

# XXVI REUNION DE SISTEMATIZACION DE BANCOS CENTRALES AMERICANOS E IBERICOS

---

La Habana, Cuba, 26 al 30 de octubre de 1998

---

## XXVI REUNION DE SISTEMATIZACION DE BANCOS CENTRALES AMERICANOS E IBERICOS

### CONTINGENCIA INFORMATICA

#### BANCO DE LA REPUBLICA

Octubre de 1.998

#### 1. Introducción

*Cuando ocurra un incidente, revise detenidamente los PROCEDIMIENTOS DE ACTIVACION DEL PLAN, luego inicie los pasos apropiados.*

El propósito de este documento es el de exponer la metodología que está siguiendo el Banco de la República para la administración de la contingencia informática, al igual que el restablecimiento del negocio, el cual es el elemento principal de todo plan de contingencia.

#### 2. Equipo inicial

El Equipo inicial para el desarrollo del plan de "Continuidad del Negocio" es un grupo interdisciplinario de personas pertenecientes a las diversas áreas del Banco involucradas en un eventual proceso de atención de emergencias y recuperación del negocio.

Estas áreas son: Unidad de Seguridad Informática, quien coordina la actividad, el Departamento de Control Interno, el departamento de Auditoría y el área involucrada.

Adicionalmente, se cuenta con el apoyo de las áreas de: Unidad de Riesgos Profesionales, el Departamento de Edificios y el Departamento de Protección y Seguridad para la integración del plan objeto de este proyecto con los planes desarrollados a nivel de cada área y a integral.

#### MISIÓN

Este Equipo es el encargado de proponer a la Alta Gerencia del Banco de la República un Plan de Continuidad para el Departamento *afectado*.

#### VISIÓN

Al finalizar el trabajo de este equipo, el Banco de la República contará con un documento que contendrá el "Plan de Continuidad para el Departamento *afectado* del Banco de la República" el cual es apoyado por la Alta Gerencia.

#### INTEGRANTES

Unidad de Seguridad Informática

Departamento de Control Interno

Departamento *afectado*

Departamento de Informática

Departamento de Auditoría

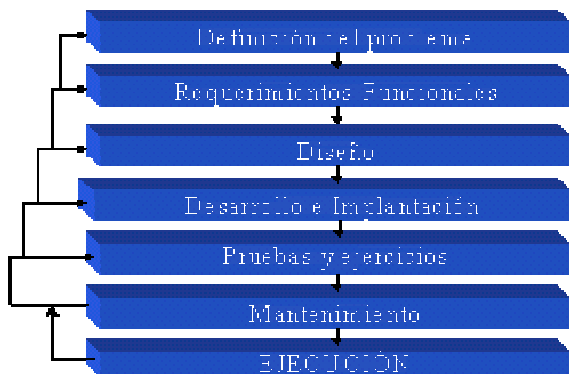
### 3. Metodología empleada

La Unidad de Seguridad Informática del Banco de la República en conjunto con las áreas funcionales está adelantando la construcción del *Plan de continuidad del Negocio para el Banco*, el cual pretende que la disponibilidad de las áreas funcionales críticas para la operación del Banco de la República sea adecuada.

Como parte integral de este plan se están adelantando por separado los *Planes de contingencia para las áreas funcionales*, los cuales buscan mitigar el impacto causado por el riesgo de que en un momento dado no se tenga disponibilidad de algún recurso requerido para la operación adecuada de dichas áreas.

Para la construcción de los planes de contingencia, el personal encargado de este proyecto ha sido certificado por el *Disaster Recovery Institute International (D.R.I.I.)*, este instituto además de presentar una metodología de trabajo, ofrece cursos de certificación, seminarios, revistas, etc. Para el mayor aprovechamiento y buen empleo de la metodología. Adicionalmente, debido a su cobertura internacional, existen diversos proveedores de servicios y de herramientas, así como otros profesionales certificados en este instituto y que por lo tanto siguen esta metodología, de tal forma que además de poder lograr soluciones integrales, se pueden intercambiar experiencias y conocimientos.

La metodología propuesta por el D.R.I.I. consta de seis (6) fases que se enuncian en el siguiente gráfico:



#### Fase 1. Definición del problema

En esta fase se deben desarrollar las siguientes tareas:

Conformación del equipo inicial de trabajo. Para comenzar a construir el plan de contingencia del área, se debe conformar un equipo interdisciplinario apoyado por la dirección del área funcional y motivado por la Unidad de Seguridad Informática, a este equipo pertenece como parte fundamental una persona idónea del área funcional quien actuará como coordinador y líder de la contingencia para el área apoyado en la coordinación general que se encuentra en la Unidad de Seguridad Informática, adicionalmente participan en este equipo representantes de las áreas de Auditoría y de Control Interno.

Familiarización de la metodología por parte del equipo de trabajo. El equipo debe conocer a fondo la metodología de trabajo que se está empleando en el Banco de la República para este tipo de proyectos. Para lo cual existen documentos y cuentan con el apoyo de las personas certificadas en ésta, de la Unidad de Seguridad Informática.

Definición de objetivos, alcance y escenarios del problema. El equipo inicial deberá definir los objetivos, el alcance y los escenarios que serán abarcados con el plan que se está construyendo.

Estructurar la administración del proyecto. Siguiendo el modelo de metodología presentado por el D.R.I. 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) y reportes de progreso (se deben realizar presentaciones a las directivas y proponer ajustes para aprobación).

Aprobación por parte de las directivas. Una vez terminadas estas tareas el grupo debe presentar un informe a las directivas, 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 presentados.

## 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 el área realiza y deben ser priorizados de acuerdo a la razón de ser del área dentro del Banco de la República. Para cada prioridad se debe señalar cual es el Tiempo Máximo de Espera para ser reanudados.

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

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

Análisis de riesgos y controles. Para llevar a cabo el análisis de riesgos y controles se debe recopilación de la bitácora de problemas, soluciones y controles existentes para las aplicaciones y facilidades e Identificar los documentos, procedimientos y estándares existentes. Posteriormente, analizar las posibles amenazas a los recursos y la exposición de estos a posibles riesgos.

Análisis de Impactos. Una vez determinados los riesgos sobre los recursos, analizar el impacto de estos sobre la operación del área funcional, tomando los costos tanto de nivel cualitativo como cuantitativo. Incluyendo un análisis costo/beneficio de la implantación de un control

Aprobación por parte de las directivas. Una vez terminadas estas tareas el grupo debe presentar un informe de recomendaciones a las directivas, 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 presentados.

## Fase 3. Diseño y desarrollo

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 identificar 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 llevar a cabo las estrategias y controles que deben entrar a operar durante una contingencia, deben identificarse las personas necesarias para llevar a cabo la recuperación, estas

personas deben ser agrupadas de acuerdo al carácter de las tareas a realizar durante ésta. Así mismo identificar el inventario de recursos de cada equipo de trabajo.

Organigrama de contingencia. Debe conformarse un organigrama de contingencia que permita que las personas adecuadas tomen las decisiones del momento. Este organigrama puede estar conformado por personas diferentes al organigrama de la organización con el fin de distribuir las tareas y evitar tropiezos para decisiones que deben ser tomadas con rapidez.

Diseñar el sistema de notificación. Con el fin de mantener el orden y respetar los conductos regulares durante los momentos de crisis, debe ser claro para todas las personas que laboran en el área como notificar y a quien los sucesos que se presenten durante las etapas de una emergencia.

Empalmar con planes ya existentes de otras áreas funcionales. Debido a que el plan que se está construyendo forma parte de un conjunto de planes de contingencia que conforman el Plan de Continuidad del Negocio para el Banco de la República, no debe permanecer aislado, sino que en este momento debe revisar otros planes paralelos en los que pueda apoyarse, con los cuales tiene que interactuar y a los que posiblemente servirá de apoyo.

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

Aprobación por parte de las directivas. Una vez terminadas estas tareas el grupo debe presentar un informe de recomendaciones a las directivas, 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 presentados.

#### Fase 4. Implantación

En esta fase se implantan las estrategias y controles diseñadas y aprobadas por la dirección, se realiza la compra y adquisición de los recursos necesarios para la recuperación, la firma de contratos, se escriben los procedimientos y responsabilidades para cada integrante de los equipos de recuperación en cada momento de la recuperación y se preparan los sitios de recuperación.

Aprobación por parte de las directivas. Una vez terminadas estas tareas el grupo debe presentar un informe a las directivas, 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 presentados.

#### Fase 5. Pruebas y ejercicios

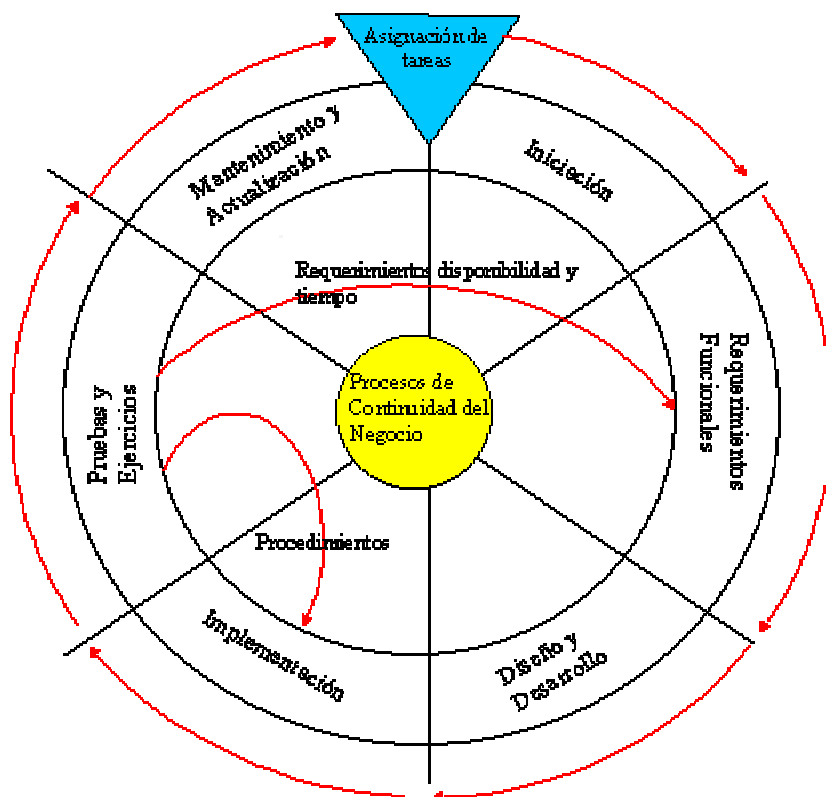
Diseñar las pruebas a realizar, las cuales consisten en simulacros de las situaciones que se contemplan en el plan, las cuales buscan entrenar al personal y probar los controles implantados y calcular los tiempos de respuesta tanto del personal como de los controles.

En esta fase también se debe concientizar a todo el personal de la posibilidad de ocurrencia de un incidente.

Cada prueba debe ser evaluada para retroalimentar el plan.

#### Fase 6. Mantenimiento

Un plan de contingencia no es un proyecto con inicio y fin, sino que es un proceso que nunca termina, por lo tanto debe diseñarse un plan de mantenimiento continuo para que este permanezca útil. El D.R.I. presenta el siguiente modelo que representa el ciclo natural de la construcción de un plan de contingencia:



En este modelo se puede observar que las fases de la metodología son realizadas iterativamente de manera natural, con el fin de refinar cada una de estas fases con elementos que se obtienen en fases posteriores, de esta manera, mas que un proyecto de "plan de contingencia" es un proceso que nunca termina, pero que permite que la organización logre los objetivos de control frente a un desastre.

#### 4. Objetivos y alcance del plan

##### Objetivos

El plan de recuperación ha sido desarrollado para lograr los siguientes objetivos:

Contar con una serie de acciones consolidadas y organizadas para administrar las actividades de respuesta y recuperación a seguir en caso una interrupción del servicio, evitando la confusión y reduciendo la exposición al error.

Proveer indicaciones y respuestas apropiadas a cualquier interrupción para reducir los impactos sobre el BANCO DE LA REPUBLICA resultantes de una interrupción temporal del servicio.

Garantizar la prestación del servicio para las operaciones esenciales de una manera eficiente, en caso de una falla en el servicio, incrementando la habilidad del BANCO DE LA REPUBLICA para recobrase de los daños a sus recursos.

##### Alcance

Este plan esta diseñado para proveer una respuesta rápida a los siguientes escenarios:

Incidentes que puedan causar daño físico en alguno de los pisos donde laboran las áreas, impidiendo el acceso.

Incidentes que puedan afectar directamente el acceso al edificio tal como una tempestad, evacuación del edificio debido a un atentado de bomba, un atentado externo tal como un fuego cerca de la instalación ó desordenes públicos.

Impedimentos o desastres regionales no esperados tales como Terremotos, que afecten el sector del Centro de la Ciudad.

Incidentes externos o internos, que potencialmente podría causar una interrupción en el negocio, tal como pérdida de potencia o del servicio de telecomunicaciones.

Falla sobre los componentes funcionales que interactuan en el servicio y que impiden que éste opere normalmente.