE FONDOS	POST-VENTA	Depósito de efectivos bóveda BCR	SIAF, BACTRADER
25.	TRANSFERENCIA DE FONDOS	POST-VENTA	Retiro de fondos del BCR	SIAF, BACTRADER
26.	SERVICIOS EMPRESARIALES	POST-VENTA	Abono de planillas - haberes	Transactor

Línea de Negocio: Negociación y Ventas

	Macroproceso	Proceso	Sub-proceso	Aplicaciones
27.	TRADING Y VENTAS	POST-VENTA	Ingreso / retiro de custodia	Bansud
28.	TRADING Y VENTAS	POST-VENTA	Liquidación	BACTRADER–BACCAMBIOS

29.	TRADING Y VENTAS	POST-VENTA	Pago	LBTR, SIAF, Transactor, Swift, EB-LINK
30.	TRADING Y VENTAS	POST-VENTA	Verificación y Confirmación Op.	WEB FIS (Sistema de firmas)

Línea de Negocio: Servicios de Agencias

	Macroproceso	Proceso	Sub-proceso	Aplicaciones
31.	SERVICIOS	POST-VENTA	Inicio de operaciones de promotor servicios	Transactor
32.	SERVICIOS	CHEQUES VIAJEROS GERENCIA - GIROS	Anulación de valorados emitidos	Transactor
33.	SERVICIOS	CHEQUES VIAJEROS GERENCIA - GIROS	Pago de cheque (Giros, Gerencia)	Transactor
34.	SERVICIOS	POST-VENTA	Habilitación de efectivo a las agencias	Transactor
35. B	SERVICIOS	POST-VENTA	Remesas de excedentes de agencias	Transactor
36.	SERVICIOS	POST-VENTA	Cierre de operaciones de promotor servicios	Transactor

En la siguiente tabla se indican los impactos tangibles e intangibles de todos los sub-procesos críticos mencionados anteriormente por línea de negocio.

Los Impactos tangibles se clasifican en rangos por pérdidas financieras en distintos tiempos.

Rango (US$)	Simbología
0-10M	A
10M-50M	B
50M-100M	C
100M-1MM	D
Mayor a 1MM	F

Los impactos intangibles clasificados de 1 a 5, siendo 1 el menor impacto y 5 el mayor impacto para los diferentes ámbitos.

Línea de Negocio: Banca Minorista

N°	Macroproceso	Proceso	Sub-proceso	Impacto Tangible						Impacto Intangible						
				3 horas	1 día	3 días	1 semana	2 semana	1 mes	Pérdida de la productivida	Deterioro de la imagen	Pérdida de ventaja competitiva	Deterioro del servicio al cliente	Deterioro de relaciones con	Incumplimiento regulaciones	Stress / Moral de los empleados
1.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Bloqueo de cuenta							3	3	2	3	2	5	3
2.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Pago de cheques							5	5	5	5	5	5	5
3.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retención de Fondos							3	3	3	3	5	5	3
4.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retiros de cuenta							5	5	5	5	5	5	5
5.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Suspensión de cheques							3	5	5	5	5	5	3

N°	Macroproceso	Proceso	Sub-proceso	Impacto Tangible						Impacto Intangible						
				3 horas	1 día	3 días	1 semana	2 semana	1 mes	Pérdida de la productividad	Deterioro de la imagen	Pérdida de ventaja competitiva	Deterioro del servicio al cliente	Deterioro de relaciones con	Incumplimiento regulaciones	Stress / Moral de los empleados
6.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Transferencia de fondos							4	5	4	5	3	3	3
7.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Pago de cuotas / cancelación de créditos							5	3	4	5	3	4	4
8.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retiro de libre disponibilidad de ctas CTS							5	5	4	5	3	4	4
9.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Bloqueo de tarjeta Efectivo							1	4	4	4	4	2	3
10.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Revocatoria y Anulación de cheques MB							3	3	3	3	5	5	3

Nº	Macroproceso	Proceso	Sub-proceso	Impacto Tangible						Impacto Intangible						
				3 horas	1 día	3 días	1 semana	2 semana	1 mes	Pérdida de la productivida	Deterioro de la imagen	Pérdida de ventaja competitiva	Deterioro del servicio al cliente	Deterioro de relaciones con	Incumplimiento regulaciones	Stress / Moral de los empleados
11.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Canje de Entrada	D	D	D	E	E	E	4	3	4	4	5	3	4
12.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Canje de Salida	D	D	D	E	E	E	5	5	5	5	5	5	5
13.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Rechazo Canje de Entrada	B	B	B	B	C	C	4	3	4	4	5	5	4
14.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Rechazo Canje de Salida	B	B	B	B	C	C	5	3	4	4	5	5	4
15.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Depósitos en cuenta							5	5	5	5	5	3	5
16.	BCA	POST-	Liberación de							3	5	3	5	5	5	4

N°	Macroproceso	Proceso	Sub-proceso	Impacto Tangible						Impacto Intangible						
				3 horas	1 día	3 días	1 semana	2 semana	1 mes	Pérdida de la productivida	Deterioro de la imagen	Pérdida de ventaja competitiva	Deterioro del servicio al cliente	Deterioro de relaciones con	Incumplimiento regulaciones	Stress / Moral de los empleados
	COMERCIAL-PERSONAL CAPTACIONES	VENTA	Fondos													
17.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Pago a cuenta de tarjeta de crédito							5	3	4	5	3	4	4
18.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Cargos en cuentas de ahorro/corrientes /unicas							4	3	3	3	2	2	3
19.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Abonos en cuentas de ahorros / corrientes /únicas							4	3	3	3	2	2	3
20.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Protesto (letras) - Garantías							5	5	2	5	2	2	5

N°	Macroproceso	Proceso	Sub-proceso	Impacto Tangible						Impacto Intangible						
				3 horas	1 día	3 días	1 semana	2 semana	1 mes	Pérdida de la productivida	Deterioro de la imagen	Pérdida de ventaja competitiva	Deterioro del servicio al cliente	Deterioro de relaciones con	Incumplimiento regulaciones	Stress / Moral de los empleados
21.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Ejecución (carta fianza)- Garantías							5	5	2	5	2	2	5

Línea de Negocio: Liquidación y Pagos

N°	Macroproceso	Proceso	Sub-proceso	Impacto Tangible						Impacto Intangible						
				3 horas	1 día	3 días	1 semana	2 semana	1 mes	Pérdida de la productividad	Deterioro de la imagen	Pérdida de ventaja competitiva	Deterioro del servicio al	Deterioro de relaciones	Incumplimiento	Stress / Moral de los
22.	TRANSFERENCIA DE FONDOS	ENVIO / RECEPCION	Transferencia a/de bancos locales (BCR)	A	B	B	C	C	D	3	4	5	5	4	1	3
23.	TRANSFERENCIA DE FONDOS	POST-VENTA	Retiros de efectivos bóveda bcr							5	1	1	1	5	5	5
24.	TRANSFERENCIA DE FONDOS	POST-VENTA	Depósito de efectivo bóveda bcr							5	1	1	1	5	5	5
25.	TRANSFERENCIA DE FONDOS	POST-VENTA	Retiro de fondos del Bcr							5	5	2	5	2	2	5
26.	SERVICIOS EMPRESARIALES	POST-VENTA	Abono de planillas - haberes							5	5	4	5	5	1	4

Línea de Negocio: Negociación y Ventas

N°	Macroproceso	Proceso	Sub-proceso	Impacto Tangible						Impacto Intangible						
				3 horas	1 día	3 días	1 semana	2 semana	1 mes	Pérdida de la productividad	Deterioro de la imagen	Pérdida de ventaja competitiva	Deterioro del servicio al	Deterioro de relaciones	Incumplimiento	Stress / Moral de los
27.	TRADING Y VENTAS	POST-VENTA	Ingreso/retiro de custodia	A	A	A	B	C	D	3	2	2	4	5	5	3
28.	TRADING Y VENTAS	POST-VENTA	Liquidación	B	B	C	D	D	D	5	5	5	5	5	5	5
29.	TRADING Y VENTAS	POST-VENTA	Pago	B	B	C	D	D	D	5	5	5	5	5	5	5
30.	TRADING Y VENTAS	POST-VENTA	Verificación y Confirmación Op.	B	B	C	D	D	D	5	5	5	5	5	5	5

Línea de Negocio: Servicios de Agencias

				Impacto Tangible						Impacto Intangible						
N°	Macroproceso	Proceso	Sub-proceso	3 horas	1 día	3 días	1 semana	2 semana	1 mes	Pérdida de la productividad	Deterioro de la imagen	Pérdida de ventaja competitiva	Deterioro del servicio al	Deterioro de relaciones	Incumplimiento	Stress / Moral de los
31.	SERVICIOS	POST-VENTA	Inicio de operaciones de promotor servicios							5	5	5	5	5	5	5
32.	SERVICIOS	CHEQUES VIAJEROS GERENCIA - GIROS	Anulación de valorados emitidos							5	5	3	5	5	5	5
33.	SERVICIOS	CHEQUES VIAJEROS GERENCIA - GIROS	Pago de cheque (Giros, Gerencia)							5	5	5	5	5	5	5
34.	SERVICIOS	POST-VENTA	Habilitación de efectivo a las agencias							5	5	5	5	2	2	5
35.	SERVICIOS	POST-VENTA	Remesas de excedentes de							5	1	1	1	1	5	5

			agencias													
36.	SERVICIOS	POST-VENTA	Cierre de operaciones de promotor servicios						5	1	5	1	1	5	5	

5.5 Procedimientos de Entrada y Salida de los procesos críticos del Negocio

En tabla que se muestra a continuación se indican las interdependencias de entrada y salida para cada proceso crítico por línea de negocio.

Línea de Negocio: Banca Minorista

N°	Macroproceso	Proceso	Sub-proceso	Interdependencia de Entrada			Interdependencia de Salida		
				Importancia1	Importancia2	Importancia3	Importancia1	Importancia2	Importancia3
1.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Bloqueo de cuenta						
2.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Pago de cheques						
3.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retención de Fondos						
4.	BCA COMERCIAL-	POST-	Retiros de cuenta						

N°	Macroproceso	Proceso	Sub-proceso	Interdependencia de Entrada			Interdependencia de Salida		
				Importancia1	Importancia2	Importancia3	Importancia1	Importancia2	Importancia3
	PERSONAL CAPTACIONES	VENTA							
5.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Suspensión de cheques						
6.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Transferencia de fondos						
7.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Pago de cuotas / cancelación de créditos						
8.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Retiro de libre disponibilidad de ctas CTS						
9.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Bloqueo de tarjeta Efectivo						
10.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Revocatoria y Anulación de cheques MB						
11.	BCA COMERCIAL-PERSONAL	POST-VENTA	Canje de Entrada				CCE		

N°	Macroproceso	Proceso	Sub-proceso	Interdependencia de Entrada			Interdependencia de Salida		
				Importancia1	Importancia2	Importancia3	Importancia1	Importancia2	Importancia3
	CAPTACIONES								
12.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Canje de Salida	agencias			CCE		
13.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Rechazo Canje de Entrada	negocios		CCE			
14.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Rechazo Canje de Salida			CCE			
15.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Depósitos en cuenta						
16.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Liberación de Fondos						
17.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Pago a cuenta de tarjeta de crédito						
18.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Cargos en cuentas de ahorro/corrientes /unicas						

N°	Macroproceso	Proceso	Sub-proceso	Interdependencia de Entrada			Interdependencia de Salida		
				Importancia1	Importancia2	Importancia3	Importancia1	Importancia2	Importancia3
19.	BCA COMERCIAL-PERSONAL CAPTACIONES	POST-VENTA	Abonos en cuentas de ahorros / corrientes /únicas						
20.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Protesto (letras) - Garantías						
21.	BCA COMERCIAL-PERSONAL COLOCACIONES	POST-VENTA	Ejecución (carta fianza)- Garantías						

Línea de Negocio: Liquidación y Pagos

N°	Macroproceso	Proceso	Sub-proceso	Interdependencia de Entrada			Interdependencia de Salida		
				Importancia 1	Importancia 2	Importancia 3	Importancia 1	Importancia 2	Importancia 3
22.	TRANSFERENCIA DE FONDOS	ENVIO / RECEPCION	Transferencia a/de bancos locales (BCR)	Instrucción	Autorización		Gestión de Negocios		
23.	TRANSFERENCIA DE FONDOS	POST-VENTA	Retiros de efectivos bóveda bcr						
24.	TRANSFERENCIA DE FONDOS	POST-VENTA	Depósito de efectivo bóveda bcr						
25.	TRANSFERENCIA DE FONDOS	POST-VENTA	Retiro de fondos del Bcr						
26.	SERVICIOS EMPRESARIALES	POST-VENTA	Abono de planillas - haberes						

Línea de Negocio: Negociación y Ventas

N°	Macroproceso	Proceso	Sub-proceso	Interdependencia de Entrada			Interdependencia de Salida		
				Importancia1	Importancia2	Importancia3	Importancia1	Importancia2	Importancia3
27.	TRADING Y VENTAS	POST-VENTA	Ingreso/retiro de custodia	Instrucción de Tesorería			Entrega a la contrapartе		
28.	TRADING Y VENTAS	POST-VENTA	Liquidación	Registro Op.			-		
29.	TRADING Y VENTAS	POST-VENTA	Pago	Registro Op.					
30.	TRADING Y VENTAS	POST-VENTA	Verificación y Confirmación Op.	Confirmación Op.			-		

Línea de Negocio: Servicios de Agencias

N°	Macroproceso	Proceso	Sub-proceso	Interdependencia de Entrada			Interdependencia de Salida		
				Importancia 1	Importancia 2	Importancia 3	Importancia 1	Importancia 2	Importancia 3
31.	SERVICIOS	POST-VENTA	Inicio de operaciones de promotor servicios						
32.	SERVICIOS	CHEQUES VIAJEROS GERENCIA - GIROS	Anulación de valorados emitidos						
33.	SERVICIOS	CHEQUES VIAJEROS GERENCIA - GIROS	Pago de cheque (Giros, Gerencia)						
34.	SERVICIOS	POST-VENTA	Habilitación de efectivo a las						

			agencias						
35.	SERVICIOS	POST-VENTA	Remesas de excedentes de agencias						
36.	SERVICIOS	POST-VENTA	Cierre de operaciones de promotor servicios						

Anexo 1 : MATRIZ DE EVALUACIÓN DE RIESGOS PARA EL PCN

AMENAZAS	Probabilidad de Ocurrencia	Descripción del Impacto		Cuantificación del Impacto	Nivel de Exposición	Medidas Preventivas	Posibles Escenarios de Contingencia *
		Primario	Secundario				
Terremoto	Media	• Pérdida o daño de equipos e información • Daños Personales • Pérdida de infraestructura	• Incendio • Perdida de electricidad, agua y comunicaciones • Indisponibilidad del personal y trauma	Alto	Alto	• Mejoras estructurales • Anclaje de equipos • Capacitación, procedimientos y suministros para Emergencias • Sitios alternativos	1 2 3 4
Incendio	Alta	• Pérdida o daño de equipos e información • Daños Personales • Daño a las instalaciones	• Daños por agua • Perdida de electricidad, agua y comunicaciones • Contaminación tóxica	Alto	Alto	• Capacitación, procedimientos y suministros para Emergencias • Sistema automático contra incendios con agente limpio • Asegurar activos y documentos	1 2 3 4
Fuga / Daño por agua	Alta	• Pérdida o daño de equipos e información • Daño a las instalaciones	• Humedad • Perdida de electricidad, agua y comunicaciones	Alto	Alto	• Sensores • Cambios estructurales • Reubicación de equipos • Clausura de Baño en el CC	4
Explosión / Atentados	Media	• Pérdida o daño de equipos e información • Daños Personales • Daño a las instalaciones	• Incendio • Perdida de electricidad, agua y comunicaciones • Contaminación tóxica • Indisponibilidad del	Alto	Alto	• Administración y seguridad de las instalaciones • Ubicar equipo sensible lejos del perímetro del edificio	1 2 3 4

AMENAZAS	Probabilidad de Ocurrencia	Descripción del Impacto		Cuantificación del Impacto	Nivel de Exposición	Medidas Preventivas	Posible Escenario de Contingencia
		Primario	Secundario				
Fallas de Hw / SO	Media	• Pérdida de información • Pérdida de capacidad de procesamiento	• Degradación del servicio al cliente • Pérdida de trabajo en progreso • Acumulación de transacciones sin procesar	Alto	Alto	• Protección física de activos • Mantenimiento preventivo • Respaldos redundantes	1 2 3 4
Fallas de SW	Alta	• Pérdida de información o integridad de la misma • Pérdida de capacidad de procesamiento	• Degradación del servicio al cliente • Pérdida de trabajo en progreso • Acumulación de transacciones sin procesar	Alto	Alto	• Control de cambios • Respaldos	1 2 3 4
Pérdida de energía eléctrica	Baja	• Pérdida de información o integridad de la misma • Pérdida de iluminación, uso de equipos y servicios de AC	• Daño de equipos • Se compromete la seguridad de las instalaciones	Alto	Medio	• Fuentes de poder (UPS) • Generadores • Protectores de picos	1 2 3 4

Falla en las comunicaciones	Baja	• Pérdida de transmisión de voz y datos	• Degradación del servicio al cliente • Pérdida de trabajo en progreso • Acumulación de transacciones sin procesar	Alto	Medio	• Protección de equipos e infraestructura de comunicaciones • Anillos de fibra • Planes alternativos de emergencia	1 2 3

AMENAZAS	Probabilidad de Ocurrencia	Descripción del Impacto		Cuantificación del Impacto	Nivel de Exposición	Medidas Preventivas	Posible Escenario de Contingencia
		Primario	Secundario				
Virus/ Ataque de Hackers	Media	• Pérdida de información o integridad de la misma • Incapacidad para usar computadoras y redes	• Pérdida de capacidad local de procesamiento • Degradación del servicio al cliente	Medio	Medio	• Control de accesos • Control de virus • Concienciación y disciplina • Administración de pistas de auditoria	1 2 3
Asalto / Toma de rehenes	Bajo	• Interrupción del servicio al cliente • Daños Personales • Pérdida de activos • Trauma del personal	• Pérdida de confianza de clientes y empleados	Alto	Medio	• Control de accesos • Vigilancia visible • Planes de respuesta	1 2 3
Disturbios civiles / huelgas	Media	• Disminución del personal • Disminución de	• Daños a la propiedad	Medio	Medio	• Manejo de RRHH y personal de backup • Asegurar la propiedad	1 2 3

		suministros o servicios • Intimidación al personal y/o clientes				• Seguridad de personal y clientes • Planes alternativos • Evitar cobertura negativa de medios de comunicación	
Errores del Personal de Sistemas	Media	• Pérdida de información o integridad de la misma • Pérdida de capacidad de procesamiento	• Degradación del servicio al cliente • Pérdida de trabajo en progreso • Acumulación de transacciones sin procesar	Alto	Alto	• Control de cambios • Respaldos • Capacitación del personal	1 2 3 4

Anexo 7

ANALISIS DE COSTOS DE CONSTRUIR UN CENTRO DE COMPUTO ALTERNO PROPIO

Análisis de Costo Centro de Computo Alterno Propio

Opción 1:
En esta opcion se tendría que hacer un upgrade al servidor principal AS/400 el cual representa un costo significativo.

Upgrade AS/400	300,000
Servidores Intel	70,000
Construcción CC	55,000
Mantenimiento Upgrade (1000 mes 13)	19,786
Mantenimiento Intel (100 x año x serv)	1,900
Mantenimiento 3590	15,203
Traslado Equipos	3,500
Operación / mtto CC (1000 mensual)	31,186
Comunicaciones (Router, Sw itch)	5,000
Total (US $)	**501,575**

Opción 2:
Aquí el AS/400 seria el mismo que tenemos, la desventaja es que su crecimiento estaría limitado, y tarde o temprano se tendría que ser un Up-grade o adquirir uno nuevo.

Servidores Intel	70,000
Construcción CC	55,000
Mantenimiento Intel (100 x año x serv)	1899.73
Mantenimiento 3590 (487.5 mensual)	15,203
Traslado Equipos	3,500
Operación / mtto CC (1000 mensual)	31,186
Comunicaciones (Router, Sw itch)	5,000
Unidades de Cinta (DDS3, TSM, LTO)	20,000
Total (US $)	**201,789**

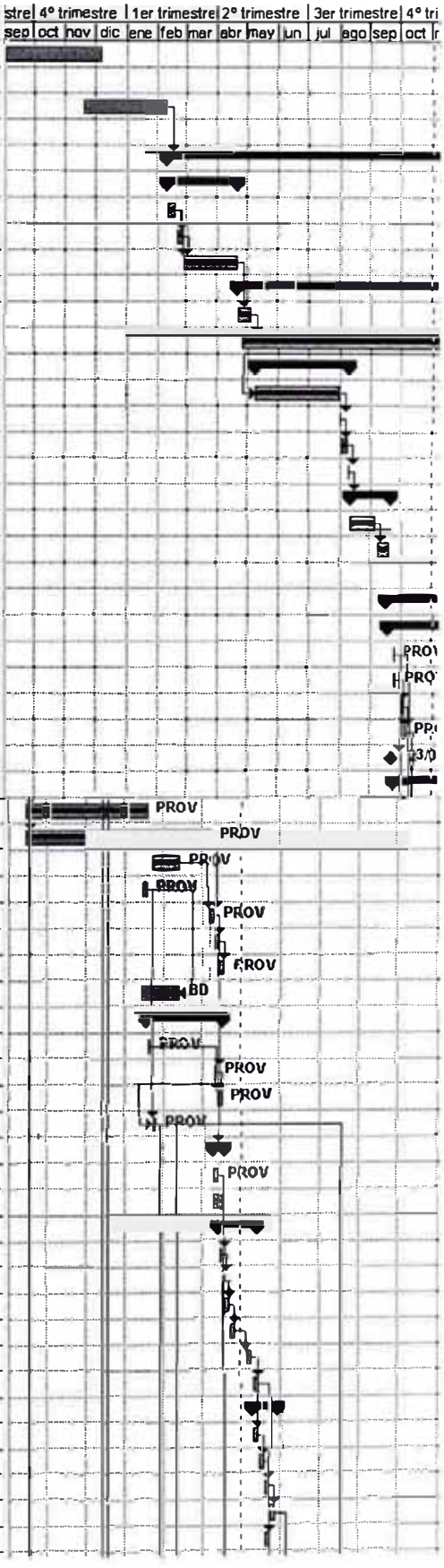
El Costo es alto, se tendría que analizar otras opciones.

Anexo 8

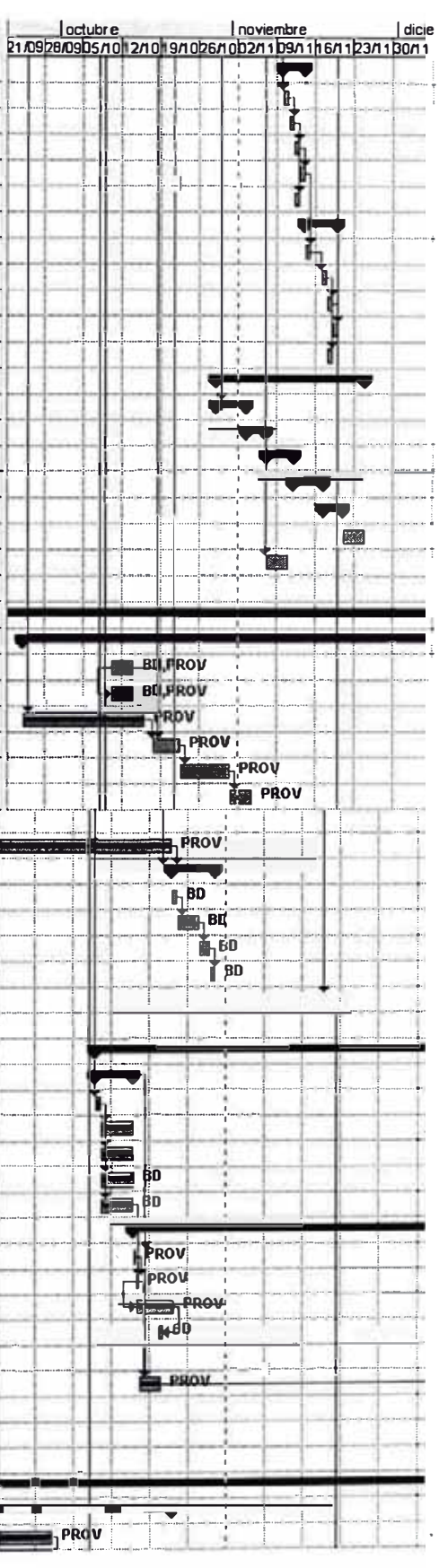
PLAN DE TRABAJO

CRONOGRAMA DE ACTIVIDADES

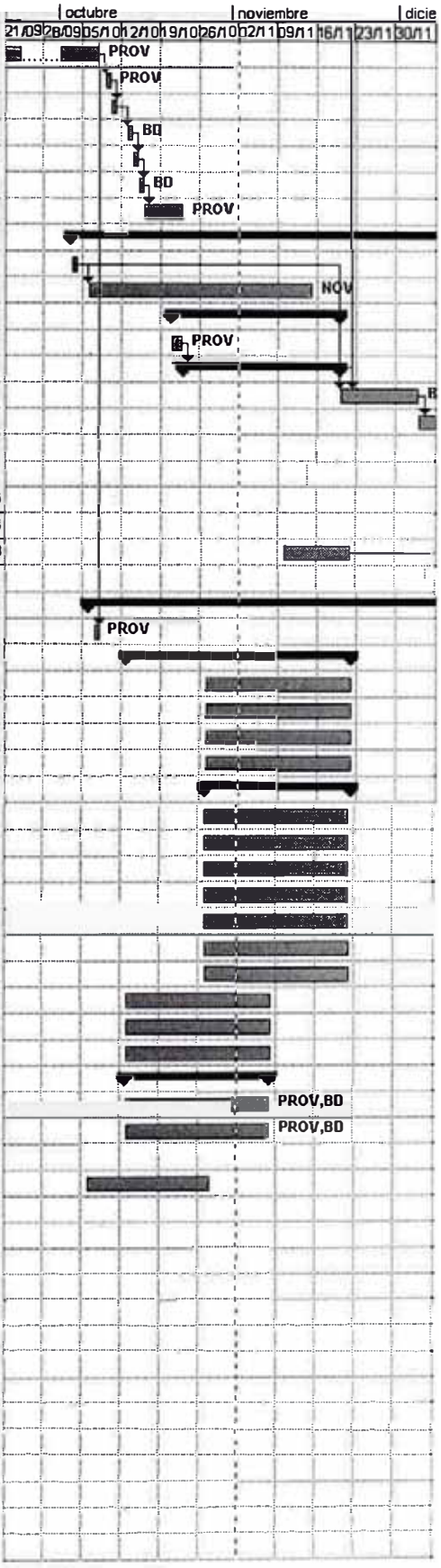
	Nombre de tarea	Duración	Inicio	Fin
1	PLAN DE CONTINUIDAD DE NEGOCIO	4 mss	lun 19/08/02	vie 06/12/02
2				
3	PLAN DE CONTINGENCIA INFORMTICA (PCI)	3 mss	mar 19/11/02	lun 10/02/03
4				
5	CENTRO DE COMPUTO ALTERNO	202 días?	mar 11/02/03	jue 20/11/03
6	Analisis de Mercado	50 días	mar 11/02/03	lun 21/04/03
7	Otros Bancos	5 días	mar 11/02/03	lun 17/02/03
8	Proveedores	5 días	mar 18/02/03	lun 24/02/03
9	Visita a/de proveedores	2 mss	mar 25/02/03	lun 21/04/03
10	Plan de Respaldo	152 días	mar 22/04/03	ue 20/11/03
11	Objetivos del Centro de Computo Alterno	10 días	mar 22/04/03	lun 05/05/03
12	Selección de Sistemas a respaldar	30 sems	jue 24/04/03	ue 20/11/03
13	Analisis de cotizaciones	67 días?	jue 08/05/03	vie 08/08/03
14	Evaluacion de Propuestas	3 mss	jue 08/05/03	mié 30/07/03
15	Presentacion de opciones	1 día?	ue 31/07/03	jue 31/07/03
16	Analisis y Sistemas	1 sem	vie 01/08/03	jue 07/08/03
17	Toma de Decision	1 día?	vie 08/08/03	vie 08/08/03
18	Coordinaciones con el Proveedor	30 días	lun 11/08/03	vie 19/09/03
19	Reuiniones con el Proveedor, para ajuste de propuesta	1 ms	lun 11/08/03	vie 05/09/03
20	Ajustes de Contrato	10 días	lun 08/09/03	vie 19/09/03
21				
22	Servicio de contingencia para el Banco del Dinero (CCA)	132.5 días	mié 17/09/03	jue 25/03/04
23	Etapa 1 - Implantación del proyecto	97.5 días	mié 17/09/03	jue 05/02/04
24	Kickoff	1 día	mar 23/09/03	mar 23/09/03
25	Entrega de relación de personal del proveedor asignada al proy	3 días	mié 24/09/03	vie 26/09/03
26	Entrega de relación de personal de Bco Dinero asignado al proy	3 días	lun 29/09/03	mié 01/10/03
27	Definición de plan de reuniones de control del proyecto	3 días	jue 02/10/03	lun 06/10/03
28	Firma del acta de inicio del servicio	0 días	mar 23/09/03	mar 23/09/03
29	Habilitación de facilidades de HW	43 días	mié 24/09/03	lun 24/11/03
30	Importación de upgrade Servidor iSeries	15 días	mié 24/09/03	mié 15/10/03
31	Importación de Blade xSeries	22 días	mié 24/09/03	lun 27/10/03
32	Planeamiento de Sitio	3 días	vie 17/10/03	mar 21/10/03
33	Instalación física de Servidor iSeries	1 día	mié 15/10/03	mié 15/10/03
34	Instalación física de Blade	1 día	lun 27/10/03	lun 27/10/03
35	Revision de HW de servidores X series	1 día	mar 28/10/03	mar 28/10/03
36	Actualizacion del Firmware del Hardware	1 día	mié 29/10/03	mié 29/10/03
37	Validación de configuración de RAID y Mirror iSeries	5 días	mié 15/10/03	mar 21/10/03
38	Configuración de RAID y Mirror en servidor iSeries	9.5 días	jue 16/10/03	mié 29/10/03
39	Configuracion de discos del iSeries en Raid 5	0.5 días	jue 16/10/03	jue 16/10/03
40	Configuración de RAID y Mirror en servidores	0.5 días	mar 28/10/03	mar 28/10/03
41	Documentacion del RAID Aplicado, configuración y espe	1 día	mar 28/10/03	mié 29/10/03
42	Instalación de Sistema Operativo OS400 5.1 + fixes	0.5 días	vie 17/10/03	vie 17/10/03
43	Instalación de SO y aplicativos en servidores Intel	2 días	mar 28/10/03	mié 29/10/03
44	Entrega de todos los Drivers (Tarjeta de Red, Video, Ra	1 día	mar 28/10/03	ma[illegible]
45	Reunion de coordinacion para determinar configuracion	2 días	mar 28/10/03	mié[illegible]
46	Instalacion del BDC (Backup Domain Controller Dom_	5 días	mié 29/10/03	mar 04/11/03
47	Instalacion del Sistema Operativo	0.5 días	mié 29/10/03	mié 29/10/03
48	Instalacion de Parches y Sofware de Seguridad	0.5 días	mié 29/10/03	mié 29/10/03
49	Instalacion de Servicios Wins, DHCP,DNS	1 día	jue 30/10/03	jue[illegible]
50	Pruebas en la red del Proveedor	1 día	vie 31/10/03	vie[illegible]
51	Pruebas de Promocion a PDC y Replicacion de cuentas	1 día	lun 03/11/03	un 03/11/03
52	Elaboracion de Documento de Recuperacion en caso de	1 día	mar 04/11/03	mar 04/11/03
53	Instalacion deDinero Bolsa (Dedicado)	4 días	mar 04/11/03	vie 07/11/03
54	Sistema Operativo	1 día	mar 04/11/03	mar 04/11/03
55	Configuracion del Aplicativo	1 día	mié 05/11/03	mié 05/11/03
56	Pruebas en la RED del Proveedor	1 día	jue 06/11/03	jue 06/11/03
57	Elaboracion de Documento de Recuperacion en caso de	1 día	vie 07/11/03	vie 07/11/03
58	Pruebas de funcionamiento redundancia de component	1 día	jue 06/11/03	jue 06/11/03



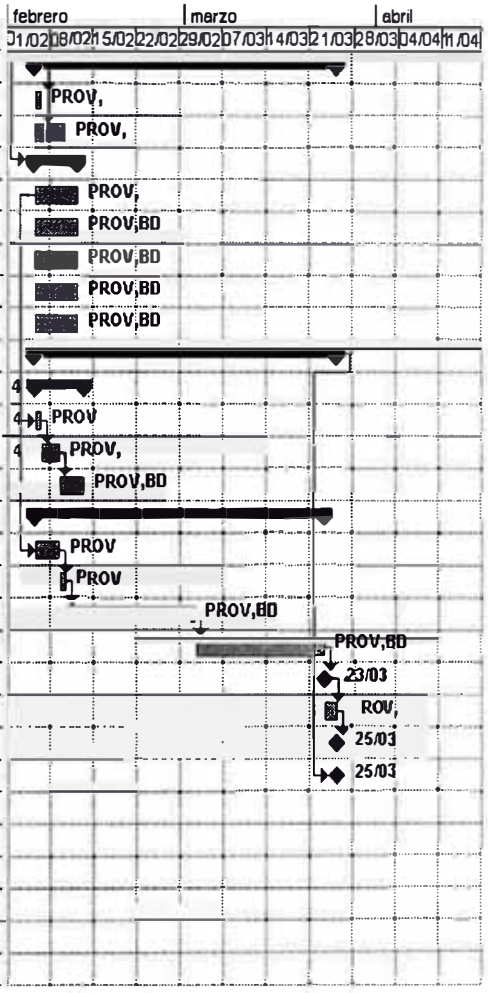
	Nombre de tarea	Duración	Inicio	Fin
59	**Instalacion del Macrofiche (Compartido)**	**4 días**	**lun 10/11/03**	**jue 13/11/03**
60	Sistema Operativo	1 día	lun 10/11/03	lun 10/11/03
61	Configuracion del Aplicativo	1 día	mar 11/11/03	mar 11/11/03
62	Pruebas en la RED del Proveedor	1 día	mié 12/11/03	mié 12/11/03
63	Elaboracion de Documento de Recuperacion en caso de	1 día	jue 13/11/03	jue 13/11/03
64	Pruebas de funcionamiento redundancia de componente	1 día	mié 12/11/03	mié 12/11/03
65	**Instalacion del SIG-Bussiness Object (Compartido)**	**4 días**	**vie 14/11/03**	**mié 19/11/03**
66	Sistema Operativo	1 día	vie 14/11/03	vie 14/11/03
67	Configuracion del Aplicativo	1 día	lun 17/11/03	lun 17/11/03
68	Pruebas en la RED del Proveedor	1 día	mar 18/11/03	mar 18/11/03
69	Elaboracion de Documento de Recuperacion en caso de	1 día	mié 19/11/03	mié 19/11/03
70	Pruebas de funcionamiento redundancia de componente	1 día	mar 18/11/03	mar 18/11/03
71	**Servidores de Ventanilla (Dedicados)**	**19 días**	**mié 29/10/03**	**lun 24/11/03**
72	**Diseño**	**3.5 días**	**mié 29/10/03**	**l un 03/11/03**
76	**Instalacion tx1**	**3.5 días**	**lun 03/11/03**	**j ue 06/11/03**
80	**Instalacion db1**	**3 días**	**vie 07/11/03**	**m ar 11/11/03**
83	**Instalacion tx2**	**3.5 días**	**mié 12/11/03**	**lun 17/11/03**
87	**Pruebas Internas**	**3.5 días**	**lun 17/11/03**	**jue 20/11/03**
91	Elaboracion de Documento de Recuperacion en caso de	2 días	vie 21/11/03	lun 24/11/03
92	Instalacion de las 5 PCs entregadas por el Proveedor	2 días	vie 07/11/03	lun 10/11/03
93	**Pruebas de aplicativos Business Object, Macrofiche, Banktrade**	**2 días**	**vie 26/12/2003**	**lun 29/12/03**
94	**Habilitación de facilidades de SW**	**79 días**	**mié 17/09/03**	**vie 09/01/04**
95	**SW de replicación MIMIX**	**73 días**	**mié 24/09/03**	**jue 08/01/04**
96	Definición de configuración de replicación	2 días	vie 10/10/03	lun 13/10/03
97	Definición de journalización de datos y objetos	2 días	vie 10/10/03	lun 13/10/03
98	Adquisición de licencia de MIMIX	15 días	mié 24/09/03	mié 15/10/03
99	Instalación de MIMIX	3 días	vie 17/10/03	mié 22/10/03
100	Configuración de MIMIX	7 días	mié 22/10/03	vie 31/10/03
101	Activación de journalización de datos y objetos	2 días	vie 31/10/03	mar 04/11/03
102	Pruebas de replicación ***	3 días	mar 06/01/04	jue 08/01/04
103	Adquisición de licencia BRMS	25 días	mié 17/09/03	mié 22/10/03
104	Instalación y configutación de BRMS	6 días	jue 23/10/03	jue 30/10/03
105	Instalacion	1 día	jue 23/10/03	jue 23/10/03
106	Configuracion	2 días	vie 24/10/03	lun 27/10/03
107	Pruebas	2 días	mar 28/10/03	mié 29/10/03
108	Documentacion	1 día	jue 30/10/03	jue 30/10/03
109	Instalación y configuración de sistemas de Bco en iSeries**	1 día	jue 20/11/03	jue 20/11/03
110	Full backup de servidor iSeries	1 día	vie 09/01/04	vie 09/01/04
111	**Habilitación de Comunicaciones**	**68.25 días**	**jue 09/10/03**	**vie 16/01/04**
112	**Coordinación**	**5 días**	**jue 09/10/03**	**mié 15/10/03**
113	Reunión de coodinación de esquema de red	1 día	jue 09/10/03	jue 09/10/03
114	Determinación del esquema de direccionamiento IP	4 días	vie 10/10/03	mié 15/10/03
115	Definición de la configuración de subredes IP y SNA	4 días	vie 10/10/03	mié 15/10/03
116	Determinación de puertos a ser utilizados en replicación	4 días	vie 10/10/03	mié 15/10/03
117	Definición de conf necesaria en RMS para servidores ir	4 días	vie 10/10/03	mié 15/10/03
118	**Implantación**	**63.25 días**	**jue 16/10/03**	**vie 16/01/04**
119	Creación de VLAN en el CCA para el servicio contratad	0.5 días	jue 16/10/03	jue 16/10/03
120	Configuración en TSM para acceso a servidores Intel	0.5 días	jue 16/10/03	jue 16/10/03
121	Habilitación router en el Proveedor (4Mbps)	5 días	jue 16/10/03	jue 23/10/03
122	Contratación de enlace de 4Mbps entre el Banco y el Pr	1 día	lun 20/10/03	mar 21/10/03
123	Instalación de enlace de 4Mbps entre el Banco y el Prov	10 días	mar 23/12/03	jue 08/01/04
124	Configuración de Red Multiservicio (ruteo y seguridad)	2 días	vie 17/10/03	lun 20/10/03
125	Pruebas de conectividad LAN	3 días	vie 09/01/04	mar 13/01/04
126	Pruebas de conectividad WAN	2 días	mié 14/01/04	jue 15/01/04
127	Pruebas de conectividad de extremo a extremo	0.25 días	vie 16/01/04	vie 16/01/04
128	**Tareas Paralelas de Migración**	**82 días**	**mié 17/09/03**	**mié 14/01/04**
129	**Migración aplicativo Comercio Exterior**	**25 días**	**mié 17/09/03**	**mié 22/10/03**
130	Definición de entorno de pruebas	10 días	mié 17/09/03	mar 30/09/03



	Nombre de tarea	Duración	Inicio	Fin
131	Pruebas de código - interfases	10 días	mié 17/09/03	mar 07/10/03
132	Configuración de solución de acceso BD - conexión SQ	1 día	jue 09/10/03	jue 09/10/03
133	Pruebas de acceso BD - conexión SQL	1 día	vie 10/10/03	vie 10/10/03
134	Pruebas de aplicacion	1 día	lun 13/10/03	lun 13/10/03
135	Replicación de la solución	1 día	mar 14/10/03	mar 14/10/03
136	Pase a produccion	1 día	mié 15/10/03	mié 15/10/03
137	Documentacion de contingencia de Comercio Exterior er	5 días	jue 16/10/03	mié 22/10/03
138	**Migración aplicativo Bandinero**	**65 días**	**vie 03/10/03**	**mié 07/01/04**
139	Reunión con Novatronic para definición de APIs	1 día	vie 03/10/03	vie 03/10/03
140	Cambios y pruebas de APIs ***	30 días	lun 06/10/03	vie 14/11/03
141	**Preparación de ambiente de desarrollo**	**22 días**	**mar 21/10/03**	**mié 19/11/03**
142	Instalación HW y SW servidor iSeries	2 días	mar 21/10/03	mié 22/10/03
143	**Configuración de ambiente Aplicativos Bandi**	**20 días**	**jue 23/10/03**	**mié 19/11/03**
162	Conversión de programas	10 días	jue 20/11/03	mié 03/12/03
163	Pruebas de funcionalidad con usuarios	20 días	jue 04/12/03	lun 05/01/04
164	Pase a producción	2 días	mar 06/01/04	mié 07/01/04
165	Migración a SO 5.1 y App servidor desarrollo BS	5 días	mar 30/12/03	mié 07/01/04
166	Migración a SO 5.1 servidor producción BS	2 días	mar 06/01/04	mié 07/01/04
167	Configuración de herramientas de control de cambios	1 día	mié 07/01/04	mié 07/01/04
168	Definición de esquema de seguridad con TCP/IP	10 días	lun 10/11/03	vie 21/11/03
169	Implantación de esquema de seguridad	5 días	jue 08/01/04	mié 14/01/04
170	**Definición Inicial de Procedimientos del servicio**	**67 días**	**lun 06/10/03**	**lun 12/01/04**
171	Entrega de procedimientos del Centro de Computo Alterno	1 día	mar 07/10/03	mar 07/10/03
172	**De Operación**	**30 días**	**lun 13/10/03**	**vie 21/11/03**
173	Monitoreo de Sistema Operativo iSeries	20 días	lun 27/10/03	vie 21/11/03
174	Monitoreo de Sistema de Replicación	20 días	lun 27/10/03	vie 21/11/03
175	Monitoreo de Redes	20 días	lun 27/10/03	vie 21/11/03
176	Copias de respaldo	20 días	lun 27/10/03	vie 21/11/03
177	**Políticas de backups**	**20 días**	**lun 27/10/03**	**vie 21/11/03**
178	Politica de Backup Diario	20 días	lun 27/10/03	vie 21/11/03
179	Politica de Backup Mensual	20 días	lun 27/10/03	vie 21/11/03
180	Politica de Medios	20 días	lun 27/10/03	vie 21/11/03
181	Politica de Movimientos	20 días	lun 27/10/03	vie 21/11/03
182	Envío y retiro de cintas	20 días	lun 27/10/03	vie 21/11/03
183	Definicion de Cintotecas	20 días	lun 27/10/03	vie 21/11/03
184	Documentacion de la Politicas aplicadas	20 días	lun 27/10/03	vie 21/11/03
185	Escalamiento de problemas	20 días	lun 13/10/03	vie 07/11/03
186	Envío y retiro de cintas	20 días	lun 13/10/03	vie 07/11/03
187	Ejecución de reprocesos	20 días	lun 13/10/03	vie 07/11/03
188	**Administrativos**	**20 días**	**lun 13/10/03**	**vie 07/11/03**
189	Visitas de inspección solicitadas por Bcodel Dinero	20 días	lun 13/10/03	vie 07/11/03
190	Generación de reportes	20 días	lun 13/10/03	vie 07/11/03
191	Prueba de procedimientos	3 días	jue 08/01/04	lun 12/01/04
192	Definición de proc de recuperación en contingencia DRP	15 días	lun 06/10/03	lun 27/10/03
193	**Prueba unitaria del servicio (sin usuarios)**	**18.5 días**	**lun 12/01/04**	**jue 05/02/04**
194	**Planeamiento**	**6 días**	**lun 12/01/04**	**lun 19/01/04**
195	Reunión de definición de prueba unitaria	1 día	lun 12/01/04	lun 12/01/04
196	Definición de tareas de pruebas	5 días	mar 13/01/04	lun 19/01/04
197	Definición de criterios de culminación de prueba	1 día	mar 13/01/04	mar 13/01/04
198	**Desarrollo**	**9 días**	**mar 20/01/04**	**vie 30/01/04**
199	Ejecución de prueba	4 días	mar 20/01/04	vie 23/01/04
200	Evaluación de la Prueba	1 día	lun 26/01/04	lun 26/01/04
201	Documentación y ajustes de procedimientos de operaci	4 días	mar 27/01/04	vie 30/01/04
202	Generación de informe de prueba	0.5 días	mar 27/01/04	mar 27/01/04
203	Entrega de informe de las actividades ejecutadas por el Pro	0.5 días	mar 27/01/04	mar 27/01/04
204	Aprobación de informe	7 días	mar 27/01/04	jue 05/02/04
205	Firma del Acta de Conformidad de la Etapa I	0 días	jue 05/02/04	jue 05/02/04
206	**Etapa 2 - Operación del Servicio**	**35 días**	**jue 05/02/04**	**jue 25/03/04**



	Nombre de tarea	Duración	Inicio	Fin
206	⊟ **Etapa 2 - Operación del Servicio**	**35 días**	**jue 05/02/04**	**jue 25/03/04**
207	Redefinición del plan de reuniones de control del proyecto	1 día	jue 05/02/04	vie 06/02/04
208	Planeamiento del cronograma de pruebas de contingencia	3 días	jue 05/02/04	mar 10/02/04
209	⊟ **Afinamiento de los Procedimientos de Operación**	**5 días**	**jue 05/02/04**	**jue 12/02/04**
210	Monitoreo de recursos	5 días	jue 05/02/04	jue 12/02/04
211	Copias de respaldo	5 días	jue 05/02/04	jue 12/02/04
212	Generación de reportes	5 días	jue 05/02/04	jue 12/02/04
213	Escalamiento de problemas	5 días	jue 05/02/04	jue 12/02/04
214	Actualización de Procedimientos	5 días	jue 05/02/04	jue 12/02/04
215	⊟ **Implantación de norma de seguridad GSD331**	**35 días**	**jue 05/02/04**	**jue 25/03/04**
216	⊟ **Revisión de la norma de seguridad**	**6 días**	**jue 05/02/04**	**vie 13/02/04**
217	Reunión interna	1 día	jue 05/02/04	vie 06/02/04
218		1 día	vie 06/02/04	lun 09/02/04
219	Desarrollo de la norma	4 días	lun 09/02/04	vie 13/02/04
220	⊟ **Identificación de apéndices que aplican al proyecto**	**33 días**	**jue 05/02/04**	**mar 23/03/04**
221	Identificación de apéndices	2 días	jue 05/02/04	lun 09/02/04
222	Coordinación de entrevistas con los especialistas	1 día	lun 09/02/04	mar 10/02/04
223	Desarrollo de los apéndices	15 días	mar 10/02/04	mar 02/03/04
224	Revisión y verificación de los apéndices	15 días	mar 02/03/04	mar 23/03/04
225	Aprobación de la norma y apéndices	0 días	mar 23/03/04	mar 23/03/04
226	Elaboración plan de acción de los apéndices	2 días	mar 23/03/04	jue 25/03/04
227	Inicio ejecución planes de acción	0 días	jue 25/03/04	jue 25/03/04
228	Firma de acta de conformidad de etapa de Operación	0 días	jue 25/03/04	jue 25/03/04



Anexo 9

ROLES EN EL PROYECTO

ROLES DEFINIDOS PARA EL PROYECTO DE IMPLEMENTACION DEL CENTRO DE COMPUTO ALTERNO PARA EL BANCO DEL DINERO.

ROL	DESCRIPCIÓN	NOMBRE(S)
Ejecutivo del Proyecto o Gerente de Unidad	Ejecutivo de cargo gerencial quien se mantendrá informado del proyecto y a quien se escalará los temas relacionados al servicio. Existe un Ejecutivo a Nivel Gerencial por parte del Banco y su par parte del Proveedor. Participaran de las reuniones ejecutivas para evaluar el avance del proyecto y tomar decisiones si existieran actividades que puedan poner en riesgo el proyecto o en todo caso barreras que se presenten que afecten los tiempos o costos.	
Gerentes o líder del Proyecto	Ejecutivo designado como dueño o responsable del servicio. Dicho ejecutivo y sus delegados tendrán la suficiente autoridad y atribución para resolver los conflictos que puedan poner en riesgo los objetivos, metas o resultados del servicio. Existe un Gerente por parte del Banco y un por parte del Proveedor del servicio, quienes tendrán sus reuniones periódicas (semanales y quincenales), para evaluar el avance del proyecto y las acciones a tomar por tareas que se puedan atrasar o por las tareas siguientes a la reunión.	
Equipo Consultivo	Este equipo esta conformado por el Comité Operativo de Seguridad Informática (COSI), en la cual participan un representante de las diversas áreas de negocio y control del Banco, como Negocios, Recursos Humanos, Sistemas, Auditoria, Seguridad Física y Seguridad Informática, Operaciones y Riesgos (8 miembros). Quienes tienen la función de revisar, evaluar y emitir opinión sobre este proyecto y todos aquellos que tengan que ver el riesgo Operativo del Banco ligado a los sistemas de información.	
Líder Usuario	Ejecutivo del Banco designado como responsable para llevar a cabo las actividades necesarias con los usuarios de las diversas áreas del Banco para cumplir con las pruebas periódicas del Centro de Computo Alterno. Responsable de la capacitación de los procedimientos al personal involucrado de acuerdo a lo establecido en el Plan de Continuidad Informático.	

ROL	DESCRIPCIÓN	NOMBRE(S)
Líder Técnico	Ejecutivo responsable del diseño de la arquitectura tecnológica de la solución para el problema planteado. Llevara a cabo la implementación del CCA con el equipo de especialistas tecnológicos tanto del Banco como del proveedor.	
Especialistas en Aplicativos de Negocios que funcionen AS/400 e Intel	Personas con conocimientos técnicos sobre la plataforma AS/400 e Intel y los aplicativos del Banco que corran sobre los mismos. Quienes montaran los Sistemas de Negocios del Banco y los dejaran funcionando de acuerdo a lo establecido para un desastre en el Centro de Computo Principal.	
Especialistas de SW especializado y Comunicaciones	Personas con conocimiento técnico sobre software de base (Sistemas operativos y afines), replicación, backup, Redes y Seguridad, quienes instaran y configuraran dichos aplicativos de acuerdo a los estándares del Banco.	
Coordinador del Servicio	Responsable de la coordinación y gestión del Centro de Cómputo de Servicios, para dar el mejor servicio al Banco. Esta a cargo de la administración permanente de la infraestructura y recursos provistos y que forman parte del servicio. Asimismo, es el responsable de coordinar las labores de implementación, producción y pruebas de contingencia.	
Especialistas Técnicos para la operación.	Especialistas encargados del mantenimiento y soporte de servidores y comunicaciones durante la operación en el CCA por parte del proveedor.	
Operadores	Personas con conocimiento técnico sobre labores de operación de sistemas y cuya responsabilidad es apoyar al Coordinador de Servicio en todas las gestiones y labores que él considere pertinente realizar	

Anexo 10

CONTROL DE CAMBIOS

PROCEDIMIENTO DE CONTROL DE CAMBIOS

Cualquier requerimiento que implique cambios en las funciones y/o características de los servicios descritos, será tratado según lo establecido en el presente procedimiento, denominado “Procedimiento de Control de Cambios”.

Solicitud de Cambio

Un cambio podrá ser originado por iniciativa de cualquiera de las Partes. Para asegurar un tratamiento uniforme, se usará un formato con el siguiente contenido:

- Solicitante del cambio
- Descripción del cambio
- Justificación
- Identificación preliminar de los componentes de servicio afectados.

Calificación del Cambio

Las solicitudes de cambio serán canalizadas al Coordinador del Servicio de la otra Parte, quien efectuará un análisis preliminar para calificar el cambio.

Calificaciones posibles:

- Cambio menor, en adelante “MEJORA” .

  Si el requerimiento está enmarcado en el alcance de lo establecido en la presente Propuesta y no afecta ni los costos ni los cronogramas o su efecto es manejable.
- Cambio mayor, en adelante “CAMBIO” .

Si el requerimiento está enmarcado en el alcance del proyecto y afecta los costos y/o cronogramas de los mismos.

- Cambio sustancial, en adelante "MODIFICACIÓN" .

  Si el requerimiento no está enmarcado en el alcance de la presente Propuesta y/o afecta substancialmente los costos y/o los cronogramas de los Servicios.

Procedimiento para cada caso:

Para las MEJORAS se aplicará el siguiente procedimiento:

- El Coordinador de Servicios comunicará formalmente a su Contraparte que el cambio solicitado es una MEJORA.
- Cualquiera de las Partes podrá hacer observaciones a la calificación dentro de los tres días hábiles siguientes a la comunicación formal. De no mediar respuesta en el plazo indicado, esta calificación se dará por aprobada.
- Aprobada la calificación como MEJORA, ésta pasará a formar parte del plan de trabajo y cada Parte se asegurará de cumplir con las responsabilidades que ésta genere.

Para los CAMBIOS se aplicará el siguiente procedimiento:

- Análisis detallado del CAMBIO, a cargo del Coordinador del Servicio del proveedor, para evaluar su impacto en los cargos y/o en los términos y condiciones de los Servicios.

- Elevación al Coordinador del Servicio del Banco para que decida su incorporación.
- Decisión:
  - Aceptado, en cuyo caso será incorporado a los Servicios y cada parte asumirá las nuevas responsabilidades que ésta genere.
  - Rechazado, en cuyo caso será archivado junto con la información pertinente a los Servicios.
  - Se definirá un límite de tiempo.
    - Comunicación formal

Para las MODIFICACIONES se aplicarán las siguientes estipulaciones:

En cualquier momento de la vigencia de este Proyecto, cualquiera de las Partes podrá solicitar MODIFICACIONES al Proyecto, solicitando tal(es) MODIFICACIÓN(ES) por escrito a la otra Parte. Dentro de los treinta (30) días hábiles de recepción de tal solicitud, la parte receptora enviará una respuesta a la otra Parte. Si la solicitud de MODIFICACIÓN fue originada por el Banco, el proveedor comunicará por escrito a el Banco si la MODIFICACIÓN puede ser hecha y su efecto en los Apéndices, Cargos y otros términos y condiciones de este Proyecto.

Si el proveedor solicita la MODIFICACIÓN, el Banco notificará por escrito al Proveedor si autoriza su realización bajo los términos y condiciones revisados, o rechaza la MODIFICACIÓN propuesta. Las MODIFICACIONES acordadas deberán ser incorporadas como una modificación a las secciones pertinentes. De estar pendiente un acuerdo para implantar MODIFICACIONES, el proveedor procederá según los

últimos términos y condiciones autorizados del Proyecto. Para la incorporación de las modificaciones, ajustes o revisiones a este Proyecto, se observarán las siguientes reglas:

a) No podrán modificarse la naturaleza u objeto de este proyecto.
b) No podrá alterarse o gravarse, en grado tal que resulte excesivamente oneroso, el objeto de las prestaciones de futuro cumplimiento a cargo de una de las Partes.
c) Deben mantenerse substancialmente las condiciones técnicas para la ejecución del Proyecto.
d) Debe guardarse el equilibrio financiero del Proyecto para ambas Partes.
e) Debe reconocerse al Proveedor y/o a sus subcontratistas, los nuevos costos provenientes de la MODIFICACIÓN, de ser ésta aceptada. Ambas Partes deberán firmar una autorización escrita para implementar cualquier mejora, cambio o modificación.

Anexo 11

TIEMPOS DE RECUPERACION

Tiempos de Recuperación

Introducción.

La ventana de recuperación está dada por la suma de múltiples factores entre los que se encuentran principalmente :

- Políticas del Banco para switchear hacia el ambiente de contingencia.
- Ventana de recuperación ofrecida por la herramienta de replicación del Computador Central y los procedimientos de contingencia del Centro de Cómputo Alterno.
- Ventana de recuperación ofrecida por la solución de restauración de datos y reinstalación de programas de los servidores Intel, de acuerdo a los procedimientos del Banco.
- Ventana de recuperación ofrecida por la solución de comunicaciones provista por el Cliente para switchear a los usuarios hacia el ambiente de contingencia.

A manera de referencia, cabe señalar que la recuperación de un sistema, basado en plataforma AS/400 y con software de recuperación MIMIX es tradicionalmente menor a 2 horas, llegando en algunos casos a ser menor a 30 minutos. Esto dependerá de múltiples factores como son la optimización de los procedimientos de recuperación, la decisión del Cliente de switchear hacia el ambiente de contingencia y de la cantidad de datos utilizada.

En relación a los servidores Intel, la ventana de recuperación se da por el tiempo que demore ejecutar los procedimientos de restauración y reinstalación del Cliente.

Se requiere la ejecución de pruebas de contingencia y afinamiento de procedimientos entre el Cliente y el proveedor para fijar una ventana de recuperación objetivo.

A continuación se describe lo definido por el Banco con respecto a este tema y que esta definido en el Plan de Contingencia Informático.

Recuperación

El Período de Recuperación es la ventana disponible para la restauración de servicios informáticos críticos. Estos períodos están basados en estimaciones de los Directores Informáticos responsables de los sistemas. Estos no están basados en riesgo de negocio o en evaluación de impacto o en consulta detallada con otras áreas impactadas del negocio.

La siguiente tabla identifica el tiempo de interrupción máxima aceptable (MAO) para los sistemas de información y es una estimación de tiempo de recuperación máxima basada en la opinión del gerente responsable del plan así:

Sistemas	MAO (en horas)
Sistema de Ventanillas	1.0
Mesa de Dinero	0.5
Bandinero (AS/400)	0.5
Agente de Bolsa	1.0

Tipos de Escenarios considerados

Los tipos de contingencia que han sido considerados en este estudio son los siguientes:

a) Caída de las comunicaciones entre una Agencia y el centro de Cómputo

Esta contingencia considera la interrupción de los servicios de sistemas con la oficina central o hacia una sucursal, ocasionado por la interrupción de las comunicaciones, suponiendo que los servidores y todo el resto de la plataforma informática permanecen disponibles.

b) Indisponibilidad de la Infraestructura de TI en una Agencia del Banco.

Esta contingencia ocurre cuando una sucursal queda imposibilitada de utilizar sus recursos de Tecnología de la Información por pérdida de sus propios equipos o por un desastre mayor que ha dejado a la sucursal inhabilitada de funcionar.

c) Indisponibilidad total del Centro de Cómputo.

Esta contingencia considera la destrucción total del Centro de Cómputo del Banco del Dinero ubicado en la oficina principal, por un desastre natural (mal tiempo, terremoto, etc.), por fallas tecnológicas (incendio, fallas eléctricas, corte de energía en el sector, etc.) o por acontecimientos sociales tales como atentados terroristas. En estas circunstancias los

equipos de procesamiento de información (AS/400, servidores de archivo, servidores de aplicaciones, etc.) quedan imposibilitados para llevar a cabo sus funciones totalmente.

Es importante señalar que un escenario puede considerar al mismo tiempo más de uno de estos tipos de contingencias, en cuyo caso se aplicarán los procedimientos que se definan para cada uno en forma simultánea.

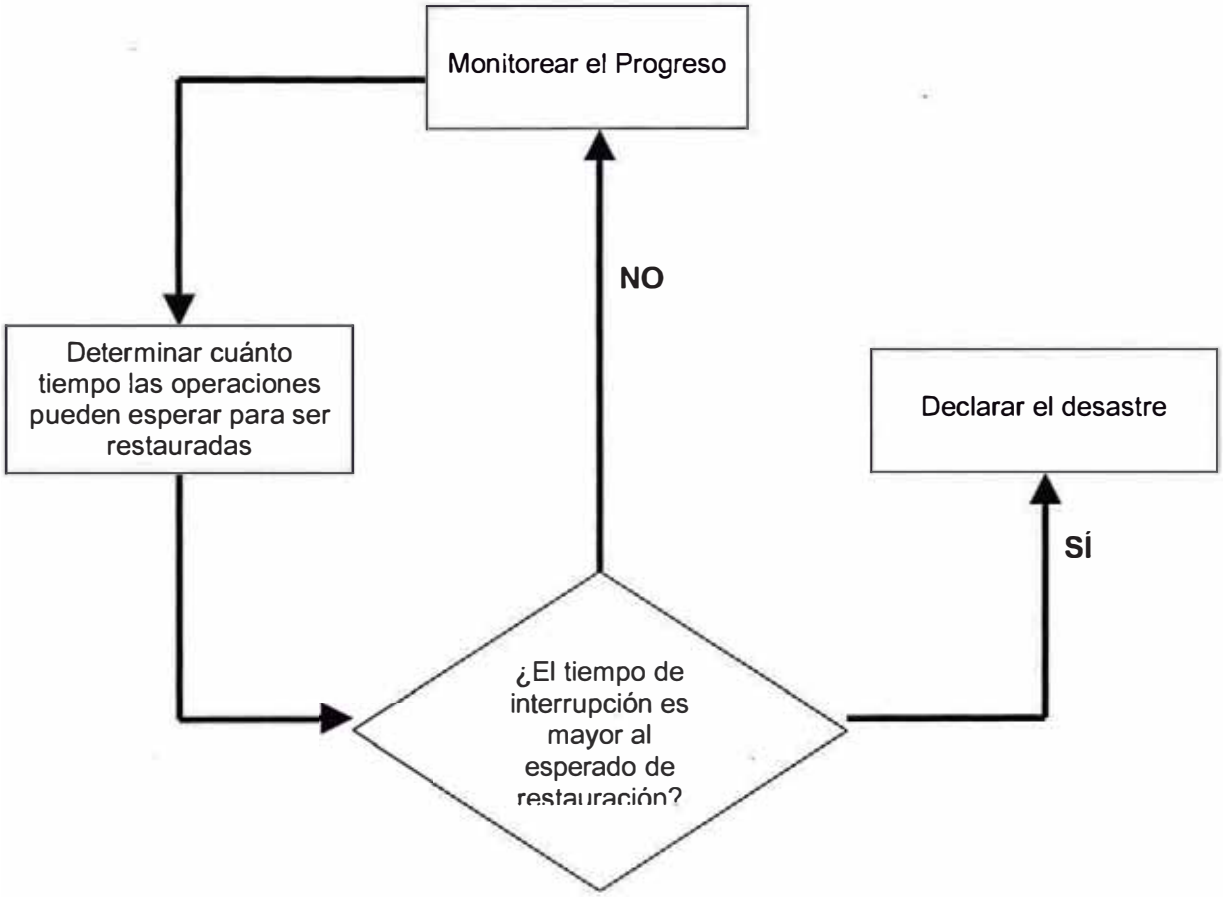
Prioridad de Recuperación

La prioridad de recuperación de los sistemas se define de acuerdo a los resultados del Análisis del Impacto en el Negocio (BIA), que se ha desarrollado en el Banco. Al identificar los procesos críticos y los sistemas que lo apoyan se ha llegado a la siguiente lista de aplicaciones críticas y cuya recuperación tiene que tomar la prioridad indicada:

Prioridad	Sistema	MAO
1	Bandinero (AS/400)	0.5
2	Mesa de Dinero	0.5
3	Sistema de Ventanillas	1
4	Agente de Bolsa	1

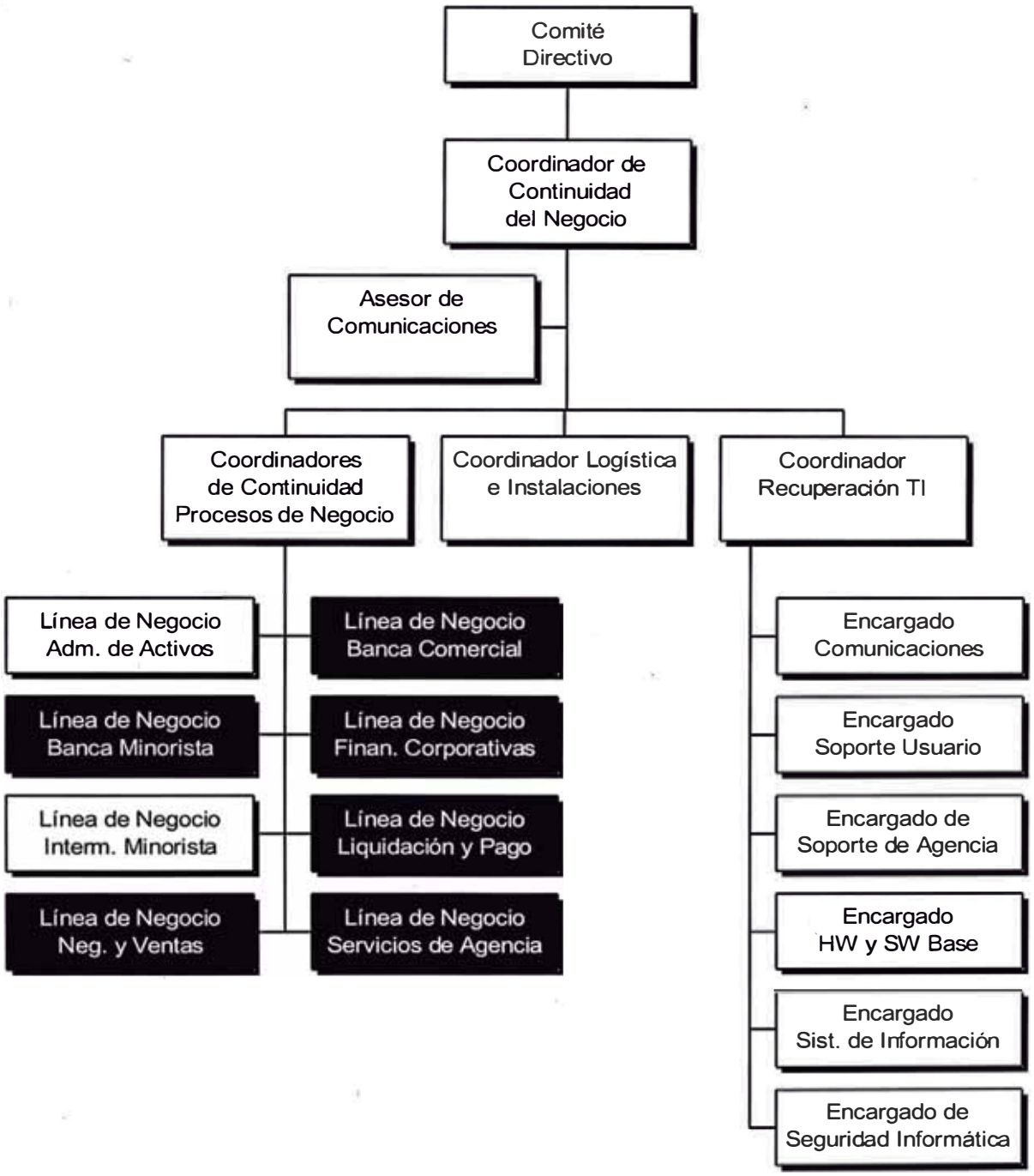
Criterio de Activación del Plan

El siguiente diagrama muestra los criterios que deberán ser usados para activar el Plan de Recuperación de TI:



Debe notarse que una interrupción no es solamente un evento que reduce la efectividad de los sistemas, un evento que es extraordinario, causa una pérdida de procesos de negocio claves y tiene un impacto alto en la organización. 'Un desastre' es una interrupción que excede el MAO.

El siguiente diagrama muestra la relación existente entre los variados equipos que participan en un proceso de Continuidad del Negocio ante una contingencia y el equipo de Recuperación de TI. Este equipo de recuperación se forma cuando se declara el desastre.



Anexo 12

INFRAESTRUCTURA DEL CENTRO DEL CENTRO DE COMPUTO ALTERNO

Infraestructura del Centro de Cómputo Alterno

Ubicación	La Molina
Ventas y Paredes	El Centro de Cómputo del Proveedor cuenta con paredes y vidrios externos blindados y reforzados.
Puertas de Seguridad	El Centro de Cómputo del Proveedor cuenta con puertas de acceso blindadas.
Servicio de Vigilancia	Se dispone de vigilancia las 24 horas.
Circuito Cerrado de Televisión	Se cuenta con cámaras de circuito cerrada de Televisión monitoreada las 24 horas por personal del departamento de Seguridad del Proveedor.
Control de Acceso	El Centro de Cómputo es un área restringida dentro del Proveedor y sólo permite acceso a personal autorizado. El sistema de control de acceso incluye lectoras de badge, lectoras biométricas y clave de acceso.
Personal Administrativo	El servicio incluye personal administrativo 24 horas al día.
Falso Piso y Techo	El Centro de Cómputo cuenta con falso piso y techo
Área	Se dispone de 150 m2 Centro de Cómputo, con capacidad de crecimiento de 90 m2. Adicionalmente se dispone de un área de 80 m2 para usuarios del servicio
Temperatura	Se dispone de equipos de aire acondicionado que mantienen el Centro de Cómputo a 18°C , con una humedad relativa de 40%.
Luminosidad	La iluminación del Centro de Cómputo es a través de fluorescentes, que proporcionan una luminosidad de 500 LUX.
Supresión de Fuego	Se dispone del sistema FM200 y de extintores manuales.
Luces de Emergencia	Se dispone de luces de emergencia fluorescentes conectadas al UPS del centro de cómputo.
Alarmas	El Centro de Cómputo cuenta con alarmas con detectores de humo, así como con alarmas contra intrusión.

UPS	El Centro de Cómputo cuenta con equipos redundantes con una capacidad instalada de 270 KW. El uso actual es de 60 KW. Este equipo permite una autonomía de 20 minutos.
Grupo Electrógeno	Se cuenta con un equipo de marca Caterpillar de 1350 KW el cual permite switchear en menos de un minuto.
Registros Vitales	Se dispone de un área para almacenar los cartuchos correspondientes a respaldos de registros vitales operativos y respaldos de información requeridos por y para las actividades del Centro de Cómputo.
Pozo a Tierra	Existe un pozo de tierra para los equipos de Centro de Cómputo.

Anexo 13

FIREWALL DEL CENTRO COMPUTO ALTERNO

Cisco IOS Firewall

Mientras que la seguridad de la red viene siendo cada vez mas crítica para asegurar las transacciones de negocios, los negocios deben integrar la seguridad en el diseño e infraestructura de su red.

Es más efectivo aplicar las políticas de seguridad cuando son un componente inherente de la red.

El Cisco IOS ® Firewall es una opción específica de seguridad para el Software Cisco IOS. Este integra funcionalidad de un firewall robusto y la detección de intrusos para cada perímetro de la red. Agrega mayor profundidad y la flexibilidad a las soluciones existentes de seguridad del Cisco IOS (es decir, autentificación, cifrado y redundancia), entregando características de seguridad avanzada: estado de las sesiones, filtrado basado en aplicaciones; autenticación y autorización dinámica por usuario; filtrado de URLs, entre otros.

Cuando está combinado con el Cisco IOS IPSec y Tecnologías del Cisco IOS como L2TP tunneling y Calidad del Servicio (QoS), el Firewall del Cisco IOS proporciona una solución Red Privada Virtual (VPN) completa e integrada.

Funcionalidad de Firewall basada en router

El Firewall del Cisco IOS está disponible en una amplia gama de releases del Software Cisco IOS. Ofrece aplicación sofisticada de la seguridad y politicas para las conexiones dentro de una organización (Intranet) y entre las redes de socios (Extranets) , así como para la conectividad de Internet para las oficinas remotas y sucursales. El Firewall del

Cisco IOS integra el ruteo multiprotocolo con la aplicación de las políticas de seguridad y permite a los administradores configurar un router Cisco como un firewall. Es escalable permitiendo a los clientes elegir la plataforma del router basándose en el ancho de banda, densidad de la LAN/WAN y requerimientos de multiservicio; simultáneamente, se beneficia de la seguridad avanzada.

Beneficios Claves

El Firewall del Cisco IOS interopera con el Software Cisco IOS, proporcionando los siguientes beneficios:

• Flexibilidad: Instalado en un router Cisco, el Firewall del Cisco IOS es una solución "todo en uno", solución escalable que realiza el enrutamiento multiprotocolo, seguridad del perímetro, detección de intrusos, funcionalidad VPN y autenticación y autorización por usuario.

• Protección de la inversión - Integrando la funcionalidad del firewall en un router multiprotocolo mejora la inversión de un router existente, sin el costo y la curva de aprendizaje asociada a la nueva plataforma.

• Soporte VPN - Implementando el Firewall del Cisco IOS con el cifrado del Cisco IOS y características del QoS VPN permite asegurar, transmisión de bajo costo a través de redes públicas. Se asegura de que el tráfico de la aplicación crítica reciba entrega de prioridad alta.

• Implementación Escalable - El Firewall del Cisco IOS está disponible para una amplia gama de plataformas de routers. Es escalable para satisfacer los requisitos del ancho de banda y rendimiento de las redes.

• Provisionamiento más fácil - Combinando el Cisco IE2100 y aplicación del Cisco IOS XML, permite a un administrador de red poder usar cualquier router Cisco con poca o no pre-configuración para un destino dado. El router extrae el release más reciente del Software Cisco IOS de la configuración del router y su configuración de políticas de seguridad para el firewall cuando está conectado a Internet.

• El Cisco IOS Firewall se apoya en la mayoría de plataformas de los routers Cisco, entregando así, importantes beneficios que incluyen la integración del mutiservicio (data/voz/video/marcado), seguridad avanzada para conexiones dialup. En los routers Cisco 7100, 7200 y 7400 Series, las ventajas adicionales incluyen el enrutamiento y seguridad integrados en el Gateway de Internet para la premisa de equipamiento de clientes de las grandes empresas y de los proveedores de servicios.

Cisco IOS Firewall Highlights

• Stateful IOS Firewall inspection engine - Provee un control de acceso seguro de usuarios internos basado por aplicación para todo el tráfico a través de perímetros, tales como perímetros entre las redes de la empresa privada e Internet. También conocido como Control de Acceso Basado en Contexto (CBAC).

• Detección de Intrusos - El servicio de inspección profunda de paquetes en línea que provee monitoreo en tiempo real, intercepción y respuesta al mal uso de la red, con un amplio conjunto de los ataques más comunes y recolección de información de la detección de firmas de intrusos.

• Firewall Voice Traversal - Proporcionado por la inteligencia del nivel de aplicación del protocolo en cuanto al flujo de llamadas y los canales asociados que están abiertos. Los protocolos de voz actualmente soportados son H.323v2 y SIP.

• Inspección ICMP - Permite respuestas a paquetes ICMP (es decir, ping y traceroute) originado desde dentro del Firewall, mientras sigue denegando otro tráfico ICMP.

• Proxy de Autenticación - Permite la autentificación y autorización dinámica por usuario para comunicaciones basadas en LAN, http y dial-in; auntentica usuarios contra los estándares de la industria. Soporte seguro del SSL id de usuario y contraseñas para http (HTTPS) proporciona mayor confidencialidad. Los protocolos de autenticación TACAS+ y RADIUS permiten a los administradores de red definir políticas de seguridad individuales por usuario.

• Administración de la política del URL de destino - Diversos mecanismos que soportan el almacenamiento local de las peticiones previas, tablas estáticas predeterminadas de permiso y negación de URLs, tan bien como el uso de bases de datos externas, proporcionadas por Websense Inc. Y N2H2 Inc. Esto es más conocido como filtrado URL.

• Firewalls por usuario - Permite a los proveedores de servicios proporcionar una solución de Firewall de banda ancha administrable en el mercado, descargando el único Firewall, ACLs, y otros ajustes base por usuario, usando el perfil de almacenamiento después de auntenticación servidor AAA.

• Aprovisionamiento del Router y Firewall del Cisco IOS - Cero (0) toques provistos por el versionamiento y seguridad de las políticas del router, tales como las reglas del Firewall.

• Detección y Prevención de "Denial of Service" - Defiende y protege los recursos del router contra los ataques comunes, revisa las cabeceras de paquetes y descarta los paquetes sospechosos.

• Mapeo Dinámico de Puertos - Permite aplicaciones soportadas por el Firewall en puertos no estándar.

• Bloqueo de Applets de Java - Se defiende contra applets de Java no identificados o maliciosos.

• VPNs, Cifrado IPSec y Soporte de QoS -

– Opera con el cifrado, tunneling y características de QoS del Software Cisco IOS para asegurar VPNs.

– Provee cifrado de túneles escalable en el router mientras integra fuerte seguridad en el perímetro, manejo de ancho de banda avanzado, detección de intrusos y validación de niveles de servicio.

– Basado en estándares para interoperatividad.

• Alertas en Tiempo Real - Alertas Log para los ataques de negación de servicio u otras condiciones pre configuradas. Esto es configurable por aplicación y por características.

• Registros auditables - Detalla transacciones y registra el tiempo, host fuente, host destino, puertos, duración y el total de los bytes transmitidos para reportes detallados. Esto es configurable ahora por aplicación, basado por características.

• Integración con el Software Cisco IOS - Interopera con las características del software Cisco IOS, integrando la aplicación de las políticas de seguridad en la red.

• Filtrado de tráfico Básico y Avanzado -

– Listas de Control de Acceso estándares y extendidas (ACLs) - Aplica controles

de acceso a segmentos específicos de la red y define que tráfico pasa a través de un segmento de red.

– Cerradura y Llave - ACLs dinámicos conceden acceso temporal a través de firewalls sobre la identificación de usuarios (nombre de usuario/Contraseña).

• Soporte de Políticas Basadas en Multi-Interfaz - Proporciona la capacidad de controlar el acceso de usuarios por dirección IP e interface, según lo determinado por las políticas de seguridad.

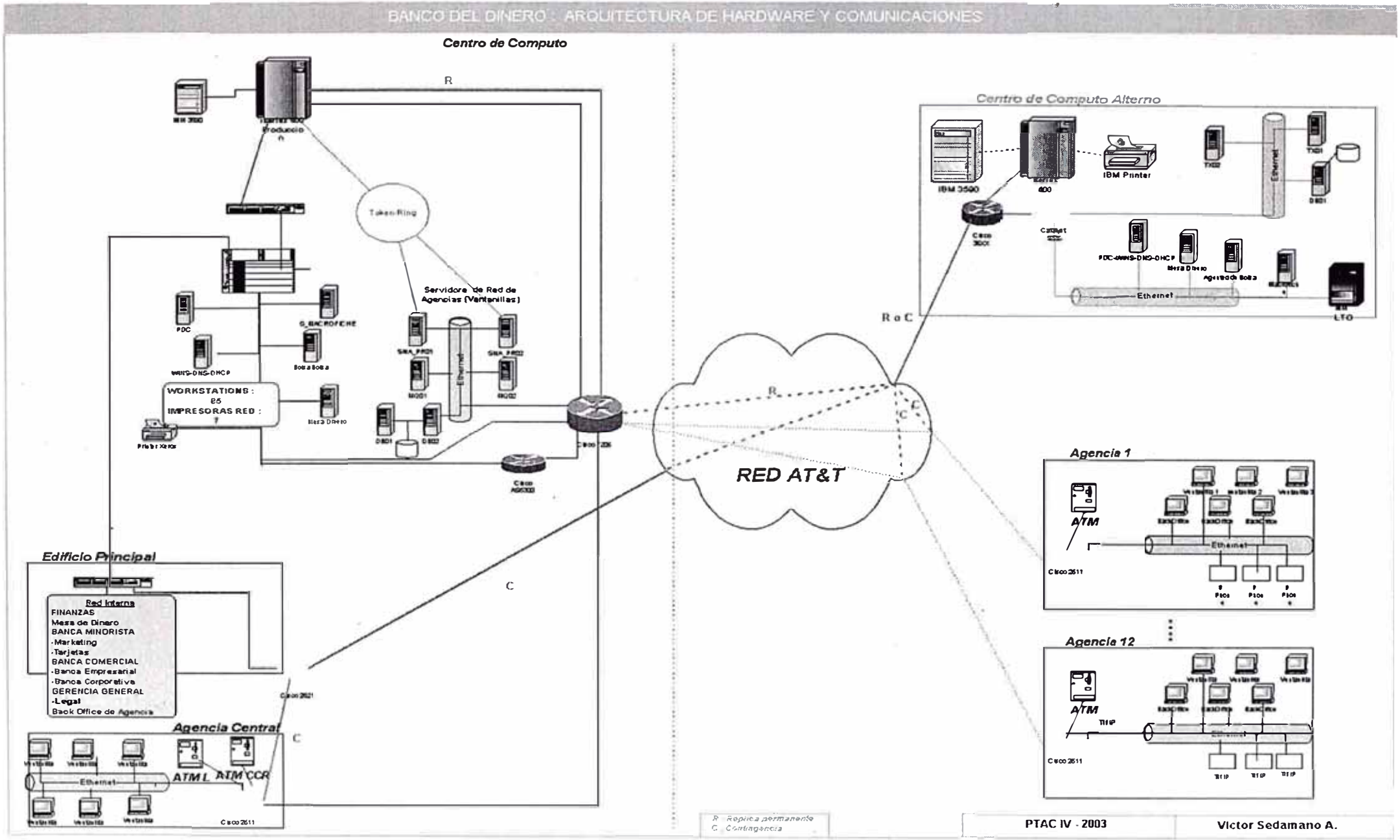
• Traducción de la Dirección de Red (NAT) - Oculta la red interna del exterior para una seguridad elevada.

• Listas de Acceso Basada en Tiempo - Define la política de seguridad basada en la hora y el día de la semana.

• Autenticación del Router Vecino - Se asegura que los routers reciban información de enrutamiento confiable de fuentes confiables.

Anexo 14

DIAGRAMA DE RED DEL PROYECTO


BANCO DEL DINERO : ARQUITECTURA DE HARDWARE Y COMUNICACIONES
Centro de Computo
R
Token Ring
Servidores de Red de Agencias (Ventanillas)
PDC
WINS-DNS-DHCP
Bolsa Bolsa
Mesa Dinero
WORKSTATIONS : 65
IMPRESORAS RED : 7
Ethernet
Cisco 7206
Cisco AGS30
RED AT&T
R o C
Centro de Computo Alterno
IBM 3590
IBM Printer
Cisco 3600
Ethernet
LTO
Edificio Principal
Red Interna
FINANZAS
Mesa de Dinero
BANCA MINORISTA
·Marketing
·Tarjetas
BANCA COMERCIAL
·Banca Empresarial
·Banca Corporativa
GERENCIA GENERAL
·Legal
Back Office de Agencia
Cisco 2621
Agencia Central
C
ATM LE
ATM CCR
Ethernet
Cisco 2611
Agencia 1
ATM
Cisco 2611
Agencia 12
ATM
TRIP
Cisco 2611
R : Replica permanente
C : Contingencia
PTAC IV - 2003
Victor Sedamano A.

Anexo 15

ENCUESTA DE LAS PRUEBAS DE CONTINGENCIA

Propósito

El propósito de este documento es identificar en qué medida se está logrando los objetivos planteados, evaluando el nivel de satisfacción con los productos, servicios y el soporte que el área del Centro de Cómputo de Alterno contratado.

En las próximas páginas se incluyen preguntas con dos (2) columnas de respuestas. La primera columna indica su nivel de satisfacción con el ítem a evaluar. La segunda columna indica la importancia del ítem en sus operaciones.

Adicionalmente, se provee espacios para comentarios relativos a algún aspecto específico, ya sea positivo y/o negativo.

Los resultados de estas evaluaciones son continuamente revisados por los Gerentes del CCA y el personal del área, para determinar requerimientos de cambio, puntualizar tendencias e identificar oportunidades que mejoras en los servicios.

EVALUACIÓN DE LA PRUEBA

Para cada una de las siguientes preguntas, indique por favor, que tan importante es el ítem para Ud., y que tan satisfecho está Ud. con el desempeño del personal del Centro de Cómputo Alterno, marcando UNO SOLO de los recuadros apropiados. Sus comentarios serán altamente apreciados.

	Satisfacción	PREPARACIÓN Importancia
Programación de su prueba de recuperación, incluyendo la disponibilidad de las fechas y horas solicitadas	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
Preparaciones previas a la prueba; intercambio de información técnica, documentación y revisión preliminar.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
Documentación del área de CCA incluyendo mapas, guía de orientación, direcciones y diagrama del sitio.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
Configuración y habilitación del Hardware / Software del sistema.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
Configuración y habilitación del Hardware / Software de la Red	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia

Por favor use el espacio de abajo para escribir comentarios relativos a la fase de PREPARACIÓN

AMBIENTE

	Satisfacción	Importancia
La seguridad y protección del personal durante su estadía en el De Cómputo Alterno.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
La utilidad y funcionalidad del Centro de Cómputo Alterno, sala de operación y oficinas.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
La comodidad, orden y limpieza del Centro de Cómputo Alterno.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
Disponibilidad de útiles de escritorio en la oficina del Centro de Cómputo Alterno.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia

Por favor use el espacio de abajo para escribir comentarios relativos al AMBIENTE durante su estadía:

EQUIPOS

	Satisfacción	Importancia
El desempeño y confiabilidad de los equipos en el Centro de Cómputo Alterno.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
El desempeño y confiabilidad de los servicios del proveedor de telecomunicaciones.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
El servicio de transporte de los equipos, al Centro de Cómputo del Banco.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
La instalación y conexión de los equipos, en el Centro de Computo Alterno.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia

Por favor use el espacio de abajo para escribir comentarios de los EQUIPOS durante el proceso de prueba.

GRUPO DE SOPORTE DEL CCA

	Satisfacción	Importancia
Soporte recibido por el Coordinador del CCA	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
Atención recibida por el Coordinador del CCA	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
Soporte recibido por el (los) especialista(s) de soporte técnico.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
Soporte recibido por el (los) especialista(s) de Telecomunicaciones	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia
Disponibilidad del personal de soporte del CCA, cuando fue necesario.	☐ Muy Satisfecho ☐ Satisfecho ☐ Algo Satisfecho ☐ Insatisfecho ☐ Muy Insatisfecho ☐ No Aplica	☐ Extremadamente Importante ☐ Importante ☐ Algo Importante ☐ Muy poco Importante ☐ Sin importancia

Por favor use el espacio de abajo para escribir comentarios del apoyo recibido del GRUPO DE SOPORTE DEL CENTRO DE CÓMPUTO DE SERVICIOS durante el proceso de prueba.

_____

_____

_____

_____

_____

Como un todo, ¿Cuan satisfecho está usted con CCA
I

☐ Muy Satisfecho
☐ Satisfecho
☐ Algo Satisfecho
☐ Insatisfecho
☐ Muy Insatisfecho

Por favor use el espacio de abajo para escribir comentarios relativos a su SATISFACCIÓN. Por favor siéntase libre en incluir tanto experiencias positivas como aspectos en los cuales Ud. ha quedado insatisfecho. También, use este espacio para comunicar cualquier comentario adicional o sugerencia que tenga, para ayudarnos a mejorar la CALIDAD de este servicio de Centro de Computo Alterno. Agregue páginas adicionales de ser necesario.

GRACIAS POR SU TIEMPO Y DEDICACIÓN

Anexo 16

PROCEDIMIENTO PARA EL USO DEL CENTRO DE COMPUTO ALTERNO EN CASO DE CONTINGENCIA

PROCEDIMIENTOS PARA EL USO DEL CCA EN CASO DE CONTINGENCIA

1.- PROCEDIMIENTO PARA LA REALIZACIÓN DE PRUEBAS DEL PLAN DE CONTINGENCIA

El Banco deberá contar con su Plan de Contingencia debidamente documentado, donde se definen los pasos a seguir para la Declaración de una Contingencia, la realización de las pruebas, la restauración de los diferentes aplicativos críticos, la solución de las comunicaciones y el mantenimiento del plan entre otros.

El proveedor facilitará los diferentes recursos técnicos, físicos y humanos para permitir las pruebas del Plan de Contingencia en forma exitosa.

Modelo de solicitud para la realización de la prueba

Propósito

El propósito de este documento es identificar todos los elementos necesarios que involucran una prueba con la finalidad de alcanzar los objetivos deseados, los puntos que el Banco deberá completar son:

- Tipo de Prueba
- Fecha tentativa de la prueba.
- Personal del Banco a participar
- Sistema Operativo y Programas productos (Nivel y Versión)
- Aplicaciones
- Configuración de Hardware y Telecomunicaciones

- ¿Requiere Ud. de algún servicio adicional?
- Soporte de Asesoría
- Objetivos y tareas de la prueba

En las próximas páginas se incluyen las preguntas que el Banco deberá llenar y una vez completada se enviará al Coordinador de Planeamiento, quien confirmará la fecha de realización de la prueba.

Instrucciones para la realización de las pruebas

- Contactar al Coordinador de Planeamiento del proveedor para coordinar las pruebas del Plan de Contingencia y acordar la fecha conveniente para realizar una reunión previa antes de la prueba. En esta reunión se revisarán los objetivos de la prueba y el equipo requerido.
- El Coordinador de Planeamiento le enviará una Solicitud para la Realización de Pruebas en la cual el Banco identificará tipo de prueba, personal a participar, aplicaciones críticas a probar, software a utilizar, etc.
- El día definido para las pruebas, el Banco se presentará en la garita principal de las oficinas del Proveedor indicando que se desplazarán al Centro de Cómputo de Respaldo del Proveedor.
- El Vigilante les entregará un badge de visitante con el que ingresarán hasta recepción, aquí notificará su presencia con la recepcionista la que lo contactará con el Coordinador de Soporte Técnico asignado, el cual lo guiará hasta el Centro de Cómputo de Respaldo del Proveedor.

- El Banco debe registrar los medios magnéticos, módems, interfaces y cualquier otro artículo eléctrico o electrónico en la garita principal del Proveedor , para evitar inconvenientes en el momento de retirarlos.
- El Coordinador de Soporte Técnico dará el apoyo necesario al Banco para el éxito de su prueba.
- El Banco inicia la restauración de sus procesos en el equipo de respaldo, realiza la prueba de comunicaciones y la prueba con los usuarios, de acuerdo con su Plan de Contingencia.

Instrucciones una vez terminada la prueba

Una vez que las pruebas terminen es responsabilidad del Banco realizar las siguientes funciones para permitir la continuidad del servicio ofrecido por el Proveedor.

- Revisar las configuraciones de comunicaciones que permitieron la prueba en forma exitosa, para su documentación y/o actualización en el Plan de Contingencia.
- Tomar nota de los tiempos de recuperación y las desviaciones encontradas en las pruebas, para documentar y/o actualizar el Plan de Contingencia.
- Realizar el proceso de borrado de la información almacenada en los equipos de uso compartido.
- Firmar en señal de aceptación el registro de uso del Centro de Cómputo Alterno por la prueba realizada.
- Llenar la Encuesta de Satisfacción sobre el resultado de la Prueba.

- Informar en la garita principal el retiro de los medios magnéticos, módems, interfaces y cualquier otro artículo eléctrico o electrónico de propiedad de Cliente y que hayan sido registrados en la garita principal del proveedor.
- Devolver el badge que es facilitado en forma diaria, en la garita principal del Proveedor.
- El Coordinador de Planeamiento remitirá una comunicación al Banco indicando el resultado de la prueba y los compromisos adquiridos por ambas partes, en caso de que existan. Esto para que el uso del Centro de Cómputo Alterno sea exitoso.

FORMATO SOLICITUD PARA LA REALIZACIÓN DE PRUEBAS

Centro de Cómputo Alterno

CLIENTE: _____ Fecha: _____

Fecha tentativa de la prueba: _____

1) Tipo de prueba: ----- Batch ----- Online ------ Completa

2) Personal del Banco a participar:

Nombre Cargo

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

3) Sistema Operativo y Programas productos (Nivel y Versión)

_____ _____
_____ _____
_____ _____
_____ _____

4) Aplicaciones

_____ _____
_____ _____
_____ _____

5) Configuración de Hardware y Telecomunicaciones:
La configuración que Ud. tendrá disponible es aquella que figura en su contrato. Para el caso de pruebas con comunicación, especifique cuales serán las agencias y/o locales que se conectarán con el Proveedor.

_____ _____
_____ _____
_____ _____

6) ¿Requiere Ud. de algún servicio adicional?:
Si tiene algún costo adicional, se informará oportunamente.

_____
_____
_____

7) El Banco deberá traer los insumos necesarios para la prueba. El proveedor le puede proporcionar los insumos, si este es el caso se procederá a facturar posteriormente.
Solicito al Proveedor que me proporcione los siguientes insumos para la prueba:

_____
_____
_____

8) Soporte de Asesoría:

Ud. cuenta con nuestro soporte para la revisión de su Plan y/o procedimientos de contingencia, así como la revisión de los pasos a seguir para la realización de la prueba.

El personal del Prvoveedor del Servicio de Continuidad Operacional tiene la experiencia y conocimiento en todos los temas relacionados a la Contingencia.

Si Ud. requiere una reunión antes de la prueba señale una fecha tentativa para la reunión.

9) Objetivos y tareas de la prueba:

Por ejemplo, restaurar su sistema operativo, sus aplicaciones (nombrando cada una de ellas, etc.). Considere incluir los elementos y pautas que se utilizarán para medir el éxito de la prueba.

Cliente Servicio de Continuidad Operacional

2. PROCEDIMIENTO PARA LA DECLARACION DE UNA CONTINGENCIA

Distribución

Es importante que la siguiente información sea distribuida y suministrada a la(s) persona(s) que ustedes han designado como autorizadas para establecer el contacto con el proveedor, para permitirnos iniciar nuestros procedimientos de preparación de las instalaciones y recursos en forma real. Esto nos ayudará a suministrarles el soporte adecuado que ustedes requieren en cualquier Contingencia.

Teléfonos para contacto

Una vez que haya sido Declarada la Contingencia en las instalaciones del Banco, el funcionario autorizado notificará la **Declaración de Contingencia** de su compañía, para lo cual deberá notificar al AREA de SEGURIDAD del Proveedor.

Solicite que el Coordinador de turno del Centro de Cómputo Alterno, sea informado inmediatamente, para que la llamada le sea devuelta y se activen los procedimientos para la utilización de los recursos que el proveedor tiene destinados para tal fin.

3.- PROCEDIMIENTO PARA USO DEL CENTRO DE COMPUTO DE RESPALDO

Plan de Contingencia

El Banco deberá contar con su Plan de Contingencia debidamente documentado y actualizado de acuerdo con el resultado de las pruebas realizadas anteriormente, donde se definen los pasos a seguir para la declaración de una contingencia, la realización de las pruebas, la restauración de los diferentes aplicativos críticos, la solución de las comunicaciones y el mantenimiento del Plan, entre otros. El proveedor facilita los diferentes recursos técnicos, físicos y humanos para permitir la recuperación en caso de contingencia, en forma exitosa.

Instrucciones para la utilización del Centro de Cómputo Alterno en caso de alguna contingencia

Una vez Declarada la Contingencia y contactado al proveedor, se realizarán los siguientes pasos:

- El Banco enviará por escrito la relación de personas adicionales que ingresarán a las instalaciones del Proveedor , indicando su nombre y documento de identificación.
- El Banco dentro de las 48 horas deberá formalizar por escrito la Declaración de Contingencia.
- El personal del Banco se presentará en la garita principal del Proveedor indicando que se desplazarán al Centro de Cómputo de Respaldo (BCRS).
- El Vigilante les entregará un badge de visitante con el que ingresarán hasta recepción, aquí notificará su presencia con la recepcionista la que lo contactará

con el coordinador de Soporte Técnico, el cual lo guiará hasta el Centro de Cómputo de Respaldo (BCRS).

- El Banco debe registrar los medios magnéticos, módems, interfaces y cualquier otro artículo eléctrico o electrónico en la garita principal del Proveedor , para evitar inconvenientes en el momento de retirarlos.
- El Coordinador de Turno del Centro de Cómputo de Respaldo dará el apoyo necesario al personal del Banco para el éxito de su recuperación.
- El Banco inicia la restauración de sus procesos en el equipo de respaldo, realiza la configuración de sus comunicaciones y opera el Centro de Cómputo de Respaldo para superar la contingencia.
- El Banco está en pleno contacto con Coordinador de Turno del Centro de Cómputo de Respaldo, quien los orientará en la prestación del servicio.

Instrucciones una vez superada la contingencia

Una vez que la contingencia es superada es responsabilidad del Banco realizar las siguientes funciones para permitir la continuidad del servicio ofrecido por el Proveedor .

- Realizar los diferentes respaldos de seguridad de finalización de la contingencia.
- Realizar el proceso de borrado de la información almacenada en los equipos de respaldo de uso compartido.
- Firmar en señal de aceptación el registro de uso del Centro de Cómputo de Respaldo, por Contingencia.
- Llenar la Encuesta de Satisfacción sobre el resultado del servicio de uso del Centro de Cómputo de Respaldo.

- Informar en la garita principal el retiro de los medios magnéticos, módems, interfaces y cualquier otro artículo eléctrico o electrónico de propiedad de Cliente y que hayan sido registrados en la garita principal de las oficinas del proveedor.
- Devolver el carnet que es facilitado en forma diaria, en la garita principal de las oficinas del Proveedor.
- El Coordinador de Planeamiento, remitirá una comunicación al Banco indicando el uso del Centro de Cómputo de Respaldo y los tiempos consumidos.

4.- PROCEDIMIENTO PARA ALMACENAMIENTO DE REGISTROS VITALES

Con el fin de facilitar la operación diaria del Banco en el evento de una contingencia, el proveedor ha asignado un espacio, ubicado en Centro de Cómputo Alterno del proveedor, donde serán almacenados los diferentes backups de la información generada para la operación del Centro de Cómputo Alterno en caso de Contingencia.

Características de los lockers para almacenamiento de los registros vitales

Lugar: Centro de Cómputo Alterno del Proveedor.

Ubicación: La Molina

Área del espacio: 0.30 X 0.40 X 0.35 mts.

Horario de atención: 24 horas al día

En el caso de requerirse un backup fuera del horario establecido, deberá coordinarse con el operador de turno del área del Servicio de Continuidad Operacional.

Instrucciones para la utilización de los lockers de almacenamiento de registros vitales

El Banco de acuerdo con sus procedimientos de backup, se desplazará al Centro de Cómputo de Respaldo del Proveedor, en los horarios indicados anteriormente y entregará al Operador de Turno los medios magnéticos para su custodia.

El Banco llenará los diferentes formatos entregados por el Operador del Centro de Cómputo de Respaldo del Proveedor.

Anexo 17

REPORTE MENSUAL DE GESTION DEL CCA

INFORME MENSUAL

Proyecto : Centro de Cómputo Alterno– Banco del Dinero

Período: : 1 Septiembre 2003 - 30 Septiembre 2003

Fecha de entrega : 07 de Octubre de 2003

INDICE

Introducción

El presente documento detalla los hechos relativos al servicio de Centro de Cómputo Alterno del Banco del Dinero así como la disponibilidad del servicio correspondiente al mes de septiembre.

Hechos Relevantes

1. 04 Septiembre 18:16 – 21:19

   Por solicitud del Banco según el formato TE-001 se ejecutó la restauración del proceso de la fecha 03 de Septiembre (cinta BD-002-005).

2. 15 Septiembre 01:00 – 01:45

   Instalación de últimos PTFs de sistema operativo por sugerencia de especialista iSeries

3. 17 Septiembre 10:00 – 12:50

   Se registró una degradación en la comunicación del enlace de la línea dedicada. El proveedor del servicio reportó la existencia de una falla técnica en el nodo de San Isidro del Circuito Digital. Este incidente se encuentra detallado en el documento CO-001 entregado en la reunión de Comité Operativo del día 18 de Septiembre.

4. 20 Septiembre 10:20 – 10:35

   Se realizó cambio preventivo de fuente poder reduntante del servidor que había presentado reportes de falla en la bitácora (log) del sistema operativo.

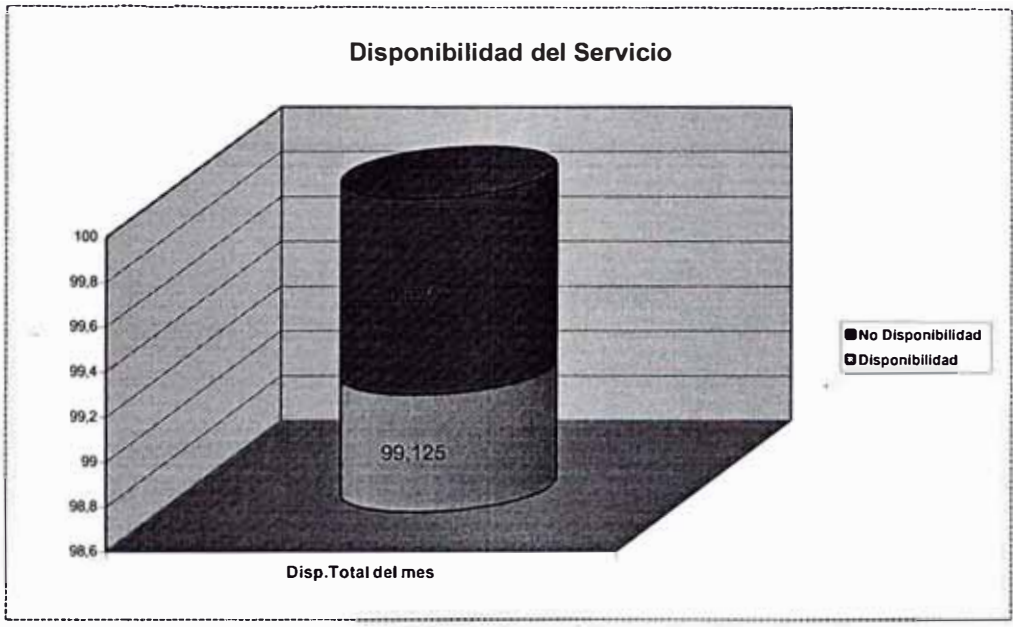
Reportes Estadísticos

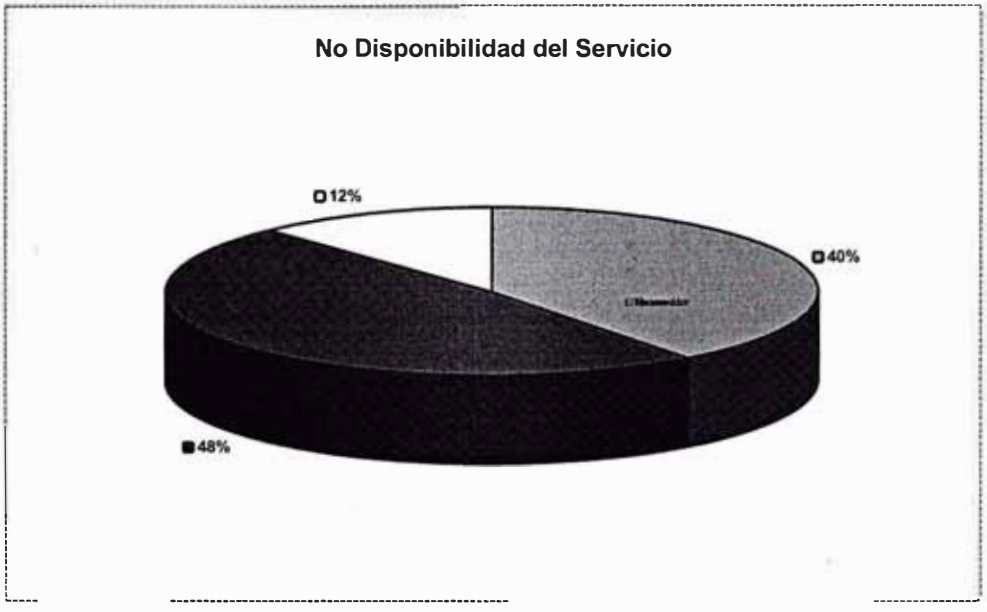
Resumen de incidentes

Fecha	Período		Descripción
04/09/2002	Inicio:	18:16	Por solicitud del Banco según el formato TE-001 se ejecutó la restauración del proceso de la fecha 03 de Septiembre (cinta BD-002-005).
	Fin:	21:19	
15/09/2002	Inicio:	01:00	Instalación de PTFs en los servidores.
	Fin:	01:45	
17/04/2002	Inicio:	10:20	Degradación del enlace de la línea dedicada debido a una falla en el nodo de San Isidro del Circuito Digital.
	Fin:	12:50	
20/04/2002	Inicio:	10:20	Cambio de fuente poder reduntante en el servidor Generales Desarrollo
	Fin:	10:35	

Disponibilidad del servicio

Fecha	Periodo		Tiempo			Descripción
			Proveedor	Terceros	Mant.	
04/04/2002	Inicio:	18:16		3:03		Por solicitud del Banco según el formato TE-001 se ejecutó la restauración del proceso de la fecha 03 de Septiembre (cinta BD-002-005).
	Fin:	21:19				
15/04/2002	Inicio:	01:00			0:45	Instalación de PTFs en los servidores.
	Fin:	01:45				
17/04/2002	Inicio:	10:20	2:30			Degradación del enlace de la línea dedicada debido a una falla en el nodo de San Isidro del Circuito Digital.
	Fin:	12:50				
Tiempo de No Disponibilidad			2:30	3:03	0:45	
No Disponibilidad total del mes (hh:mm)			**6:18**			
Porcentaje de disponibilidad del mes			**0,99125**			


Disponibilidad del Servicio
100
99,8
99,6
99,4
99,2
99
98,8
98,6
99,125
Disp.Total del mes
No Disponibilidad
Disponibilidad


No Disponibilidad del Servicio
12%
40%
48%

Anexos

Actas de Reunión del día 18 de septiembre

CCA Banco del Dinero

Comité Operativo

Fecha: 25/09/2002

Asistentes:

AAA	Gerente de Proyecto Banco del Dinero
BBB	Gerente de Proyecto del Proveedor

Agenda:

No	Descripción
A01	Revisión del avance del proyecto

Compromisos / Acuerdos:

No	Descripción	Responsable	Fecha
A01-01	Instalación de PTFs en el servidor	El Proveedor	19/09/02
A01-02	Entrega de procedimientos modificados según observaciones del Banco del Dinero.	El Proveedor	23/09/02
A01-03	Entrega del los datos actualizados del personal de contacto del Banco del Dinero.	Banco del Dinero	15/09/02
A01-04	Entrega del informe sobre la degradación de la línea del circuito digital CO-001	El Proveedor	----

Anexo 18

ROLES DE LA BRIGADA DE CONTINGENCIA

Roles del Equipo de Recuperación

Función	Roles y Responsabilidades
Comité Directivo	Equipo de Gerentes del Banco, que serán responsables de tomar las decisiones estratégicas en escenarios de contingencia. Ver composición del Comité Directivo en Anexo 1: "Lista de Contactos".
Coordinador de Continuidad del Negocio	La misión de este Coordinador será dirigir y coordinar las decisiones y acciones a seguir ante un escenario de contingencia, coordinando tanto la ejecución del Plan de recuperación de TI como el Plan de Continuidad del Negocio. Ver cargo y persona asignada a este rol en Anexo 1: "Lista de Contactos".
Asesor de Comunicaciones	Encargado de las relaciones públicas internas y externas del Banco ante una crisis de continuidad. . Ver cargo y persona asignada a este rol en Anexo 1: "Lista de Contactos".
Coordinadores de Continuidad Procesos de Negocio	Responsables de dar soporte a cada una de las funciones de negocio de las que son responsables, manteniendo la relación con las otras líneas de negocio y con el equipo de Recuperación de TI, en especial, con el Encargado de Sistemas de Información. Las personas que conformarán cada uno de estos equipos deberán pertenecer a las áreas que administran los procesos de negocio de la línea. En el organigrama se han marcado con azul aquellas Líneas de Negocio que han sido definidas como críticas en el Análisis de Impacto del Negocio (BIA) y cuyos procesos tienen prioridad de recuperación (ver sección 2.3 de este Plan). Ver cargo y persona asignada a este rol en Anexo 1: "Lista de Contactos".
Coordinador Logística e Instalaciones	El Coordinador de Logística e Instalaciones determinará y proveerá los suministros físicos necesarios para la continuidad del negocio en un escenario de contingencia. Además, decidirá en conjunto con los Coordinadores de Continuidad de Procesos de Negocio la reestructuración del personal y departamentos. También coordinará con el grupo de Tecnología de Información alternativas de comunicación y acceso a la red si es necesario. También se encargará de velar por la seguridad del Banco, resguardando los perímetros internos y externos a las instalaciones. Ver cargo y persona

Función	Roles y Responsabilidades
	asignada a este rol en Anexo 1: "Lista de Contactos".
Equipo de Recuperación	
Coordinador Recuperación TI	Encargado de coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado. • Decidir la activación del Plan de Recuperación de TI. • Identificar y determinar el daño a la infraestructura de la tecnología. • Activar al personal necesario y supervisar sus actividades. • Recuperar las cintas de respaldo del almacenaje externo y entregarlas en el sitio de recuperación. • Supervisar / vigilar la recuperación de infraestructura de tecnología en el sitio de recuperación alterno. • Contactar a los proveedores para el hardware de reemplazo para sistemas afectados. • Instalar y probar PC's en el sitio de recuperación. • Operar y apoyar la infraestructura de tecnología. • Asistir a las reuniones del estado de la recuperación y comunicar al personal las necesidades y prioridades. Ver cargo y persona asignada a este rol en Anexo 1: "Lista de Contactos".
Encargado Comunicaciones	Responsables por mantener, recuperar y/o restaurar las telecomunicaciones entre las dependencias del Banco y el Centro de Cómputo. Ver cargo y persona asignada a este rol en Anexo 1: "Lista de Contactos".
Encargado Soporte Usuario	Responsable de mantener estable los servicios del Área de Sistemas a los usuarios en un escenario de contingencia. Ver cargo y persona asignada a este rol en Anexo 1: "Lista de Contactos".
Encargado de Soporte de Agencia	Responsable de mantener estable la Infraestructura Tecnológica de las Agencias y sus servicios a los usuarios en un escenario de contingencia. Ver cargo y persona asignada a este rol en Anexo 1: "Lista de Contactos".
Encargado HW y SW Base	Responsable por evaluar el daño en la plataforma tecnológica básica del Banco y coordinar y dirigir las acciones necesarias para su recuperación en el Centro de Cómputo alternativo y su restauración a condiciones normales. Ver cargo y persona asignada a este rol en Anexo 1: "Lista de Contactos". El encargado de software deberá realizar la recuperación de la

Función	Roles y Responsabilidades
	plataforma base de los sistemas críticos para el banco de acuerdo al Anexo 7 : "Procedimientos de recuperación de plataforma y sistemas de aplicación"
Encargado Sist. de Información	Responsable por la recuperación priorizada de los sistemas de información de apoyo a los procesos de negocios críticos del Banco así como de su consistencia e integridad. Además mantendrá la coordinación estrecha con los coordinadores de la continuidad de los procesos de negocio de las líneas ante una contingencia. Ver cargo y persona asignada a este rol en Anexo 1: "Lista de Contactos". La recuperación priorizada de los sistemas de información deberá realizarse tomando como base el Anexo 7: "Procedimientos de Recuperación de plataforma y sistemas de aplicación"
Encargado de Seguridad Informática	Supervisor del cumplimiento de los controles que permitan asegurar la integridad, confidencialidad y disponibilidad de la información en una contingencia. Ver cargo y persona asignada a este rol en Anexo 1: "Lista de Contactos".