



**V REUNIÓN DE AUDITORES INTERNOS DE  
BANCA CENTRAL  
LIMA (PERÚ)**

**AUDITORÍA A LOS PLANES DE  
CONTINGENCIA Y CONTINUIDAD**

**Rafael García Saura  
Banco de España**

**Noviembre de 1999**



**BANCO DE ESPAÑA**

---

INSPECCIÓN DE SERVICIOS

## **AUDITORIA A LOS PLANES DE CONTINGENCIA Y CONTINUIDAD**

### ***I. INTRODUCCIÓN***

Para que una organización funcione correctamente y alcance los objetivos propuestos por la Dirección son necesarios unos activos o recursos. Estos recursos pueden ser humanos, materiales (edificios, instalaciones, hardware, etc.) e inmateriales (software, conocimiento acumulado, credibilidad o buena imagen, etc.).

Todos estos recursos se encuentran en un entorno de incertidumbre, que, en ocasiones, puede mostrarse agresivo y provocar interrupciones inesperadas del funcionamiento normal de la actividad de la empresa.

La mayor parte de estas interrupciones suelen ser temporales y las condiciones vuelven a ser normales en un período que no ocasiona situaciones críticas para la actividad normal de la empresa. Sin embargo, puede

haber circunstancias que generen interrupciones prolongadas, que lleguen a influir en la capacidad de funcionamiento de los servicios o impidan el desarrollo normal de los mismos en los locales habituales.

Para prever las consecuencias de estas situaciones y definir las estrategias que aseguren la continuidad de la actividad en el menor tiempo y con el menor trastorno posible, se hace preciso la elaboración de planes de contingencia y continuidad o de reanudación para las distintas actividades de las empresas con el fin de:

- ◆ Asegurar que todos los recursos conocidos y disponibles se utilizan para recuperar las funciones de la actividad tras una emergencia o desastre que haya afectado al edificio actual.
- ◆ Proporcionar un conjunto de procedimientos que serán ejecutados para restablecer los procesos prioritarios lo antes posible y con el menor impacto sobre la actividad, empleados, proveedores y clientes de la empresa.

Con respecto a estos planes, la misión de la Auditoría Interna debe consistir en comprobar que en la política de seguridad de la Entidad se contempla la existencia de planes de contingencia y continuidad o de reanudación de la actividad ante desastres; que dichos planes están formalizados por escrito y aprobados por la Dirección; que los empleados que tienen asignadas responsabilidades para su ejecución los conocen y están preparados para realizarlos; que abarcan todos los ámbitos críticos de la empresa y que en función de dicho aspecto se ha estable-

cido el orden de prioridad en la recuperación; y que tengan garantizada su actualización mediante revisiones y pruebas periódicas, otorgando con todo ello a la Institución la capacidad suficiente para dar continuidad a las operaciones ordinarias, dentro de los plazos previamente establecidos.

A lo largo de las siguientes líneas se tratará de hacer una exposición, en primer lugar, sobre la necesidad, concepto, estructura y criterios de elaboración de los planes de contingencia y continuidad o de reanudación de la actividad. En segundo lugar, se desarrolla una propuesta de programa de auditoría de dichos planes. Finalmente, se hace una breve referencia al plan de contingencia y de reanudación de la actividad del Banco de España.

## ***II. PLANES DE CONTINGENCIA Y CONTINUIDAD***

### ***II.1. Necesidad de los planes***

Como se ha indicado anteriormente, para que una organización funcione correctamente y alcance los objetivos propuestos por la Dirección son necesarios unos activos o recursos, que pueden ser humanos, materiales (edificios, instalaciones, hardware, etc.) e inmateriales (software, conocimiento acumulado, credibilidad o buena imagen, etc.).

También se ha afirmado, que estos recursos se encuentran en un entorno de incertidumbre, estando sometidos a **Amenazas**, que son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Las causas de estas amenazas son de diversos tipos: humanas, que a su vez, pueden ser intencionadas o no intencionadas, estas últimas como consecuencia de errores; y no humanas: accidentes o desastres (de origen natural o industrial), averías, interrupciones de servicios o suministros esenciales.

Por otra parte, hay que considerar la **Vulnerabilidad** de los activos, que es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo. Es una propiedad derivada de la relación entre activo y amenaza, que depende de la frecuencia en que la amenaza se convierta en una agresión materializada sobre el activo.

Asimismo, debe considerarse el **Impacto** en un activo, que es la consecuencia sobre éste de la materialización de una amenaza. El impacto será cualitativo cuando se produzcan pérdidas funcionales y cuantitativo si las pérdidas se pueden traducir en dinero de forma directa o indirecta.

Finalmente, el **Riesgo** es la probabilidad de que se produzca un impacto determinado en un activo, en una parte de la organización o en toda ella. El análisis de riesgo permite calcular un indicador ligado al par de valores, también calculados, de la vulnerabilidad y el impacto, am-

bos derivados a su vez de la relación entre el activo y la amenaza, para decidir si dicho riesgo es asumible o aceptable.

Fruto de una decisión y con el objeto de reducir el riesgo surge un conjunto de acciones que constituyen la **Función de salvaguarda**, que se materializa en el correspondiente **Mecanismo de salvaguarda** o conjunto de procedimientos o dispositivos que reducen el riesgo y que opera de dos formas posibles, que son, en general, alternativas:

- Neutralizando otra acción: la amenaza
- Modificando el estado de seguridad del activo agredido con reducción posterior al evento productor de dicho impacto.

Estas funciones y mecanismos de salvaguarda se clasifican según su forma de actuación, en dos grandes tipos:

- Preventivos: que actúan sobre la vulnerabilidad de los activos y reducen la potencialidad de materialización de la amenaza. Son salvaguardas preventivas la detección preventiva y la concienciación, información y formación del personal.
- Curativos o restablecedores: que actúan sobre el impacto y reducen su gravedad. Son salvaguardas curativas la corrección y la recuperación. Dentro de esta última merece destacarse el mecanismo de salvaguarda más importante: **los planes de contingencia y continuidad o de reanudación de la actividad**.

Resulta imposible garantizar que no ocurran hechos imprevistos que pro-

voquen desastres, por lo que una de las finalidades de estos planes consiste en minimizar la ocurrencia de éstos, así como tener definida y poner en marcha la organización necesaria para poder aplicar las acciones, procedimientos y recursos para la vuelta a la normalidad en el menor tiempo posible.

## ***II.2. CONCEPTO, CRITERIOS DE ELABORACIÓN Y ESTRUCTURA***

El proyecto, elaboración, puesta en vigor y mantenimiento de un plan de contingencia y continuidad o de recuperación de la actividad (en adelante Plan) debe estar enmarcado en la política general de seguridad de la organización, emanada de la alta Dirección. Es una labor de significativa envergadura y complejidad que debe estar sujeta a los correspondientes requisitos de planificación previa y rigor en su desarrollo. La falta de estos requisitos puede dar lugar a elaborar un Plan que no cumpla o no satisfaga los objetivos para él establecidos y resulte ineficaz en el caso de tener que ponerlo en práctica ante una interrupción de las actividades.

Por otra parte, el alcance y complejidad del Plan, en cuanto a las acciones, funciones y recursos que debe contemplar, estará determinado por el grado en que las actividades ordinarias de la organización dependan del funcionamiento del centro de proceso de datos, y por el carácter crítico de algunas de las aplicaciones informáticas para el funcionamiento normal de la empresa. Es obvio, que para el desarrollo de

las actividades de los Bancos Centrales el correcto funcionamiento de dicho centro es vital.

Con respecto a los sistemas informáticos, debe darse por supuesto que, previamente, se han implantado en la Entidad las medidas de seguridad física y lógica que aseguran la integridad, fiabilidad y disponibilidad de la información, siguiendo los principios del plan de seguridad informática de la Entidad. Por otra parte, debe existir un plan de protección civil que establezca los procedimientos y medios para la evacuación del personal de los edificios.

Por todo lo anterior, se pueden definir los planes de contingencia y continuidad o de recuperación de la actividad como una estrategia planificada, integrada por una organización, unos procedimientos operativos y unos recursos (humanos, técnicos y logísticos), que tienen como objetivo la restauración eficaz de los servicios paralizados o degradados por cualquier contingencia.

En consecuencia, el Plan debe contemplar un conjunto de normas, procedimientos de actuación, acciones, recursos humanos y técnicos, junto con la organización y coordinación necesaria de todos ellos, para dar respuesta a pérdidas de información o a cualquier interrupción, total o parcial, de las operaciones o de los servicios informáticos, con el fin de minimizar los efectos de estos sucesos en las actividades de la Organización y lograr en el menor plazo posible la recuperación o restauración de los distintos servicios.

Por lo tanto, es imprescindible conocer las funciones críticas de la Entidad y analizar y establecer su respaldo posible una a una, para poder realizar la restauración progresiva de las mismas en orden a su importancia.

Se trata, en primer lugar, de establecer una lista de elementos críticos (hardware, software, bases de Datos, aplicaciones, sistemas operativos, equipos, comunicaciones, periféricos, etc.) según el impacto que su carencia o mal funcionamiento causaría en el funcionamiento normal de la Institución y en el desarrollo de sus actividades.

Para ello, de cada uno de estos elementos se determina el tiempo durante el cual sería posible para la empresa asumir su falta de funcionamiento, ordenándolos de menor a mayor tiempo. De este modo, los elementos más críticos aparecerán en los primeros lugares. La elaboración de esta lista de elementos críticos requerirá la participación de los usuarios y propietarios de las aplicaciones que se considerasen críticas, además de todas las áreas del centro de proceso de datos.

Una vez realizado lo anterior, se debe determinar lo que podríamos denominar como nivel aceptable de seguridad. Se trata de encontrar un punto de equilibrio entre la seguridad que proporciona la disminución de riesgos, que de la implantación de estas medidas se puedan derivar, y el coste de implantación y mantenimiento de las técnicas y procedimien-

tos a emplear. Por ello, es necesario tratar de cuantificar dos tipos de magnitudes:

- ◆ Por un lado, los costes de los daños que pueden ocasionar en la empresa el impacto derivado de la materialización de las amenazas.
- ◆ Por el otro, los costes de implantación y mantenimiento de las medidas apropiadas para su contención.

En cuanto a su estructura, el Plan debe determinar con precisión el procedimiento a seguir antes de declarar la situación de emergencia, así como las personas que, en su caso, deben efectuar dicha declaración; identificar los servicios que se consideran críticos para el funcionamiento de la Entidad; contemplar los procedimientos y procesos de respaldo y los acuerdos con los proveedores; y definir la estructura de los distintos equipos de recuperación de la actividad así como sus funciones.

Para el caso de una destrucción o inhabilitación del centro de proceso de datos que impida la reanudación de las operaciones de forma inmediata, aunque sea de forma parcial o degradada, el Plan debe recoger la ubicación, características y necesidades para la utilización de un centro alternativo de respaldo (Centro Backup) hasta la reconstrucción o recuperación del centro origen.

El Plan debe ser sobre todo una organización viva, con distintos equipos que tienen previsto qué hacer y cómo en situaciones de emergencia,

para acelerar la restauración de los servicios dentro del tiempo previsto en el mismo, a fin de que no se produzcan pérdidas de cualquier tipo.

La puesta en práctica del Plan, dependiendo del alcance del siniestro, dará lugar a implicaciones de servicios y áreas de la Organización que en la elaboración del Plan han debido tomar parte, bien como equipo de desarrollo o al menos manifestando su opinión y conformidad.

Por último, el Plan debe adaptarse permanentemente a las circunstancias cambiantes, tanto del negocio como del entorno y de los medios tecnológicos y humanos disponibles en cada momento, por lo que deben realizarse pruebas sistemáticas para mantenerlo eficazmente al día, revisándolo y actualizándolo con una periodicidad anual, como mínimo. Asimismo, el Plan debe contemplar la formación y entrenamiento del personal para caso de siniestros.

### ***III. PROPUESTA DE PROGRAMA DE AUDITORÍA DEL PLAN***

Por lo expuesto anteriormente, podemos establecer que el objetivo general del programa de auditoría consiste en verificar la existencia de unos planes de contingencia y de continuidad o de recuperación de la actividad ante desastres; que contemplan un conjunto de procedimientos de actuación y de recursos necesarios para la restauración progresiva de los servicios en el caso de paralización de las actividades; en los

que están involucradas todas las áreas, departamentos y servicios de la Organización y que se mantienen debidamente actualizados, realizándose pruebas periódicas para comprobar su eficacia.

El logro de estos objetivos generales implica la verificación y evaluación de los siguientes aspectos del Plan:

### **III.1. Existencia y criterios de elaboración**

### **III.2. Contenido y finalidad**

### **III.3. Mantenimiento y pruebas**

#### **III.1. Existencia y criterios de elaboración**

El objetivo de este apartado es comprobar que en la Entidad realmente existe un plan de contingencia y continuidad o de reanudación de la actividad ante desastres, (en adelante Plan) formalizado por escrito y aprobado por la Dirección, que garantiza el respaldo de los recursos críticos y la recuperación de los servicios ante interrupciones imprevistas, permitiendo a la empresa dar continuidad a las operaciones ordinarias dentro de los plazos previamente establecidos.

Asimismo, se trata de verificar si los pasos seguidos en el desarrollo del Plan, así como las actividades, recursos y funciones implicados,

han sido objeto de planificación previa y en determinar si el proceso seguido en su elaboración ha sido idóneo para garantizar el resultado de un Plan eficaz de cara a la restauración progresiva de los servicios.

Las respuestas a las siguientes cuestiones permitirán valorar el cumplimiento de los objetivos propuestos:

- ¿Existe un Plan que está formalizado por escrito y aprobado por la Dirección?
- ¿La política de seguridad de la Entidad contempla la elaboración y el mantenimiento de un Plan, así como las medidas de salvaguarda que aseguran la fiabilidad, integridad y disponibilidad de la información?
- ¿El Plan se elaboró con arreglo a un proyecto documentado y autorizado, que se conserva adecuadamente?
- ¿En dicho proyecto se consideraron las posibles amenazas sobre los recursos, se definieron las actividades a realizar para la elaboración del Plan y se designaron a las personas encargadas de ejecutarlas?
- ¿En el alcance o ámbito a considerar por el Plan se tuvieron en cuenta todos los entornos y los grados de siniestralidad a los que el Plan debe dar respuesta?
- ¿En el estudio previo se incluyó la justificación de la inversión para garantizar la continuidad de los servicios?
- ¿En la elaboración del Plan participaron, además de todas las áreas

del centro de proceso de datos, los usuarios y propietarios de las aplicaciones?

- ¿En la elaboración del Plan se ha tenido en cuenta el plan de emergencia de los edificios?
- ¿La documentación del proyecto incluye el análisis de riesgos y, en caso afirmativo, la metodología utilizada para dicho análisis se estima correcta?
- ¿Se identificaron e inventariaron los recursos de todo tipo (hardware, aplicaciones en explotación, software de sistemas, otros) a incluir en el análisis de riesgos y se determinaron aquellos recursos que resultaban críticos para la Institución, efectuándose una estimación de la repercusión de un posible siniestro en los citados recursos?
- ¿Según el análisis de riesgos realizado se ha dado prioridad a los recursos y funciones más críticos para la organización?
- ¿Se han determinado los tiempos críticos de demora o de servicio interrumpido y el impacto económico y de imagen que pudiera ocasionar la interrupción total o parcial de los servicios?
- ¿Para la selección de recursos con los que dar respuesta a cada una de las situaciones de siniestro consideradas, se elaboró un estudio de las diversas alternativas, el cuál se conserva adecuadamente y se estima conforme?
- ¿Se han adoptado las medidas de prevención precisas para garantizar la disponibilidad de los medios mínimos necesarios para la recuperación de los recursos considerados críticos?

- ¿Se ha considerado la posibilidad de utilizar un centro de respaldo y la necesidad y disponibilidad de recursos (materiales y humanos) que ello implica?
- ¿Se han contemplado las alternativas para un siniestro que afecte al sistema de comunicaciones?
- ¿Ante la imposibilidad de usar los sistemas informáticos, se han establecido otros procedimientos alternativos para el funcionamiento de los distintos departamentos?
- ¿Se ha previsto en el proyecto algún plazo para la actualización del plan?

Como resumen de este apartado, debe efectuarse una valoración conjunta con respecto a la consecución de los objetivos a lograr en esta fase del Plan.

### **III.2. Contenido y finalidad**

El contenido del Plan debe ser el resultado final de la ejecución del proyecto y el desarrollo del mismo. Ha de estar debidamente aprobado y formalizado por escrito de forma pormenorizada, con el fin de minimizar la toma de decisiones llegado el caso de tener que ponerlo en práctica.

La revisión del contenido del Plan tiene por objeto comprobar que responde al proyecto autorizado y elaborado según los criterios expuestos en el apartado anterior; y que, siguiendo las instrucciones y procedi-

mientos indicados y utilizando los medios y recursos definidos, el equipo de recuperación podrá dar respuesta a una situación de emergencia en las actividades, garantizando la continuidad de las mismas y la prestación de servicios a la Organización con los niveles de calidad y puntualidad previstos en el referido Plan en función del alcance o gravedad del siniestro.

Las respuestas a las siguientes cuestiones permitirán valorar si el Plan en su contenido cumple los objetivos propuestos:

- ¿Están razonablemente contemplados y definidos los posibles sucesos que pudieran ocurrir y las situaciones, diferentes de la de normalidad, que se pudiesen dar?
- ¿Se determina con precisión el procedimiento a seguir antes de declarar la situación de emergencia, así como las personas que, en su caso, deben efectuar dicha declaración?
- ¿Están contempladas las actuaciones de respuesta para recuperar la actividad y definidas según un orden de prioridades?
- ¿Se asignan responsabilidades en su ejecución, que son conocidas por los empleados designados y éstos cuentan con la formación y entrenamiento necesarios para caso de siniestro?
- ¿Existe un equipo de dirección de la reanudación y un responsable del mismo para dirigir y coordinar las distintas actividades durante la contingencia o desastre?
- ¿Del equipo de reanudación y de cualquier otro previsto en el Plan, se han definido su componentes y funciones, así como los procedimientos y actividades que cada equipo ha de realizar para cada uno

de los niveles de siniestro contemplados, incluida la reconstrucción del centro de proceso de datos si fuese necesario?

- ¿Para la reanudación del funcionamiento de las aplicaciones críticas están definidas las necesidades de hardware, software y comunicaciones?
- ¿Están definidas unas normas sobre copias de seguridad de ficheros, que están aprobadas, actualizadas y se cumplen?
- ¿Están definidos unos procedimientos de obtención de copias de forma controlada y éstas se renuevan en los períodos establecidos?
- ¿Existe un inventario detallado de las copias de seguridad necesarias para la recuperación de los ficheros de las aplicaciones críticas y están definidas sus características?
- ¿La documentación correspondiente a las aplicaciones críticas existe y al igual que las copias de seguridad de los ficheros se conservan en otro edificio?
- ¿Están definidas las condiciones de custodia, acceso y uso de las copias de seguridad?
- ¿Está detallada la ubicación del centro alternativo de respaldo de proceso de datos, así como la configuración del mismo?
- ¿En relación con dicho centro, también se contemplan los requerimientos de hardware, software de explotación, ficheros, acuerdos con los proveedores, así como la inclusión del software de seguridad de dicha instalación?
- ¿Se han tenido en cuenta el área de comunicaciones, las redes corporativas, las redes de área local?

- ¿De los ordenadores personales que tienen información crítica existen procedimientos de recuperación específicos?
- ¿Están definidos unos procedimientos manuales de respaldo?

Como resumen de todo lo anterior, deberá efectuarse una valoración general de que el Plan garantiza la recuperación del nivel y calidad de servicio de la Entidad, dentro de los plazos previamente determinados.

### **III.3. Mantenimiento y pruebas**

Si la finalidad del Plan es dar respuesta lo más rápidamente posible a una interrupción de las actividades, con motivo de un incidente o siniestro, es imprescindible que para satisfacer dicha finalidad esté totalmente actualizado.

Igualmente, para garantizar su eficacia, el Plan debe ser probado periódicamente, además de cuando se produzcan modificaciones en el entorno informático que de alguna manera afecten a su contenido y puesta en marcha.

Dependiendo del alcance o magnitud de las modificaciones, las labores de adaptación del Plan pueden realizarse directamente variando su contenido (por ejemplo, los cambios de personal o las direcciones de localización de proveedores), o requerir un proceso más laborioso incluyendo la repetición de fases de desarrollo del Plan (por ejemplo, con mo-

tivo de modificaciones significativas de aplicaciones o de implantación de otras nuevas).

Las principales causas para la actualización del plan son las siguientes: añadir, cambiar o eliminar responsabilidades de la función; el cambio de Personal; las mejoras tecnológicas que se incorporen (hardware y software); la variación en el resultado del análisis de riesgos o del impacto en la actividad.

El objetivo de este apartado es verificar si se realizan puntualmente las labores de mantenimiento y pruebas del Plan, en consonancia con las modificaciones e innovaciones del entorno informático, de forma que dicho Plan se encuentre siempre a punto para ponerlo en marcha si fuera necesario.

Las respuestas a las siguientes cuestiones permitirán valorar si el mismo cumple los objetivos propuestos:

- ¿Están designadas las personas responsables del mantenimiento del Plan?
- ¿Está definido un calendario de actualizaciones para las diferentes funciones?
- ¿Se cumplen los plazos establecidos para la revisión y actualización del Plan?
- ¿Ante cambios significativos en los recursos de la empresa o en el entorno en el que se encuentra, se realiza una actualización del Plan?
- ¿Las actualizaciones realizadas se registran?

- ¿Se han planificado pruebas del Plan y establecido los plazos, motivos y responsable de las mismas?
- ¿Las pruebas se realizan puntualmente dejando constancia documental y se corrigen los fallos detectados?

Como resumen de este apartado, debe efectuarse una valoración conjunta con respecto a la consecución de los objetivos propuestos para el mismo.

Por último, debe efectuarse una evaluación conjunta del Plan.

#### ***IV. PLAN DE CONTINGENCIA Y DE REANUDACIÓN DE LA ACTIVIDAD DEL BANCO DE ESPAÑA***

Con el fin de poder asegurar una continuidad de la actividad con éxito y para asegurar que los clientes sigan recibiendo un servicio de la más alta calidad, el Banco de España desarrolló en el año 1996 un Plan de contingencia y de reanudación de la actividad (en adelante PRA) cuyo objetivo prioritario es que las funciones críticas de la actividad del Banco se reanuden en 2 horas y el resto de las funciones en 7 días.

Además de lo anterior el PRA persigue los siguientes objetivos:

- Prevenir o minimizar el peligro para las vidas del personal o de que alguien resulte herido.
- Prevenir o minimizar la pérdida o la corrupción de archivos de datos considerados como cruciales para la continuidad de las operaciones.
- Proteger la propiedad del Banco de España y otros activos (datos de clientes, pedidos, etc.).
- Iniciar los procedimientos de recuperación del desastre.
- Continuar con las funciones de las unidades de la actividad del Banco de España que se hayan visto afectadas por la situación.
- Recuperarse de una emergencia o desastre lo antes y lo más ordenadamente posible.
- Prevenir o minimizar el daño a los recursos informáticos, equipos de oficina, documentación, y otros materiales.
- Minimizar el número de decisiones a tomar tras un desastre.
- Minimizar la dependencia sobre una persona en particular durante el proceso de recuperación.
- Minimizar la necesidad de probar acciones de recuperación corriendo el riesgo de cometer errores cuando ocurra una emergencia o desastre.

El criterio o punto de partida para la elaboración del PRA fue que la reanudación o recuperación del desastre de la organización debía tener un enfoque global y no ser sólo un problema informático, por lo que cada Oficina será responsable del desarrollo y mantenimiento de su propio PRA y de las previsiones de tiempos de recuperación.

En consecuencia, cada oficina determinó de entre los sistemas de información de su propiedad o que utilizaba por delegación de otra, los que consideraba críticos para el mantenimiento de su actividad. En función de sus necesidades críticas, cada Oficina elaboró unas relaciones de recursos mínimos necesarios a utilizar en caso de desastre: de contacto con empleados críticos; de medios mínimos; de equipos de recuperación, de materiales críticos de almacenaje externo; de inventario de hardware y de software; de contacto con clientes, de proveedores y de apoyo a la Organización. Estas relaciones cada Oficina debe mantenerlas actualizadas permanentemente.

En cuanto al centro de proceso de datos, después de evaluar un conjunto de alternativas y tener en cuenta la importancia que para el Banco de España supone la continuidad del mismo, se decidió crear un centro de respaldo permanente, con el propósito de poder recuperar en dos horas su funcionamiento así como el de las aplicaciones que sustentan las operaciones del Banco y, por otra parte, evitar la pérdida de datos.

Se decidió que el ordenador que concentrase todas las operaciones del Banco será el situado en el edificio A, mientras que el ordenador situado en el edificio C será su centro de respaldo, para ello, se estableció un procedimiento de reanudación de la producción en el edificio C, configurando el ordenador de dicho edificio de forma que reprodujera permanentemente el entorno operativo del ordenador central.

Asimismo, para evitar la pérdida de datos se estableció un sistema de copia simultánea de los datos de A (Producción) en discos situados en los dos edificios, utilizando una unidad criptográfica y líneas de alta velocidad, comprobándose que dichas copias no suponían retardos apreciables para la producción.

El hecho de que se prevea que todas las funciones de la actividad tengan que reanudar sus operaciones en un edificio diferente al actual requiere que se haga una copia de seguridad de todos los datos necesarios y que se mantenga actualizada en cada uno de los edificios.

Por otra parte, el procedimiento de contingencia y de reanudación de la actividad implica la posible necesidad de utilizar los servicios del centro de respaldo. Ello conlleva, para asegurar su éxito y su eficacia, la creación de unas estructuras de trabajo perfectamente definidas, así como la definición clara y completa de las acciones a realizar.

Los equipos definidos para intervenir en caso de contingencia son: el Equipo de Dirección de la Reanudación (EDR) y los Equipos de Recuperación de las Oficinas.

♦ ***Equipo de Dirección de la Reanudación (EDR),***

Estará integrado por el Director General Adjunto del Departamento de Régimen Interior y los jefes de las Oficinas de Administración y

Obras e Informática y Organización y del Servicio de Seguridad. Sus funciones son: evaluar el alcance del desastre o contingencia; asignar la prioridad de las actuaciones; dirigir la recuperación de la actividad; informar al Gobernador, Subgobernador y Directores Generales; y activar los equipos de reanudación de las Oficinas.

◆ ***Equipos de Recuperación de las Oficinas***

Cuando ocurra el desastre, se activan los procedimientos de notificación y se forman los equipos necesarios para la reanudación de la actividad en el Banco de España. Estos equipos serán responsables de la recuperación de cada oficina y reportarán al Equipo de Dirección de la Recuperación y obedecerán sus instrucciones. Estos equipos son los siguientes:

**Equipo de Respuesta a la Emergencia de la Oficina**

Este equipo estará formado por el jefe y subjefes de la oficina y será el encargado de tomar decisiones. Su función principal es la evaluación de los daños y la recuperación de las funciones críticas de la oficina.

**Equipo de Iniciación a la Recuperación de la Oficina.**

Este equipo estará formado por subjefes, jefes de sección y miembros clave de cada función de la actividad. Su función principal será recuperar el material crítico del edificio de almacenamiento externo

y restablecer las operaciones críticas en el edificio o en otra zona alternativa.

#### **Equipo de Coordinación con Informática**

Este equipo coordinará, junto con la oficina de Informática, las necesidades de acceso y disponibilidad a los sistemas de información, datos y comunicaciones.

#### **Equipo de Rehabilitación**

Este equipo ayudará al Equipo de Respuesta a la Emergencia de la oficina según indique la evaluación de los daños. Tendrá como misión identificar y conservar todo el material que se ha salvado para su futuro uso.

En cuanto al mantenimiento y revisión del PRA, el administrador del plan de cada oficina es responsable de asegurarse de que el plan está mantenido y de que las actualizaciones se distribuyen a las personas correspondientes. El administrador solicitará de las personas de cada función específica para que le entreguen las actualizaciones necesarias sobre sus áreas respectivas.

Los principales motivos para realizar el mantenimiento del PRA son los siguientes: añadir, cambiar o eliminar responsabilidades de la función; el cambio de personal; las mejoras tecnológicas que se incorporen (hardware y software); la variación en el resultado del análisis de riesgos o del impacto en la actividad.

Finalmente, todos los cambios producidos serán anotados en el registro de mantenimiento del PRA.

Madrid, 30 de septiembre de 1999