UNIVERSIDAD NACIONAL DE LA MATANZA
SECRETARIA DE POSGRADO

TESIS DE
MAESTRIA EN
INFORMATICA

"Modelo para la elaboración de las Especificaciones Técnicas de un Plan de Contingencia y Continuidad del Negocio"

Autor: Javier A. Cereghetti

Director de Tesis: Jorge Eterovic

Buenos Aires, marzo de 2006

INDICE

Agradecimientos

Agradezco a las muchas personas que me ayudaron a llegar a este momento de felicidad

En primer lugar, deseo agradecer al Ing. Jorge Eterovic quien ha sido el mentor fundamental de este proyecto desde el día en que se lo presenté. Me dedicó su tiempo, releyendo el material una y otra vez, corrigiéndolo y dándome una certera orientación en la manera de llevarlo adelante.

Agradezco también a mi familia por su apoyo incondicional durante este tiempo y a ellos también les he restado muchas horas. A pesar de ello sin embargo están convencidos, como lo estoy yo, de que el estudio y la capacitación son las mejores opciones para poder crecer y superarse.

Para finalizar, también deseo expresar mi sincero reconocimiento a la Licenciada Mercedes Mayol Lassalle. Ella me ha incentivado a llevar adelante esta maestría y ha allanado el camino en las instancias más complicadas.

"Modelo para la elaboración de las Especificaciones Técnicas de un Plan de Contingencia y Continuidad del Negocio"

1. Introducción

Definición del Problema

Todos los negocios están expuestos a imprevistos que pueden exponerlos a perder su información. Un desastre externo, una falla en los sistemas o una intrusión pueden ocurrir en cualquier momento y en esta era de comercio electrónico la información debe mantenerse segura pero accesible.

La continuidad del negocio es vital para el éxito de la empresa y esto ya no es solo una preocupación del Departamento de Tecnología Informática (TI), sino que involucra a toda la organización en sus diferentes áreas de negocio y para permitirla es necesario determinar cuales son las necesidades de recuperación de la empresa, identificar cuales son las prioridades críticas del negocio y establecer un programa completo de continuidad de las operaciones.

Sin embargo, son pocos los casos en que las empresas cuentan con una estrategia de seguridad informática, o con un plan que aporte una solución que permita darle continuidad al negocio si llegase a ocurrir alguna contingencia.

1.2 Tema sobre el cual se realizará el estudio

El presente estudio tendrá como objetivo desarrollar un Modelo de un plan de contingencia y establecer los requerimientos necesarios para la construcción de un Centro de Procesamiento Alternativo para una entidad financiera, que cuenta con una Casa Central, situada en la Ciudad Autónoma de Buenos Aires y 345 sucursales, distribuidas en el ámbito de la provincia de Buenos Aires.
Cuenta con un solo Centro de Procesamiento de Datos y todas las sucursales se encuentran conectadas a él en forma on-line, utilizando para ello las redes

públicas. El Centro de Procesamiento de Datos funciona bajo la modalidad 7 x 24, es decir, debe proveer servicios informáticos durante todos los días de la semana, durante las 24 hs.

La realización este estudio no solo obedece a las necesidades y riesgos planteados anteriormente, sino que también pretende cumplir con lo exigido por el Banco Central de la Republica Argentina (B.C.R.A.) en la circular "A 3198". En la misma se establecen los requerimientos operativos mínimos del área de Sistemas de Información y Tecnología Informática, para todas las entidades que controla y en los puntos 5.6. y 7.1 hace referencia explícita a los Planes de Contingencia[1].

1.3 - Justificación del Estudio

Con el crecimiento de los mercados, la globalización y la incorporación masiva de tecnología a las empresas, se ha vuelto cada vez más complejo y vulnerable el funcionamiento de las mismas, y si bien la "continuidad del negocio" y la "recuperación de desastres" no significan lo mismo, se debe entender que la recuperación ante un desastre es parte de mantener la continuidad del negocio.

En la medida en que el ambiente de tecnología cambia para atender al mercado del comercio electrónico, es necesario evaluar permanentemente los riesgos y cuantificar los probables impactos financieros en la empresa ante una eventual falla en la prestación de servicios, ya que también se incrementa el número de amenazas dirigidas contra la infraestructura de TI. Es por eso que una estrategia de seguridad es esencial para proteger la información vital y asegurar la continuidad de las operaciones de la empresa.

[1] Ver anexo D

En cada empresa los requerimientos son diferentes, sin embargo, existen lineamientos generales que pueden ayudar a cualquier compañía a diseñar un plan de contingencia y continuidad acorde a sus necesidades.

Hoy en día cualquier plan de negocio que se pretenda desarrollar en una organización tiene asociado un plan del área de tecnología. Este plan contempla desde la arquitectura de los sistemas y su infraestructura tecnológica hasta su mantenimiento operativo. Bajo esta nueva perspectiva, lo que se plantea es contar con un ambiente de recuperación de la infraestructura tecnológica que le permita a la empresa poder seguir operando ante una contingencia, dentro de los tiempos y con los servicios mínimos indispensables requeridos para el tipo de negocio que se desarrollará.

1.4 Alcance

El objetivo de éste trabajo de tesis es desarrollar un modelo que le permita a una empresa del sector financiero establecer las especificaciones técnicas básicas para contratar un Servicio de Procesamiento Informático Alternativo, de manera tal que pueda continuar con sus actividades de procesamiento si ocurriera un siniestro o contingencia que le impidiera hacerlo desde su Centro de Procesamiento Principal. Además se establecerán los lineamientos generales para la elaboración de un plan General de Recuperación ante Desastres que le permita:

- Reanudar lo antes posible el procesamiento en el Centro de Procesamiento Alternativo.
- Minimizar la cantidad de decisiones a tomar en el momento de la contingencia para minimizar la pérdida de información y su impacto comercial.
- Organizar las tareas necesarias para reparar o reemplazar el área dañada en el menor tiempo posible.
- Asegurar la continuidad del negocio.

- Recuperar la operatividad del Centro de Procesamiento Principal y las comunicaciones.

1.5 Hipótesis

El siguiente trabajo se desarrolla sobre la hipótesis de la imposibilidad de acceso a las instalaciones informáticas del Centro de Procesamiento Principal ante una contingencia en el mismo, o en sus alrededores.

2. Definiciones y Consideraciones de un Plan de Contingencia

A continuación se definirán y desarrollaran los elementos a tener en cuenta para la implementación de un plan de contingencia.

2.1. Plan de Contingencia

Una contingencia puede ser definida como un evento no esperado y con la característica de prestar una baja probabilidad de ocurrencia y un alto nivel de incertidumbre con relación a sus causas y efectos, como por ejemplo inundación, terremoto, incendio, falla técnica, etc. Cuando el evento tiene consecuencias devastadoras para la empresa, en intensidad y duración, se *califica* de desastre, cualquiera sea la causa.

Basado en los relativamente pocos antecedentes de desastres ocurridos en instalaciones de procesamiento de datos, podría ser que la instalación tenga una baja probabilidad de verse involucrada en uno.

Sin embargo, es conveniente no correr riesgos de que las instalaciones sufran una interrupción imprevista y extendida de los servicios que prestan, porque ocasionaría como resultado directo, una dramática interrupción de los negocios.

Deben tomarse medidas contra este riesgo; ellas pueden compararse con una póliza de seguro, con la diferencia de que ninguna compañía de seguros puede revertir esa situación, o en alguna forma convertir en dinero, la pérdida de capacidad de dar soporte al negocio.

El Plan de Contingencia incluye medidas contra el riesgo de desastre. El mismo deber ser parte del sistema de planificación de la empresa y requiere la intervención de todas las áreas involucradas.

La responsabilidad primaria por las funciones del negocio, aun en caso de desastre, reside en cada Unidad de Negocio. Son estas Unidades de Negocio las que deben establecer cuales serían las alternativas posibles ante la no disponibilidad de los servicios de procesamiento de datos.

En esta decisión, los usuarios tendrán el soporte de las áreas de tecnología para llegar a un acuerdo acerca de todo servicio residual disponible durante la contingencia. Deben también lograrse acuerdos acerca de las condiciones bajo las cuales el plan de contingencia ha de ser activado, como por ejemplo: duración probable de la falta de servicios, la perdida (total o parcial) de la capacidad de procesamiento de una o varias ubicaciones, etc.

Todas las funciones, niveles y departamentos deben tener su propio Plan de Contingencia y una copia de los planes de otras funciones, niveles y departamentos cuyas actividades en alguna forma interactúan con las propias. Los planes de contingencia deben prever el uso de recursos comunes por múltiples usuarios.

El Comité de Sistemas, integrado por representantes de las gerencias de Sistemas, Operaciones, Seguridad Lógica, Seguridad Física y Administración, debe revisar periódicamente los planes de contingencia, los que deberán estar documentados y ser probados.

2.2 Programa de aplicaciones vitales

La supervivencia de la empresa luego de un desastre que involucre la instalación de procesamiento de datos, depende de la disponibilidad de una instalación alternativa capaz de manejar la carga de trabajo.

Cualquiera sea el criterio para la selección de esa instalación alternativa, cuanto mayor sea la carga de trabajo, mas alto serán el costo y la complejidad de la recuperación.

Estas consideraciones llevan a la conclusión que, mas que enfocar la atención en la carga total de trabajo, se deberá enfocar en aquellas aplicaciones cuya apropiada ejecución es esencial para el negocio. Estas serán las que llamamos "**Aplicaciones Vitales**".

La identificación y asignación de prioridades a las Aplicaciones Vitales incluye a:

- Usuarios de información producida por las mismas
- Quien suple u origina la información (Propietario de la Información)
- Gerencia responsable de la aplicación
- Proveedor del servicio
- Auditor
- Alta gerencia

Para cada Aplicación Vital, se debe determinar:

- El período de tiempo en el cual las aplicaciones pueden no estar disponibles sin sufrir un daño irreversible
- La pérdida potencial que podría sufrir la empresa en función del tiempo en que la aplicación no esté disponible
- El nivel aceptable de degradación del servicio
- El tiempo aceptable de ese nivel degradado de servicio

Todos los programas, procedimientos operativos, documentación, formularios y datos necesarios para el correcto funcionamiento de las aplicaciones también son vitales, como lo es la lista de las personas responsables.

2.2.1 Objetivos

El objetivo de un programa de Aplicaciones Vitales es identificar aquellas que contengan información necesaria en caso de desastre, para seleccionar los métodos más eficientes y económicos para su protección y hacerlas fácilmente disponibles en caso de una emergencia. La responsabilidad de implementar un programa de Aplicaciones Vitales es del Comité de Sistemas.

La responsabilidad por la implantación de ese programa reside en las unidades de negocio: cada función, nivel y departamento debe determinar cuales son sus aplicaciones vitales y proveer a su protección conforme a los lineamientos fijados por el administrador de seguridad.

2.2.2 Selección de programas y archivos esenciales

- Establecer qué información debe estar disponible para reconstruir la función identificada.
- Decidir los requerimientos de información basados en las condiciones y procedimientos siguientes a un desastre.
- Seleccionar los registros que contienen esa información.
- Crear aquellos registros que no existen pero que serían necesarios para continuar la operación luego de un desastre.

2.2.3 Protección de Aplicaciones Vitales

Protección de las Aplicaciones Vitales significa la capacidad de tenerlos disponibles luego de un desastre, para su uso como soporte de los procedimientos de respaldo y recuperación. La mejor forma de lograr este objetivo es copiar cada Aplicación Vital en el medio apropiado (que casi siempre es el mismo del original) y mantenerlo en un almacenamiento remoto, seguro y cuidadosamente elegido.

Este almacenamiento debe estar suficientemente lejos de la instalación primaria y de la de respaldo, para minimizar la probabilidad de que se vea envuelto en el mismo desastre. La seguridad física y el control de acceso a este almacenamiento deben ser tan estrictos como las medidas usualmente tomadas para el primario.

Las Aplicaciones Vitales deben ser seleccionadas y almacenadas conforme a las reglas que aseguren la efectividad del programa y que permitan que una persona no familiarizada con las operaciones pueda llevarla a cabo.

2.3. Plan de Recuperación de desastres

El Plan de Recuperación ante Desastres es el plan que la empresa debe desarrollar para manejar contingencias, cuyo rango va desde pequeños problemas hasta desastres mayores. Si embargo, la primera preocupación es la elección de facilidades alternativas para el procesamiento de datos. Algunas posibilidades son:

El lugar de procesamiento alternativo pertenece a otra organización; en este caso debe firmarse un acuerdo a fin de cubrir:

- Compatibilidad de equipos
- Acceso a las instalaciones
- Prioridad de procesamiento

- Requerimiento de personal
- Entrenamiento
- Medidas de Seguridad
- Confidencialidad del personal y de los datos
- Pruebas

El lugar de procesamiento alternativo pertenece a un consorcio formado por un grupo de organizaciones. Bajo condiciones normales, es usado para el procesamiento de aplicaciones no vitales, prestación de servicios de procesamiento, etc. En caso de desastre en las instalaciones de una de esas organizaciones, ésta instalación alternativa se pone a disposición de sus procedimientos de respaldo y recuperación. Cada una de las empresas firma un convenio en el que se establece que, en caso de desastre en una de ellas, otra, seleccionada conforme a reglas preestablecidas, le proveerá de capacidad de procesamiento de sus Aplicaciones Vitales.

La instalación alternativa pertenece a una empresa de servicios de computación. Se firma un contrato de tiempo compartido (time-sharing), usualmente por una cantidad de horas mensuales bajo condiciones normales, y, en caso de desastre, esa cantidad se incrementa. Pueden ofrecer este servicio en una instalación específicamente montada para fines de respaldo.

El lugar alternativo pertenece a la misma empresa y es solo un local vacío. El edificio, instalaciones y servicios están listos, pero los equipos de computación se suponen disponibles a corto plazo, por el proveedor habitual. Esta solución es muy cara y no permite probar el Plan de Recuperación ante Desastres.

La instalación alternativa es propia de la empresa. En ésta solución se decide, como enfoque estratégico, dividir la capacidad de computación en dos o más instalaciones. Esta pareciera ser la mejor solución desde el punto de vista de efectividad y costo. En efecto, si la carga de trabajo ha de ser dividida entre dos computadores, cada uno de ellos deberá tener capacidad suficiente para procesar las Aplicaciones Vitales de ambos. Este concepto ha sido adoptado

por algunos de los grandes centros de procesamiento de datos consiste en tener todas las Aplicaciones Vitales en una instalación y dedicar la capacidad de la segunda al desarrollo de las aplicaciones.

Se debe prestar especial consideración a la red de comunicaciones. La red deber permitir la conmutación a la instalación de respaldo y la forma de implementarse este requerimiento depende fundamentalmente de las características físicas y lógicas de la misma. Dado que la empresa que brinda las comunicaciones está directamente involucrada, se deberá trabajar en conjunto para la implementación de esta solución.

2.4 Plan de Emergencia

El objetivo del Plan de Emergencia es contener el daño causado por un desastre a fin de preservar la capacidad de cumplimiento de la misión de la Unidad de Negocio y proveer seguridad al personal.

Esto está ligado tanto a la seguridad física como también a los Planes de Evacuación del personal, entrenamientos, etc.

2.5 Plan de Respaldo

El objetivo del Plan de Respaldo es mantener activas las operaciones críticas entre el momento de la caída del servicio y su recuperación. Esto significa que al menos las operaciones vitales, quizás con un menor nivel de servicio, deben sobrevivir en cada Unidad de Negocio, a fin de que la empresa en su conjunto sobreviva.

La responsabilidad por el Plan de Respaldo es del propietario del servicio que se asume ha de faltar. En términos generales, en caso de cualquier falla de un servicio, quien lo suministra tiene la responsabilidad de disparar el Plan de

Recuperación; mientras que el propietario del servicio tiene la responsabilidad de implementar el Plan de Respaldo.
Las operaciones de respaldo deben garantizar la capacidad de procesamiento mínima para la continuidad del negocio. Con frecuencia el desarrollo de un Plan de Respaldo requiere la participación del proveedor del servicio y debe incluir el diseño de tareas que puedan ser movidas de una instalación a otra y la identificación de múltiples fuentes alternativas capaces de correr cada tarea.

2.6 Plan de Recuperación

El objetivo del Plan de Recuperación contempla la restauración temporal o permanente de la capacidad del Centro de Procesamiento. El responsable del Centro de Procesamiento es responsable por el Plan de Recuperación y debe, en primer lugar, identificar los recursos críticos para sus tareas y planificar la recuperación.

Cada recurso toma un tiempo diferente para su reemplazo. Algunos dispositivos pueden ser rápidamente reemplazados, mientras otros requieren un tiempo más prolongado. Los edificios no pueden ser reemplazados tán rápidamente como los dispositivos y en general, el personal requiere más tiempo para ser reemplazado que cualquier otro recurso.

El plan de recuperación consiste de dos partes; la primera es la lista de actividades, dividida en antes y después del desastre; y la segunda contiene la documentación necesaria para el re-arranque.

Actividades:
Antes del desastre, la organización debe:

- Elegir la capacidad alternativa de procesamiento.
- Rediseñar la red o prever un sistema de conmutación para respaldar sus aplicaciones en línea, en su instalación de respaldo.
- Proveer el equipo apropiado.

- Hacer convenios con los proveedores de los servicios necesarios para la instalación alternativa.
- Planear y comenzar la instalación.
- Definir e implementar los procedimientos de respaldo, incluyendo qué sistemas y programas se requerirán, cuando copiarlos para su almacenamiento de seguridad y como trasladar esas copias al almacenamiento de seguridad.
- Probar el Plan.

Luego del desastre, se deberá:

- Manejar la emergencia de acuerdo con el plan de recuperación.
- Reunir al personal clave de procesamiento de datos, en una reunión de inicio de la recuperación.
- Evaluar la duración de la interrupción del servicio.
- Evaluar la disponibilidad de la instalación para las Aplicaciones Vitales.
- Decidir el traslado a la instalación de respaldo.
- Establecer prioridades de reinicio de las Aplicaciones Vitales.
- Organizar la restauración de registros vitales (programas, documentación, etc.)
- Notificar del desastre al personal y si es necesario, a los clientes y al publico.

Documentación:

La segunda parte del plan es su documentación. Ella es necesaria para el soporte de las actividades del plan y debe contener:

- Configuración de la instalación alternativa.
- Plano de su instalación mostrando no solo los equipos, sino también los servicios (tablero eléctrico, aire acondicionado, etc.)
- Operaciones normales y de respaldo para la instalación alternativa.
- Configuración de la red y operaciones de conmutación.
- Descripción de los medios de transporte para personal y archivos.
- Descripción del almacenamiento de seguridad y de sus procedimientos de acceso.
- Lista del personal clave (por lo menos para cada función principal) incluyendo domicilio y números telefónicos.
- Descripción de tareas del personal clave en caso de desastre.
- Lista de proveedores de equipos, programas, material auxiliar, y servicios públicos con domicilios y teléfonos.
- Lista de aplicaciones y registros vitales.
- Convenios de nivel de servicios post-desastre para las aplicaciones vitales.
- Requerimientos de seguridad post-desastre.
- Descripción de los registros vitales mantenidos en el almacenamiento de seguridad.
- Resultados de las pruebas del plan de recuperación de desastres
- Descripción de todo otro aspecto dependiente de la instalación.

Los planes de recuperación, así como todos los otros planes de contingencia, son en sí mismos registros vitales.

2.6.1 Prueba y Entrenamiento

Un Plan de Recuperación ante Desastres que no haya sido probado hasta asegurar su completa operatividad, no funcionará adecuadamente cuando el problema se presente.

El gerente de producción es responsable del entrenamiento de su personal y de los usuarios en la conducción de las pruebas del Plan de Recuperación de los servicios de procesamiento de datos.

2.6.1.1 Prueba

La prueba consiste en poner el plan en operación, paso a paso. Puede ser conducida de tal manera que, primero, la operatividad de la instalación alternativa, servicios, equipos y programas del sistema sea asegurada; luego cada Aplicación Vital debe ser probada primero independientemente, y luego con las otras aplicaciones.

Durante cada sesión de prueba todo problema que se presente debe ser anotado, aun cuando no comprometa la prueba, la que finaliza con la terminación exitosa del sistema o aplicación probada o cuando aparezca un problema insalvable.

Los errores en el procedimiento de recuperación, así como todo otro error, deben ser corregidos y la prueba repetida en la misma sesión, si fuera posible, o bien en una nueva sesión. Las pruebas deben realizarse sobre una base regular (no menos de dos veces al año) e involucrar el personal de usuarios.

Cada sesión de prueba debe ser dedicada a un número de aplicaciones vitales. Cada aplicación vital debe ser probada con una frecuencia que dependerá de su importancia y complejidad. Así como el Plan de Recuperación ante Desastres del área de procesamiento de datos, cada uno de los otros planes de contingencia deberán ser probados.

La prueba de un Plan de Emergencia implica notificar al personal de una emergencia simulada e iniciar el procedimiento de evacuación. Consiste asimismo en la verificación periódica de los equipos instalados para prevenir, detectar y tratar de evitar los eventos no deseados.

Las pruebas de un Plan de Respaldo deben verificar la operatividad de los procedimientos alternativos diseñados para mantener las Aplicaciones Vitales trabajando aun en el caso de pérdida de los servicios normales de procesamiento de datos. Los resultados de las pruebas deben ser analizados y certificados por los auditores internos.

2.6.1.2 Entrenamiento

Luego del desarrollo y la aprobación del Plan de Recuperación, es necesario realizar un entrenamiento del personal de las diferentes áreas involucradas.

El personal que deba operar la instalación alternativa luego del desastre es la encargada de llevar adelante las pruebas. Es, asimismo, una buena idea asegurarse que los miembros del grupo de recuperación ante desastres puedan realizar otras tareas, aparte de las que se espera normalmente de ellos. Por ejemplo, los programadores integrantes del grupo deberían ser capaces de arrancar y operar el sistema.

2.7 Opciones de la recuperación comerciales

Dependiendo de la tolerancia predeterminada a la pérdida de información, necesidades y presupuesto, se puede decidir restaurar el ambiente operacional en días, horas y hasta minutos.

Es necesario poder establecer cuanta pérdida es aceptable; por cuanto tiempo y cuanto costará. A media que aumenta el tiempo en volver a poner en

funcionamiento los procesos aumenta el costo al no poder brindar los servicios necesarios para la operación normal de la empresa.

Es necesario establecer un balance entre el costo que demanda implementar una solución, para lo que habrá que establecer cual es el máximo costo tolerable, y el tiempo que se tarde en solucionar una contingencia.

2.7.1 Tiempo de recuperación

El tiempo en que se pueden recuperar los datos desde los distintos medios de almacenamiento tiene directa relación con el costo de la solución a implementar, según la siguiente ecuación: a menor tiempo de demora, mayor costo

Cuanto menor sea el tiempo que se quiera demorar entre el momento en que se declara una emergencia y la posibilidad de restaurar los servicios, mayor será el monto que habrá que invertir en infraestructura tecnológica.

La posibilidad de tener los datos en forma espejada entre el Centro de Procesamientos Principal y el Centro Alternativo ofrece la posibilidad de restaurar más rápidamente los sistemas, pero es a la vez, la solución más costosa.

Una solución óptima seria la de encontrar un punto de equilibrio entre el tiempo de respuesta que se espera que la solución brinde y el costo económico que demanda implementar dicha solución

En resumen, un buen plan de continuidad debe contemplar, como muestra la figura 1, todos los aspectos relacionados con el negocio, como ser: los procesos, los servicios a brindar, la infraestructura, el personal, etc. Todas las áreas de la empresa deben trabajar en armonía para conseguir un desarrollo óptimo del plan.

Cada Unidad de Negocio debe determinar cuáles son sus Aplicaciones Vitales y en conjunto con el área de TI, deben proveer a su protección conforme a los lineamientos fijados por el Administrador de Seguridad.

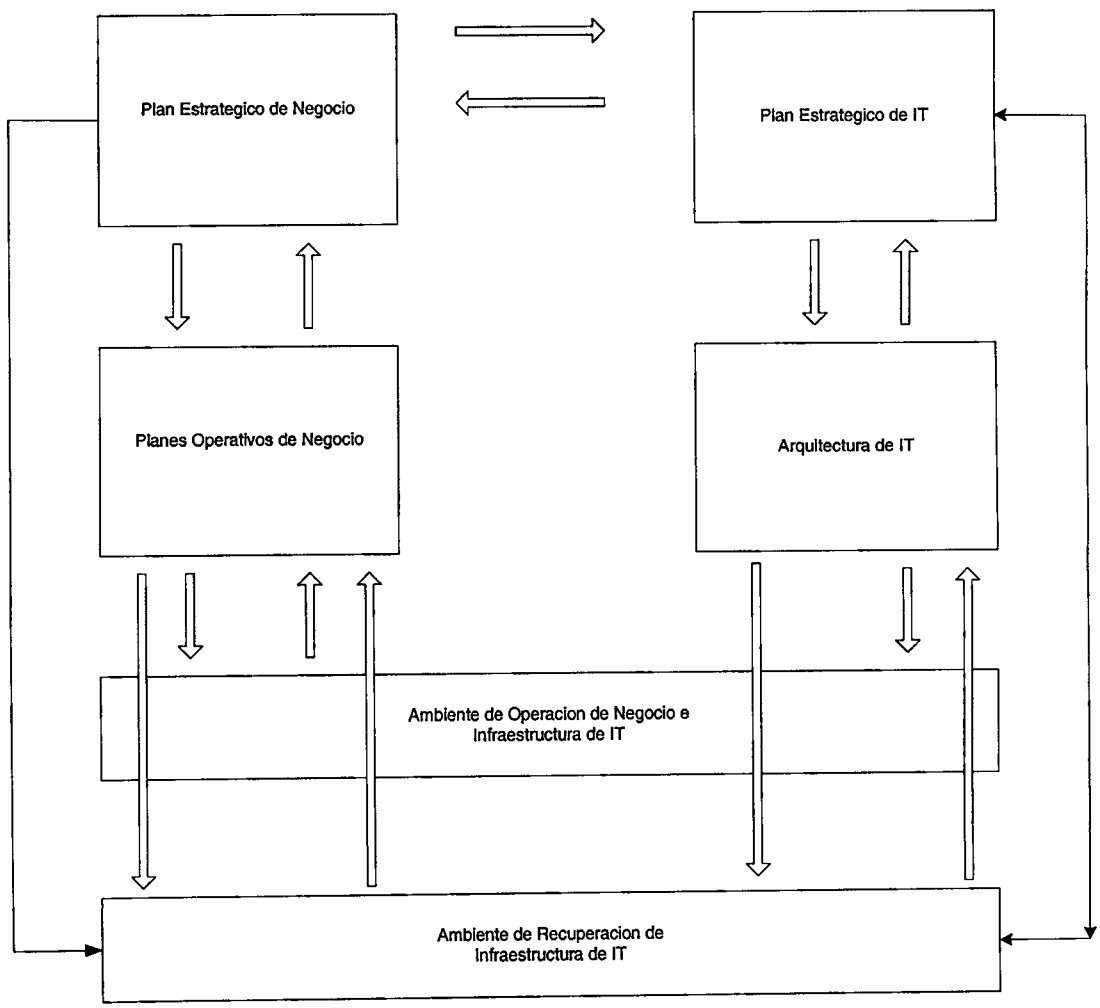

Figura 1

3. Descripción de la Organización

3.1 Centro Principal de Procesamiento

3.1.1 Recursos Humanos

El área de operaciones cubre esta necesidad dar servicios dividiendo a su personal en 3 turnos de 8 horas cada uno, siendo sus horarios de 6 a 14 hs. de 14 a 22 hs. y de 22 a 06 hs.

Cada turno de operaciones cuenta con:

- 2 Operadores de Periféricos
- 2 Operadores de Impresoras
- 3 Job-Streamers / Carga de Máquina
- 1 Jefe de Turno

El área de Soporte Técnico esta compuesto por:

- 3 Administradores de Base de Datos
- 3 Administradores de TS (Transacción Server CICS)
- 2 Especialistas en Comunicaciones
- 2 Especialistas en Sistemas Operativos
- 2 Especialistas en Almacenamiento
- 1 Jefe

3.1.2 Hardware

CPU: Se trata de una CPU IBM modelo 2064-103 de aproximadamente 647 MIPS, según las tablas de comparación de unidades centrales de procesamiento. Esta CPU cuenta con 8 GB de memoria principal, 3 procesadores y 50 canales de entrada / salida.

Esta unidad central de procesamiento esta dividida según el esquema de Particiones Lógicas o "LPAR ", según los siguientes porcentajes:

- Partición de producción 50 % del procesador o sea 325 MIPS
- Partición de desarrollo 40 % o sea 258 MIPS
- El 10 % restante para la partición de test o sea 64 MIPS.

Storage o almacenamiento principal: Esta compuesto por una unidad EMC2 modelo 8730-036, equipada con 8 GB de memoria cache, configurada en Raid 5 el 75 % de su capacidad y en RAID 1 el 25 % restante. Cuenta con 911 dispositivos con una capacidad total de 3,146 TB.

Estos dispositivos están asignados de la siguiente forma: 2,282 TB para la arquitectura OS/390 y 0,864 TB para las plataformas de sistemas abiertos UNIX. Existe una segunda unidad EMC2 modelo 5430-018 configurada con 4 GB de memoria cache, en modalidad Raid 5 con una capacidad de almacenamiento de 0,703 TB, distribuidos en 0,527 TB para la arquitectura OS-390 y 0,176 TB para sistemas abiertos.

Medios Magnéticos removibles: El centro cuenta con una unidad IBM modelo 3590 configurada con cuatro bocas de procesamiento; una unidad IBM modelo 3490 con cuatro bocas y una unidad Storage-Teck modelo 4480 con dos bocas también. Para el procesamiento de cintas abiertas cuenta con tres unidades Storage-Teck modelo 3420.

Sub sistema de Impresión: Para este rubro el centro cuenta con tres sistemas IBM System 4000, con compatibilidad AFP, que incluyen equipos de pre y post procesamiento del papel. Además hay instaladas dos impresoras IBM modelo Infoprint 60 que trabajan con papel cortado.

Facilidades de comunicaciones: el Centro cuenta con equipos de comunicaciones marca IBM modelo 3745 con su expansión 3746 modelo 900

con capacidad de memoria de 16 MB. El equipamiento se encuentra configurado con 100 líneas LIC tipo 1 V24 y 5 líneas LIC tipo 3 V35.

3.1.3 Descripción del servicio.

A continuación se describe en forma general el servicio que se requiere contratar:

- Contar con los vínculos de comunicaciones (fibras ópticas) entre el centro básico y el alternativo de forma tal que esto permita que se implemente un esquema de mirroring de datos entre dos configuraciones de discos; una ubicada en la instalación del Centro Principal y la otra en el Centro Alternativo.

- Esta actualización se hará por medio de herramientas de hardware y su software de control asociado, pero sin intervención del sistema operativo principal OS-390.

3.1.3.1 Características generales del servicio.

Para cumplir con estos requerimientos el Centro Alternativo deberá ofrecer equipamiento de procesamiento basado en tecnología conocida como Mainframe sobre una plataforma OS-390, además deberá contar con facilidades de equipamiento para recibir las conexiones de los diferentes operadores de comunicaciones, que hoy prestan servicio a la empresa, y a los cuales ésta le solicitará implementar la capacidad de doble ruta de acceso (una al Centro Principal como es actualmente y otra alternativa en el centro que sea seleccionado).

Complementariamente, con esta capacidad de procesamiento, deberá poner a disposición instalaciones para albergar al personal que actuará en caso de ocurrir una contingencia. El mismo deberá conformar dos equipos, uno de soporte técnico y operaciones y otro de mantenimiento de sistemas.

Dependiendo de la duración de la emergencia, el grupo de mantenimiento de sistemas pude pasar a formar parte del plan de operación. La cantidad de personas necesarias para el área de soporte y operación es de 25, debiendo prever al menos 20 estaciones de trabajo, conectadas con el Mainframe.

Dentro de estas estaciones de trabajo deberán existir al menos 6 estaciones del tipo "pantalla boba" de la línea IBM 3270, conectadas por medio de unidades de la familia 3174, trabajando en modalidad local.

Toda esta infraestructura deberá estar disponible para su uso, a partir de 1 (una) hora de declarada formalmente la contingencia, situación que se adelantará por medio de una llamada telefónica al Centro Alternativo y luego será perfeccionada mediante un acta a firmar por ambas partes.

3.2 Configuración requerida por la Organización

A continuación se detallan las características aproximadas del equipamiento necesario, entendiendo que los valores de potencia a ofertar podrán ser mayores que los fijados en este requerimiento, pero en ningún caso, menores.

Como parte de las especificaciones de equipamiento, será necesario también especificar la modalidad de uso de los mismos, detallando si será de uso exclusivo de nuestra empresa, o compartida, dado que esta definición tendrá implicancias de performance, capacidad de crecimiento, confidencialidad, etc.

La configuración que deberá estar disponible en el plazo máximo de una hora, a partir de la declaración de la contingencia será:

- Unidad central de procesamiento:

  De aproximadamente 1000 MIPS (millones de instrucciones por segundo), con una memoria primaria de 2 (dos) GB y 2 (dos) GB de memoria expandida. Deberá contar con dos adaptadores OSA fast ethernet, mas un adaptador Giga Byte express.

- Capacidad de almacenamiento (Storage):

  1 (un) TB distribuido en direcciones de discos en emulación IBM modelo 3390-3. Preferentemente la capacidad de Storage debería ser provista por medio de unidades EMC2 modelo 8730-36 con 8 giga bytes de memoria en el controlador.

  En caso de que las unidades de discos a ofertar sean de otra marca o modelo deberán contar con la facilidad de hacer "mirroring" con las unidades actualmente existentes en el Centro Principal, que son EMC2 8730-36 y asegurar la total compatibilidad y transparencia entre ambos, fundamentalmente en lo relativo al esquema de alta disponibilidad de datos.

  Para la implementación de esta facilidad será necesario contar con vínculos de fibra óptica entre el Centro Principal y el Centro Alternativo. Estos serán provistos y contratados por nuestra parte, aunque como un adicional podrán ser ofertados dentro de la propuesta solicitada por el presente documento.

- Facilidades de comunicaciones:

  Deberá ofrecer como parte de la configuración, un equipo de comunicaciones marca IBM modelo 3745 con su expansión 3746 modelo 900 con 16 mega bytes de memoria, el cual estará configurados con 100 líneas LIC tipo 1 V24 y 5 líneas LIC tipo 3 V35.

- Unidades para Medios Magnéticos Removibles.

  La instalación alternativa deberá contar como mínimo con el siguiente equipamiento dedicado en forma exclusiva para la prestación objeto del presente pedido:

  a) Dos unidades (4 bocas) de procesamiento de cartridges modelo IBM 3590-E11
  b) Dos unidades (4 bocas) IBM modelo 3490
  c) Dos unidades de cinta abierta compatible con IBM modelo 3420-8.

- Subsistema de Impresión:

  El Centro Principal de procesamiento cuenta en la actualidad con dos sistemas InfoPrint modelo 60 más dos impresoras System 4000 con capacidad de pre y post procesamiento del papel. En este rubro es posible presentar opciones de contratos con terceras partes que puedan suministrar esta capacidad de impresión, con características de pre y post procesamiento, y soporte del software de diseño de listados basado en AFP- poscript – PCL1.

Para éste requerimiento, se deberá especificar que capacidad de impresión se ofrece, que deberá ser compatible con lo que está actualmente disponible en el Centro Principal y qué método de tercerización propone en caso de no contar con la capacidad de impresión de alto volumen solicitada.

4. Modelo del Plan de Contingencia y Continuidad del Negocio

4.1 Introducción

Se presenta un modelo que describa las acciones a desarrollar ante la posibilidad de que se presenten diferentes situaciones de emergencias que impidan la operación normal del Centro Principal de Procesamiento de la Empresa en estudio. También incluye las tareas de prevención de estas situaciones de emergencia, identificándolas y desarrollando procedimientos para tratar de evitarlas, minimizar las consecuencias en caso de que ocurran, o desarrollar alternativas para seguir operando durante el tiempo que dure la emergencia.

El presente plan se divide en tres grandes grupos de acciones:

- **Prevención**: Corresponde a los esfuerzos para identificar, evaluar y disminuir los riesgos en el área de Tecnología Informática de la empresa.
- **Planificación de la crisis**: Desarrolla un plan de cómo actuar ante una Contingencia.
- **Planificación de las Contingencias**: Desarrolla procedimientos y recomendaciones para restablecer la normal operación del Centro de Procesamiento Principal o en un Centro Alternativo.

4.2 Objetivo

Este modelo comprende los lineamientos básicos para asegurar que todos los recursos conocidos y disponibles sean utilizados para prevenir una emergencia y en caso de que esta ocurra, proveer una lista de procedimientos que serán ejecutados para restaurar el ambiente de procesamiento de datos y para asegurar la continuidad de las operaciones de manera tal que tengan el menor impacto posible para los usuarios.

Los procedimientos contenidos en este documento para las emergencias cumplen con los siguientes objetivos básicos:

- Prevenir o minimizar el peligro de vida y garantizar la seguridad de todo el personal.
- Prevenir o minimizar los daños al sistema de procesamiento de datos.
- Proveer los procedimientos de recuperación ante Contingencias.

4.3 Prevención

La prevención trata básicamente de establecer mecanismos para evitar la ocurrencia de un evento que ponga en dificultades el servicio que brinda el Centro de Procesamiento Principal o al menos que disminuya los daños causados y sus consecuencias sobre el servicio.

4.4 Niveles de Contingencia

A fin de precisar la magnitud del problema a enfrentar y evaluar la respuesta ante la emergencia, es necesario realizar una clasificación en relación con el impacto que causaría en el normal funcionamiento del Centro de Cómputos Principal, las diferentes Contingencias que se pudieran presentar.

A continuación se agrupan los diferentes eventos que pueden producir contingencias en cuatro niveles, partiendo del de menor impacto llamado de nivel uno, hasta los eventos de nivel cuatro, que impiden el funcionamiento de la empresa en su totalidad y que pueden afectarla por varias horas y hasta días enteros.

Es importante destacar que, para una correcta clasificación, es necesario considerar además del detalle de las fallas ocurridas, el horario en que estas se presentan, de manera que un mismo evento calificará distinto, dependiendo del horario en que éste se produzca.

Definiremos como "Ventana Operativa" para el servicio de las aplicaciones en línea de las diferentes sucursales, al espacio de tiempo que transcurre desde la necesidad de disponer de las mencionadas aplicaciones antes de la apertura de las sucursales, hasta el momento en que se consideran terminadas las operaciones en las mismas.

Esta ventana se especificará en cada momento del año, dependiendo de la época (vacaciones anuales, vacaciones de invierno, feriados, etc) y será tal que contemple el horario mas temprano de la sucursal que abra mas temprano, hasta el horario mas tardío de la que mas tarde cierra.

4.4.1 Nivel de Contingencia 1

Se definirá como la perdida temporal de un componente que no interrumpe las operaciones normales del Centro de Procesamiento Principal y que puede ser manejada dentro de los limites del mismo, por su personal, y que además no produce atrasos sensibles respecto del horario al que debe arribarse para que las aplicaciones on-line estén disponibles para la apertura de las sucursales.

El nivel de contingencia 1 es el menor de la escala, no implica llamar al Comité de Contingencia para su tratamiento. Aun en este nivel de Contingencia se debe informar al Comité de Seguimiento y al Comité de Calidad, para su tratamiento, y posterior toma de acciones para evitar su repetición.

Ejemplos:

- Cancelación de programas por falla de datos, falta de espacio en disco, etc.
- Indisponibilidad de un dispositivo, pero que se posee dentro de la instalación otro de su mismo tipo.
- Falla de un equipo de aire acondicionado.
- Indisponibilidad de una línea de datos, pero que tenga una ruta alternativa de acceso al punto remoto.

4.4.2 Nivel de Contingencia 2

Se definirá como la pérdida temporal de un componente vital que impide la prosecución de las tareas normales del Centro de Procesamiento Principal por hasta dos horas en el compromiso de disponibilidad de las aplicaciones on-line.

La definición de este nivel de Contingencia se deberá realizar considerando la extensión de la falla, los recursos para solucionarla y la evaluación del impacto en las diferentes áreas de la Empresa. Requiere el llamado al Comité de Contingencia y puede ser manejada dentro de los limites del Centro de Procesamiento, por su personal.

Se debe informar al Comité de Seguimiento y Calidad para su tratamiento, y posterior toma de acciones para evitar su repetición.

Ejemplos:

- Pérdida de un conjunto de datos cuya recuperación requiera procesos con altos tiempos de procesamiento (que no sean un simple restore de archivos desde un backup anterior).
- Indisponibilidad de un dispositivo, y que no se posee otro de su mismo tipo dentro de la instalación y cuyo tiempo de reparación produzca el atraso en las tareas batch. (CPU, controlador de Discos, etc.)
- Falla de los equipos de aire acondicionado, que impliquen una parada total de los equipos de procesamiento por un plazo tal que atrase las tareas

batch u on-line.

- Indisponibilidad de un canal de comunicaciones tal que impida el envío de datos a una región geográfica completa, dentro del conjunto de sucursales de la empresa.

4.4.3 Nivel de Contingencia 3

Se definirá como la pérdida temporal de uno o varios componentes vitales que impidan la prosecución de las tareas normales del Centro de Procesamiento Principal por hasta 10 horas en el compromiso de disponibilidad de las aplicaciones on-line.

La definición de este nivel de Contingencia se deberá realizar considerando la extensión de la falla, los recursos para solucionarla y la evaluación del impacto en las diferentes áreas de la Empresa. Requiere el llamado al Comité de Contingencia y no puede ser manejada dentro de los limites del Centro de Procesamiento Principal, con tan solo su personal.

Se debe informar al Comité de Seguimiento y Calidad para su tratamiento, y posterior toma de acciones para evitar su repetición.

Ejemplos:

- Pérdida de un conjunto de datos cuya recuperación requiera el desarrollo de programas, con altos tiempos de programación y procesamiento, además de la participación de un gran número de miembros del área de Proyectos.
- Indisponibilidad de la totalidad del equipamiento de procesamiento, con fallas de hardware, con falta de repuestos para su solución, o una falla en el software de base que requiere la intervención de los centros de soporte externos.
- Principio de incendio en las instalaciones, daños mayores en las instalaciones eléctricas, disparo accidental de los sistemas de extinción (sprinklers), etc.

- Indisponibilidad de un canal de comunicaciones por una falla total en el proveedor, caída de nodos nacionales, etc.

4.4.4 Nivel de Contingencia 4

Se definirá como la pérdida temporal de uno o varios componentes vitales que impide la prosecución de las tareas normales del Centro de Procesamiento Principal por mas de 10 horas y donde es posible asumir, en primera instancia, una prolongada indisponibilidad, llegando incluso a la necesidad de pasar a realizar los procesos en el Centro Alternativo de Procesamiento.

Esta opción implica redireccionar las comunicaciones, el traslado de backups de archivos, traslado del personal, la disponibilidad de insumos, etc. Tareas todas ellas de prolongado tiempo de implementación, en relación con la necesidad del servicio.

En este nivel de contingencia debe estar fuertemente involucrada la Gerencia General y las respectivas Gerencias de la Empresa. La definición de este nivel de Contingencia se deberá realizar considerando la extensión de la falla, los recursos para solucionarla y la evaluación del impacto en las diferentes áreas de la Empresa.

Requiere el llamado al Comité de Contingencia y no puede ser manejado dentro de los limites del Centro de Procesamiento, con tan solo su personal. Se debe informar al Comité de Seguimiento y Calidad para su tratamiento, y posterior toma de acciones para evitar su repetición.

Ejemplos:

- Indisponibilidad del Centro de Cómputos Principal
- Desordenes públicos o motines. Huelgas generalizadas del personal.

4.5 Análisis de Riesgos

Se definirá como Análisis de Riesgos a aquellas actividades de observación y análisis que permiten identificar las posibles causas de desastres o de interrupción del servicio. Para esta tarea de análisis es importante investigar la historia de incidentes dentro de la Empresa, así como también a nivel Nacional.

4.5.1 Actividades a realizar

- Identificar las amenazas y determinar cuales son probables que ocurran para la normal operación del Centro de Procesamiento Principal, determinando cuán vulnerables son las instalaciones y sistemas del mismo.
- Determinar alternativas ante estos riesgos.
- Evaluar alternativas.
- Calificar los riesgos.
- Asignar alternativas de acción ante la presencia de estos.
- Implementar con un plan adecuado, las soluciones.

En este punto es importante definir a que llamamos vulnerabilidad del Servicio de Procesamiento.

4.5.2 Vulnerabilidad

Se definirá como vulnerabilidad al daño que pueda sufrir la instalación, el proceso, o algún componente de la cadena de servicio informático, ante la ocurrencia de un evento. Cada grado de vulnerabilidad, tendrá asociado una probabilidad de ocurrencia.

Definiremos tres grados distintos de vulnerabilidad:

- Vulnerabilidad alta: Interrupción de las rutas, que imposibiliten la llegada de archivos sobre medios magnéticos, indispensables para el procesamiento.
- Vulnerabilidad Media: Principio de incendio en la sala de computadoras.
- Vulnerabilidad Baja: Indisponibilidad total del edificio.

El daño producido por el evento lo clasificaremos con la siguiente escala: Uno será el daño mas leve y de fácil reparación, y Cinco aquel que mayor impacto cause y que por lo tanto necesita mayor tiempo de reparación.

4.5.3. Riesgos de la tecnología y sus servicios.

Evento	Vulnerabilidad	Riesgo
Fallas de Hardware CPU	Baja	5
Fallas de Hardware Periféricos	Baja	3
Fallas de Software de Base	Baja	4
Fallas de Software Aplicativo	Medio	3
Fallas de Medio	Medio	2
Falta de Energía Eléctrica	Baja	5
Falta de Aire Acondicionando	Baja	5
Indisponibilidad de Personal	Baja	3
Corte de Comunicaciones	Media	2
Fallas Estructurales del Edificio	Baja	5
Incendio	Baja	4

4.5.4 Riesgos de la estructura de Recursos Humanos

Evento	Vulnerabilidad	Riesgo
Sabotaje	Media	5
Desordenes Públicos	Baja	3
Ilícito Informático	Media	4
Robo	Media	4
Errores de Datos	Baja	2
Amenazas de Bomba	Media	3
Uso Indebido de Info. Sensitiva	Baja	4
Huelgas	Baja	2
Desfalco o Fraude	Baja	3
Atraco Armado	Baja	4
Perdida de Personal Clave	Baja	4
Daño Malicioso al Software	Media	5
Acceso Físico de Personal no Autorizado	Baja	3
Modificación Accidental de Software	Media	2

4.5.5 Alternativas de acción ante las diferentes Contingencias.

Una vez detallados los posibles riesgos, es necesario determinar las alternativas de prevención de los mismos:

	Factibilidad	Acción	Ejemplos
La más Deseable	Pudiese ser la mas costosa o prácticamente imposible de implementar	Remover del escenario las contingencias que pudieran producir una Contingencia	Contar con un equipo de procesamiento exactamente igual al principal para caso de contingencia y que los datos se encuentren en forma "espejada"
	Alta Factibilidad de Implementación	Reducir o minimizar las condiciones que pueden causar una Contingencia	Instalar en todo el ámbito del Centro de Cómputos un sistema de prevención contra incendios.

	Factible de Implementar	Transferir la responsabilidad del riesgo a terceras partes	Tercerizar funciones. Contratar Seguros
La menos Deseable	Mínimo Impacto en caso de Contingencia	Aceptar el riesgo	No contemplar ninguna acción

En este capitulo se presentaran los diversos escenarios posibles de Contingencias y se detallan acciones o procedimientos que la Empresa deberá implementar para reducir, transferir, o asumir las amenazas que pudieran conducir a una interrupción del servicio.

4.6 Declaración de la Contingencia

La declaración de una contingencia de nivel dos o más, tiene dos etapas claramente diferenciadas.

La primera se refiere al actor que detecta la falla y la evalúa como de severidad dos o más, o que habiendo comenzado como una falla de nivel uno, por el transcurrir del tiempo es necesario elevarla a categoría dos. Este será el encargado de llamar al Comité de Contingencia.

La segunda es la que se desarrolla dentro del Comité, y donde se declara la Contingencia y se la asigna la categoría adecuada.

4.7 Manejo de la Crisis

Una catástrofe puede ocurrir en cualquier momento, aunque se hayan tomado todas las precauciones posibles, es por ello que la mejor defensa ante una falla es contar con un plan de manejo de crisis, el cual se debe practicar y probar en forma periódica a fin de asegurar su vigencia.

El objetivo principal de planificar para la Crisis es lograr la seguridad del equipo humano y del material de la Empresa, previniendo la perdida de vidas, de equipos, y cualquier otro daño que se pueda producir.

4.8 Roles y Responsibilidades

Equipo de manejo de crisis

El Comité de Contingencia realizará la evaluación de la falla presentada y según los diferentes criterios representados por las áreas involucradas en el mismo, declarará la Contingencia y le asignará un nivel, de 1 (uno) a 4 (cuatro), dependiendo de la gravedad de la misma, siendo 1 la más leve y 4 la más crítica.

Uno de los miembros del Comité de Contingencia deberá quedar comisionado para realizar el seguimiento de la evolución de la contingencia, con el fin de ir elevando la categoría de la misma según transcurra el tiempo, o se le informe de las complicaciones o dilaciones que se presentan.

Es conveniente que la misma persona sea la que informará de la totalidad de la contingencia al Comité de Calidad una vez que ésta haya concluido. El Comité de Contingencia, estará compuesto por al menos un representante de las áreas abajo listadas, y especificadas como Principales, y según el nivel de Contingencia y las características de la misma, por también un representante de las categorizadas como Secundarias.

Áreas Principales:

- Gerencia del área Operaciones
- Gerencia del área Soporte Técnico
- Gerencia del área Proyectos
- Responsable de seguridad Lógica.

Áreas Secundarias:

- Responsable del área apoyo Logístico.
- Responsable de documentación de las Contingencias.
- Responsable de seguimiento de Contingencias y de Calidad (Optativo).
- Responsable del área seguridad Física.

En los casos de Contingencias de nivel tres o cuatro, es necesario nombrar una persona a cargo de la tarea del manejo de las Relaciones Publicas y los medios, así como de la información interna de lo que esta aconteciendo.

4.9 Consideraciones a tener en cuenta ante una crisis de nivel 3 ó 4

- Solo el responsable de las Relaciones Publicas debe informar a los Medios. Otros empleados deben abstenerse de dar declaraciones de lo sucedido.
- Nunca se debe especular o hablar de suposiciones ni con posturas personales.
- Respetar el derecho del los medios de comunicación de cubrir los hechos.
- Se debe explicar como y cuando se obtuvo la información.

Respecto de la comunicación interna se deben considerar los siguientes puntos, y tener presente que los empleados son los primeros en enterarse cuando ocurre una falla:

- Controlar los rumores y las ansiedades ofreciendo información honesta y de manera frontal, indicando el hecho acaecido y las consecuencias en el ambiente de trabajo.
- No demorar en tener una posición oficial; las noticias graves viajan rápido y son fácilmente distorsionadas.

- Asegurarse que la información a suministrar sea veraz y precisa. Mucho esfuerzo vital puede ser desperdiciado tratando situaciones inexistentes.
- Establecer un teléfono de emergencias para aquellas personas que no estén presentes en las instalaciones y decidan llamar.
- Asegurarse que todos estén informados.
- Comunicar la forma en que se intentan recuperar los servicios, que acciones se tomarán y quienes son los responsables.
- Si hay empleados heridos o fallecidos, contactarse con los familiares antes que otros lo hagan.
- Asegurarse que las autoridades civiles estén enteradas para que inicien las investigaciones que establece la legislación.

4.10 Esquema de escalamiento

Durante el desarrollo de una Contingencia y según sea la clasificación de ésta y a medida que transcurre el tiempo de la misma, es necesario tener presente el esquema de escalamiento o notificación que se detalla en este punto.

Se reconocen como actores a involucrar en el desarrollo de una contingencia a:

Personal de operaciones:

- Operador
- Supervisor
- Jefe de Turno
- Analista de Carga de Máquina
- Analista de Mesa de Ayuda
- Operador de impresión
- Jefatura Departamento Servicios Procesamiento
- Gerente de Operaciones

Personal de Gerencia Proyectos:

- Analista a cargo de aplicación
- Líder de Proyecto
- Jefatura del área de Proyecto
- Gerencia de Proyectos
- Gerencia de Sistemas

Personal Soporte Técnico:

- Especialista OS/390 y software relacionado
- Especialista Comunicaciones
- Especialista CICS
- Jefe de Soporte Técnico
- Gerencia de Infraestructura Tecnológica

Personal área Comunicaciones:

- Operador Centro de Monitoreo
- Analista de enlace con proveedores externos
- Jefe de Comunicaciones
- Gerencia de Infraestructura Tecnológica

Personal del área apoyo Logístico:

- Responsable Aire Acondicionado
- Responsable sistema de detección Incendio
- Responsable área energía Eléctrica
- Responsable de área limpieza, maestranza (movimiento de equipos, papel, etc.)
- Jefatura

Personal área Seguridad lógica:

- Analista
- Jefe de Departamento

Personal área Seguridad Física:

- Analista
- Jefe de Departamento

Gerencia de enlace:

- Gerente de Sistemas
- Gerente de Sucursales
- Gerente de Coordinación Sucursales
- Gerente Comercial
- Gerente de RRHH

Gerencia General:

- Gerente General
- Comité de Contingencia

4.10.1 Procedimiento General de Escalamiento

Dada la diversidad de fallas y sus interrelaciones, el personal que se irá involucrando a ella dependerá del tipo de falla de que se trate. Se presenta el siguiente caso, a manera de ejemplo ilustrativo.

Una cancelación de un programa por error en los datos originará la intervención del analista de carga de máquina, que verificará si la carga de éstos fue correcta.

Si fue así, dará intervención al analista a cargo de la aplicación, el cual en caso de tener que recurrir a un colega de otro sistema, deberá pedir autorización al Jefe del Área de Proyectos o al Gerente de Proyectos.

Luego de localizada la falla, se deberán correr algunos procesos. Si no se cuenta con el espacio necesario en disco, se dará intervención al área de tecnología para que determine qué discos adicionales son posibles de vaciar y usar como Scratch.

Una falla en un controlador de discos, dispara la inmediata intervención del personal de soporte técnico, que ante la tardanza en solucionarlo, deberá convocar al área de Proyectos, y al área de Operaciones, para determinar que aplicaciones son factibles de procesar con el espacio disponible y cuáles pueden ser postergadas.

La consideración hecha de que los actores a involucrar dependerán del tipo de falla, no exime que cada uno de ellos involucre a su superior, según transcurra el tiempo, y según la siguiente tabla:

4.11 Tabla de Involucramiento de actores a una Contingencia

Área	Involucrado	Tiempo	Personal a Involucrar
OPERACIONES	Operador	0	Supervisor
	Supervisor	0.30	Jefe de turno
	Jefe de turno	1.00	Jefatura Departamento Servicios Procesamiento
	Jefatura Departamento Servicios Procesamiento	2.00	Gerente de Operaciones
	Gerente de Operaciones	3.00	Gerencia General
PROYECTOS	SISTEMA		
	Analista a cargo aplicación	1.00	Líder de Proyecto
	Líder de Proyecto	2.00	Jefatura del Área de Proyecto
	Jefatura del Área de Proyecto	3.00	Gerente de Proyecto
	Gerente de Proyecto	5.00	Gerencia General
SOPORTE TECNICO	Especialista Soporte Técnico	1.00	Jefe de Departamento Soporte Técnico
	Jefe de Departamento Soporte Técnico	3.00	Gerencia de Infraestructura Tecnológica
	Gerencia de Infraestructura Tecnológica	5.00	Gerencia General
COMUNICACIONES	Operador centro de Monitoreo	1.00	Analista de enlace con proveedores externos
	Analista de enlace con proveedores externos	2.00	Jefe de departamento Comunicaciones
	Jefe de departamento Comunicaciones	3.00	Gerencia de Infraestructura Tecnológica
	Gerencia de Infraestructura Tecnológica	5.00	Gerencia General
LOGISTICA	Responsable servicio Logístico	1.00	Jefatura Servicios Logísticas
	Jefatura Servicios Logísticos	3.00	Gerente General
SEG. LÓGICA	Analista Seguridad Lógica	1.00	Gerencia Seguridad Lógica
	Gerencia Seguridad Lógica	3.00	Gerente General
SEG. FISICA	Analista Seguridad Física	0.30	Gerencia Seguridad Física
	Gerencia Seguridad Física	2.00	Gerente General

En todos los casos es la Gerencia General la encargada de convocar al Comité de Contingencia para que éste pase a comandar las acciones a realizar ante la imposibilidad de operar del Centro de Procesamiento Principal.

4.12 Comité de evaluación del desarrollo de la Contingencia

Una vez convocado el Comité de Contingencia se deberá designar a uno de sus componentes para que realice el seguimiento de la contingencia.

Serán sus responsabilidades:

- Realizar un control de los tiempos de resolución de la emergencia, alertando sobre la necesidad de cambio de categoría de la misma.
- Registrar cada una de las acciones, con especial detalle en los tiempos estimados de resoluc
- Documentar las diferencias entre las acciones detalladas en el plan de contingencia, y las qu
- Para las Contingencias de categoría 2 y 3, puede desarrollar las actividades de enlace de información hacia adentro de la organización.
- Proveer al Comité de Calidad de toda la información, para la posterior evaluación y corrección de los procedimientos internos.

4.13 Comité de Calidad

Será su principal misión la de realizar el seguimiento de las fallas presentadas en todo el ámbito de la Empresa y procurar su solución. Estará compuesto por representantes de las áreas de Proyectos, Soporte Técnico y Producción.

Lo compondrá también el responsable del Comité de Contingencia y el responsable administrativo del mencionado plan. Se reunirán al menos dos veces al mes, con la misión de analizar todas y cada una de las fallas presentadas, establecer sus responsables y procurar su solución.

En cada reunión se comenzará revisando los planes presentados en la reunión anterior sobre la solución a alguna falla. Llevaran un registro de las fallas ordenadas por tipo, responsable, solución, y tiempo de reparación.

4.14 Administrador del Plan de Contingencia

Dentro de la estructura de la organización se deberá asignar la función de Administrador del Plan de Contingencia, al quién se le deberán remitir todos los cambios producidos, tanto en la plataforma tecnológica, como así también en la de los Aplicativos.

Serán sus principales responsabilidades:

- Mantener actualizado el Plan de Contingencia con todas las modificaciones que le lleguen.
- Formar parte del Comité de Contingencia, documentando cada paso realizado, cuando se haya presentado una falla.
- Presentar sugerencias para mejorar el proceso de solución de fallas, basado en su experiencia y en la recopilación de información de cada Contingencia.
- Fijar la fecha de las pruebas del Plan de Contingencia y llamar a su realización.
- Ser el representante ante los organismos de administración de catástrofes (Defensa Civil, Bomberos, Policía, etc.)
- Constituir el enlace natural con el Comité de Calidad.

4.15 Plan de prueba permanente del Plan de Contingencia

Ningún plan para afrontar un hecho fortuito puede calificarse de apropiado si no ha sido sometido a una serie de pruebas que ayuden a identificar problemas.

El plan de pruebas debe realizarse con la participación de todas las áreas y al menos dos veces al año. La misma deberá incluir a los usuarios finales.
Los beneficios del proceso de pruebas se pueden resumir en:

- Demostrar la habilidad de recuperar los servicios de la Empresa.
- Determinar la factibilidad de la estrategia de recuperación elegida.

- Ayudar a confirmar los tiempos estimados.
- Identificar las áreas del Plan detallado de Contingencia que necesitan ajuste o modificación.
- Ayudar a confirmar el correcto estado de los archivos de respaldo y su completitud para la recuperación.
- Ayudar al personal a estar entrenado.
- Involucrar al usuario final como actor importante en el proceso de recuperación.

Para minimizar el impacto sobre las operaciones, es recomendable establecer una estrategia basada en definir escenarios posibles de desastre, en función de un análisis de riesgos determinado y con ello, probar independientemente los componentes.

Al menos dos veces al año deberán probarse todos los elementos juntos y las observaciones y ajustes deberán ser documentadas y asentadas en los registros del Comité de Seguimiento de Contingencias y en el de Calidad.

Los hechos que se presenten en el desarrollo de las actividades diarias sobre fallas menores, como la pérdida de una línea de transmisión de datos o un corte de la energía eléctrica, permitirán revisar parte del plan total de contingencia.

Para realizar las diferentes pruebas del Plan Detallado de Contingencia se plantea el siguiente curso de acción:

- Planificar las pruebas, estableciendo los objetivos, el tipo de prueba, los recursos y las personas involucradas.
- Ejecutar la prueba asegurándose de mantener registros escritos de lo sucedido y el tiempo consumido por las diferentes etapas.

- Evaluar los resultados identificando los problemas encontrados, las deficiencias en la documentación y en el entrenamiento.
- Documentar lo encontrado, ajustando el plan original, informando de los cambios a todos los participantes.

5. Modelo de Requerimientos

Para tratar de asegurase que las empresas que se presenten en la licitación del servicio estén en condiciones de dar cumplimiento a los requerimientos que demanda ésta organización, ya sea en lo que hace al nivel de servios como a la disponibilidad de los mismos, se deben establecer requisitos que permitan, en cierta medida evaluar y avalar que puedan garantizarlo.

5.1 Especificaciones

Estos requisitos se solicitan para poder desarrollar una matriz comparativa, que facilite la elección del proveedor. Es imprescindible que las empresas que se postulen como alternativa de solución y que pretendan participar del proceso licitatorio, cumplan con ellos.

5.1.1 Resumen Ejecutivo

Proveer un resumen conciso de los servicios a ofrecer, dentro del presente pedido de información.

5.1.2 Perfil del Proveedor

Las siguientes son algunas preguntas que intentan obtener el perfil de la empresa oferente y verificar la experiencia en brindar el servicio solicitado en el presente documento:

- ¿Cuántos años hace que está proveyendo servicios de recuperación ante desastres?
- ¿Qué tipo de productos y servicios son ofrecidos?
- ¿Cuántos empleados tiene dedicados al soporte de recuperación ante desastres?

- ¿Cuáles fueron sus inversiones durante los últimos 12 meses, dedicadas a servicios de tecnología y cuáles las dedicadas al servicio de recuperación ante desastres?

5.1.3 Base de clientes y experiencia corporativa

- ¿En la actualidad, cuántas empresas están siendo soportados en el servicio de referencia?
- ¿Cuántas declaraciones de desastre de sus clientes ha soportado?
- ¿Cuántas pruebas de recuperación han realizado en el último año?

5.1.4 Soporte al desastre Múltiple / Regional

- ¿Cuáles son las alternativas del servicio ofertado ante desastres regionales, simultáneos o múltiples, cuando más de un cliente invoca una declaración de contingencia?
- ¿Que otro hardware adicional puede estar disponible en el momento de desastre?

5.1.5 Metodología y soporte de pruebas

- Proveer una descripción del modelo de pruebas y soporte estándar durante las pruebas.
- ¿Cuál es su política de solicitud y cancelación de pruebas?
- Nuestra empresa esta planificando pruebas trimestrales del esquema de contingencia, ¿esta periodicidad es compatible con el servicio a ofertar?

5.1.6 Referencias

Cada oferente deberá proveer un mínimo de 3 (tres) referencias de clientes, que actualmente estén bajo contrato de recuperación, preferentemente en plataforma
IBM S/390, y con capacidades de respaldo equivalentes a las solicitadas; indicando en cada caso los alcances de la solución de respaldo implementada.

5.1.7 Datos Financieros

Deberá incluir aquí toda la información financiera que considere pertinente y que permita evaluar su condición financiera, incluyendo los dos últimos balances anuales.

5.1.8 Staff y Servicios

- Indicar la cantidad de personas de soporte cuya presencia en el sitio de recuperación estarán disponible en pruebas y recuperaciones.
- Describir el área de soporte a usuarios finales disponible para nuestro personal en pruebas y desastre.
- Indicar la experiencia de su staff de soporte.
- Especificar si está en condiciones de ofrecer, en forma complementaria a la solución de respaldo, un servicio de desarrollo de Plan de Recuperación y opcionalmente, de Análisis de Riesgos.
- Qué servicios se proveen como parte del contrato estándar, y qué servicios están disponibles en forma opcional.

5.1.9 Configuración de recuperación

El proveedor deberá detallar el hardware propuesto para la solución de recuperación y proveer una comparación línea por línea entre la configuración ofrecida y la configuración de producción actual de nuestra empresa.

Es importante detallar, en caso de contar con ello, la capacidad de incrementar el equipamiento de respaldo en al menos un 50% superior a lo solicitado, para absorber crecimientos imprevistos en la configuración de producción.

Si un requerimiento específico no pudiese ser cubierto, se deberá explicar porqué y, de ser posible, ofrecer una solución alternativa. Se deberá también ofrecer el detalle de los servicios opcionales disponibles.

5.1.10 Políticas del proveedor

Definir los procedimientos de alerta y declaración de desastre.

5.1.11 Términos y Condiciones

- Especificar las previsiones para el upgrade de la configuración de recuperación durante el plazo de vigencia del contrato.
- Establecer si nuestra organización o una tercera parte independiente pueded auditar el servicio contratado.
- Adjuntar un modelo de contrato que regiría los términos y condiciones del servicio.

5.1.12 Especificaciones de las instalaciones de recuperación

- Proveer una lista con las ubicaciones de los Centros de Recuperación del proveedor, locales y regionales, dedicados exclusivamente a servicios de recuperación.
- Indicar los sitios que podrían estar disponibles localmente para el servicio ofrecido y cuál es el recomendado para nuestra organización.

5.1.13 Telecomunicaciones

- Se deberá contemplar dar acceso al "carrier" de comunicaciones seleccionado por nuestra empresa para la conexión de su red a la configuración de respaldo.
- Detallar qué configuración de comunicaciones de respaldo estará disponible, listando las unidades de control de comunicaciones y su electrónica complementaria (routers, switches, etc.) para el conexionado de los vínculos.
- Establecer que la red de telecomunicaciones para recuperación será contratada por nuestra empresa.

5.1.14 Acceso / Ocupación

El proveedor deberá brindar acceso a las instalaciones de recuperación a partir de 1 (una) hora de declarado en forma telefónica y por el personal autorizado el desastre. En el término de las siguientes 6 (seis) horas se perfeccionará esta declaración por medio de un documento firmado por ambas partes.

5.1.15 Infraestructura de las instalaciones

- Detalle del sistema de detección y supresión de incendio de las instalaciones de recuperación propuestas.
- Detalle del sistema de seguridad y del staff de seguridad provisto en las instalaciones de recuperación propuestas.
- Detalle del equipamiento de soporte ambiental de las instalaciones de recuperación propuestas:
- UPS´s, Generadores, etc.

5.1.16 Transporte / Facilidades

- En caso de contar con ello, detallar si proveerá transporte desde y hacia las instalaciones de recuperación propuestas.
- Proveer los detalles relativos a las facilidades para comidas y refrigerios para el personal de nuestra empresa en el Centro de Recuperación.

5.1.17 Información Adicional

Se deberá incluir cualquier información adicional que se considere relevante y de ayuda para nuestra organización durante el proceso de revisión. Esta información debería limitarse a lo que el proveedor considere pertinente a la respuesta, y que no haya sido solicitada por este documento. (literatura de marketing, soporte adicional ofrecido, servicios opcionales, etc.)

5.2 Análisis del Sistema de Almacenamiento

En virtud de la criticidad del negocio y de la necesidad de contar con los sistemas operando dentro del menor tiempo posible, después da haberse declarado una emergencia que impida el normal funcionamiento del Centro de Cómputos principal, puede ser necesario contar con que los datos se encuentren espejados en un centro alternativo.

Dada la cantidad y diversidad de propuestas que podrían postularse como alternativa de solución, es necesario realizar un relevamiento de cada una de ellas, para poder determinar cual es la que mejor cubre las necesidades de la organización.

Se deberá evaluar:

- La capacidad de evolución que tiene el producto.
- El impacto que provocaría la elección de la solución en la operación normal del Centro de Principal de Procesamiento.
- El impacto que se produciría en las pruebas de Centro de Procesamiento Alternativo.
- El alcance del soporte técnico del proveedor.
- La experiencia del proveedor en el mercado de almacenamiento (storage).

5.2.1 Evaluación de la capacidad de Evolución

Se medirá cual es el impacto que podría tener en la solución las constantes evoluciones que se presentan desde el punto de vista tecnológico.
Es necesario asegurar que la infraestructura elegida irá adoptando los avances que se fueran produciendo y que su implementación provoque el mínimo impacto en el plan de continuidad del negocio.
Se evaluará como han ido evolucionando las arquitecturas a través de esos avances tecnológicos, como se ha comportado la convivencia entre

dispositivos de diferentes generaciones y la capacidad de conectar nuevos servidores, de distintas plataformas y de distintos proveedores .

Un punto de vital importancia es el de poder determinar cuales son las posibilidades de adaptación de la infraestructura seleccionada a los nuevos requerimientos de negocios. Asegurar el crecimiento (implementación de nuevas soluciones, almacenamiento de grandes volúmenes de imágenes, almacenamiento de mayor cantidad de datos como resultado de fusiones o adquisiciones, conexión a mayor cantidad de servidores, etc.) a la velocidad en que el negocio lo requiera, sin afectar los procesos productivos y los planes de Disaster Recovery vigentes

5.2.2 Impacto de la solución en la operación de los dispositivos

En este punto se debe considerar el grado de rapidez y complejidad que requiera la activación de los dispositivos en el sitio remoto en caso de que ocurra alguna situación de desastre, asegurándose la rápida recuperación de los sistemas productivos ante el evento de cualquier falla, ya sea humana o ambiental

Para ello se evaluará el grado de automatización que los dispositivos soportan, si en caso de perderse la comunicación entre los servidores y los dispositivos de almacenamiento (desastre parcial), permite switchear automáticamente a los dispositivos remotos y continuar con la ejecución de los sistemas que tienen sus datos espejados sin demoras y si en caso de ocurrir un desastre total, si los datos espejados en el sitio remoto podrán ser accedidos por los servidores de contingencia sin necesidad de ejecutar redefiniciones en los sistemas operativos.
Que ofrezca la posibilidad de configurar, controlar, monitorear la actividad, diagnosticar problemas de performance y resolver automáticamente esos problemas.

Debe asegurarse que tengan la capacidad de garantizar los SLAs acordados aún en situaciones de contingencia, es decir que garantice ofrecer los mismos niveles de servicio ante una situación de contingencia

Otra alternativa a plantear en este aspecto es la capacidad de poder definir distintos niveles de servicio de acuerdo a la criticidad de las aplicaciones, la posibilidad de hacer copias remotas de datos con distintos criterios y frecuencias, de acuerdo a los niveles de importancia de los datos.

Es importante definir si permite mantener distintos modos de sincronismo en forma concurrente de acuerdo a la criticidad de cada archivo y si la comunicación entre los dispositivos puede efectuarse a cualquier distancia usando diferentes vías, si el espejado se bidireccional, lo cual provee mayor flexibilidad y si la resincronización es incremental, esto es que solo serán transmitidas las pistas que hayan sido modificadas, con lo que se ahorra mucho tiempo.

Todas las definiciones de discos a espejar, arranque y suspensión de las copias, y activación de los volúmenes espejo, deben poder monitorearse a través de herramientas de uso simple de forma que permita controlar los cambios que se produzcan, tanto durante la operación normal como en situación de contingencia manteniendo los niveles de seguridad adecuados

Otro aspecto que se debe considerar es la capacidad de integración con soluciones de backups de terceros, con el objeto de mejorar dicha prestación utilizado la facilidad de invocar software de la solución de almacenamiento de datos durante la ejecución de los mismo minimizando el impacto que tienen los backups a los procesos productivos, manteniendo operativos los sistemas mientras se ejecutan procesos administrativos.

Es recomendable que pueda efectuar rápidamente copias locales o remotas de volúmenes lógicos, con el objetivo de poderlas usar para otros procesos sin detener la producción y que puedan mantenerse múltiples copias

continuamente sincronizadas con cada volumen productivo mientras sea necesario, permitiendo que la vuelta atrás o las resincronizaciones pueden hacerse por volumen lógico completo o en forma diferencial (sólo las pistas modificadas)

5.2.3 Impacto de las pruebas de Disaster Recovery

En este punto se debe medir la capacidad de realización de pruebas en el Centro de Procesamientos Alternativo sin afectar la ejecución de las aplicaciones en el Centro de Procesamiento Principal, es decir, la posibilidad de hacer pruebas con la facilidad y frecuencia que sean necesarias según los requerimientos del negocio y también poder establecer cuál es el grado de simplificación de esos procesos de prueba.

Para que la realización de las pruebas no interrumpa el normal desenvolvimento de los procesos productivos y sin que se corran riesgos de perdidas de información es aconsejable que las copias en los dispositivos remotos de los volúmenes espejados permitan arrancar un sistema alternativo que utilice estas copias, de modo que no sea necesario suspender el espejado de datos mientras se prueba el plan de Disaster Recovery, de forma tal que en caso de tener que repetir las pruebas, sólo haría falta resincronizar los volúmenes que correspondieran

5.2.4 Alcance del soporte del proveedor

La idea que se debe tener sobre lo que es un buen soporte no debería quedarse en los servicios que brinda el proveedor ante una falla, sino que también se deberían evaluar la posibilidad que tiene de detectar y prevenir problemas técnicos en forma automática, sin afectar los procesos productivos y cual es su capacidad de realizar mantenimiento proactivo

Todos los componentes deberían ser testeados continuamente por el microcódigo que se ejecuta en ellos para detectar posibles errore y ante una eventual falla en el dispositivo lo reporte al instante y el componente comprometido deberá ser aislado y reemplazado automáticamente por el redundante asociado.

En caso de que la falla se detecte en un canal que conecta al dispositivo con un servidor, automáticamente se deberán rutear las operaciones de entrada y salida de datos a un paso alternativo.

Ante la eventualidad de falta de alimentación eléctrica, se deberán activar las baterías que permitan apagar las unidades en forma ordenada.

5.2.5 Experiencia del proveedor en el mercado de storage

En base al el reconocimiento que obtenga del mercado en cuanto a la calidad, funcionalidad y tiempo promedio de fallas de los productos, se medirá la capacidad pueda llegar a tener el proveedor para alcanzar y mantener los más altos índices de calidad de los productos.

Dentro de los puntos a considerar se evaluará si se dedica exclusivamente al diseño, fabricación y comercialización de productos de hardware, software y servicio de almacenamiento de datos y también si realiza inversiones constantes en laboratorios de conectividad donde se pruebe el 100% de los productos antes de ser entregados a los clientes.

Es deseable que pueda demostrar experiencia en soluciones de almacenamiento en el mundo, comprobando que la tecnología que el proveedor ofrece está siendo utilizada en soluciones de almacenamiento en las empresas de similares características y volúmenes de datos.

5.3 Presencia en la región:

Es deseable que el proveedor posea oficinas comerciales y técnicas propias en la región. Puede darse el caso que ante un problema del cliente, los equipos cuentan con la característica de call-home, que le permita efectuar una llamada al soporte técnico en una casa matriz fuera del pais y desde allí se analiza la solución del problema, pero debe contar con personal idóneo que se haga presente en forma directa en la instalación del cliente en caso de ser necesario.

6. Conclusiones

Hoy en día, con el grado de avance e influencia que ha tenido la Tecnología en las Empresas y la velocidad con que se desarrollan los negocios, se hace impensado que una de ellas pueda sobrevivir ante un evento que deje fuera de servicio o impida el normal funcionamiento de su Centro de Procesamiento Principal.

La tecnología brinda elementos de alta disponibilidad en sus componentes y el objetivo principal, entonces, radica en maximizar el tiempo en que los sistemas y los Centro de Cómputos estén disponibles, estén en línea y sean tolerantes a fallas, aunque existan restricciones que lo hagan difícil de cumplir.

Este incremento en el uso de la tecnología trae aparejado otro serio inconveniente, que es el incremento en el número de amenazas dirigidas contra la infraestructura crítica de la organización, por lo que una estrategia de seguridad se torna esencial e imprescindible para proteger la información vital y para poder asegurar la continuidad de las operaciones.

La integridad, confidencialidad, confiabilidad y disponibilidad de la información solo puede ser garantizada adoptando los mecanismos adecuados de seguridad en la organización por lo que resulta necesario establecer políticas y procedimientos de seguridad efectivos que disminuyan los riesgos de que se produzca un escape, alteración o destrucción de datos que sean de vital importancia para la organización.

Debe ser una premisa dentro de una empresa el proteger los recursos informáticos del daño, la alteración, el robo y la pérdida, enmarcado en un "metaobjetivo" que es el de mantener la continuidad de los procesos organizacionales que soportan los sistemas de información.

Por ello resulta imprescindible que las empresas cuenten con un Plan de Contingencia y con un Plan de Continuidad del Negocio, máxime teniendo en

cuenta, el aumento de la exposición al riesgo que implica la cada vez mayor integración y globalización de los Sistemas Informáticos.

Tanto el Plan de Contingencia, como la instalación de un Plan de Continuidad del Negocio, deben estar enmarcados dentro del modelo de seguridad informática y deben estar basados en las Políticas que la organización ha determinado como parte de su operación. Dichas Políticas deben ser periódicamente revisadas y actualizadas, debidamente divulgadas para garantizar el conocimiento de ellas por parte de todos los miembros de la organización. Deben contar con el apoyo total de las Gerencias de la Organización, contar con suficientes recursos para la implementación y un equipo de personas dedicadas a esta función, estos aspectos son básicos para lograr los objetivos buscados.

Las Políticas y los Planes de Contingencia deben estar acordes a las circunstancias del negocio, deben ser premisas no negociables.

El modelo de seguridad debe ser capaz de identificar y priorizar amenazas y planificar respuestas apropiadas para:

- Evaluar las vulnerabilidades de la organización
- Evaluar puntos de referencia existentes comparando con las mejores prácticas
- Revisar los Planes de Respuesta a Emergencias
- Dar prioridad a los planes de acción basados en efectividad, eficiencia y sustentabilidad
- Proteger, para asegurar la infraestructura critica y los procesos de las amenazas, tanto de pérdidas o daños, como de desastres, accidentes o ataques:
    - Definir políticas y asignar responsabilidades para la implementación de la seguridad
    - Extremar medidas para controlar el acceso a sitios que impliquen amenazas

- Educar a los empleados sobre políticas de seguridad y sus responsabilidades
- Monitorear los procesos para identificar amenazas
- Desarrollar protocolos de monitoreo para la detección de amenazas y ataques
- Recolectar y analizar la información sobre infracciones y anomalías
- Implementar planes de respuesta para diferentes tipos de amenazas y ataques

7. Recomendaciones

El objetivo principal que debe tener un Plan de Contingencias es el de ayudar a garantizar la continuidad del negocio y para su construcción se recomienda dividir las tareas en 5 etapas:

- Evaluación
- Planificación
- Prueba de viabilidad
- Ejecución
- Recuperación

Las tres primeras etapas hacen referencia al componente preventivo, mientras que las últimas a la ejecución del plan, una vez que ha ocurrido el siniestro.

7.1 Etapa de Evaluación

7.1.1 Constitución del grupo de desarrollo del plan.

Este grupo debe estar liderado por un responsable del plan y formado por los líderes de las áreas que se desean cubrir con dicho plan. Su elaboración ha de desarrollarse con la continua supervisión por parte de la dirección ya que durante la elaboración y/o ejecución de éste, deberán comprometerse recursos y aprobarse procedimientos especiales que requieran un nivel de autorización superior.

7.1.2 Identificación de las funciones críticas.

Consiste en identificar aquellos elementos de la empresa o funciones que puedan ser críticos ante cualquier eventualidad o desastre y jerarquizarlos por orden de importancia dentro de la organización.

7.1.3 Definición y documentación de los posibles escenarios con los que podemos encontrarnos para cada elemento o función crítica.

Puede tratarse de problemas en el hardware, software de base, de telecomunicaciones, software de aplicación propio o provisto por terceros, etc.

También deben incluirse en esta categoría los siniestros provocados por incendios, una utilización indebida de medios magnéticos de resguardo o back up o cualquier otro daño de origen físico que pudiera provocar la pérdida masiva de información. También incluir en este apartado todos aquellos problemas asociados con la carencia de fuentes de energía y de telecomunicaciones.

7.1.4. Análisis del impacto del desastre en cada función crítica.

Consiste en realizar un análisis del impacto de cada problema sobre cada una de las funciones críticas de la organización, teniendo en cuenta las siguientes prioridades:

- Evitar pérdidas de vida.
- Satisfacer las necesidades básicas.
- Reanudar las operaciones lo antes posible.
- Lograr las conexiones con los principales clientes y proveedores
- Mantener la confianza en la empresa.

Una correcta cuantificación del impacto económico de cada problema ayudará a una correcta selección de la solución alternativa.

7.1.5 Definición de los niveles mínimos de servicio.

Se trata de definir los mínimos niveles de servicio aceptables para cada problema que se pueda plantear. Es importante que dicho nivel se consensúe con cada uno de los responsables de las áreas que puedan verse afectadas.

7.1.6 Identificación de las alternativas de solución.

Se deberán identificarse las soluciones alternativas para cada uno de los problemas previsibles. Para ello se puede considerar:

- Implementar procesos manuales.
- Contratar las tareas críticas con terceros.
- Diferir la tarea crítica por un tiempo determinado.
- Otra medida que permita continuar las operaciones.

7.1.7 Evaluación de la relación costo/beneficio de cada alternativa.

De cada alternativa identificada en el punto anterior y sobre la base del impacto económico de cada problema, deberá determinarse la mejor solución desde el punto de vista costo/beneficio para cada proceso crítico y su tiempo de elaboración con un nivel de servicio que satisfaga el nivel mínimo

7.2 Etapa de Planificación

7.2.1. Documentación del plan de contingencia.

Es necesario documentar el plan, cuyo contenido mínimo será:

- Objetivo del plan.
- Modo de ejecución.
- Tiempo de duración. Recursos necesarios.
- Evento a partir del cual se pondrá en marcha el plan.
- Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades.

7.2.2. Validación del plan de contingencia.

El plan debe ser validado por los responsables de las áreas involucradas. También es necesario tener en cuenta las posibles consecuencias jurídicas que pudiesen derivarse de las actuaciones contempladas.

7.3 Etapa de Pruebas de viabilidad

7.3.1. Definir y documentar las pruebas del plan

Es necesario definir las pruebas del plan y el personal y recursos necesarios para su realización. Dichas pruebas deber ser correctamente planificadas y documentadas para lograr el éxito de las mismas.

7.3.2. Obtener los recursos necesarios para las pruebas

Deben obtenerse los recursos para las pruebas, ya sean recursos físicos o mano de obra para realizarlas.

7.3.3. Ejecutar las pruebas y documentarlas

Consiste en realizar las pruebas pertinentes para intentar valorar el impacto real de un posible problema dentro de los escenarios establecidos como posibles.

La capacitación del equipo de contingencia y su participación en pruebas son fundamentales para poner en evidencia posibles carencias del plan.

Es necesario documentar las pruebas para su aprobación por parte de las áreas implicadas.

7.3.4. Actualizar el plan de contingencia de acuerdo a los resultados obtenidos en las pruebas

Será necesario realimentar el plan de acuerdo a los resultados obtenidos en las pruebas.

Hay que tener en cuenta que el plan de contingencia general o de continuidad de operaciones de la empresa contiene los planes de contingencia específicos para cada problema definido. Los distintos planes deben integrarse en un todo, considerando las posibles relaciones mutuas

7.4 Etapa de Ejecución

En esta fase hay que tener muy presente que el plan no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la empresa.

7.5 Etapa de Recuperación

Los datos afectados por el siniestro que pudiesen haber quedado desactualizados o corruptos, deben corregirse usando los procedimientos ya definidos.

En general, la reiniciación del proceso normal no implica la cancelación del alternativo, salvo que deban utilizarse los mismos recursos. Si esto no es así, durante cierto tiempo, los procesos deberían ejecutarse en paralelo para asegurar que la reiniciación de la operación normal es correcta y, ante cualquier defecto, continuar con el de contingencia.

Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar éste ante futuras nuevas eventualidades

Como una conclusión final, el hecho de preparar, desarrollar e implementar un plan de contingencia que nos permita seguir con el normal desenvolvimiento de la empresa ante un desastre, no implica un reconocimiento de la ineficiencia en la gestión, sino todo lo contrario, supone un importante avance a la hora de superar todas aquellas situaciones que puedan provocar importantes perdidas derivadas de la paralización del negocio durante un periodo.

La seguridad informática es un campo que requiere investigación permanente, actitud proactiva y generar una cultura organizacional que simpatice por la seguridad como parte de la función de la organización. Tiene un costo, pero la inseguridad tiene un costo mayor.

8. Bibliografía

a) "Alta disponibilidad", artículo técnico. Autor: José Camilo Daccach. IBM, marzo 2004.

b) "Tips para una plan de contingencia", artículo técnico. IBM, Octubre de 2003.

c) "Planes de Contingencia", artículo técnico. Hispasecurity, Diciembre de 2000.

d) "Servicios de Continuidad y Recuperación del Negocio", IBM Technology DAY, septiembre de 2002.

e) "Business Recovery Options", IBM On Demand World, mayo de 2003.

Anexo "A" - PLIEGO DE LICITACION

SERVICIO DE RECUPERACION EN CASO DE CONTINGENCIA EN EL CENTRO DE PROCESAMIENTO

I. BASES Y CONDICIONES DE LA LICITACION

1. OBJETO Y CARACTERISTICAS DE LA LICITACION

1.1. OBJETO DEL LLAMADO

La Empresa llama a Licitación Pública para contratar un servicio de recuperación en caso de contingencia en su Centro de Procesamiento.

1.2. ACEPTACION DEL PLIEGO

La presentación de la oferta implica el conocimiento y la aceptación del pliego licitatorio.

1.3. CONSULTAS

Se deja expresamente aclarado que toda consulta, aclaración u observación, relacionada con el pliego, deberá formularse por escrito a la Oficina de Licitaciones de Servicios, para lo cual previamente se deberá adquirir el pliego. Las consultas o aclaraciones podrán realizarse con una antelación de 15 días corridos a ala fecha de apertura

La Empresa dará respuesta a las mismas igualmente por escrito, haciendo llegar copia a todos los potenciales oferentes registrados, a fin de preservar el principio de igualdad de información. Las respuestas a las consultas y las aclaraciones que la Empresa emita serán parte integrante del pliego y, consecuentemente, deberán ser presentadas debidamente suscriptas con la oferta.

La Empresa se reserva la facultad de formular aclaraciones al pliego, sin que deba mediar una consulta expresa de algún interesado.

2. CONDICIONES PARA LA PRESENTACION Y EVALUACION DE OFERTA

2.1. LICITANTES CALIFICADOS

Estarán habilitados para participar en esta licitación las personas físicas y jurídicas nacionales dedicadas a la provisión de servicios de recuperación ante contingencias en Centros de Cómputos que acrediten al solo juicio de la Empresa, suficiente capacidad económico/financiera y técnica.

2.1.1. SOCIEDADES

Deberá indefectiblemente tratarse de una sociedad comprendida en los términos de la Ley N° 19.550 de Sociedades Comerciales y sus modificaciones. No serán consideradas aquellas empresas cuyo objeto no contemple la realización de los servicios cuya provisión forma el objeto de la presente licitación.

2.2. DOMICILIO LEGAL DEL OFERENTE

Es requisito indispensable que el domicilio legal se fije en el ámbito de la Provincia de Buenos Aires, sometiéndose expresamente a la jurisdicción de los Tribunales de la Provincia de Buenos Aires.

2.3. REPRESENTANTE TECNICO

El oferente designará un REPRESENTANTE TECNICO, que asumirá su representación en todo contacto que, por razones de índole técnica referidas a la contratación de que se trata, deba efectuarse entre la Empresa y el

adjudicatario. La Empresa se reserva el derecho de solicitar la designación de otro representante cuando a su solo juicio el mismo no reúna el perfil necesario

para esta contratación. Se consignará el nombre completo, clave única de identificación tributaria o documento nacional de identidad y curriculum vitae de la persona que actuará como representante técnico titular de la propuesta. En caso de reemplazo por cualquier circunstancia, la empresa deberá comunicarlo la Empresa con 10 días de anticipación; la Empresa se reserva el derecho de su aceptación. (VER PUNTO 1 CAPITULO III CONDICIONES ESPECIALES)

2.4. ACLARACION DE LOS DOCUMENTOS DE LICITACION

A los efectos de la presentación de ofertas, la información suministrada en este llamado deberá ser considerada como no exhaustiva. Por lo tanto, los oferentes podrán solicitar todas las informaciones adicionales que juzgaren necesarias.

El adjudicatario no podrá invocar, a ningún efecto, el desconocimiento de aspectos operativos no expuestos en este llamado, cuando los mismos revistan el carácter de condicionantes de la calidad del servicio ofrecido.

2. 5. FINALIDAD Y DESEMPEÑO DE LA SOLUCION OFRECIDA

La empresa especifica el propósito general del servicio requerido, por lo que el oferente obligatoriamente deberá ofertar una solución cuya performance permita el cumplimiento de los tiempos y formas que la operativa que la Empresa requiere. Esta especificación se refiere a los elementos de plataforma informática (procesamiento de datos), las comunicaciones y el software de explotación asociado.

2.6. DOCUMENTOS DE LICITACION

En los documentos del pliego constan las características técnicas del servicio que se requiere, los procedimientos de licitación y las condiciones contractuales.

En caso de discrepancia entre los documentos de licitación, prevalecerá el orden siguiente:

Listado de bienes y servicios.
Especificaciones técnicas.
Condiciones especiales.
Condiciones generales.
Bases de la licitación.

2.7. PRESENTACION DE OFERTAS

El oferente deberá presentar un sobre principal cerrado, el cual no deberá estar individualizado más allá del número de expediente, número de licitación pública, fecha y hora de apertura cuyo contenido será el siguiente:

ANTECEDENTES DEL OFERENTE
PROPUESTA TECNICA
OFERTA ECONOMICA (Planilla de Cotización Anexo "A")
GARANTIA DE OFERTA
TODA OTRA DOCUMENTACION SOLICITADA EN EL
PLIEGO o QUE EL OFERENTE CONSIDERE NECESARIA
PARA LA EVALUACION DE L A OFERTA

Las cotizaciones serán irrevocables e incondicionadas. Los participantes presentarán la oferta en base a su propia evaluación. No podrán efectuar

reclamo alguno por inexactitud o ausencia de cualquier información y por cualquier causa.

La oferta será presentada por original y duplicado. Se deberá identificar claramente el original y la copia.

La Empresa no reconocerá costo adicional ni gasto alguno en que incurran los oferentes como consecuencia de su presentación al acto licitatorio, ni por materiales, ni por documentación presentada con motivo de sus ofertas.

2.8. FORMATO DE PRESENTACION DE OFERTAS

Los oferentes deberán presentar el sobre, observando que su presentación se ajuste a las formalidades que se detallan a continuación:

La documentación deberá estar compilada en el mismo orden que el desarrollado en el punto 3, INDICANDO TAXATIVAMENTE MEDIANTE SEPARADOR, A QUE PUNTO E INCISO DEL PLIEGO BRINDA RESPUESTA, a fin de individualizar fehacientemente la documentación aportada.

La documentación original y copia, individualizando esta última, deberá estar independientemente foliada en forma correlativa y en el mismo orden, con indicación en la última foja de que se trata del último folio agregado.

Cada oferta contendrá en su primera foja un índice donde se informe el número de foja en que se encuentra la documentación requerida.

El licitante deberá presentar la respuesta al capítulo V - ESPECIFICACIONES TECNICAS, por escrito y en soporte electrónico. Será opción del licitante presentar el soporte electrónico en CD ROM o en disquetes de 3.5", requerir sobre la misma toda la información adicional que estime necesaria para la evaluación de la propuesta.

En caso de diferencias o discrepancias entre la oferta presentada por escrito y la oferta presentada en soporte electrónico, prevalecerá el contenido del documento escrito (original). El licitante presentará tanto el original, la copia y el soporte electrónico antes de la hora fijada para el acto de apertura.

Toda la documentación deberá hallarse firmada por el oferente o su representante debidamente autorizado con poder suficiente, y el representante técnico, como constancia del conocimiento y aceptación de todas las cláusulas. La autorización para ambos representantes deberá constar por escrito adjunto a la oferta.

La oferta no deberá contener textos entre líneas, raspaduras ni tachaduras salvo cuando fuere necesario para corregir errores del licitante, en cuyo caso las correcciones deberán ser inicializadas por la persona o personas que firmen la oferta.

2.9. IDIOMA DE LA OFERTA

Las propuestas deberán estar redactadas obligatoriamente en idioma castellano, incluyendo toda la documentación.

3. CONTENIDO DE LA OFERTA

3.1. INFORMACION

Toda información requerida debe considerarse como básica, sin perjuicio del mayor abundamiento para mejor comprensión y evaluación de las ofertas.

Formarán parte de la presentación de la oferta la información indicada en los siguientes puntos:

3.2. DOCUMENTOS QUE ESTABLEZCAN LA ELEGIBILIDAD DEL LICITANTE

Acreditación de existencia a través de Estatuto Social o Contrato, debidamente actualizado a la fecha de apertura, en copias autenticadas por Escribano Público Nacional, acompañando las transformaciones, aumentos de capital, fusiones que sufriera la Sociedad a través del tiempo, debidamente inscriptos en la Inspección General de Justicia o donde legalmente corresponda.

Designación e información requerida respecto del representante técnico

Estados contables de la proponente correspondientes a los dos últimos ejercicios cerrados.

La presentación de dichos estados habrá de efectuarse de acuerdo a las normas técnico-contables usuales, con dictamen por Contador Público y legalizados por el respectivo Consejo Profesional.

A tales efectos se entenderá por Estados Contables:

Balance General (o Estado de Situación Patrimonial).
Estado de Resultados (o Estado de Ganancias y Pérdidas).
Estado de Evolución de Patrimonio Neto.
Estado de Origen y Aplicación de Fondos (Estado de Evolución de la Situación Financiera).
Notas de los Estados Contables.

Respecto de los Estados Contables correspondientes a los dos últimos ejercicios a la fecha de apertura de la presente licitación, la Empresa se reserva el derecho de solicitar la presentación del último balance, cuya obligación legal de aprobación se encuentre vigente al momento de realizar el análisis del riesgo de contratación, previo a la adjudicación.

Una copia del Pliego y texto del Decreto Ley enunciado en el punto 1.2 - NORMAS APLICABLES, así como también toda aclaración realizada por la Empresa y/o las respuestas a las consultas efectuadas por la empresa, según lo establecido en el punto 1.4 - CONSULTAS, debidamente suscriptos por el OFERENTE y su REPRESENTANTE TECNICO en todas sus hojas como constancia del conocimiento y aceptación de todas sus cláusulas.

Los oferentes deberán declarar expresamente que aceptan las disposiciones y cláusulas de este pliego y las que se apliquen subsidiariamente, de acuerdo con la reglamentación pertinente. No se considerarán ofertas que condicionen o modifiquen dichas disposiciones o cláusulas.

Constancia autenticada por Escribano Público que avale la vigencia de cobertura, en materia de riesgo de trabajo (A.R.T.) y Seguros de Vida Obligatorio sobre el personal que posee a la fecha de apertura de la licitación, junto con el respectivo comprobante de pago al día.

Fotocopia de calificadora de riesgo (sólo si se posee este tipo de calificación).

Acta de asamblea aprobatoria del último estado contable presentado (en caso de sociedad anónima)

Certificado Fiscal para contratar, vigente a la fecha de apertura de la licitación.

Fotocopia de última liquidación del IMPUESTO A LAS GANANCIAS.

Fotocopia de los Formularios 931-AFIP (APORTES Y CONTRIBUCIONES SOCIALES) y de los formularios 731 – AFIP (IVA) de los últimos tres meses vencidos.

Informe de ventas posteriores al cierre de balance con certificación emitida por Contador Público con firma Legalizada por el Consejo Profesional de Ciencias Económicas.

DOCUMENTOS PROBATORIOS DE CONFORMIDAD CON LA LICITACION

Declaración jurada de sometimiento unilateral e irrevocable efectuada por el oferente a los términos y condiciones que rigen para esta licitación, y que posee pleno conocimiento y consentimiento de las características y condiciones del servicio. Consecuentemente no podrá efectuar reclamos fundados en su ignorancia respecto de las condiciones requeridas una vez efectuada la apertura de la licitación, durante la ejecución del contrato o a la finalización del mismo.

El oferente acepta desde ya que la Empresa se reserve el derecho de requerirle en cualquier momento todos los elementos y/o aclaraciones que, a su sólo juicio, estime conveniente a fin de evaluar su continuidad en el proceso.

3.4 DOCUMENTACION TECNICA

Documentación aportada por el oferente para evaluar las características técnicas y funcionales del servicio ofrecido.

CRONOGRAMA TENTATIVO DE ACTIVIDADES detallándose tareas, fechas y responsables para cada actividad que deberá realizar el adjudicatario, acorde con el punto 1 - PLAZO DE INICIO DEL SERVICIO del capítulo II - CONDICIONES GENERALES.

Detalle exhaustivo de la propuesta con toda la documentación solicitada en el capítulo V - ESPECIFICACIONES TECNICAS.

3.5 GARANTIA DE OFERTA

PAGARE DE GARANTIA. Las ofertas deberán ser afianzadas por el proponente con un importe no menor al 5% de la misma.

Se aceptarán cotizaciones en moneda nacional o dólares estadounidenses, debiéndose presentar como garantía de oferta pagaré a la vista extendido en PESOS

3.6. MONEDA EN QUE PODRAN EXPRESARSE LAS OFERTAS

Se aceptarán cotizaciones únicamente en moneda nacional.

3.7. PLANILLA DE COTIZACION

Los oferentes deberán presentar un análisis de precios detallando los rubros de la composición de la oferta, indicativo de su estructura de costos.

La oferta económica deberá contener exclusivamente la cotización de acuerdo con los requerimientos especificados en el formulario del Anexo A - PLANILLA DE COTIZACION, no aceptándose otros cargos de cualquier naturaleza que los que estén expresamente indicados en la oferta económica.

La oferta económica deberá contener el valor cotizado por la totalidad del servicio a prestar, la Empresa no abonará gastos de traslados, viáticos etc. que pudieran existir, los que serán a cargo del adjudicatario.
La cotización deberá realizarse:

Por el servicio solicitado para un contrato por 36 meses con pago anual adelantado

El adjudicatario deberá presentar una garantía adicional, por el 100 % del monto abonado en forma adelantada.

3.7.1. OFERTA ALTERNATIVA

A partir de las características mínimas del servicio requerido, los oferentes, podrán formular propuestas alternativas con su consecuente cotización,

reservándose la Empresa a su sólo criterio la facultad de aceptar o no la misma.

3.8. PRECIOS DE LA OFERTA

Importes cotizados en moneda nacional. Transcurridos 90 días corridos computados a partir del comienzo del plazo para cumplir con las obligaciones contractuales, si sobreviniere un desequilibrio importante en las prestaciones, la parte perjudicada podrá solicitar su renegociación, fundada en pautas concretas, objetivas y oficiales referidas a los precios y/o costos que mayor relación tuvieren con el objeto de la contratación.

Para iniciar la negociaciones la Empresa requerirá exclusivamente a Organismos Oficiales la información necesaria, y podrá tener en cuenta la estructura de costo presentada en cumplimiento del punto 3.7 Planilla de Cotización del pliego.

La decisión final quedará a exclusivo criterio la Empresa y se aplicará, en su caso, desde la fecha de interposición de la solicitud de renegociación y sólo para aquellas prestaciones que, según contrato, estuvieren previstas para cumplirse a partir de la fecha de la citada solicitud y que no se encontraren en mora. La resolución que se dicte deberá ser notificada inmediatamente.
Si la Empresa resolviera rechazar totalmente la renegociación, la otra parte, luego de transcurridos noventa días corridos de la decisión, podrá solicitar la rescisión del contrato sin aplicación de penalidades, ni indemnización de daños y perjuicios.

La Empresa no otorgará dicha rescisión si hubiere establecido que con información oficial, no se ha producido desequilibrio en las prestaciones.

Los precios cotizados (unitarios y totales) deberán incluir, indefectiblemente, el importe correspondiente a la alícuota del IVA.

4. PROCESO LICITATORIO

4.1 APERTURA DE LAS OFERTAS

En lugar, día y hora fijados, un funcionario competente la Empresa, en acto formal, abrirá los sobres recibidos, en presencia de los representantes de los licitantes que deseen asistir.

En el acto de apertura de la licitación se labrará un acta, dejando constancia de los nombres de los oferentes y ofertas presentadas, suscribiendo la misma los integrantes de la mesa de apertura y asistentes que así lo deseen.

4.2 EXAMEN PRELIMINAR

En el acto de apertura la Empresa llevará a cabo una revisión preliminar de las ofertas presentadas, observando que se encuentren en orden y no comprendidas dentro de las causales que la ley determina para su rechazo en dicho acto, punto 4.3.1 - RECHAZO DE LA OFERTA EN EL ACTO DE APERTURA.

RECHAZO DE LA OFERTA

4.3.1. RECHAZO DE LA OFERTA EN EL ACTO DE APERTURA

Serán causales de rechazo de la oferta en el acto de apertura, automáticamente y sin más trámite, las siguientes:

La no inclusión de la Planilla de Cotización (Anexo "A")

La falta de presentación de la documentación exigida en el punto 3.5 - GARANTIA DE OFERTA o que dicha garantía observe una insuficiencia en un porcentaje superior al 10 % (Art. 38 del Reglamento de Contrataciones).

4.3.2 RECHAZO DE LA OFERTA A POSTERIORI DEL ACTO DE APERTURA

Serán causales de rechazo de la oferta a posteriori del acto de apertura las siguientes:

La no presentación dentro de los 4 (cuatro) días hábiles siguientes a la fecha en que el oferente recepcione la solicitud cursada por la Empresa, donde se le indique que debe presentar la documentación omitida y que ha sido requerida en el punto 3.2. - DOCUMENTOS QUE ESTABLEZCAN LA ELEGIBILIDAD DEL LICITANTE. Si vencido el plazo de intimación previsto el oferente no cumplimentara tal requerimiento, la Empresa se reserva el derecho de aceptar la propuesta si los antecedentes aportados, a su sólo criterio, le permitieran el conocimiento fehaciente del estado de situación del proponente.

La no regularización de la insuficiencia de la garantía dentro de los 2 (dos) días hábiles posteriores al acto de apertura, cuando dicha insuficiencia sea igual o menor al 10% del monto correspondiente, ello en virtud de lo previsto en el Art. 38 del Reglamento de Contrataciones N° 3300/72

4.4. METODOLOGIA DE EVALUACION

Una vez definido las ofertas que se ajusten esencialmente a los documentos de licitación, se procederá a la evaluación de los siguientes conceptos, en forma independiente:

Elegibilidad de los oferentes.
Capacidad técnica y antecedentes de los oferentes
Evaluación de características técnicas mínimas obligatorias.
Evaluación económica.

ELEGIBILIDAD DE LOS OFERENTES. A fin de evaluar la elegibilidad de los oferentes la Empresa realizará la revisión de la documentación presentada en la oferta así como también del estado de situación patrimonial, contable y financiero de cada oferente.

En el examen preliminar la Empresa determinará si cada oferta se ajusta formalmente a los documentos de licitación. A tal fin las ofertas deben cumplir con todas las estipulaciones y condiciones establecidas en dicho pliego, reservándose el derecho, cuando a su juicio se trate de temas subsanables, de requerir a los oferentes la documentación adicional necesaria que permita adecuarla a los requerimientos del pliego.

La Empresa procederá a analizar la documentación presentada por cada oferente a fin de determinar la elegibilidad de los mismos, pudiendo descartar sin más trámites a aquellos oferentes que por los antecedentes aportados, evaluaciones realizadas y/o averiguaciones practicadas, no resulten satisfactorias, sin que ello dé lugar a reclamo alguno.

La Empresa se reserva el derecho de solicitar la documentación adicional que estime pertinente y efectuar las constataciones y requerimientos adicionales que estime necesarios para evaluar la idoneidad del oferente, quedando la firma obligada a su presentación.

Asimismo, la Empresa podrá realizar auditoría contable de los oferentes "in situ" cuando así lo estime conveniente. La Empresa se reserva el derecho de inspeccionar las empresas oferentes para verificar el equipamiento con que

cuentan, su capacidad técnica y demás cumplimiento de las condiciones establecidas. La negativa a la realización de las mismas por parte de la

empresa o la no presentación de documentación requerida según el párrafo anterior, facultará al la Empresa para desestimar la oferta.

La Empresa tendrá la facultad de verificar la información consignada en la oferta en caso de considerarlo necesario.

CAPACIDAD TECNICA Y ANTECEDENTES DE LOS OFERENTES

Luego de evaluada la condición de elegibilidad de cada oferente se procederá a la revisión y valoración de las condiciones relacionadas con la capacidad técnica y los antecedentes en servicios de características técnicas similares a las licitadas.
La Empresa se reserva la facultad de verificar lo consignado, en caso de considerarlo necesario.

EVALUACION DE CARACTERISTICAS TECNICAS MINIMAS

A fin de evaluar las características mínimas se completará la matriz incluida en el pliego y se determinará si las diferentes ofertas cumplen con las especificaciones técnicas mínimas requeridas.

EVALUACION ECONOMICA

Evaluación económica: Para determinar el precio total de cada oferta y realizar la comparación económica se utilizará, según corresponda, el calculo del Valor Actual Neto. El comprador definirá la tasa de cálculo a utilizar para la evaluación del Valor Actual Neto previo al acto de apertura establecido.

4.5. ERRORES ARITMETICOS

Una vez realizada la apertura de sobres, la Empresa examinará las ofertas para determinar si hay errores de cálculo.

Los errores aritméticos serán rectificados de la siguiente manera.

Si existiere una discrepancia entre el precio unitario y el precio total que resulte de multiplicar el precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido.

Si existiere una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras.

El precio total rectificado de esta manera será considerado, a continuación, como el precio básico de la oferta.

4.6 PREADJUDICACION

El oferente que reúna condiciones de elegibilidad, antecedentes, capacidad técnica suficiente y que el servicio ofertado cumpla con las características técnicas requeridas, y su cotización económica sea la de menor precio de acuerdo a la metodología de evaluación descripta en el presente pliego, resultará preadjudicatario.

La preadjudicación se dará a conocer a través de medio fehaciente.

4.7. TOMA DE VISTA DE ACTUACIONES

En cuanto a los pedidos de vista de actuaciones, en tanto esta institución facilita el inmediato acceso a los duplicados de las ofertas, sólo serán autorizados si se hubieren incorporado al expediente nuevos actos administrativos de índole decisoria que modificaran su estado de tramitación y siempre que ello no implique una demora innecesaria, en cuyo caso quedarán disponibles luego de la respectiva preadjudicación.

4.8. IMPUGNACIONES

Respecto de las impugnaciones y / u observaciones que los oferentes realizaren con relación a las ofertas y / o actos administrativos adoptados por la Empresa, sólo serán consideradas previo depósito de la garantía a la que se refiere este punto. Respecto de aquellas que se realizaren luego de las vistas de las ofertas a posteriori del acto de apertura la Empresa se reserva el derecho de analizar las mismas en la etapa de evaluación de ofertas, tomando el oferente impugnante conocimiento de lo resuelto al tomar vista de la preadjudicación.

Toda impugnación y observación que se efectúe respecto de ofertas presentadas para la presente licitación, deberá ser explicitada en forma clara y objetiva acompañando, en tanto se tratare de temas o situaciones no

comprobables a través de los elementos administrativos obrantes en esta Empresa, las suficientes constancias o certificaciones - en original o en copias debidamente autenticadas- que respalden las manifestaciones y/o denuncias que se concreten.

Cuando se vinculen con el incumplimiento de obligaciones fiscales, previsionales y/o sociales, la presentante deberá adjuntar además copia de la denuncia de tal circunstancia ante los organismos competentes respectivos.

Consecuentemente, no se dará curso - ni contendrán entidad documental - a la interposición de reclamos que no reúnan tales requisitos.

No obstante ello, la Empresa se reserva el derecho de realizar las gestiones o verificaciones que estime menester conducentes a la finalidad licitatoria perseguida, así como de hacer cargo a los presentantes de los gastos administrativos producidos en caso de comprobarse falsedad en sus denuncias o intenciones ilícitas destinadas a la obtención de ventajas comparativas en su beneficio.

Los oferentes que formulen impugnaciones y/o planteen recursos deberán constituir una garantía de $ 100.000.-

Esta podrá ser integrada en efectivo o títulos públicos a su valor de cotización, lo que deberá cumplirse al momento de efectuar la presentación.

Si la impugnación y/o recurso fuere aceptado y resuelto favorablemente por la Empresa, la garantía será reintegrada al impugnante.

Las presentaciones que resulten infundadas y cuya interpretación, a criterio de la Empresa, no tenga más que una finalidad dilatoria del procedimiento, dará derecho a ésta a resolver el rechazo y la consecuente pérdida del 100% de la garantía y a la aplicación de las penalidades que pudieran caberle en el registro de proveedores la Empresa.

El recurso no se considerará infundado - aún cuando fuere desestimado - si a criterio de la Empresa, la cuestión planteada se hubiese basado en cuestiones dudosas de derecho y/o en hechos o aspectos técnicos de compleja interpretación, casos en los que la Empresa podrá reintegrar el 50% del monto de la garantía integrada.

En ninguno de los supuestos precitados el impugnante tendrá derecho a reclamar intereses resarcitorios.

4.9. ADJUDICACION

La adjudicación se dará a conocer a través de medio fehaciente perfeccionándose el acuerdo de voluntades en la fecha de expedición del citado despacho por parte de la Empresa

Sin perjuicio de lo arriba establecido, la Orden de Compra respectiva deberá ser retirada de la Oficina de Licitaciones de Servicios, a partir de los 3 (tres) días hábiles de recibida dicha comunicación, previo reemplazo de la garantía de oferta, conforme a lo establecido en el articulo 5.3 PAGARE DE GARANTIA del presente pliego.

En cualquier circunstancia, la Empresa se reserva el derecho de adjudicar, según convenga a sus intereses, la oferta más conveniente en función de su exclusiva evaluación.

En caso de existir una única oferta la Empresa se reserva el derecho dé proceder a su adjudicación siempre que la misma cumpla con las características mínimas requeridas, y la cotización resulte conveniente a sus intereses.-

No podrá resultar adjudicatario ningún oferente que reconozca con anterioridad al acto de apertura o con posterioridad al mismo, algún litigio pendiente con la Empresa.

Asimismo la Empresa se reserva el derecho de rechazar todas o alguna de las ofertas presentadas, así como también de anular o dejar sin efecto el llamado a licitación, cuando a su sólo juicio no se satisfagan sus intereses, o existieran razones de mérito, oportunidad o conveniencia, sin que ello genere derecho a reclamo alguno por parte de los oferentes.

4.10. MANTENIMIENTO DE LA OFERTA

El mantenimiento de oferta será de 45 (cuarenta y cinco) días corridos a partir de la fecha de apertura de la presente licitación.

Para el caso que no pudiera resolverse la adjudicación dentro del plazo de mantenimiento de la oferta estipulado en el párrafo anterior, el mismo quedará

automáticamente prorrogado por el término de 15 días, salvo manifestación expresa del oferente, efectuada con anterioridad al vencimiento.

Si dentro de este nuevo plazo continuara la imposibilidad de tomar decisiones, las ofertas se renovarán automáticamente cada (30) treinta días corridos, excepto que la empresa oferente manifieste por escrito su decisión de no continuar en el concurso con una antelación de 15 (quince) días corridos a la fecha que opere el último vencimiento.

En caso de mediar impugnación, el plazo de mantenimiento de las propuestas presentadas se considerará automáticamente ampliado en 15 (quince) días corridos, el que se adicionará al plazo de mantenimiento de oferta vigente al momento de la impugnación

5. OBLIGACIONES DE LOS ADJUDICATARIOS

5.1. RETIRO DE LA ORDEN DE COMPRA

La orden de compra deberá retirarse en la Oficina de Contratación de Licitaciones Servicios a partir de los 3 (tres) días de recibida la comunicación de la adjudicación.

5.2. CONSTANCIA DE PAGO DE OBLIGACION PREVISIONAL

La constancia de pago de la última obligación previsional vencida deberá presentarse al momento de formalizar la contratación mediante la Orden de Compra respectiva.

5.3. PAGARE DE GARANTIA

Reemplazar el pagaré de garantía de oferta

5.4. FACTURAS

Consignar indefectiblemente en las facturas que presente para el cobro:
Número de la Orden de Compra y el número de Proveedor, que será suministrado en el cuerpo de dicha Orden.
Acompañar con cada factura que se presente una fotocopia de la Orden de Compra correspondiente a esa facturación.

5.5. AUDITORIAS

Facultar a la Empresa a realizar auditorías "in situ" en cualquier momento durante toda la vigencia del contrato.

5.6. RESPONSABILIDADES

Asumir en forma única y exclusiva la responsabilidad por las obligaciones que contraiga con sus subcontratistas, quedando exenta la Empresa de todo tipo de responsabilidad ante los mismos, como así también ante terceros por los daños que el hecho de éstos les produjere.

5.7. INCUMPLIMIENTOS

En todos los casos el adjudicatario será responsable cuando por incumplimiento, la Empresa deba encomendar la ejecución total o parcial del contrato a un tercero, y será a su cargo la diferencia de precios que pudiera resultar.

5.8. RESPONSABILIDAD ANTE TERCEROS

El adjudicatario asumirá todas las responsabilidades y obligaciones inherentes y derivadas de la relación laboral con su personal, inclusive las referidas a la aplicación de medidas de seguridad establecidas por autoridad competente, con todas sus consecuencias y serán por su exclusiva cuenta todos los actos que ocasione la ejecución del servicio, incluyendo jornales, aguinaldo, aportes, indemnizaciones pertinentes por accidentes de trabajo, muerte, incapacidad total o parcial, despido ya sea justificado o no, vacaciones, preaviso, salarios caídos, obligaciones previsionales o cualquier otra que corresponda o que se encuentre establecida actualmente o que se fije en el futuro, sin exclusión alguna, igual responsabilidad asume el adjudicatario respecto a los subcontratados que eventualmente pudiera contratar.
La Empresa podrá en cualquier momento requerir se presente la documentación que acredite su cumplimiento.
Asimismo, asume totalmente la responsabilidad que por accidente de su personal y/o terceros pudieren sobrevenir como consecuencia de las tareas realizadas, no siendo en consecuencia la Empresa responsable solidariamente en virtud de los daños derivados de los mismos, y en razón que su actividad es específicamente financiera y no vinculada con el rubro aquí tratado como actividad habitual y con fines de lucro

Será responsable de los daños y perjuicios que su personal provoque a la Empresa y/o a terceros, de toda rotura, deterioro o daño de elementos, siendo responsabilidad del mismo la reposición de lo dañado o deteriorado según

corresponda, sin perjuicio de la aplicación de las penalidades que pudiesen corresponder.

Correrá por cuenta y cargo exclusivo de la adjudicataria el seguro de responsabilidad civil contra terceros, por daños que pudieran ocasionar los equipos a las personas y/o a sus bienes y el seguro servicios prestados.

II CONDICIONES GENERALES

1. PLAZO DE INICIO DEL SERVICIO

El oferente deberá fijar la fecha de disponibilidad del inicio del servicio, la cual no podrá exceder de 90 días a partir de la comunicación fehaciente de la adjudicación.
Todo retraso en el plazo de inicio previsto, que no esté debidamente autorizado permitirá a la Empresa la aplicación de las penalidades previstas en el apartado 12.3 - POR INCUMPLIMIENTO DEL CRONOGRAMA DE IMPLEMENTACION del capítulo II – CONDICIONES GENERALES.

2. DOCUMENTACION DE INCIO DEL SERVICIO

Una vez notificado en forma fehaciente la adjudicación del servicio el adjudicatario iniciará el mismo.

Para documentar el inicio del servicio se labrará un acta en donde las partes dejarán constancia del inicio de la vigencia del servicio.

3. CONSIDERACIONES DEL INICIO DEL SERVICIO

Será total responsabilidad del adjudicatario poner a disposición de la Empresa todo lo necesario para la correcta provisión del servicio. La Empresa no asumirá ningún costo de transporte o mano de obra que se requiera para el inicio del servicio.

4. INICIO DEL SERVICIO

El inicio del servicio se realizará cuando, a solo juicio de la Empresa, se cumplan las condiciones técnicas contractuales y operativas establecidas en el presente pliego.-

El inicio del servicio se realizará cuando haya sido cumplido satisfactoriamente la prueba inicial realizada por la Empresa.-

La Empresa notificará al adjudicatario en forma fehaciente el inicio del servicio.

5. PRUEBAS Y COMPROBACIONES

La Empresa contempla realizar pruebas trimestrales del servicio durante la vigencia del contrato
El Adjudicatario deberá poner a disposición de la Empresa, cuando éste lo requiera, todo lo necesario de manera de verificar que el servicio ofrecido responde a los requerimientos del presente pliego. Este requerimiento se extiende a terceros que puedan requerir inspecciones o auditorias del servicio en cuestión
Las mencionadas pruebas se coordinarán con anticipación con la Empresa.-
Dichas pruebas no implicarán reconocimiento de gasto por parte de la Empresa y se realizarán de acuerdo a una programación que se adjuntará a la notificación cursada al oferente para la presentación del equipo.

6. CAPACIDAD TECNICA Y ANTECEDENTES DE LOS OFERENTES Y BIENES OFRECIDOS

La empresas oferentes deberán incluir en su cotización todo elemento de hardware y/o software no descripto en las especificaciones técnicas mínimas pero necesario para asegurar la correcta provisión del servicio requerido.

Se deberán adjuntar folletos e información técnica de los bienes que forman parte del servicio ofrecido y en todos los casos no se admitirá especificar simplemente "según pliego" o "equivalente", como identificación del equipamiento ofrecido.
Los detalles técnicos de los bienes que forman parte del servicio ofrecido se podrán mostrar en páginas WEB.

Los adjudicatarios deberán garantizar que cualquier elemento de hardware y/o software que provean, se encuentre libre de errores relacionados con el manejo de fechas. No se aceptarán equipos a los que se deba instalar adicionales de software para posibilitar la compatibilidad solicitada.
Los siguientes requisitos serán considerados mínimos indispensables al momento de la evaluación de las ofertas presentadas.

Experiencia de la empresa: Se requiere la siguiente información:

Venta de los servicios en Argentina.
Venta de los servicios en el mundo
Ventas en proceso indicando posible fecha de inicio y finalización y grado de avance (porcentual) de los servicios.

La Empresa tendrá la facultad de solicitar la verificación de lo consignado, en caso de considerarlo necesario, debiendo el oferente facilitar la verificación.
Capacidad técnica: Se requiere la siguiente información a fin de evaluar la capacidad técnica de las empresas oferentes para la provisión del servicio requerido.
Matriz de experiencia del personal (especialistas y técnicos), indicando, en columnas separadas:

Nombre de la persona
antigüedad en la empresa.

meses de experiencia en el área

meses de experiencia en instalación, mantenimiento y soporte técnico, de los bienes ofrecidos.

curriculum vitae.

7. GARANTIA DE CONTRATO

La garantía de contrato, reviste en el presente pliego carácter de cláusula penal. El adjudicatario responderá por la suma total garantizada aún cuando el incumplimiento fuere parcial, teniendo como único límite el monto del perjuicio sufrido por la Empresa.
Lo previsto en el párrafo anterior no limita la responsabilidad del adjudicatario, con relación al cual la Empresa hace reserva de derechos por el total de los daños que se le causaren con el incumplimiento

8. GARANTIA DEL SERVICIO

A partir de la fecha de inicio del servicio el adjudicatario garantizará, toda reparación, reemplazo de componentes, adecuación o cambio de los bienes que formen parte del servicio propuesto sin cargo para la Empresa.

9. REQUERIMIENTOS MÍNIMOS SOBRE LA GARANTÍA

El servicio ofrecido deberá garantizar el cumplimiento de los tiempos descriptos a continuación:
Tiempo de disponibilidad para su uso de toda la infraestructura necesaria para continuar con el procesamiento del Centro Principal contado a partir de la declaración formal de la contingencia. Este tiempo se ha establecido en 2 horas.
Tiempo de reestablecimiento del servicio en el caso de existir caídas mientras la Empresa se encuentre procesando en el Centro Alternativo, es de 2 horas.

10. VIGENCIA DEL CONTRATO

Los oferentes realizarán sus propuestas por la prestación del servicio durante un período de 36 meses, con opción por parte de la Empresa a renovarlo por 2

(dos) períodos anuales en las mismas condiciones y precios pactados, o aplicando la consecuente rebaja según corresponda de acuerdo a precios

referenciales del mercado. El plazo comenzará a regir a partir de la adjudicación

Si a la finalización del contrato la Empresa requiriese mantener la continuidad de los servicios, hasta su total reemplazo, la adjudicataria deberá continuar brindando los mismos el tiempo necesario, el cual no podrá exceder de 12 meses, para permitir una transición ordenada. En cada caso, se reconocerá la parte proporcional del valor del servicio hasta el día de comunicación de baja.

11. RESCISION DEL CONTRATO

Transcurrido el período de 36 meses de la contratación si se optara por ejercer la opción de renovarlo, la Empresa se reserva el derecho de cancelar en cualquier momento la contratación sin invocar causa alguna, con un aviso previo de 30 (treinta días) corridos, comunicándolo por medio fehaciente, y sin derecho del adjudicatario a percibir indemnización alguna.

La Empresa, sin perjuicio de la aplicación de las penalidades que correspondieren y sin necesidad de interpelación previa judicial o extrajudicial ni de cumplimentar plazo alguno de preaviso, se reserva el derecho de rescindir el contrato, en cualquier momento, cuando mediare por parte de la adjudicataria incumplimiento o insatisfacción verificada de las obligaciones impuestas por el pliego, siempre que habiendo sido debidamente intimada, no hubiere atendido el requerimiento.

La Empresa se reserva el derecho de revocar el acto administrativo y rescindir el contrato que se celebre, cuando luego de la adjudicación comprobare administrativamente constancias indubitables de la existencia de graves irregularidades que hubiesen posibilitado la obtención indebida de ventajas por parte del proveedor, y/o existencia de vicios conocidos por el proveedor particular que afectaran originariamente el contrato y fueren susceptibles de acarrear su nulidad. Igual derecho se reserva para el supuesto que se comprobare fehacientemente que el contrato hubiese sido celebrado mediante

prevaricato, cohecho, violencia o cualquier otra maquinación fraudulenta que dé lugar a acción penal o fuere objeto de condena penal.

En los supuestos enunciados la revocación del acto administrativo y rescisión del contrato no dará lugar a reclamo ni indemnización alguna por parte del adjudicatario.

12. SERVICIOS CONEXOS

El Proveedor deberá prestar los servicios conexos indicados en Capítulo III - Condiciones Especiales., punto 2. La falta en la prestación de alguno de estos servicios establecidos será causal de rescisión del contrato, previa aplicación de las multas y/o penalidades correspondientes.

13. PENALIDADES POR INCUMPLIMIENTO

Todo incumplimiento de cláusulas contractuales puede dar lugar a sanciones que serán de dos clases, a saber: cargos y multas.

13.1. CARGOS

Cargo es una sanción compensatoria que impondrá la Empresa a la adjudicataria, estimada en dinero, que se descontará de las sumas que ésta tenga a percibir por servicios prestados o por cualquier otra causa.
Los cargos proceden en los casos descriptos a continuación.

13.1.1. POR INCUMPLIMIENTO EN EL TIEMPO DE DISPONIBILIDAD DE LA INFRAESTRUCTURA

Si ante un requerimiento de contingencia, el adjudicatario no cumple con el plazo máximo de puesta en disponibilidad de la infraestructura contratada, la Empresa aplicará un cargo correspondiente al 10% del servicio mensual contratado.

Asimismo, por cada hora de retraso en la puesta en disponibilidad de la infraestructura contratada, se aplicará un cargo del 10% del servicio mensual contratado.

POR DEMORA EN EL REESTABLECIMIENTO DEL SERVICIO ANTE UNA CAIDA

Si durante el plazo en que la Empresa utilice el Centro de Procesamiento Alternativo se produce la interrupción del servicio y éste sea reestablecido fuera del plazo máximo fijado, la Empresa aplicará un cargo del 10% del servicio mensual contratado.

Asimismo, por cada hora de retraso en la restitución, se aplicará un cargo del 10% del servicio mensual contratado.

13.2. MULTAS

Las multas serán aplicables por:

Mora en la disponibilidad de inicio del servicio adjudicado previsto en el contrato

Cualquier otro incumplimiento total o parcial del contrato

13.3. PERCEPCION DE CARGOS Y MULTAS

La percepción de los cargos y/o multas se hará efectiva, aún cuando no estuviere firme la resolución que impuso la sanción. Las sanciones impuestas por la Empresa a la adjudicataria serán descontadas automáticamente del primer crédito a su favor, provenga de esta contratación o de otras que estuvieren al cobro o en trámite en la Empresa, o, en su defecto, deberán ser efectivizadas dentro de los 3 (tres) días hábiles a partir de que la Empresa lo comunique por medio fehaciente.

Si con posterioridad se dejara sin efecto el cargo y/o la multa, se reintegrará el importe recibido dentro de los 8 (ocho) días hábiles siguientes contados a partir de la recepción de la factura pertinente por parte de la Empresa, sin que ello

genere al adjudicatario derecho alguno a la percepción de intereses, ni reclamo por daños en razón de la multa o cargo aplicados.

La reiteración en situaciones que generen la aplicación de cargos y/o multas, y/o la reiteración en el no pago de los mismos ante la intimación de la Empresa, facultará a esta última a rescindir el contrato por culpa de la adjudicataria.

14. DIVERGENCIAS CON EL ADJUDICATARIO

Cualquier divergencia que ocurra entre el adjudicatario y la Empresa, será resuelta por esta última sin perjuicio de la acción legal que pudiera corresponder al adjudicatario.
El adjudicatario en ningún momento podrá suspender por sí los trabajos en forma total o parcial, ya sea por causas de divergencias en trámite o por otras razones.

15. FORMA Y CONDICIONES DE PAGO

15.1. INICIO DE LOS PAGOS

Luego del inicio del servicio se generará una única facturación por el costo del servicio anual adelantado, la que comprenderá la totalidad de los servicios adjudicados y tareas realizadas. Los servicios deberán ser completos y contar con la conformidad pertinente de la Empresa.

15.2. FORMA DE PAGO

El pago se efectuará a los 10 (diez) días corridos de la fecha de presentación de la factura. Se deja establecido que el pago se hará efectivo indefectiblemente por medio de acreditación en cuenta corriente abierta a nombre del adjudicatario.

A tal efecto las facturas en cuestión deberán ser presentadas por triplicado en el Departamento de Ordenes de Pago.
Los importes que se coticen indefectiblemente deben incluir todos los impuestos que la oferente debiere tributar.

EN LAS FACTURAS DEBERAN CONSTAR INDEFECTIBLEMENTE LOS NUMEROS DE EXPEDIENTE, ORDEN DE COMPRA Y PROVEEDOR, QUE SERAN SUMINISTRADOS EN EL CUERPO DE DICHA ORDEN. La omisión de tales datos implicará la no recepción de las facturas por parte de la Empresa.

QUEDA EXPRESAMENTE PROHIBIDA LA CESION DE FACTURAS, CERTIFICADOS Y/O CUALQUIER OTRO TITULO DEL QUE EMERJA UN CREDITO A FAVOR DEL ADJUDICATARIO QUE DEBA SER ABONADO POR LA EMPRESA.
LOS MISMOS PODRAN SER CEDIDOS SOLO MEDIANTE CONFORMIDAD EXPRESA POR ESCRITO DE LA EMPRESA, LA QUE A SU SOLO ARBITRIO SE RESERVA LA FACULTAD DE SU AUTORIZACION. EN EL SUPUESTO DE OTORGAR LA CONFORMIDAD.

16. CONTENIDO DE LOS ANEXOS

ANEXO "B" - PLANILLA DE COTIZACION

El anexo "B" incluye la planilla de cotizaciones que los proveedores deberán completar en forma obligatoria a fin de presentar su cotización económica.

ANEXO "C" - FORMULARIO DE GARANTIA DE LA SOLUCION

El anexo "C" incluye el formulario de garantía de solución que los oferentes deberán conformar e incluir en sus ofertas según lo descripto en el capítulo II CONDICIONES GENERALES punto 8- GARANTIA DE LA SOLUCION.

III. CONDICIONES ESPECIALES

REPRESENTANTE TECNICO

El oferente designará un representante técnico cuyas responsabilidades incluyen :
Ser el contacto primario del adjudicatario con la Empresa.
Asumir responsabilidad general para administrar y coordinar la provisión de servicios.
Asumir su representación en contacto que, por razones de índole técnica referidas a la contratación de que se trata, deba efectuarse entre el adjudicatario y la Empresa

2. PRESTACION DE SERVICIOS CONEXOS

El adjudicatario deberá prestar los servicios que se describen a continuación:
Instalación y puesta en marcha de todos los bienes que formen parte del servicio provisto hasta quedar en correctas condiciones de funcionamiento.
Servicio de asistencia técnica en todo el período de prestación del servicio.

DISPONIBILIDAD DEL SERVICIO

El plazo para poner el servicio en condiciones de funcionamiento es de 90 días contados a partir de la fecha fehaciente de la adjudicación.
El tiempo de disponibilidad para el uso de toda la infraestructura necesaria para continuar con el procesamiento del Centro Principal contado a partir de la declaración formal de la contingencia se establece en 2 horas.
El tiempo establecido para el reestablecimiento, en caso de interrupción del servicio, del Centro de procesamiento Alternativo, durante el plazo en que la Empresa lo utilice, se establece en 2 horas.

ESPECIFICACION DE MARCAS

Se deja expresamente establecido que cuando se mencionan marcas, modelos y/o versiones, se hace al sólo efecto de indicar calidades mínimas de los bienes que forman parte del servicio propuesto pudiendo los oferentes proponer otras marcas y modelos de calidades equivalentes o superiores, quedando a criterio exclusivo de la Empresa determinar el grado de equivalencia del mismo.

IV. LISTADO DE BIENES Y SERVICIOS

A continuación se describe el listado de Bienes y Servicios incluidos en el presente pliego de licitación.

ITEM	DESCRIPCION
1	SERVICIO DE RECUPERACIÓN ANTE CONTINGENCIAS EN EL CENTRO DE PROCESAMIENTO PRINCIPAL.
	- CON CAPACIDAD DE ALMACENAMIENTO PROVISTA POR EL OFERENTE
	- CON CAPACIDAD DE ALMACENAMIENTO PROVISTA POR LA EMPRESA

V. ESPECIFICACIONES TECNICAS

1. OBJETIVO.

El presente documento contempla las necesidades básicas para la obtención de ofertas para la provisión de un servicio de recuperación ante contingencias en el centro de procesamiento principal de la Empresa. El mencionado servicio deberá permitir a la misma continuar con sus actividades de procesamiento central si se presentara un siniestro o contingencia.

Asimismo el Servicio de Recuperación ante contingencias incluirá la elaboración de un Plan General de Recuperación ante desastres que permita:

Reanudar en el menor tiempo posible las actividades del Centro de procesamiento.

Minimizar la cantidad de decisiones a tomar, atenuando la pérdida de información y su impacto comercial.

Organizar las tareas necesarias para reparar o reemplazar el área dañada en el menor tiempo posible.

Dar cumplimento en su totalidad a las normativas del Banco Central de la Republica Argentina que regulan el servicio informático, tomando como referencia la circular número A3198 y todas las relacionadas.

2. ALCANCE DEL SERVICIO.

Asegurar la continuidad del negocio de la Empesa en lo relativo a la tecnología de procesamiento y comunicaciones.

Recuperar la operatividad de procesamiento y de comunicaciones del Comprador, para el equipamiento y plataformas que se contemplen en el presente concurso de servicios y en los anexos que se agreguen durante la vigencia del convenio.

HIPOTESIS DE TRABAJO

El siguiente trabajo se desarrolla sobre la hipótesis de la existencia de una contingencia o desastre que torne inoperante el Centro de Procesamiento Principal de la Empresa.

SERVICIO SOLICITADO.

a) Centro de Procesamiento Alternativo.

El adjudicatario deberá poner a disposición de la Empresa un Centro de Procesamiento Alternativo que contemple el equipamiento mínimo necesario para continuar con las actividades ante la presencia de una contingencia en su Centro de Procesamiento Principal.

El centro alternativo deberá ofrecer equipamiento de procesamiento basado en Arquitectura OS/390. Además deberá contar con el equipamiento necesario para recibir las conexiones de los diferentes operadores de comunicaciones, que actualmente prestan servicio a la Empresa. Los operadores de comunicaciones que actualmente prestan servicio a la Empresa deberán implementar la capacidad de doble ruta de acceso: una al Centro de Procesamiento Principal y otra al Centro de Procesamiento Alternativo seleccionado.

El Centro de Procesamiento Alternativo deberá disponer de las instalaciones necesarias para albergar el personal de la Empresa que sea necesario para continuar la operatoria en el período de contingencia.
Para ello el proveedor deberá prever puestos de trabajo con sus correspondientes estaciones de trabajo para cada persona, conectadas con el equipamiento central en emulación IBM 3270. Dentro de estos puestos de trabajo deberán existir al menos 4 estaciones del tipo pantalla "boba" de la

línea IBM 3270, conectadas por medio de unidades de la familia IBM 3174, trabajando en modalidad local.

Adicionalmente estos puestos deberán contar con facilidades telefónicas hacia el exterior en algunos casos y mediante internos entre todas ellas.

Toda esta infraestructura deberá estar disponible para su uso, a partir de 2 (dos) horas de declarada formalmente la contingencia, situación que se adelantará por medio de una llamada telefónica al Centro de Procesamiento Alternativo y luego será perfeccionada según un acta a firmar por ambas partes.

b) Plan de Recuperación.

Se requiere la confección de un Plan de Recuperación ante desastres que garantice las operaciones de las aplicaciones críticas que actualmente se desarrollan en el Centro de Procesamiento Principal de la Empresa.
Los objetivos y alcances del mencionado Plan de Recuperación contemplan:
Reanudar en el menor tiempo posible el procesamiento informático.
Minimizar la cantidad de decisiones a tomar y por lo tanto atenuar la perdida de información, así como el impacto comercial sobre los clientes.
Organizar las tareas necesarias para reparar o reemplazar el área dañada en el menor tiempo posible.
Asegurar la continuidad del negocio.
Recuperar la operatividad del Centro de Procesamiento Principal y las comunicaciones correspondientes.
Proveer procedimientos para la recuperación efectiva de las tareas informáticas.

5. CARACTERÍSTICAS DEL CENTRO DE PROCESAMIENTO PRINCIPAL ACTUALMENTE INSTALADO

A los fines de brindar mayor información, se describe a continuación el equipamiento actualmente en uso en el Centro de Procesamiento Principal de la Empresa:

CPU: Se trata de una CPU IBM modelo 2064-103 de aproximadamente 647 MIPS, según las tablas de comparación de unidades centrales de procesamiento. Esta CPU cuenta con 8 GB de memoria principal, 3 procesadores y 50 canales de entrada / salida.

Esta unidad central de procesamiento esta dividida según el esquema de Particiones Lógicas o "LPAR ", según los siguientes porcentajes:
Partición de producción 50 % del procesador o sea 325 MIPS
Partición de desarrollo 40 % o sea 258 MIPS
El 10 % restante para la partición de test o sea 64 MIPS.

Storage o almacenamiento principal: Esta compuesto por una unidad EMC2 modelo 8730-036, equipada con 8 GB de memoria cache, configurada en Raid 5 el 75 % de su capacidad y en RAID 1 el 25 % restante. Cuenta con 911 dispositivos con una capacidad total de 3,146 TB.

Estos dispositivos están asignados de la siguiente forma: 2,282 TB para la arquitectura OS/390 y 0,864 TB para las plataformas de sistemas abiertos. (UNÍX)

Existe una segunda unidad EMC2 modelo 5430-018 configurada con 4 GB de memoria cache, en modalidad Raid 5 con una capacidad de almacenamiento de 0,703 TB, distribuidos en 0,527 TB para la arquitectura OS-390 y 0,176 TB para sistemas abiertos.

Medios Magnéticos removibles: El centro cuenta con una unidad IBM modelo 3590 configurada con cuatro bocas de procesamiento; una unidad IBM modelo 3490 con cuatro bocas y una unidad Storage-Teck modelo 4480 con dos bocas también.

Para el procesamiento de cintas abiertas cuenta con tres unidades Storage-Teck modelo 3420.

Sub sistema de Impresión: Para este rubro el centro cuenta con tres sistemas IBM System 4000, con compatibilidad AFP, que incluyen equipos de pre y post procesamiento del papel.

Además hay instaladas dos impresoras IBM modelo Infoprint 60 que trabajan con papel cortado.

Facilidades de comunicaciones: el Centro cuenta con equipos de comunicaciones marca IBM modelo 3745 con su expansión 3746 modelo 900 con capacidad de memoria de 16 MB.

El equipamiento se encuentra configurado con 100 líneas LIC tipo 1 V24 y 5 líneas LIC tipo 3 V35.

6. CARACTERÍSTICAS DEL SERVICIO REQUERIDO.

a) Tiempo de disponibilidad del Centro de Procesamiento Alternativo.
La efectiva utilización del Centro de Procesamiento Alternativo estará determinada por las características de la contingencia o desastres.
Los oferentes deberán presentar, en consecuencia, un servicio sin restricciones en cuanto al tiempo de utilización del Centro de Procesamiento Alternativo.

Las opciones cotizadas deberán contemplar una duración tal que le permita a la Empresa restablecer la operación normal de su Centro Principal.

b) Modalidad de abono

Tiempo de utilización del Centro de Procesamiento alternativo. Los oferentes deberán presentar un servicio con diferentes posibilidades en cuanto al tiempo de utilización del Centro de procesamiento Alternativo según se describe a continuación:

Servicio sin restricciones.
Servicio de 3 (tres) días anuales (acumulables).
Servicio de 5 (cinco) días anuales (acumulables).
Servicio de 10 (diez) días anuales (acumulables)

c) Inicio de Actividades.

El inicio del servicio relacionado con el punto 4.a) Centro de Procesamiento Alternativo , será independiente de la concreción del punto 4.b) Plan de Recuperación, respectivamente, pudiendo comenzar antes de la finalización de este último.

d) Etapas del Servicio Requerido.
Se ha estructurado el servicio requerido en función de la necesidades de la Empresa.
El servicio ofrecido permitirá que se implemente un esquema de espejado Remoto (Mirroring) de datos entre dos configuraciones de discos; una configuración ubicada en el Centro de Procesamiento Principal y otra en el Centro de Procesamiento Alternativo.
Esta actualización de datos entre el Centro de Procesamiento Principal y el Centro de Procesamiento Alternativo se hará por medio de herramientas de hardware y su software de control asociado, pero sin intervención del sistema operativo principal (OS/390)

Mientras no se disponga del vínculo de comunicaciones que conecte el Centro de Procesamiento Principal y el Centro de Procesamiento Alternativo y ante la ocurrencia de una contingencia, se hará presente personal de la Empresa en

el centro de Procesamiento Alternativo, con los medios magnéticos conteniendo la versión de la información necesaria para establecer una imagen del Centro de Procesamiento Principal, en el menor tiempo posible. Esta etapa durará hasta contar con vínculos de comunicaciones (fibras ópticas) entre el Centro de Procesamiento Principal y el Centro de procesamiento Alternativo.

7. CARACTERÍSTICAS DEL CENTRO DE PROCESAMIENTO ALTERNATIVO REQUERIDO POR LA EMPRESA.

A continuación se listan las características mínimas del equipamiento necesario, entendiendo que los valores de potencia a ofertar podrán ser mayores que los fijados en este documento, pero en ningún caso menores.

La configuración especificada deberá estar disponible en el plazo máximo de 2 (dos) horas, a partir de la declaración de la contingencia por parte del Comprador.

a) Unidad central de procesamiento:

CARACTERÍSTICAS	ESPECIFICACIÓN REQUERIDA	ESPECIFICACIÓN OFRECIDA	OBSERVACIÓN
Capacidad de procesamiento	500 MIP		
Memoria primaria	2 GB		
Memoria expandida	2 GB		
Adaptadores OSA Fast Ethernet	2		
Adaptador Giga Byte express	1		
Sistema Operativo			
Deberá poder procesar un sistema operativo Z/OS Release 1.1 con direccionamiento de 64 bits	SI		
En el caso de que el servicio ofrecido no contemple una CPU dedicada al procesamiento del Comprador, la arquitectura de procesamiento deberá estar basada en un esquema LPAR, con parámetros de definición de la partición, tal que los porcentajes de procesador y de memoria, respecto del total del equipo, aseguren la	SI		

CARACTERÍSTICAS	ESPECIFICACIÓN REQUERIDA	ESPECIFICACIÓN OFRECIDA	OBSERVACIÓN
continuidad del procesamiento del Centro de Procesamiento Principal actualmente instalado.			

b) Capacidad de almacenamiento:

b.1) La capacidad de almacenamiento más abajo especificada deberá ser cotizada en dos modalidades, a saber:

- El equipamiento de almacenamiento será ofrecido por el Adjudicatario como parte del servicio.

- El equipamiento de almacenamiento será provisto por la Empresa, y el Adjudicatario solo debe cotizar el soporte ambiental del mismo (housing). En esta opción el Adjudicatario deberá integrar bajo su responsabilidad este equipamiento con el resto de la arquitectura de procesamiento.

b.2) Características mínimas del almacenamiento:

CARACTERÍSTICAS	ESPECIFICACIÓN REQUERIDA	ESPECIFICACIÓN OFRECIDA	OBSERVACIONS
Capacidad de almacenamiento (sin contemplar el esquema de RAID 1, distribuido en	4,5 TB		

CARACTERÍSTICAS	ESPECIFICACIÓN REQUERIDA	ESPECIFICACIÓN OFRECIDA	OBSERVACIONS
direcciones de discos en emulación IBM modelo 3390-3)			
Considerando el esquema de "hot stand by" requerido para el almacenamiento, el equipamiento necesario para brindar la capacidad de almacenamiento requerida deberá ser de exclusivo uso para el Comprador.	SI		
La capacidad de almacenamiento deberá ser provista preferentemente por medio de unidades EMC2 idénticas a las instaladas en el Centro de Procesamiento Principal.	SI		
En el caso de ofrecer otra marca o modelo, del equipo de almacenamiento, deberá asegurar la facilidad de espejado remoto (Mirroring) con las unidades actualmente	SI		

CARACTERÍSTICAS	ESPECIFICACIÓN REQUERIDA	ESPECIFICACIÓN OFRECIDA	OBSERVACIONS
existentes en el Centro de Procesamiento Principal asegurando la total compatibilidad y transparencia entre ambos, fundamentalmente en lo relativo al esquema de alta disponibilidad de datos.			
Para la implementación del esquema "Hot Stand By" el Comprador proveerá vínculos (fibras ópticas) entre el Centro de Procesamiento Principal y el Centro de Procesamiento Alternativo.	SI		

c) Facilidades de comunicaciones.

CARACTERISTICAS	ESPECIFICACIÓN REQUERIDA	ESPECIFICACIÓN OFRECIDA	OBSERVACIÓN
Equipo de comunicaciones marca IBM modelo 3745 con su expansión 3746 modelo 900.	SI		
Memoria	16 MB		
Configurado con 100 líneas LIC tipo 1 V24 y 5 líneas LIC tipo 3 V35	SI		
Este equipamiento de comunicaciones idealmente debería estar dedicado a la Empresa, para poder asegurar los parámetros de performance requerida por el servicio on-line requerido por la Empresa.	SI		

Unidades para Medios Magnéticos Removibles.

CARACTERÍSTICAS	ESPECIFICACIÓN REQUERIDA	ESPECIFICACIÓN OFRECIDA	OBSERVACIÓN
Cantidad de unidades (4 bocas) de procesamiento de cartdriges modelo IBM 3590-E11 ó compatible.	2		
Cantidad de unidades (4 bocas) IBM modelo 3490 ó compatible.	2		
Cantidad de unidades de cinta abierta compatible con IBM modelo 3420-8.	2		
El equipamiento requerido deberá estar dedicado en forma exclusiva para la prestación del servicio requerido.	SI		
Se considera parte del servicio, la tarea de toma periódica (diaria) de copias de seguridad de los discos que residen en el Centro de Procesamiento Alternativo, a través de las unidades de cartdriges mas arriba especificadas.La ejecución	SI		

CARACTERÍSTICAS	ESPECIFICACIÓN REQUERIDA	ESPECIFICACIÓN OFRECIDA	OBSERVACIÓN
de la mencionada copia de seguridad se realizara en coordinación con el centro principal de Guanahani.			
Los medios magnéticos (cartdriges) serán provistos por el Comprador.	SI		
Los oferentes deberán detallar la modalidad operativa que instrumentarán para tal fin.	Especificar		

e) Sub-Sistema de Impresión.

Los oferentes deberán cotizar el equipamiento necesario a fin de brindar a la Empresa una capacidad de impresión que cubra los volúmenes de impresión que se consignan a continuación:

PERIODO DE TIEMPO	VOLUMEN
Diarios	Se imprimen 5.000.000 (cinco millones) de líneas por día, excepto los sábados y domingos
Mensuales	Una vez al mes se imprimen 32.000.000 de líneas, que se suman para ese día a las diarias. Durante el mes se imprimen adicionalmente 20.000.000 de líneas, correspondientes a los procesos de tarjeta de crédito.
Trimestrales	Una vez cada tres meses se imprimen 73.000.000 líneas, que se suman a las diarias y a las mensuales para el mes del proceso trimestral

f) Características generales del centro de procesamiento alternativo.

Los oferentes deberán detallar la ubicación del / los Centro (s) de Procesamiento Alternativo ofrecido, dedicados exclusivamente al servicio requerido.

Los oferentes deberán especificar cuales son los operadores de comunicaciones que tienen actualmente acceso al Centro de Procesamiento Alternativo.

Los oferentes deberán detallar la configuración de comunicaciones de respaldo que estará disponible, listando las unidades de control de comunicaciones y su electrónica complementaria (routers, switches, etc.) para la conexión de los vínculos de comunicaciones.

g) Infraestructura de las instalaciones.

Los oferentes deberán detallar el sistema de detección y supresión de incendio de las instalaciones del Centro de Procesamiento Alternativo.
Los oferentes deberán detallar el sistema de seguridad y el personal de seguridad provisto en las instalaciones del Centro de Procesamiento Alternativo.
Los oferentes deberán detallar el equipamiento de soporte ambiental de las instalaciones del Centro de Procesamiento Alternativo, en particular considerando lo siguiente:

Sistemas de Aire Acondicionado
UPS
Generadores
Etc.

h) Seguridad

Los oferentes deberán detallar los sistemas de seguridad tanto física como lógica de acceso a la información residente en el servicio propuesto.
Este detalle será de gran relevancia en la evaluación técnica de las propuestas a realizar, dado la confidencialidad de los datos depositados en las instalaciones del proveedor.

i) Capacidad de ampliación del centro de procesamiento alternativo

Los oferentes deberán considerar en su oferta que el Centro de Procesamiento Alternativo deberá reflejar el crecimiento en la capacidad de procesamiento del Centro de Procesamiento Principal.
Una vez por año, se realizará una reunión entre el Adjudicatario y la Empresa, para analizar el crecimiento de la capacidad de procesamiento en el Centro de

Procesamiento Principal y la consecuente adecuación de ésta, en el Centro de Procesamiento Alternativo.

Anexo "B" - PLANILLA DE COTIZACION

NOMBRE DEL OFERENTE _____

LICITACION N° _____

NOTA: Si bien las planillas de cotización del presente anexo contienen columnas para el valor mensual del servicio para los años 1º, 2º y 3º, queda a criterio del oferente ampliar el número de columnas según las variaciones del precio mensual que su propuesta contenga para el plazo de 36 meses considerado.

Los oferentes cotizarán:

Servicio sin restricciones

ITEM	DESCRIPCION	PRECIO ANUAL AÑO 1	PRECIO ANUAL AÑO 2	PRECIO ANUAL AÑO 3	PRECIO TOTAL PERIODO 36 MESES
1	Servicio de recuperación ante contingencias en el centro de procesamiento principal de la empresa				
	Con capacidad de almacenamiento provista por el oferente 4.5 tb				
	Con capacidad de almacenamiento provista por la empresa 4.5 tb				
	Con capacidad de almacenamiento provista por el oferente 6 tb				
	Con capacidad de almacenamiento provista por la empresa 6 tb				

b) Servicio de 3 (tres) días anuales (acumulables)

ITEM	DESCRIPCION	PRECIO ANUAL			PRECIO TOTAL PERIODO 36 MESES	PRECIO POR DIA ADICIONAL		
		AÑO 1	AÑO 2	AÑO 3		AÑO 1	AÑO 2	AÑO 3
1	Servicio de recuperación ante contingencias en el centro de procesamiento principal de la Empresa							
	Con capacidad de almacenamiento provista por el oferente 4.5 tb							
	Con capacidad de almacenamiento provista por la Empresa 4.5 tb							
	Con capacidad de almacenamiento provista por el oferente 6 tb							
	Con capacidad de							

ITEM	DESCRIPCION	PRECIO ANUAL			PRECIO TOTAL PERIODO 36 MESES	PRECIO POR DIA ADICIONAL		
		AÑO 1	AÑO 2	AÑO 3		AÑO 1	AÑO 2	AÑO 3
	almacenamiento provista por la Empresa 6 tb							

C) Servicio de 5 (cinco) días anuales (acumulables)

ITEM	DESCRIPCIÓN	PRECIO ANUAL			PRECIO TOTAL PERIODO 36 MESES	PRECIO POR DIA ADICIONAL		
		AÑO 1	AÑO 2	AÑO 3		AÑO 1	AÑO 2	AÑO 3
1	Servicio de recuperación ante contingencias en el centro de procesamiento principal de la Empresa							
	Con capacidad de almacenamiento provista por el oferente 4.5 tb							
	Con capacidad de almacenamiento provista por la Empresa 4.5 tb							
	Con capacidad de almacenamiento provista por el oferente 6 tb							
	Con capacidad de provista por la Empresa 6 tb							

d) Servicio de 10 (diez) días anuales (acumulables)

ITEM	DESCRIPCION	PRECIO ANUAL			PRECIO TOTAL PERIODO 36 MESES	PRECIO POR DIA ADICIONAL		
		AÑO 1	AÑO 2	AÑO 3		AÑO 1	AÑO 2	AÑO 3
1	Servicio de recuperación ante contingencias en el centro de procesamiento principal de la Empresa							
	Con capacidad de almacenamiento provista por el oferente 4.5 tb							
	Con capacidad de almacenamiento provista por la Empresa 4.5 tb							
	Con capacidad de almacenamiento provista por el oferente 6 tb							
	Con capacidad de provista por la Empresa 6 tb							

COTIZACION ALTERNATIVA

ITEM	DESCRIPCION	PRECIO UNICA VEZ	PRECIO MENSUAL	PRECIO TOTAL PERIODO 36 MESES
1	SERVICIO DE RECUPERACIÓN ANTE CONTINGENCIAS EN EL CENTRO DE PROCESAMIENTO PRINCIPAL.			
	CON CAPACIDAD DE ALMACENAMIENTO PROVISTA POR EL OFERENTE			
	CON CAPACIDAD DE ALMACENAMIENTO PROVISTA POR LA EMPRESA			

TODOS LOS PRECIOS DEBEN EXPRESARSE EN PESOS E INCLUIR EL IMPUESTO AL VALOR
AGREGADO IVA.

FIRMA DE OFERENTE_____

Anexo "C" - GARANTIA DE SOLUCION

Buenos Aires, _____

Sres. De La Empresa

Por la presente garantizo el funcionamiento de los equipos ofertados en esta propuesta desde el momento de la recepción definitiva por parte vuestra Empresa y durante toda la vigencia de la garantía.

Durante dicho lapso me comprometo a cumplir con el servicio de asistencia técnica y de mantenimiento según lo previsto en el pliego, sin cargos, ni gastos adicionales para la Empresa, reemplazando cualquier componente del herramental, que experimentare falla por causas no atribuibles al uso indebido, por uno de iguales o superiores características, asegurando la prestación ininterrumpida del servicio.

Sin más saludo a Uds. muy atentamente.

Anexo "D" - CIRCULAR 3198 (B.C.R.A.)

BANCO CENTRAL DE LA REPUBLICA ARGENTINA

COMUNICACIÓN "A" 3198	12/12/00

A LAS ENTIDADES FINANCIERAS:

Ref.: Circular RUNOR – 1 – 413
Requisitos operativos mínimos del área de sistemas
de información (SI) – Tecnología informática.
Texto ordenado

Nos dirigimos a Uds. para poner en su conocimiento el texto ordenado de las normas de referencia, en función de las disposiciones divulgadas oportunamente a través de las Comunicaciones "A" 2659, "A" 3149 y "B" 6776.

Saludamos a Uds. muy atentamente.

BANCO CENTRAL DE LA REPUBLICA ARGENTINA

Alfredo A. Besio
Gerente de Emisión Normas

Alejandro Henke
Subgerente General de Regulación y Régimen Informativo

Con copia a las cámaras electrónicas de compensación

B.C.R.A	TEXTO ORDENADO DE LAS NORMAS SOBRE . REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) - TECNOLOGÍA INFORMÁTICA

Índice

B.C.R.A	TEXTO ORDENADO DE LAS NORMAS SOBRE . REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) - TECNOLOGÍA INFORMÁTICA

Sección 6. Seguridad lógica.

6.1. Administración y control.
6.2. Política de seguridad informática.
6.3. Acceso y autenticación de los usuarios.
6.4. Mantenimiento de archivos de auditoria.
6.5. Restricción de acceso a utilitarios sensitivos.
6.6. Separación física del personal según sus funciones.
6.7. Puesta de programas "en producción".

Sección 7. Continuidad del procesamiento de datos.

7.1. Resguardo de la información.
7.2. Plan de contingencias.
7.3. Seguridad física y ambiental.

Sección 8. Teleprocesamiento y telecomunicaciones.

Sección 9. Sistemas aplicativos.

9.1. Documentación técnica.
9.2. Operaciones activas y pasivas.
9.3. Sistema de información de gestión.
9.4. Generación de información para el Banco Central de la República Argentina.

Sección 10. Sistema de transferencias de fondos (SWIFT, MEP, otros) y cámaras compensadoras electrónicas.

Sección 11. Cajeros automáticos, banca telefónica y "home banking".

11.1. Funcionamiento.
11.2. Apertura.
11.3. Transacciones.
11.4. Archivo de respaldo.
11.5. Clave de identificación del cliente.
11.6. Número de transacción.
11.7. Banca telefónica.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 1. Generalidades

.

Los procedimientos que deben llevarse a cabo para el desarrollo de la tarea y control de las áreas de sistemas de información, los cuales involucran al Directorio, Consejo de Administración o autoridad equivalente, Gerencia General, Gerencia de Sistemas de Información (SI) y personal de la entidad, deben estar diseñados para proveer un grado razonable de seguridad en relación con el logro de los objetivos y los recursos aplicados en los siguientes aspectos:

1.1. Eficacia.

La información y los procesos relacionados deben ser relevantes y pertinentes para el desarrollo de la actividad. Debe presentarse en forma correcta, coherente, completa y que pueda ser utilizada en forma oportuna.

1.2. Eficiencia.

El proceso de la información debe realizarse mediante una óptima utilización de los recursos.

1.3. Confidencialidad.

La información crítica o sensible debe ser protegida a fin de evitar su uso no autorizado.

1.4. Integridad.

Se refiere a la exactitud que la información debe tener, así como su validez acorde con las pautas fijadas por la entidad y regulaciones externas.

1.5. Disponibilidad.

Los recursos y la información deben estar disponibles en tiempo y forma, cuando sea requerida.

1.6. Cumplimiento.

Se refiere al cumplimiento de las normas internas y de todas las leyes y reglamentaciones a las que están sujetas las entidades financieras.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 1. Generalidades

1.7. Confiabilidad.

Los sistemas deben brindar información correcta para ser utilizada en la operatoria de la entidad, en la presentación de informes financieros a los usuarios internos y en su entrega al Banco Central de la Republica Argentina y demás organismos reguladores.

Todos estos aspectos deben ser aplicados a cada uno de los recursos intervinientes en los procesos de tecnología informática, tales como: datos, sistemas de aplicación, tecnología, instalaciones y personas.

Las secciones siguientes de la presente norma enumeran una serie de requisitos mínimos que las entidades (entidades financieras y cámaras de compensación de fondos) deberán cumplir, los que serán sometidos a supervisión por parte de la Superintendencia de Entidades Financieras y Cambiarias.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 2. Organización y control del área de sistemas de información.

2.1. Dependencia funcional.

Dentro de la estructura organizacional, el área de sistemas de información debe depender
funcionalmente de un nivel tal que permita garantizar su independencia de las áreas usuarias.

2.2. Delimitación de tareas.

El área debe presentar una clara delimitación de las tareas entre desarrollo y mantenimiento de sistemas, operaciones, soporte técnico y supervisión, de manera que garantice una adecuada segregación de funciones y no impida un control por oposición de intereses. Asimismo, deberá mantener una separación de funciones entre desarrollo y mantenimiento de sistemas y administración de bases de datos.

En las entidades con hasta 10 sucursales la función de soporte técnico podrá depender funcionalmente del sector de operaciones.

2.3. Plan de sistemas.

Debe existir un plan formal que permita una supervisión continua y directa de las tareas que
realizan los distintos sectores y que contenga un cronograma de las actividades del área, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante un período de un año.

Asimismo, debe existir un plan estratégico, que contenga los proyectos principales y los cronogramas de su implementación, para un período de por lo menos 3 años.

2.4. Controles y mantenimiento de archivos.

El control gerencial del área debe ser formal, manteniéndose en archivo - durante 2 años- los documentos escritos en los que los sectores informan a sus supervisores las distintas actividades realizadas, con el objeto de permitir un adecuado control del cumplimiento de las políticas, objetivos y planeamientos definidos por la gerencia.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 2. Organización y control del área de sistemas de información.

2.5. Autoridades responsables del área.

En las entidades con más de 10 sucursales deberá existir un Comité de Sistemas para el tratamiento institucional de políticas, objetivos y planeamiento del área de sistemas de información en el cual deben intervenir los máximos niveles directivos y/o gerenciales de las áreas que disponga la entidad, formalizando el contenido de las reuniones mediante actas, las que se deberán mantener archivadas durante un período de por lo menos 2 años.

Las entidades financieras deberán informar mediante nota dirigida a la Gerencia de Auditoria Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias, el nombre, dirección, cargo y teléfono de la máxima autoridad responsable del área, actualizando los cambios dentro de los 3 días hábiles de producidos. En caso de poseer un Comité de Sistemas, corresponderá designar a uno de sus integrantes para que sea registrado.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 3. Normativa y procedimientos de operación de sistemas y tecnología.

3.1. Estructura funcional.

Deben existir políticas generales, una clara definición de las misiones y funciones de todos los puestos de trabajo (responsabilidad, dependencia, funciones que supervisa, etc.), estándares y procedimientos escritos que sean la base de la planificación, el control y la evaluación gerencial del área.

3.2. Estándares.

Deben existir manuales con estándares de metodología para el diseño, desarrollo y mantenimiento de los sistemas aplicativos. Su aplicación regirá para todos los nuevos sistemas y para las modificaciones cuyos desarrollos sean posteriores a la fecha de la presente comunicación.

3.3. Documentación.

3.3.1. De las aplicaciones.

Debe existir documentación de los sistemas aplicativos; la operación de los procesos informáticos; los procesos de recuperación de datos y archivos; los procesos de copias y resguardo de datos; la seguridad física y lógica; la administración de la red de telecomunicaciones; los procedimientos para la puesta en marcha de programas en producción; el tratamiento de los requerimientos de usuarios; los manuales de usuario; los procedimientos de transferencias de fondos, etc.

3.3.2. Del equipamiento informático.

Debe existir documentación detallada sobre el equipamiento informático, que incluya diagramas y distribución física de las instalaciones, inventario de "hardware" y "software" de base, diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos. Esta información comprende tanto al centro de procesamiento de datos principal como de los secundarios, redes departamentales, sucursales, transferencias de fondos y al centro alternativo para contingencias.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 4: Control de operaciones computarizadas o procesos

4.1. Planificación y documentación de operaciones.

Debe existir una adecuada planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información, que deberá incluir como mínimo el detalle de los procesos a realizar, los controles que se efectúan, los mecanismos de registración de los hechos y problemas, los procedimientos sobre cancelaciones y reprocesos en cada una de las actividades, las relaciones con otras áreas y los mecanismos de distribución de la información.

4.2. Control.

4.2.1. De cambios en el "software" de aplicación.

Deben existir procedimientos de control para garantizar la efectivización correcta de cambios cuando corresponda, tales como cambios de programas en bibliotecas de producción, archivos, definiciones de diccionarios de datos, órdenes de ejecución de programas, etc

4.2.2. De integridad y validez de la información procesada.

Los sistemas de información computarizados deben tener incorporados en su programación validaciones y controles mínimos para asegurar la integridad y validez de la información que procesan (referidos a fechas, número de cuentas, número de clientes, tasas de interés, plazos, importes, etc.).

4.2.3. De las operaciones y procesos.

En los casos en que existan distintos centros de procesamiento, debe haber un responsable por el control centralizado de las operaciones y procesos que se realicen en ellos.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 5: Proveedores externos

5.1. Contratos.

Las entidades podrán tercerizar actividades relacionadas con Tecnología Informática o Sistemas de Información, en las condiciones fijadas por la Circular CREFI – 2 en su Capítulo II, Sección 6, con proveedores externos, con los que deberán suscribir contratos formales sobre el alcance y las condiciones de las actividades que se tercericen. Los contratos deberán fijar como mínimo: el alcance de las actividades; los niveles mínimos de prestación; la participación de subcontratistas; los derechos a realizar auditorias por parte de la entidad; compromisos de confidencialidad; los mecanismos de resolución de disputas; la duración del contrato; cláusulas de terminación del contrato; los mecanismos de notificación en cambios del gerenciamiento; el procedimiento por el cual la entidad pueda obtener los datos, los programas fuentes, los manuales y la documentación técnica de los sistemas, ante cualquier situación que pudiera sufrir el proveedor externo por la cual dejara de prestar sus servicios o de operar en el mercado, a fin de poder asegurar la continuidad de procesamiento.
Además, los contratos deben establecer claramente la "no existencia" de limitaciones para la Superintendencia de Entidades Financieras y Cambiarias, en cuanto a: el acceso a los datos y a toda documentación técnica relacionada (diseño de archivos, tipo de organización, etc.) y a la realización de auditorias periódicas en las instalaciones del proveedor, a fin de verificar el cumplimiento de todos los aspectos contemplados en estas normas.

5.2. Condiciones normativas y regulatorias.

Serán las mismas exigibles para las actividades centralizadas y deberán acreditarse cuando se realicen en dependencias de terceros. No podrán tercerizarse actividades con proveedores que a su vez tengan contratada la función de auditoria interna y/o externa de dichas actividades.

5.3. Responsabilidades funcionales.

La gerencia superior de la entidad es la responsable primaria sobre el control de las actividades que han sido delegadas mediante un contrato de tercerización.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 5: Proveedores externos

5.4. Capacitación del personal técnico.

La entidad debe contar con recursos humanos técnicamente capacitados, ya sea a través de agentes bajo relación de dependencia o de terceros que no estén vinculados con los proveedores externos, para ejercer un control eficiente sobre las actividades que desarrolla el proveedor externo (pasaje de programas a producción, separación de ambientes, administración de usuarios, actividades realizadas con la clave maestra –"master password"-, integridad de los datos, plan de contingencias, etc.).

5.5. Separación de ambientes.

Con el objeto de delimitar lógica y/o físicamente el entorno en el cual se realizan las actividades de la entidad, deberá existir una adecuada separación entre los ambientes de procesamiento propios y los correspondientes a los proveedores externos.

5.6. Plan de contingencias.

A los fines de no cesar en sus actividades normales y asegurar la continuidad del procesamiento ante cualquier situación que pudiera sufrir el proveedor externo por la cual dejara de prestar sus servicios, la entidad deberá contar con un plan de contingencias.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 6: Seguridad Lógica

6.1. Administración y control.

Dentro de la estructura de la entidad debe existir una función para la administración y control de la seguridad de acceso a los datos que garantice su independencia del área de sistemas de información
En las entidades de hasta 10 sucursales esta función podrá ser desempeñada por el máximo responsable del área

6.2. Política de seguridad informática.

Debe existir una política formal de seguridad informática, en la que se detallen como mínimo los siguientes aspectos: nivel de confidencialidad de los datos, procedimientos de otorgamiento de claves de usuarios para el ingreso a los sistemas, estandares fijados para el acceso y autenticación de usuarios, cursos de accion en caso de inicio de sumarios a empleados o desvinculacion de estos o de terceros de la entidad

6.3. Acceso y autenticación de los usuarios.

Se deben fijar, como mínimo, los siguientes valores: 4 caracteres de longitud para las "passwords", la no repetición de las últimas 5 palabras claves, etc. Asimismo, se deben establecer, como topes máximos, los siguientes recaudos: desactivar la terminal luego de 3 intentos de accesos fallidos, desconexión por inactividad de la terminal a los 30 minutos, intervalo de caducidad automática de las claves a los 30 días, etc.

6.4. Mantenimiento de archivos de auditoria.

El sistema de seguridad debe mantener durante 3 años, utilizando para ello soportes de almacenamiento no reutilizables (papel, CD, disco óptico u otras tecnologías de esa característica), los archivos de claves o "passwords" encriptadas. Además, deberá generar reportes de auditoria sobre intentos de violaciones y sobre el uso de utilitarios sensitivos y las actividades de los usuarios con atributos de administración y accesos especiales.
El administrador de la seguridad lógica es el responsable primario del control y seguimiento diario y formal de estos archivos y reportes.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 6: Seguridad Lógica

6.5. Restricción de acceso a utilitarios sensitivos.

Debe restringirse el acceso a utilitarios sensitivos que permitan modificar datos en el ambiente de producción, dejando documentado cuando ello ocurra.

6.6. Separación física del personal según sus funciones.

El esquema de seguridad debe incluir una apropiada separación de los ambientes de desarrollo y mantenimiento de sistemas y operaciones (producción), no permitiendo el ingreso de analistas y programadores al entorno productivo, ni de operadores al ambiente o a las herramientas de desarrollo.

6.7. Puesta de programas "en producción".

La puesta en producción de los programas debe ser realizada por personal que no tenga relación con el área de desarrollo y mantenimiento de sistemas, mediante un procedimiento que garantice la correspondencia entre los programas "fuentes" y "ejecutables".

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 7: Continuidad del procesamiento de datos

7.1. Resguardo de la información.

Deben existir procedimientos de resguardo de datos ("backups"), conteniendo una planificación detallada con la cantidad, frecuencia, lugares apropiados de almacenamiento tanto internos como externos, inventarios detallados, responsable y forma de la administración de los medios magnéticos. Estos procedimientos deben prever, como mínimo, la generación de 2 copias de resguardo, manteniendo el almacenamiento de una de ellas en un edificio ubicado a una distancia razonable del centro de procesamiento.
Los períodos de retención de los resguardos de datos y programas (diarios, semanales, mensuales, "software" que los administra, etc.) deben asegurar su recuperación ante cualquier inconveniente de procesamiento que se presente.
Asimismo, los respaldos de información contable (datos filiatorios, saldos al inicio del mes, movimientos, etc.) deben mantenerse disponibles, por duplicado y en condiciones de ser procesados, durante 10 años.
Se deben realizar pruebas formales y debidamente documentadas de recuperación y de integridad de los resguardos de datos ("backups").

7.2. Plan de contingencias.

Se debe contar con un plan de contingencias/emergencias, probado en forma integral como mínimo anualmente, que establezca con claridad y precisión los cursos de acción a seguir, los tiempos, las responsabilidades, los archivos, las telecomunicaciones y todos aquellos recursos necesarios para lograr la continuidad del procesamiento, ante una situación que afecte el normal desarrollo de las tareas de producción.
Se debe disponer de equipamiento alternativo (propio o por convenios formales con terceros) para el procesamiento y las telecomunicaciones, a efectos de poder superar posibles fallas o interrupciones de las actividades en sus equipos habituales. Deberá estar localizado en un edificio ubicado a una distancia razonable del centro de procesamiento.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 7: Continuidad del procesamiento de datos

7.3. Seguridad física y ambiental.

Las instalaciones deben tener una apropiada seguridad física y ambiental, con adecuados controles de acceso. Se debe permitir el acceso al área de procesamiento sólo a personal autorizado y en ella no debe haber material combustible innecesario. Deben instalarse controles de detección automática de humo/calor y elementos para la extinción de incendios.

Los listados y documentación de datos, programas y sistemas deben estar resguardados con adecuadas medidas de seguridad, como así también debe existir un procedimiento para determinar su destrucción o desecho, una vez cumplido su período de retención.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 8: Teleprocesamiento y telecomunicaciones

Se deben establecer mecanismos de protección de los datos que se transmiten por la red de telecomunicaciones mediante técnicas adecuadas de encripción por "hardware" y/o "software".
Se debe contar, dentro de las redes de telecomunicaciones, con un "software" debidamente administrado, a fin de proveer una adecuada seguridad para los accesos a las redes, los cambios a su sistema operativo y el monitoreo de la actividad que se desarrolla en ellas.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 9: Sistemas aplicativos

9.1. Documentación técnica.

Por cada sistema aplicativo, se debe mantener actualizada la documentación técnica que contenga, como mínimo: objetivos, alcances, diagrama del sistema, registro de modificaciones, lenguaje de programación, propiedad de los programas fuentes, problemas o limitaciones conocidas, descripción del "hardware" y "software" utilizados, su interrelación con las redes de telecomunicaciones, descripción de las pantallas que permiten la modificación directa de datos de producción (cambio de parámetros, fórmulas, tasas, datos, etc.).

9.2. Operaciones activas y pasivas

Deben registrarse, administrarse y procesarse en los sistemas aplicativos correspondientes, no pudiendo efectuarse en forma manual, en planillas de cálculo o con otros "software" utilitarios.
Para el caso de nuevos servicios o productos la entidad contará con un período máximo de 90 días corridos, a partir de la primera operación, para registrar/administrar estas operaciones en los sistemas aplicativos correspondientes. En estos casos deberán contar con la autorización formal del Comité de Sistemas de la entidad y su comunicación al área de auditoria interna.
En los archivos de las aplicaciones correspondientes a operaciones pasivas, deben figurar individualmente los datos filiatorios (apellido y nombre, CUIT/CUIL/CDI, en este último caso, cuando corresponda, número de documento, etc.) de todos los titulares de cada una de las cuentas.
Todos los sistemas aplicativos deben emitir diariamente un listado ordenado por sucursal y
cuenta, con los movimientos "fecha-valor" procesados, los que deberán ser mantenidos en archivo durante 3 años, a los efectos de su posterior revisión por los responsables del control.
Cuando no exista este tipo de movimientos, en el listado deberá figurar una leyenda que indique esta situación.
El sistema de contabilidad debe tener controles necesarios para impedir el ingreso de asientos diarios desbalanceados, dar de baja cuentas que tengan o hayan tenido saldos durante el ejercicio, dar de alta cuentas con saldo sin la contrapartida correspondiente, modificar saldos de cuentas sin movimientos y otras registraciones de esta naturaleza.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 9: Sistemas aplicativos

El período máximo para el ingreso de asientos "fecha-valor" en el sistema de contabilidad es de 5 días para el personal que debe ingresar movimientos contables normalmente. Superado dicho plazo y dentro del mes abierto (aproximadamente 40 días corridos para las entidades que no tienen filiales en el exterior y 60 días corridos para aquellas que las tengan), se deberán ingresar transacciones sólo con autorización de la máxima autoridad contable de la entidad, expresada con su firma y sello en los comprobantes correspondientes y la utilización de su clave de acceso personal ("password"), o en su defecto con autorización de un funcionario designado por el Gerente General, de acuerdo con lo que dispongan las normas aprobadas por el Directorio o autoridad equivalente de la entidad. En estos casos, deben ser notificadas las auditorias internas y externas.
El período máximo para el ingreso de movimientos "fecha-valor" en los sistemas aplicativos es de 5 días.
Se debe contar con un archivo con "clave de cliente único" de manera que permita establecer correctamente la totalidad de las operaciones pasivas y activas de cada cliente en la entidad.

9.3. Sistema de información de gestión.

Las entidades deben contar con un sistema de información de gestión para ser utilizado por las máximas autoridades en la toma de decisiones, que obtenga e integre en forma totalmente automatizada los datos que residen en los archivos o bases de datos de sus aplicaciones.

9.4. Generación de información para el Banco Central de la República Argentina.

Las entidades deben contar con sistemas automatizados de generación de información al Banco Central de la Republica Argentina, evitando el reingreso o intercambio no automatizado de datos entre distintos ambientes.
En los casos en que se deba producir ingreso manual de información, por no residir ésta en sus archivos, ello debe ser realizado a través de programas específicos, en un entorno de seguridad apropiado, en archivos independientes, sin posibilidad de modificar la información ya generada en forma automatizada.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 9: Sistemas aplicativos

La Superintendencia de Entidades Financieras y Cambiarias verificará especialmente que la información correspondiente a la clasificación de la cartera de consumo se debe generar en forma automatizada y no debe existir la posibilidad de modificarla para mejorarla, sin perjuicio de la aplicación en el futuro de esa restricción a otras informaciones.
Se debe establecer un procedimiento de control centralizado que permita verificar periódicamente la efectivización, por parte de las sucursales, del cierre de cuenta de los firmantes de cuentas corrientes inhabilitados por el Banco Central de la República Argentina.
La información al Banco Central de la República Argentina de los cheques rechazados y sus firmantes debe generarse automáticamente por el mismo sistema aplicativo que administra las cuentas corrientes o por un subsistema que tome automáticamente los datos
generados por este sistema. En los casos en que el cheque no haya sido firmado por todos sus titulares, los que no firmaron deberán ser eliminados en un proceso posterior.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 10: Sistema transferencia de fondos (SWIFT, MEP, otros) y cámaras compensadoras electrónicas

Los sistemas que se utilicen para la transferencia de fondos deben cumplir con los requisitos mínimos de controles internos establecidos en las Secciones 6. y 7., en lo que se refiere a la seguridad física y lógica y operación de los equipos.
No deben existir usuarios con atributos simultáneos de ingreso, verificación y/o envío de mensajes, a fin de poder asegurar un adecuado control por oposición de intereses. Se deberán designar responsables individuales por cada uno de los atributos mencionados.
Los listados que reflejen la actividad diaria deberán ser controlados y mantenidos en archivo durante 10 años a efectos de su posterior revisión por los responsables del control y en virtud de las normas contables legales.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 11: Cajeros automáticos, banca telefónica y "home banking"

11.1. Funcionamiento.

Los cajeros automáticos ("ATM's") que conformen una red administrada por una entidad y/o por terceros, deben funcionar en un esquema de proceso en tiempo real y conexión directa ("on-line") con el computador que administra la red y la base de datos que opera.
En caso de interrupción del vínculo entre un cajero automático y el computador que lo administra, el cajero deberá quedar fuera de servicio para todo tipo de transacciones monetarias hasta la normalización del proceso.

11.2. Apertura.

La apertura de los cajeros automáticos debe ser realizada por dos personas, dejando constancia escrita en un acta de su participación y resultado de la conciliación, balanceo de billetes, conformidad de depósitos, tarjetas retenidas, totales, diferencias si las hubiera, etc.

11.3. Transacciones.

En las transacciones cursadas por cajeros automáticos que impliquen movimientos de fondos, se deberá emitir el comprobante correspondiente o, como mínimo, se deberá dar la opción al usuario para que se imprima o no.
Los cajeros automáticos, en todos los casos, deberán imprimir, en tiempo real, un listado o cinta de auditoria, en la que quede reflejada toda su actividad (consultas, transacciones, mensajes del "software" y sensores, etc.) con detalle de fecha, hora e identificación del cajero automático.

11.4. Archivo de respaldo.

Se debe generar un archivo en soporte magnético, con todas las transacciones y mensajes del sistema, para uso de los responsables del control y auditoria. Este archivo debe reunir todas las condiciones de seguridad e integridad con el fin de garantizar su confiabilidad y mantenerse disponible durante 5 años.

B.C.R.A	REQUISITOS OPERATIVOS MINIMOS DEL AREA DE SISTEMAS DE INFORMACIÓN (SI) – TECNOLOGÍA INFORMÁTICA
	Sección 11: Cajeros automáticos, banca telefónica y "home banking"

11.5. Clave de identificación del cliente.

Se deberán fijar medidas para establecer apropiadamente la "clave de identificación del cliente" ("PIN") y el mantenimiento de su confidencialidad, debiendo estar encriptados en todos los lugares en que se aloje o transmita y restringir su acceso con apropiados y justificados niveles de seguridad.
Asimismo los programas, archivos y medios magnéticos que contengan fórmulas, algoritmos y datos utilizados para calcular el "PIN" deben estar sujetos a las mismas condiciones de seguridad.
El procedimiento de embozado de tarjeta y generación de "PIN" debe contemplar una adecuada separación de funciones a fin de no concentrar en un mismo sector o funcionario ambas actividades.
Los procesos de generación e impresión de los "PIN" deben asegurar que éstos no aparezcan impresos en forma visible y/o asociados al número de cliente, ni se puedan visualizar por pantalla, a fin de garantizar su confidencialidad.
Los "PIN" y las tarjetas no deben ser entregados en forma conjunta, sino formar parte de procedimientos separados.
Los sistemas que requieran "PIN" para ser utilizados, deben restringir el acceso del cliente
después de, como máximo, tres intentos fallidos.

11.6. Número de transacción.

La entidad debe proveer al cliente de un número de transacción por cada operación cursada.

11.7. Banca telefónica.

Los sistemas de banca telefónica que realicen operaciones de movimientos de fondos, no
pueden funcionar basándose en que el cliente tenga que comunicar su "PIN" a un interlocutor humano.