GUÍA PARA LA ELABORACIÓN

DE PLANES DE CONTINGENCIA

Abril de 2006
Bogotá, D.C., Colombia

ASOCIACION BANCARIA
Y DE ENTIDADES FINANCIERAS
DE COLOMBIA

Presidente
PATRICIA CÁRDENAS SANTA MARÍA

Vicepresidente Económico
CARLOS ALBERTO SANDOVAL

Director de Operación Bancaria
RICARDO NIETO

Asesora de Comunicaciones
MARÍA CONSTANZA MEJÍA M.

Asociación Bancaria y de Entidades Financieras
de Colombia - Asobancaria
Carrera 9 No. 74 - 08 Piso 9
Teléfono: 326 6600
Fax: 326 6601
www.asobancaria.com
info@asobancaria.com

Diseño y armada electrónica
Formato Comunicación Diseño Ltda.

Impresión
Offset Gráfico Ltda.

Bogotá, mayo de 2006

TABLA DE CONTENIDO

1. INTRODUCCIÓN **8**

1.1 Objetivo 8
1.2 Alcance 8
1.3 Audiencia 8
1.4 Condiciones generales 8
1.5 Organización del documento

2. METODOLOGÍA DRII **10**

2.1 Fase 1. Inicio y administración 10
2.2 Fase 2. Requerimientos funcionales 11
2.3 Fases 3 y 4. Diseño e implementación 12
2.4 Fase 5. Pruebas 13
2.5 Fase 6. Mantenimiento 13

3. INICIO Y ADMINISTRACIÓN **14**

3.1 Presentación del proyecto 14
3.1.1 Participantes 14
3.1.2 Fecha de inicio y fecha de terminación 14
3.1.3 Mecanismo de reporte y seguimiento 14
3.2 Objetivos y alcance 14
3.2.1 Objetivos 14
3.2.2 Alcance 14

3.3 Equipos y responsabilidades 14
3.3.1 Equipo Administración del proyecto 14
3.3.2 Equipo Atención de la emergencia 15
3.3.3 Equipo Evaluador de riesgos 15

4. REQUERIMIENTOS FUNCIONALES 15

4.1 Conocimiento del negocio 15
4.1.1 Descripción funcional del negocio 15
4.1.2 Selección de procesos críticos 15
4.1.3 Identificación de tiempos críticos 16

4.2 Inventario de recursos 16
4.2.1 Inventario de información 17
4.2.2 Inventario tecnológico 18
4.2.3 Inventario de instalaciones físicas 19
4.2.4 Inventario de recurso humano 19

4.3 Análisis de riesgos 19

4.4 Análisis de impacto 20
4.4.1 Propósito 20
4.4.2 Impacto externo 21
4.4.3 Impacto interno 21
4.5 Prioridad de reanudación 21

5. DISEÑO E IMPLEMENTACIÓN 22

5.1 Recursos mínimos 23
5.1.1 Personal 23
5.1.2 Computacional 23

5.1.3 Comunicaciones (red y voz) 23
5.1.4 Elementos logísticos 24
5.2 Registros vitales 24
5.3 Notificación 24
5.3.1 Notificación interna o externa: activación y retorno de contingencia 25
5.3.2 Delegación de autoridad 25
5.4 Programación centro alterno 25
5.4.1 Ubicación y mecanismo de ingreso 25
5.4.2 Distribución 25
5.5 Descripción de estrategias 25

6. CAPACITACIÓN Y PRUEBAS 27

6.1 Capacitación 29
6.2 Pruebas 29
6.2.1 Periodicidad 29
6.2.2 Descripción de pruebas

7. MANTENIMIENTO 30

7.1 Políticas de mantenimiento 31
7.2 Bitácora 31
7.3 Mecanismo de almacenamiento 31
7.4 Mecanismo de actualización 31
7.5 Mecanismo de distribución 31

LAS ENTIDADES MIEMBROS DE LA ASOCIACIÓN BANCARIA Y DE ENTIDADES FINANCIERAS DE COLOMBIA (ASOBANCARIA)

C O N S I D E R A N D O

Que parte del plan de continuidad de negocios se fundamenta en la existencia de un esquema para la elaboración de planes de contingencia, que sirva de guía y soporte de la alta gerencia;

Que para prestar sus diferentes servicios y satisfacer los requisitos regulatorios las entidades financieras requieren una infraestructura de soporte robusta, que debe respaldarse con medidas que permitan garantizar la continuidad de las operaciones y la disponibilidad de la información en tiempo real;

Que las entidades financieras han venido estableciendo una serie de medidas para disminuir el riesgo y dar cumplimiento a lo exigido en Basilea II;

R E C O M I E N D A N

Que las entidades financieras utilicen el presente documento como "GUÍA PARA LA ELABORACIÓN DE PLANES DE CONTINGENCIA".

1. INTRODUCCIÓN

1.1 Objetivo

Tener una guía para la elaboración de planes de contingencia. El documento se elaboró según los requerimientos de la metodología del *Disaster Recovery Institute International (DRII*).
El documento se puede usar también para aquellos eventos de interrupción contemplados en el análisis de riesgos que cada entidad ha de realizar.

1.2 Alcance

En esta guía se encuentran las pautas, reglas y recomendaciones que se deben seguir para que una entidad financiera esté en capacidad de reanudar operaciones cuando lo requiera. Los procedimientos del presente documento no cubren un sistema manejador global de incidentes para prevención y atención de desastres, puesto que éste es un trabajo complementario que cada entidad debe efectuar.

1.3 Audiencia

- Este documento se dará a conocer a todo el personal de la entidad involucrado en la operación de la misma, al cual se le entregará periódicamente en estos procedimientos.
- Las áreas de la entidad como guía para la recuperación de los procesos a su cargo ante una eventual amenaza.

1.4 Condiciones generales

Los procedimientos descritos se revisarán, periódicamente, según se indica en el capítulo de mantenimiento del plan.

1.5 Organización del documento

Este documento está organizado de tal manera que no se requiere leerlo por completo para determinar las acciones y actividades necesarias para la recu-

peración. En lugar de esto, hay una combinación de listas de chequeo y procedimientos que se deben llevar a cabo en el momento del desastre, dependiendo de la amenaza ocurrida y la estrategia escogida.

El documento cuenta con siete secciones, además de ésta, la primera, donde se detallan elementos básicos de la guía; en la segunda, se describe brevemente la metodología del DRII, mientras que los capítulos restantes, están en el orden secuencial que presenta la metodología.

En el capítulo 3, "Inicio y administración", se hallan los objetivos de continuidad de la organización y del proyecto, las políticas de continuidad dadas por la alta gerencia que son generales para todos los planes de la organización, así como los supuestos y el esquema de administración para el plan específico que se va a desarrollar.

En el capítulo 4, "Requerimientos funcionales", se encuentra todo el estudio de amenazas, vulnerabilidades, valoración de datos, análisis de riesgos e impacto del negocio, al igual que horarios críticos que ayudan a determinar las estrategias seleccionadas para minimizar el riesgo de interrupción de las operaciones críticas del área.

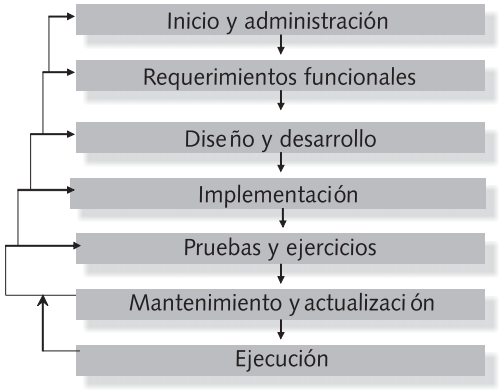
En el capítulo 5, "Diseño e implementación", se detallan las estrategias que se han implementado y que corresponden a un riesgo específico. Se describen también los escenarios, los equipos de trabajo, los procedimientos de activación y retorno, además de los esquemas de comunicación, registros vitales, esquemas de notificación etc.

En el capítulo 6, "Capacitación y pruebas", se tratan las pruebas realizadas, sus listas de chequeo, actividades, alistamiento, tiempos, resultados, evaluación, conclusiones y recomendaciones.

En el capítulo 7, "Mantenimiento", están la bitácora de cambios al plan, y la forma de distribución y actualización del plan.

2. METODOLOGÍA DRII

La metodología propuesta por el *DRII* consta de siete fases, que se enuncian en el siguiente gráfico:



2.1 Fase 1. Inicio y administración

En esta fase se deben desarrollar las siguientes tareas:

Conformación del equipo inicial de trabajo. Para comenzar a construir los planes de contingencia de cada área, se conformará un equipo interdisciplinario apoyado por la dirección general de la entidad y coordinado por la dirección del área funcional.

Familiarización de la metodología por parte del equipo de trabajo. El equipo conocerá a fondo la metodología de trabajo empleada para este tipo de proyectos.

Definición de objetivos, alcance y escenarios del problema. El equipo inicial definirá los objetivos, el alcance y los escenarios que se abarcarán con el plan que se está construyendo.

Estructurar la administración del proyecto. Siguiendo el modelo de metodología presentado por el DRII, es necesario establecer una buena administración del proyecto, la cual incluye, creación (definir tareas y duración,

establecer relaciones entre las tareas, asignar recursos), administración (es un proceso que nunca termina, se debe hacer seguimiento y ajustes al proyecto que reflejen los cambios efectuados) y reportes de progreso (se deben realizar presentaciones a los directivos y proponer ajustes para su aprobación).

Aprobación por parte de los directivos. Una vez terminadas estas tareas, el grupo debe presentar un informe a los directivos, quienes después de revisarlo deciden si dan su aprobación para que el proyecto siga adelante o, en caso contrario, solicitan revisión de alguno de los puntos expuestos.

2.2 Fase 2. Requerimientos funcionales

En esta fase se deben desarrollar las siguientes tareas:

Identificación de las funciones y servicios críticos del área. En este punto se deben enumerar todas las funciones y servicios que se realizaran en el área y se priorizan de acuerdo con la razón de ser del área dentro de la entidad. Para cada prioridad se señalará el tiempo máximo de espera para que se reanuden los servicios.

Identificación de recursos críticos. Determinar, para cada función y servicio, en qué recursos (computacionales o logísticos) se apoya, y de esta manera establecer la criticidad de los recursos. Adicionalmente, identificar los registros de datos e información vital para la operación de dichas funciones y servicios.

Recopilación de información. Recolectar los datos de los empleados, clientes y proveedores que se involucran en las funciones, proceso y servicios del área.

Análisis de riesgos y controles. Para llevar a cabo este análisis se estudiarán las soluciones y controles existentes para las aplicaciones y se identificarán los documentos, procedimientos y estándares existentes. Posteriormente, se analizarán las posibles amenazas de los recursos y la exposición de éstos a posibles riesgos.

Análisis de impactos. Una vez determinados los riesgos sobre los recursos, se analizará el impacto de éstos sobre la operación del área funcional, tomando los costos tanto de nivel cualitativo como cuantitativo e incluyendo un análisis costo/beneficio de la implantación de un control.

Aprobación por parte de los directivos. Después de terminadas estas tareas, el grupo presentará un informe de recomendaciones a los directivos, quienes después de revisarlo deciden si dan su aprobación para que el proyecto siga adelante o, en caso contrario, solicitan revisión de alguno de los puntos expuestos.

2.3 Fases 3 y 4. Diseño e implementación

En esta fase se desarrollan las siguientes tareas:

Diseño de estrategias y controles. Una vez identificados los riesgos, se deben diseñar estrategias y controles para mitigarlos. Para cada uno de estos controles se identificarán claramente los recursos necesarios y la forma de consecución de los mismos (desarrollo, compra de recursos, contrataciones, convenios, etc.).

Identificar equipos para operación en contingencia. Para implementar las estrategias y controles que entrarán a operar durante una contingencia, las cuales identificarán las personas necesarias para llevar a cabo la recuperación, las cuales se agruparán de acuerdo con el carácter de las tareas que se van a realizar. Así mismo, se identificará el inventario de recursos de cada equipo de trabajo.

Orgranigrama de contingencia. Se conformará un organigrama de contingencia, que permita que las personas adecuadas tomen las decisiones del momento. Este organigrama puede estar integrado por personas diferentes del organigrama de la organización, con el fin de distribuir las tareas y evitar tropiezos para tomar decisiones de carácter urgente.

Diseñar el sistema de notificación. Con el propósito de mantener el orden y respetar los conductos regulares durante los momentos de crisis, todas las personas que laboran en el área deben tener claro cómo notificar y a quién los sucesos que se presenten durante las etapas de una emergencia.

Empalmar con planes ya existentes de otras áreas funcionales. En razón de que el programa que se está construyendo forma parte de un conjunto de planes de contingencia que conforman el Plan de Continuidad del Negocio

para la entidad, éste no debe permanecer aislado, sino que se debe revisar contra otros programas paralelos en los que pueda apoyarse, con los cuales tiene que interactuar y a los que posiblemente servirá de soporte.

Contenido tentativo del plan. Elaborar un bosquejo de lo que contendrá el plan de contingencia para el área específica que se está trabajando.

Aprobación por parte de los directivos. Después de analizadas estas tareas, el grupo presentará un informe de recomendaciones a los directivos, quienes después de revisarlo deciden si dan su aprobación para que el proyecto siga adelante o, en caso contrario, solicitan revisión de alguno de los puntos expuestos.

En esta fase se implantan las estrategias y controles diseñados y aprobados por la dirección, se realiza la compra y adquisición de los recursos necesarios para la recuperación, se firman contratos, se escriben los procedimientos y responsabilidades para cada integrante de los equipos de recuperación en cada momento de ésta y se prepararan los sitios de recuperación.

Aprobación por parte de los directivos. Una vez terminadas estas tareas, el grupo presentará un informe a los directivos, quienes después de revisarlo deciden si dan su aprobación para que el proyecto siga adelante o, en caso contrario, solicitan revisión de alguno de los puntos expuestos.

2.4 Fase 5. Pruebas

Diseñar las pruebas que se van a realizar, las cuales consisten en simulacros de las situaciones que se contemplan en el plan, con miras a entrenar al personal y probar los controles implantados, así como calcular los tiempos de respuesta del personal y de los controles. También se concientizará a todo el personal de la posibilidad de ocurrencia de un incidente. Cada prueba se debe evaluar para retroalimentar el plan.

2.5 Fase 6. Mantenimiento

Un plan de contingencia no es un proyecto con inicio y fin, sino que es un proceso que nunca termina; por tanto, debe diseñarse un plan de mantenimiento continuo para que éste permanezca vigente y funcional.

3. INICIO Y ADMINISTRACIÓN

3.1 Presentación del proyecto

3.1.1 Participantes

Se definirán claramente las personas del área que elaborarán el plan de contingencia.

3.1.2 Fecha de inicio y fecha de terminación

Se fijará una fecha de inicio específica y una fecha tentativa de terminación.

3.1.3 Mecanismo de reporte y seguimiento

Se especificará(n) el (los) mecanismo(s) de reporte y seguimiento acordado(s) con los directivos del área.

3.2 Objetivos y Alcance

3.2.1 Objetivos

- Se enumerarán los objetivos generales del plan.
- Se enumerarán los objetivos específicos del plan.

3.2.2 Alcance

- Se enumerarán los escenarios para los que el plan está diseñado.

3.3 Equipos y responsabilidades

Se asignarán responsabilidades para la administración del proyecto y se conformarán los grupos de trabajo encargados del plan de contingencia del área, detallando los roles e integrantes de cada equipo. A continuación se muestran algunos ejemplos.

3.3.1 Equipo Administración del proyecto

Es el equipo encargado de evaluar las decisiones que se toman en cada una de las fases, y de aprobar las estrategias y el presupuesto involucrado; además, velará por la vigencia del plan del área y mantendrá certificada el área en continuidad del negocio.

3.3.2 Equipo Atención de la emergencia

Es el equipo que atiende la emergencia en primera instancia y realiza las respectivas acciones de notificación en el área.

3.3.3 Equipo Evaluador de riesgos

Es el equipo encargado de evaluar periódicamente los riesgos inherentes al servicio y mantener enterado al equipo de continuidad del negocio de la necesidad de generar nuevas estrategias o de hacer mantenimiento al plan.

4. REQUERIMIENTOS FUNCIONALES

4.1 Conocimiento del negocio

4.1.1 Descripción funcional del negocio

Se realizará una descripción del área en cuestión incluyendo sus objetivos y responsabilidades.

4.1.2 Selección de procesos críticos

4.1.2.1 Criticidad

Se identificarán todos los procesos críticos que se realizan en el área, las actividades involucradas en ellos de manera secuencial, su periodicidad y se calificará su criticidad de 1 a 3, donde 1 es el nivel más alto.

Se suministrará la siguiente información para cada proceso:

- Número del proceso o tarea
- Nombre del proceso
- Descripción del proceso o tarea
- Producto o servicio relacionado con el proceso

4.1.2.2 Información externa de apoyo

Para los procesos de criticidad 1 y 2, se identificará la información que no pertenece al área y que apoya el proceso. Se relacionarán las áreas con las que interactúa el proceso y el tipo de información a través del cual interactúan. Si el proceso no interactúa con otras áreas, se debe especificar el nombre del área que ejecuta el proceso en la dependencia origen y en la dependencia destino; de lo contrario, se deben anotar todas las dependencias tanto origen como destino.

- Dependencia origen*:* áreas o departamentos de donde proviene la información.
- Dependencia destino*:* áreas o departamentos hacia donde se dirige la información.

4.1.3 Identificación de tiempos críticos

4.1.3.1 Horarios, RTO y RPO

Se establecerán los horarios críticos de ejecución de los procesos con prioridades 1 y 2 y el tiempo máximo que tienen para su recuperación (RTO), así como el punto de recuperación de los datos que se requieran para el proceso (RPO).

- Frecuencia de ejecución
  D: Diario; S: Semanal; Q: Quincenal; M: Mensual; B: Bimestral; T: Trimestral; R: Semestral; A: Anual; O: Ocasional.

- Tiempo esperado de recuperación
  Se refiere al tiempo máximo que el proceso puede esperar sin que impacte de manera considerable a los clientes, entes de control, usuarios internos y entes externos.

- Tiempo límite de ejecución
  Hace referencia a los procesos que se deben ejecutar en una fecha específica o a una hora determinada.

  - Fecha máxima de ejecución: último día en el que se puede ejecutar el proceso. Ej.: Día 10 (transmisión balance a la Superintendencia Bancaria); Todos los días (transmisión de tasas a la Superintendencia Bancaria).

  - Hora máxima de ejecución: hora límite para ejecutar el proceso. Ej.: 8:00 a.m. (transmisión de tasas a la Superintendencia Bancaria).

4.2 Inventario de recursos

Se debe hacer un inventario de todos los recursos que soportan cada proceso dentro del área, ya que éstos son la fuente fundamental del análisis de riesgo. Se debe realizar una descripción detallada de cada uno de ellos (recursos de

tipo información, tecnológico, instalaciones físicas y humano, entre otros), indicando si forman parte esencial del sistema o proceso o si, por el contrario, en ausencia de éste el proceso puede llevarse a cabo aunque sea de manera parcial.

4.2.1 Inventario de información

Se han de incluir el tipo de información, su descripción y el mecanismo en la que ésta es actualiza.

4.2.1.1 Entidades externas y clientes

Se debe relacionar (para cada proceso crítico definido anteriormente) todo el intercambio de información con los clientes y los entes externos, puesto que es importante tener en cuenta la información que envía o recibe la entidad y el medio de intercambio.

- Número del proceso o tarea: este número debe coincidir con el número del proceso asignado en la selección de procesos críticos.
- Entidad externa o cliente: se debe especificar con quién se realiza el intercambio de información.
- Entrega/Recepción: se debe especificar si la información la entrega el banco o si, por el contrario, la recibe.
- Descripción: Se debe proporcionar una breve descripción del tipo de información que se intercambia.
- Medio de transmisión o intercambio: Se debe especificar el medio de transmisión de la información (L: listado; D: disquete; C: cinta; E: correo; CD: unidad de CD; V: videolínea; I: Internet; M: módem; R: RDSI; etc.).
- Periodicidad: Se debe relacionar la periodicidad con la que se envía o se recibe la información (D: Diario; S: Semanal; Q: Quincenal; M: Mensual; B: Bimestral; T: Trimestral; R: Semestral; A: Anual; O: Ocasional).

4.2.1.2 Proveedores

Se debe relacionar (para cada proceso crítico definido anteriormente) todo el intercambio de información con los proveedores, ya que es importante tener en cuenta la información que envía o recibe la entidad y el medio de intercambio.

- Número del proceso o tarea: este número debe coincidir con el número del proceso asignado en la selección de procesos críticos.
- Nombre del proveedor: se debe especificar el nombre del proveedor.
- Servicio prestado: se debe proporcionar una breve descripción del servicio que proporciona el proveedor.
- Entrega/Recepción: se debe especificar si la información la entrega el banco o si, por el contrario, la recibe.
- Descripción: se debe proporcionar una breve descripción del tipo de información que se intercambia.
- Medio de transmisión o intercambio: Se debe especificar el medio de transmisión de la información (L: listado; D: disquete; C: cinta; E: correo; CD: unidad de CD; V: videolínea; I: Internet; M: módem; R: RDSI; etc.).
- Periodicidad: se debe relacionar la periodicidad con la que se envía o se recibe la información (D: Diario; S: Semanal; Q: Quincenal; M: Mensual; B: Bimestral; T: Trimestral; R: Semestral; A: Anual; O: Ocasional).

4.2.2 Inventario tecnológico

Se deben detallar los elementos que forman parte del recurso tecnológico, incluyendo servidores, direcciones IP y esquema de comunicaciones, entre otros.

4.2.2.1 Diagrama de estructura tecnológica

Se debe detallar la estructura tecnológica con la que cuenta la entidad para soportar cada proceso.

4.2.2.2 Software

Se debe especificar, para cada proceso, el software requerido para que éste se pueda llevar a cabo, incluyendo la versión y los parches instalados, la fecha de la última actualización, el tipo de mantenimiento y los sistemas con los que interactúa.

4.2.2.3 Hardware y periféricos

Se debe especificar, para cada proceso, el hardware requerido para que éste se pueda llevar a cabo, incluyendo el equipo, discos, sistema operativo, memoria y tipo de mantenimiento.

4.2.2.4 Comunicaciones

Se debe especificar, para cada proceso, la necesidad de comunicación para que éste se pueda llevar a cabo, incluyendo una descripción exacta del origen y el receptor de la comunicación, el proveedor que presta el servicio y el medio físico empleado para realizarla.

4.2.3 Inventario de instalaciones físicas

Se debe identificar, para cada proceso, la ubicación física donde se desarrollan las actividades de las personas que intervienen en éste, tanto empleados como usuarios externos. Esto incluye la ciudad, la edificación, el piso y el dueño de la propiedad.

4.2.4 Inventario de recurso humano

Se debe identificar, para cada proceso, a todas las personas que intervienen en éste, tanto internas de la entidad como externas. Hay que incluir una breve descripción de lo que cada una hace, el número de personas que realizan la actividad y el área a la que pertenecen. Se debe suministrar la siguiente información sobre el (los) responsable(s) de cada proceso crítico:

- Nombre del responsable: apellidos y nombres de la persona encargada de realizar el proceso.
- Cargo del responsable: cargo de la persona encargada del proceso.
- Nombre de otras personas que conocen el proceso: relacionar los apellidos y nombres de otras personas que pueden ejecutar el proceso, en caso de que la persona titular no lo pueda llevar a cabo.

4.3 Análisis de riesgos

El análisis de riesgos está orientado a determinar un conjunto de estrategias (independientes o conjuntas) que deberán implementarse para que cada proceso tenga unas condiciones mínimas para poder reanudarse. Para la obtención de estas estrategias se determina el número de ocurrencias anuales de las amenazas, factor de exposición, vulnerabilidades frente a las pérdidas y valoración del riesgo por recurso en cada actividad que interviene; adicionalmente, se recomienda hacer controles preventivos ante ciertas amenazas.

Entre los factores que hay que considerar dentro del análisis de riesgos se encuentran los siguientes:

- Identificación de amenazas
  - Historia de incidentes por recurso y amenaza
  - Probabilidad de ocurrencia
  - Exposición por amenaza
  - Impacto por amenaza
- Recomendación de controles preventivos
- Identificación de estrategias por recurso
- Asignación de estrategias por amenazas

4.4 Análisis de impacto

4.4.1 Propósito

El objetivo de un «**análisis de impacto**» es poder determinar la exposición financiera y el impacto operacional ante la interrupción de las funciones críticas del negocio de una compañía.

Un análisis de impacto está diseñado para asegurar un entendimiento de las funciones y sistemas vitales del área dentro de la organización. El impacto de cada una de estas funciones se identifica, evalúa y categoriza de acuerdo con los marcos de tiempo requeridos para la recuperación del negocio.

Los propósitos generales de la realización de este análisis son:

- Identificar las consecuencias de la interrupción en lo referente a pérdidas financieras, gastos adicionales e imagen de la organización.
- Identificar el máximo período de interrupción que la organización puede tolerar.
- Determinar qué nivel de pérdidas financieras es aceptable para la organización en conjunto y para una función específica del negocio.
- Dejar datos para realizar un análisis costo / beneficio.
- Establecer o confirmar prioridades de recuperación para aplicaciones críticas, sistemas y prioridades de recuperación de negocios.

Entre los factores que hay que considerar dentro del análisis de impactos se encuentran los siguientes:

- Valoración cuantitativa del impacto
- Valor aceptable de pérdida
- Valoración cualitativa del impacto

4.4.2 Impacto externo

Se refiere al impacto (alto, medio o bajo) que puede generar en los clientes o en los organismos externos el hecho de no prestar el servicio o no generar la información a tiempo.

Los entes externos pueden ser la Superintendencia Financiera, la Asociación Bancaria, la DIAN, el Banco de la República, Deceval, DCV, ATATEC, MEC o IQ Outsourcing, entre otros.

4.4.3 Impacto interno

Se refiere al impacto que afecta únicamente a la institución.

- Impacto financiero (alto, medio o bajo): se refiere al impacto que puede tener, en el aspecto económico, el hecho de dejar de prestar el servicio o prestarlo a destiempo, ocasionando pérdida de clientes y de ingresos, multas o litigios.

  - **Valor en $ (pesos) de la pérdida de ingresos:** se refiere al valor de la pérdida de ingresos, por ejemplo, por dejar de recibir comisiones. El valor de la pérdida debe tenerse en cuenta de acuerdo con la periodicidad del proceso, de tal manera que si la periodicidad es diaria, la pérdida ha de ser diaria.

  - **Valor en $ (pesos) de la multa:** se refiere al valor de la multa por incumplimiento. Debe tomarse en cuenta de acuerdo con la periodicidad del proceso, de modo que si la periodicidad es diaria, la multa ha de ser diaria.

- Impacto operativo (alto, medio o bajo): se refiere al impacto que pueden ocasionar grandes pérdidas de información o altos costos de recuperación.

4.5 Prioridad de reanudación

Una vez realizado el análisis anterior, se priorizan los procesos en una "Matriz de tiempos de recuperación".

En esta matriz se presentan los procesos del área en el orden en que se recuperarán, de acuerdo con la información suministrada por los usuarios.

5. DISEÑO E IMPLEMENTACIÓN

En esta etapa se determinan los recursos mínimos para trabajar en un centro alterno, se describen las estrategias y se formalizan los procedimientos de reanudación y recuperación correspondientes a las estrategias alternas de contingencia identificadas en la etapa anterior. Así mismo, deben definirse los procedimientos de notificación y escalamiento de emergencias, los criterios y procedimientos de activación de los planes de contingencia, al igual que los equipos de reanudación y recuperación, encargados de coordinar las actividades de recuperación en el evento de activación del plan. A continuación se detallan aún más algunas actividades de la etapa.

- Requerimientos mínimos.
  - Identificar recursos de personal, computacionales, de comunicaciones, implementos de oficina y espacio físico y amoblado para operar en centros alternos a corto, mediano y largo plazos.

- Definición de programas de registros vitales y almacenamiento alterno.
  - Identificación de los registros vitales.
  - Protección y recuperación de registros vitales.
  - Backups fuera del sitio.

- Definición de procedimientos de escalamiento y notificación del plan.
  - Respuesta inicial, procedimientos de emergencia.
  - Recuperación en el sitio alterno.
  - Recuperación de actividades en paralelo.
  - Recuperación en el sitio original o alterno.

- Delegación y designación de autoridad.

- Procedimientos de activación del plan.
  - Activación de los equipos de recuperación de desastres y continuidad del negocio (árbol de llamadas).
  - Activación del sitio de recuperación y notificaciones.
  - Requerimientos de los usuarios finales y personal de las áreas funcionales.

- Monitoreo de la recuperación y progreso de la reanudación.
- Revisiones para conducir a la pos-reanudación.

➢ Adquisición del hardware, software, líneas de comunicación, etc.

➢ Negociación y firma de contratos con los vendedores.

➢ Preparación de los sitios.

5.1 Recursos mínimos

Se deben prever, para cada área en particular, el peor escenario de desastre y la necesidad de desplazamiento a un centro alterno. Ante esta situación, hay que establecer los períodos de operación en el centro alterno, definiendo un corto, mediano y largo plazos. A continuación se procede a determinar y a describir los recursos mínimos requeridos para los períodos descritos.

5.1.1 Personal

Se deben identificar, para cada período, el número de personas requeridas para llevar a cabo cada proceso, incluyendo una breve descripción de sus funciones.

5.1.2 Computacional

Se deben identificar, para cada período, los elementos computacionales requeridos para llevar a cabo cada proceso, incluyendo equipos, discos, sistema operativo, memoria y software.

Adicionalmente, se ha de describir la forma como se proveerán recursos a mediano y largo plazos (se compran, se alquilan, provienen de directivos, etc.)

5.1.3 Comunicaciones (red y voz)

Se deben identificar, para cada período, los elementos de comunicación necesarios para llevar a cabo cada proceso, incluyendo puntos de red y líneas telefónicas, con sus respectivas características.

5.1.4 Elementos logísticos

5.1.4.1 Espacio físico

Se deben identificar, para cada período, los elementos de espacio físico que se requieren, incluyendo tamaño, seguridad y privacidad, entre otros.

5.1.4.2 Amoblado

Se deben identificar, para cada período, los elementos de mobiliario que se requieren, como escritorios y sillas, por ejemplo.

5.1.4.3 Documentos e implementos de oficina

Se deben identificar, para cada período, los documentos e implementos de oficina necesarios para efectuar cada una de las actividades programadas.

5.2 Registros vitales

Se debe establecer, para cada área en particular, el esquema de respaldos de aquella información vital requerida para llevar a cabo cada proceso que no reside en los dispositivos de almacenamiento alternos.

Servidores de estaciones PC

Se deben incluir los datos que hay que respaldar, el día y la hora en que se hace el respaldo o la periodicidad, el tipo de respaldo, el tiempo de retención de la información y la instalación o ubicación donde se encontrarán estos registros vitales. Adicionalmente, se deberán especificar los usuarios que tendrán acceso a esta información.

5.3 Notificación

La notificación tanto interna como externa para la reanudación y el retorno deberá hacerse en el momento del incidente. Para esto deberá elaborarse un esquema general de notificación y esquemas particulares si es necesario. Es recomendable realizar estos esquemas gráficamente e incluir una breve descripción de cada uno para mayor claridad.

5.3.1 Notificación interna o externa: activación y retorno de contingencia

En todos los casos se debe incluir el cargo de la persona que notifica, el de la persona notificada y el medio de comunicación empleado.

5.3.2 Delegación de autoridad

En todos los casos se debe incluir el tipo de autorización, el responsable actual (cargo) y a quién se le delega la autorización (cargo). Adicionalmente, hay que proporcionar información sobre el proceso o procedimiento al que hace referencia la autorización.

5.4 Programación centro alterno

En este capítulo se consolidan la información del centro alterno, su ubicación, el mapa de los elementos que están en el sitio, la funcionalidad de cada puesto de trabajo y el responsable de los elementos que allí se encuentran.

5.4.1 Ubicación y mecanismo de ingreso

Se debe especificar la ubicación del centro alterno y el procedimiento para ingresar, teniendo en cuenta consideraciones de horario (hábil o no hábil).

5.4.2 Distribución

Se debe especificar la ubicación de cada elemento de *hardware,* incluyendo direcciones IP, *software* instalado y funciones que se realizarán en el.

Se debe especificar la ubicación de cada elemento de oficina incluyendo equipos de transmisión de fax, escáner y fotocopiadoras, entre otros.

Se debe especificar la ubicación de todos los útiles de oficina.

5.5 Descripción de estrategias

Se deben describir, para cada estrategia, todos los elementos que intervienen en ésta, los procedimientos necesarios para su ejecución, los escenarios en los que se puede aplicar, los equipos que participan y los controles requeridos en cada una de las actividades.

Estrategia Núm. 1: [Nombre de la estrategia]

1. Escenarios

Se deben especificar los incidentes o amenazas para los que sirve esta estrategia.

2. Equipos de trabajo

Se deben especificar las personas que intervienen para la reanudación del servicio o recuperación de la falla hasta la normalidad. Hace referencia a las personas que conforman los equipos que se describen a continuación:

2.1 Equipo de reanudación (ERO)

Es el equipo responsable de reanudar el servicio, es decir, aquellas personas que técnica u operativamente son quienes deben realizar las acciones de la estrategia de contingencia para restablecer el servicio.
Se debe diferenciar (en caso de ser diferentes) a las personas encargadas de la parte tecnológica de las responsables de la parte operativa, incluyendo el área a la que pertenecen y el cargo.

2.2 Equipo de recuperación (ERP)

Es el equipo encargado de que los escenarios de falla para esta estrategia sean atendidos y recuperados a un estado de operación normal. Se deben incluir el escenario de falla y el responsable, incluyendo el área a la que pertenece y el cargo. Adicionalmente, en caso de existir y de ser relevante, se debe incluir el proveedor del sistema afectado.

3. Recursos específicos

Tiene que ver con los elementos propios de la estrategia, la cantidad, ubicación y el responsable de proveer el recurso. Si el responsable es un proveedor, se debe explicar en qué condiciones entrega el elemento; si existe un contrato, se debe hacer referencia a éste y anexarlo.

4. Controles

Se deben enumerar, para cada proceso, las actividades de la estrategia que hay que controlar, indicando el mecanismo de control y el verificador.

5. Proceso de activación

La estrategia sugiere un flujo de actividades para reanudar el servicio oportunamente. A continuación se detallan el procedimiento técnico u operativo y el responsable. Si se necesita describir el procedimiento de una manera más explícita, deberá haber un pie de página con el documento que podrá encontrar en los anexos.

5.1 Estrategia técnica

Hay que relacionar cada una de las actividades y al equipo responsable, si no es explícito en la descripción de la actividad.

5.2 Estrategia operativa

Hay que relacionar cada una de las actividades y al equipo responsable si no es explícito en la descripción de la actividad.

6. Proceso de retorno

La estrategia sugiere un flujo de actividades para retornar a la normalidad. A continuación se detallan el procedimiento técnico u operativo y el responsable. Si se necesita describir el procedimiento de una manera más explícita, deberá haber un pie de página con el documento que podrá encontrar en los anexos.

6.1 Estrategia técnica

Se deben relacionar cada una de las actividades y al equipo responsable si no es explícito en la descripción de la actividad.

6.2 Estrategia operativa

Se deben relacionar cada una de las actividades y al equipo responsable si no es explícito en la descripción de la actividad.

6. CAPACITACIÓN Y PRUEBAS

En esta etapa se capacita y concientiza a todos los niveles de la organización en lo referente a los planes de contingencia de los procesos del negocio. Así mismo se planean y realizan las pruebas a los planes de contingencia, luego se hace la evaluación respectiva.

A las personas de las áreas se las deberá capacitar en el detalle de los planes, así como concientizar de la importancia del plan, pues ellas serán las encargadas de ponerlos en funcionamiento en caso de presentarse un evento no deseado. A los jefes de dichas áreas también se les capacitará y concientizará, ya que son los responsables de la correcta ejecución de los planes.
En la capacitación sobre los planes de contingencia se deberán incluir las definiciones de los términos usados, los objetivos del plan, los supuestos y limitaciones (alcance del plan), el análisis de riesgos realizado, el análisis de impacto del negocio y los escenarios contemplados, así como las estrategias y procedimientos definidos, asignando a cada uno de los participantes su rol dentro de dichos planes.

Igualmente, durante esta etapa se debe establecer un programa de pruebas con escenarios lo más reales posible, planeados en el tiempo, teniendo en cuenta los requerimientos de cada prueba, y con una revisión exhaustiva de los resultados de las mismas, para generar mejoras a los planes. El objetivo de las pruebas es verificar los procedimientos establecidos, probar los controles definidos, reanudar operaciones en sitios alternos o con elementos reducidos, determinar el conocimiento que tienen las personas de su función en dichos procedimientos, establecer los tiempos de recuperación y, en general, detectar fallas y aplicar correctivos.

Las pruebas pueden ser de dos tipos: anunciadas o no anunciadas. Estas últimas son las más reales y se realizan normalmente luego de algunas pruebas avisadas. Así mismo, pueden hacerse pruebas de escritorio, donde un grupo de personas que conocen el proceso (podrían ser quienes ejecutan el proceso a diario), se reúnen para revisar los procedimientos, a la luz de su conocimiento y experiencia, con el fin de determinar puntos de mejoramiento.

Luego de cada prueba el coordinador de contingencia hará un informe completo, dirigido a los participantes y a los directores de las áreas, en el que se contemple toda la información acerca de la prueba, escenarios, objetivos, alcance, y se informen los resultados de la misma y las mejoras realizadas a los planes.

6.1 Capacitación

Se debe elaborar una lista de las actividades programadas en la capacitación, con su responsable, fecha de ejecución y resultado, indicando las formas en las que se capacitará y concientizará al personal del área y demás personas involucradas en todo lo relacionado con el plan de contingencia.

6.2 Pruebas

El objetivo de las pruebas es verificar los procedimientos establecidos, probar los controles definidos, reanudar operaciones en sitios alternos, o con elementos reducidos, conocer a las personas en su rol, establecer los tiempos de recuperación y en general, detectar fallas y aplicar correctivos.
Es importante asegurarse de que el procedimiento de recuperación sea factible y práctico, identificar deficiencias en procesos existentes, demostrar la habilidad del área para recuperarse y tener la certeza de que las personas de los equipos de recuperación y reanudación son capaces de trabajar en conjunto y bajo la presión de incidentes con diferente magnitud.

Se debe hacer un cronograma de pruebas en el que se indiquen la estrategia que se va a probar y el tipo de prueba (tecnológico/operativo), e incluir una breve descripción de lo que se quiere realizar.

6.2.1 Periodicidad

La periodicidad de cada una de las pruebas asegura su vigencia. Por tal motivo, se deben especificar las estrategias que se probarán regularmente, indicando su periodicidad y sus responsables.

6.2.2 Descripción de pruebas

6.2.2.1 Objetivos

Se deben precisar los objetivos específicos de cada prueba que se vaya a realizar.

6.2.2.2 Planeación

Se debe definir la prueba, proporcionando la siguiente información:

- Título
- Clase de prueba (tecnológica, operativa, de notificación, etc.)
- Sistemas de información (si se requieren)
- Duración aproximada de la prueba
- Participantes
- Criterios de evaluación

6.2.2.3 Ejecución, resultados y mejoras

Se debe realizar una bitácora de ejecución con los resultados obtenidos y las mejoras hechas al plan, incluyendo fecha de ejecución, resultados y responsables.

7. MANTENIMIENTO

El objetivo de esta etapa es desarrollar procedimientos y mecanismos de mantenimiento y actualización de los planes definidos, con el fin de garantizar que éstos se podrán utilizar efectivamente en una emergencia, velando porque su información se encuentre actualizada, completa y precisa.

Así mismo, en esta etapa se busca implementar mecanismos que aseguren que el plan es consistente con los procedimientos actuales de la organización o área, que los mecanismos de comunicación y procesamiento de datos se prueban periódicamente y que los miembros de la organización conocen todos los cambios realizados a los planes. Además, se velará por establecer los procedimientos de revisiones periódicas de los mismos.

Igualmente, en esta etapa deben definirse los mecanismos de divulgación y distribución de los planes, así como las estrategias de actualización, cuando se hagan modificaciones a los mismos. Deben definirse, además, dónde residirán los documentos de los planes y las copias de seguridad de los mismos.

7.1 Políticas de mantenimiento

Se debe hacer una lista de medidas mediante las cuales se mantendrá el plan de contingencia. Se Incluyen resultados, resoluciones y reuniones, entre otros.

7.2 Bitácora

Cada vez que se modifique el plan, se deberá llevar una bitácora en la que se indiquen las causas por las que se ha modificado, la fecha, el elemento cambiado, la descripción de la modificación, quién la hizo y si ya se distribuyó o no.

7.3 Mecanismo de almacenamiento

Una vez terminado el plan de contingencia, éste se deberá almacenar en diferentes medios y ubicaciones. Es recomendable tener copias impresas, por si los documentos magnéticos no están disponibles en el momento de un incidente. Dichas copias se deben almacenar también en los centros alternos.

7.4 Mecanismo de actualización

Cada vez que se modifique el plan es necesario actualizar todas las copias existentes. Es de gran importancia verificar que todas las copias contengan la misma información.

7.5 Mecanismo de distribución

Cada vez que se modifique o actualice el plan, se deberán distribuir y divulgar las nuevas actualizaciones para que todos los participantes conozcan los cambios realizados. En caso de requerir nuevas pruebas y capacitaciones al personal involucrado en la contingencia, éstas se tendrán que realizar con la mayor brevedad posible.