

**IV REUNIÓN DE AUDITORES INTERNOS DE  
BANCA CENTRAL.  
CARTAGENA DE INDIAS (COLOMBIA)**

**EVALUACIÓN DE RIESGOS Y AUDITORÍA INTERNA**

**Rafael García Saura  
Banco de España  
Julio de 1998**



BANCO DE ESPAÑA

---

## **EVALUACIÓN DE RIESGOS Y AUDITORÍA INTERNA**

### **I. INTRODUCCIÓN**

El riesgo es un elemento inherente de la actividad bancaria y afecta tanto a los bancos privados como a los bancos centrales. Al igual que cualquier actividad empresarial, por el simple hecho de encontrarse en un entorno de incertidumbre, la actividad bancaria se ve sometida a una serie de riesgos, motivados, precisamente, por la falta de certeza sobre el futuro de sus operaciones y de la organización.

La primera pregunta que tendríamos que hacernos es ¿que entendemos por riesgo?. Si acudimos a la definición que de dicha palabra da la Real Academia Española: "Contingencia o proximidad de un daño" o más bien de la frase correr riesgo: "estar una cosa expuesta a perderse o a no verificarse", se ha de manifestar que estas definiciones son muy amplias y que pueden aplicarse a muy diversos aspectos y situaciones, tanto en el ámbito empresarial como fuera del mismo.

No obstante, dichas definiciones reflejan claramente lo que la asunción de un riesgo puede suponer para cualquier empresa: contingencia y probabilidad o proximidad de un peligro o daño, así como sus características típicas:

aleatoriedad e incertidumbre, puesto que no es previsible de antemano si el riesgo va o no a concretarse definitivamente en un siniestro. Así podemos afirmar que el riesgo es una situación en la que no existe garantía de éxito seguro, lo que, en términos económicos va íntimamente relacionado con la posibilidad de obtener un lucro.

El logro de la eficiencia en la gestión determina que no puedan eliminarse todos los riesgos y que, necesariamente, deban asumirse algunos de ellos, pero que tampoco puedan ignorarse, pues ello podría derivar en serios problemas para la entidad.

Conocer los riesgos a que estamos sometidos; cuales son, de entre todos ellos, los que van a tener una influencia significativa en la entidad; comprobar si existen herramientas, decisiones o acciones que se puedan tomar para reducirlos o eliminarlos; calcular los costes asociados a esas acciones; etc., son algunas de las cuestiones que deben realizarse antes de emprender cualquier actividad.

En este aspecto, la misión de la Auditoría Interna debe consistir, por una parte, en ayudar a la Dirección en el proceso de identificación, evaluación y control de los riesgos de la entidad, y por otra, verificar y evaluar el cumplimiento de las directrices de la Dirección en la gestión de los riesgos. Por otra parte, la evaluación de riesgos realizada por la Auditoría Interna podrá constituir la base sobre la que se estructure su plan de trabajo anual.

Al estudiar los riesgos en los que puede incurrir un banco central o cualquier entidad, habitualmente, existe una gran preocupación por los riesgos derivados de sus operaciones activas (riesgo de crédito, riesgo de tipo de interés, etc.), probablemente porque sean los que requieran mayor atención, además de poder ser cuantificados y suponer, casi siempre, mayor incertidumbre. Pero en

casi todas las entidades existe otro riesgo muy importante: el riesgo derivado del mal funcionamiento de su sistema informático de información. Este riesgo tiene mayor trascendencia en aquellos bancos centrales de cuyo sistema informático de información depende el funcionamiento de gran parte del mercado financiero.

A lo largo de las siguientes líneas se tratará de hacer una breve exposición de los principios relativos al control y gestión que deben regir los riesgos derivados de las operaciones activas, de nuestras entidades, para a continuación incidir especialmente en los riesgos que para cualquiera de nuestras entidades pueden derivarse de los sistemas informáticos de información (en adelante sistemas de información) y de las actuaciones a seguir para su gestión y reducción. Para concluir esta exposición, haré referencia a un riesgo que afecta directamente a los auditores: el riesgo de auditoría o riesgo de emitir un informe erróneo.

## **II. CONTROL Y GESTIÓN DE RIESGOS**

En el desarrollo de sus actividades los Bancos Centrales asumen diferentes tipos de riesgos. Estos pueden clasificarse en dos categorías principales: cuantificables (riesgos de crédito, interés, país, etc.) y no cuantificables (fraude, malversación, riesgo operativo de sus sistemas de información, etc.).

El control de todos estos riesgos es un aspecto importante del sistema de control interno de la entidad, y, consecuentemente, de la Auditoría Interna al ser una de sus funciones la revisión regular del alcance y la eficacia de los sistemas de control interno.

Toda organización, pública o privada, necesita implantar medidas que le

permitan identificar los riesgos, de cualquier naturaleza, que puedan afectar a la consecución de sus objetivos; y lo que es más importante, gestionar el riesgo de una manera eficaz de acuerdo con técnicas preventivas.

En la banca central, como en la mayoría de las entidades, debe ser una práctica habitual el establecer políticas y directrices para la gestión de los riesgos originados por sus actividades. Estas políticas y directrices, así como los procedimientos para ponerlas en ejecución deberán haber sido aprobados por la alta dirección y estar recogidos por escrito, los cuáles deben indicar aquellos tipos y niveles de riesgo que la Institución estará dispuesta a asumir, además de definir claramente las líneas de autoridad y de responsabilidad en la gestión de los mismos.

Para que este proceso de gestión de riesgos sea eficaz debe estar basado en unos principios generales y reunir una serie de componentes, relativos en ambos casos al proceso de detección, medición (en el caso de riesgos cuantificables) y control de las posiciones para las principales categorías de riesgos asumidos. Entre los principios generales en los que debe basarse la gestión de riesgos se pueden destacar los siguientes:

- a) Establecer una función independiente de gestión de riesgos, para supervisar todas las actividades y cubrir todas las facetas de los mismos.
- b) Para cada tipo de riesgo, establecer las políticas adecuadas de asunción de riesgos; esto implica fijar unos límites operativos apropiados para los riesgos cuantificables, definir unos procedimientos adecuados para mitigar los no cuantificables y determinar el procedimiento de autorización necesario para emprender nuevas actividades.

- c) El cumplimiento de las políticas y de los límites debe ser vigilado de forma continua y establecerse unos procedimientos bien definidos de seguimiento de los posibles incumplimientos. Asimismo, dichas políticas y límites deben revisarse periódicamente teniendo en cuenta la evolución del mercado.

De acuerdo con estos principios, los componentes que debe reunir todo proceso de gestión de riesgos son los siguientes:

### **Cuantificación global de los riesgos**

Los riesgos deben medirse y agregarse de forma que la dirección pueda valorarlos de forma consolidada. La cuantificación de riesgos debe incluir la determinación de posibles acontecimientos o cambios en el comportamiento del mercado que pudieran tener efectos desfavorables.

### **Limitación de riesgos**

Deben establecerse unos límites globales para cada clase de riesgos que pueden originarse de las actividades de la entidad. Asimismo, debe existir un sistema de control, de forma que las posiciones que superen determinados niveles de riesgo preestablecidos reciban inmediata atención.

### **Información**

Un sistema de información a la dirección preciso, completo y rápido es fundamental para garantizar una actuación prudente en las actividades de la entidad.

### **Evaluación y revisión de la gestión**

Los diferentes componentes del proceso de gestión de riesgos deben ser regularmente revisados y evaluados. Esta revisión deberá tener en cuenta cualquier cambio en las actividades de la entidad y en el mercado.

### **Control interno**

La existencia de un buen sistema de control interno deberá favorecer la eficacia en la gestión de los riesgos. Estos controles deberán estar en línea con los objetivos y controles generales internos de la entidad. El control de las conciliaciones se estima particularmente importante.

### **Auditoría Interna**

La auditoría interna tiene un papel importante en la evaluación de la eficacia general de las funciones de gestión de riesgos de la entidad. Deberá evaluar con regularidad la eficacia de los controles internos relativos a la cuantificación, información y limitación de riesgos. Asimismo, deberá analizar las situaciones en que se superen los límites de riesgo y verificar la fiabilidad y rapidez de la información facilitada a la alta dirección.

Por otra parte, para la Auditoría Interna la evaluación de los distintos riesgos puede servir como determinante de la planificación de su trabajo, pues supone poder determinar de la forma más objetiva posible cuáles son las áreas de la entidad a las que debe dar prioridad en sus análisis o bien, cuales son los riesgos sobre los que debe centrar sus recursos.

La inclusión de algún sistema de valoración del riesgo reduce la subjetividad en la selección de áreas de trabajo y en la asignación de prioridades,

ya que complementa la propia opinión, basada en la experiencia, con una serie de elementos cuantificables. No obstante, no elimina por completo tal subjetividad, lo cual es importante en la medida en que ésta compila toda la experiencia.

No existe un modelo estándar de valoración del riesgo que pueda ser aplicado a cualquier empresa, pues cada una tiene sus propias características, y el auditor debe buscar las magnitudes más representativas del riesgo. Lo importante es conocer la filosofía de los métodos de valoración del riesgo, para poder luego adaptarlos a cada caso concreto.

En este sentido, los principales aspectos de un sistema de valoración del riesgo serían:

- a) Agrupar las principales áreas de actividad de la empresa a efectos de auditoría.
- b) Identificar los elementos que mejor pueden definir su importancia.
- c) Analizar el peso específico de estos elementos sobre el total de los mismos, con el fin de establecer ponderaciones.
- d) Introducir el factor experiencia, con la finalidad de enriquecer el modelo mediante un mecanismo de retroalimentación (feed-back).

El producto final sería una relación de áreas de trabajo con una puntuación que permitiría asignar prioridades y ajustar los recursos de forma eficiente.

Antes de analizar los riesgos que para cualquiera de nuestras entidades

pueden derivarse de los sistema de información, a continuación se realiza una breve descripción de los principales riesgos activos, cuya gestión debe llevarse a cabo en la forma expuesta anteriormente.

### **Riesgo de crédito**

La concesión de un préstamo o crédito supone un riesgo en función de la solvencia del deudor, del plazo, de la cuantía, del tipo de crédito, de la garantía específica de la operación, de la finalidad, de la concentración, de la moneda, del país, etc.

El Banco de Pagos Internacionales, en un informe sobre sistemas de compensación, define el riesgo de crédito como el "riesgo de que una contrapartida no satisfaga una obligación cuando ésta venza y nunca pueda saldar esa obligación por su valor total. La bancarrota de una contrapartida es, a menudo, asociada con este tipo de problemas, pero también puede haber otras causas."

Asimismo, el Banco de España en la circular 4/1991, de 14 de junio, sobre normas de contabilidad de las entidades de depósito, identifica dos factores de riesgo de crédito: riesgo de insolvencia y riesgo-país.

El Riesgo de insolvencia mide la posibilidad de que los fondos prestados en una operación financiera no se devuelvan en el plazo fijado de vencimiento.

El Riesgo-país mide, con respecto a las inversiones internacionales, un conjunto de factores objetivos, tales como la inestabilidad política o el deterioro económico que puedan hacer improbable que un determinado país haga frente a sus obligaciones financieras. La citada circular del Banco de España establece, asimismo, su definición: "Se entiende por riesgo-país el que concurre en las

deudas de un país, globalmente consideradas, por circunstancias distintas del riesgo comercial habitual. Comprende el riesgo soberano y el riesgo de transferencia.

El Riesgo soberano es el de los acreedores de los estados o de las entidades garantizadas por ellos, en cuanto pueden ser ineficaces las acciones legales contra el prestatario o último obligado al pago por razones de soberanía.

El Riesgo de transferencia es el de los acreedores extranjeros de los residentes de un país que experimenta una incapacidad general para hacer frente a sus deudas, por carecer de la divisa o divisas en que estén denominadas."

### **Riesgo de tipo de interés**

El riesgo de tipo de interés es el que se deriva de las fluctuaciones en los tipos de interés de los activos y pasivos que se mantienen en cartera. Entre los posibles factores que determinan la variación de los tipos de interés pueden citarse: la política monetaria, el déficit público, la tasa de inflación y los tipos de interés exteriores.

### **Riesgo de tipo de cambio**

Por riesgo de tipo de cambio se entiende la probabilidad de incurrir en pérdidas como consecuencia del mantenimiento de posiciones en moneda extranjera y de la evolución adversa de las cotizaciones de las divisas. Estas posiciones se refieren tanto a los activos y pasivos patrimoniales como a derechos y obligaciones.

Como posibles causas de variación de los tipos de cambio se pueden

citar los diferenciales existentes entre las tasas de inflación y los tipos de interés nacional y extranjeros.

### **III. RIESGOS DE LOS SISTEMAS DE INFORMACIÓN**

El Sistema de Información de una organización está expuesto constantemente a un conjunto indeterminado de eventos que pueden impedir el cumplimiento adecuado de los tres objetivos esenciales previstos en la realización de todo sistema:

- **La disponibilidad de la información**, lo que supone que el sistema se encontrará operativo en todo momento, evitándose las pérdidas de datos o la imposibilidad de procesarlos.
- **La integridad del sistema**, es decir, la información puesta a disposición de los usuarios o utilizada por los distintos subsistemas será actualizada, exacta, autorizada, oportuna y completa. Para ello se deberán evitar las modificaciones no requeridas y los errores de todo tipo.
- **La confidencialidad de los datos**. Cada usuario tendrá acceso únicamente a la información que le corresponde y la manipulará según unas restricciones preestablecidas.

Para identificar los riesgos potenciales a los que está expuesta la función de información, podemos clasificar los riesgos atendiendo a su origen, distinguiendo entre los que podemos denominar riesgos accidentales de aquellos otros de origen intencionado.

Entre los riesgos de origen accidental podemos considerar: desastres naturales, incendios, inundaciones, averías de diverso tipo, etc.. Entre los de

origen intencionado se pueden destacar: fraudes, sabotajes, sustracciones de información, difusión incontrolada de la misma al exterior y la introducción de virus informáticos.

Además de los anteriores, el uso de la tecnología de la información implica otros riesgos adicionales, como son la pérdida de datos y programas debido a medidas de seguridad inadecuadas, fallos en los equipos o sistemas, procedimientos inadecuados de copias y reconstrucción, información imprecisa a la dirección a consecuencia de unos sistemas de desarrollo pobres, con el peligro de que algunas decisiones puedan basarse en informaciones poco fiables o engañosas procedentes de unos sistemas de información mal diseñados o mal controlados y, finalmente, la falta de disponibilidad de instalaciones alternativas y compatibles en caso de interrupciones prolongadas en el funcionamiento del equipo.

Frente a estos riesgos potenciales, se pueden adoptar alguna de las siguientes posturas: aceptar el riesgo, dada en muchos casos su baja posibilidad de ocurrencia; transferir el riesgo, contratando los correspondientes seguros - esta transferencia no parece posible en el caso de bancos centrales y, por otra parte, alguna información perdida podría ser irremplazable-; evitar o tratar de minimizar el riesgo.

Como es lógico, un banco central sólo puede optar por la última de las opciones contempladas. Para ello, las medidas de carácter preventivo que consigan evitar o minimizar la probabilidad de ocurrencia de los riesgos citados se han de basar en dos actuaciones: en primer lugar, en la definición de unos controles organizativos e internos, sustentados por un conjunto de principios generales, cuyo objeto sea proteger los sistemas de información y lograr que cumplan los objetivos para los que fueron diseñados. Ello lleva consigo la elaboración y puesta en marcha de un Plan de Seguridad Informática. En

segundo lugar, la implantación de la Auditoría Informática Interna, que pueda asegurar la idoneidad y la eficacia de los controles internos establecidos a los sistema de información, así como proponer las mejoras que sean susceptibles de incorporar, como resultado de sus evaluaciones.

Los principios generales en los que deben basarse los controles organizativos e internos de los sistemas de información son los siguientes:

- a) Establecer unos procedimientos, aprobados por la alta dirección, para la formulación, aprobación, implantación y revisión de planes estratégicos y a corto plazo de adquisición de tecnología de la información, para garantizar la existencia y el mantenimiento de una plataforma técnica adecuada, de acuerdo con las necesidades presentes y futuras de la entidad.
- b) Definir las políticas, normas, procedimientos y controles de todos los aspectos relacionados con las actividades de los sistemas de información, con el fin de facilitar su coordinación con las demás funciones organizativas que mantienen o utilizan dichos sistemas y para servir también como base para la planificación, control y evaluación de estas actividades.
- c) Establecer y mantener sistemas de desarrollo y metodologías de control de calidad, que puedan ofrecer una garantía razonable de que los sistemas cumplen con las funciones para las que han sido diseñados y proporcionan una documentación normalizada que facilite su uso (por usuarios y operadores) y su futuro mantenimiento.
- d) Establecer unos procedimientos para la contratación de servicios externos (outsourcing).

- e) Mantener una adecuada separación entre los sistemas de desarrollo y los demás entornos, de forma que cada uno solamente pueda acceder a la información del otro a través de controles estándares.
- f) Dotar a los sistemas de unos controles y unos rastros de auditoría (incluyendo los equipos de reserva) que garanticen la veracidad y la integridad de los datos de entrada y de salida, la autorización para utilizarlos, el arranque de procesos en caso de interrupción y la auditoría de transacciones.
- g) Establecer unas políticas y procedimientos de seguridad física para minimizar los riesgos de interrupción de las operaciones y limitar el acceso al material sensible sólo a las personas autorizadas.
- h) Establecer unos procedimientos y controles de seguridad lógica para restringir el acceso a los datos y a los programas a las personas autorizadas (claves de acceso, encriptación, etc.) y comunicar e investigar las violaciones de las normas de seguridad.
- i) Definir y mantener un plan de contingencias para garantizar la continuidad de las operaciones vitales y permitir la reanudación, dentro de un tiempo razonable, del funcionamiento normal después de cualquier interrupción imprevista debida a diferentes clases de contingencias. El plan de contingencias debe estar sujeto a comprobaciones periódicas.
- j) Garantizar que la función de auditoría interna pueda asegurar la idoneidad y la eficacia de los controles internos de los sistemas de información, así como la calidad de dichos sistemas.

Como se ha mencionado anteriormente, la aplicación de estos principios lleva consigo la elaboración y puesta en marcha de un Plan de Seguridad Informática. Se conoce como Seguridad Informática en el ámbito de los sistemas de información, al conjunto de técnicas, medidas y procedimientos encaminados a garantizar el logro de los objetivos esenciales en el desenvolvimiento de dichos sistemas.

La Seguridad Informática se puede considerar integrada por dos grandes áreas: la seguridad física y la seguridad lógica.

Correspondería a la seguridad física el conjunto de mecanismos, normas y procedimientos encaminados a la protección contra daños eventuales de las personas, las instalaciones, los equipos centrales o periféricos y los elementos de comunicación.

La Seguridad lógica engloba el conjunto de medidas, operaciones y técnicas orientadas a la protección de la información contenida o a contener dentro del sistema, contra la destrucción, la modificación indebida, la divulgación incontrolada o el retraso en su elaboración.

Para conseguir un nivel óptimo de seguridad lógica, se han de adoptar diferentes medidas de protección, que podemos considerar agrupadas en torno a las tres fases fundamentales en el desarrollo de un sistema, a saber:

### **1. En la fase de diseño y realización de aplicaciones:**

Inclusión en la programación de controles formales y lógicos, para prevenir la aparición de errores en la introducción y captura de datos.

Introducción de controles de protección en los programas y ficheros de datos, para evitar la modificación accidental de éstos a lo largo de algún proceso.

Adecuado grado de calidad y detalle en toda la documentación necesaria.

Para ello sería conveniente utilizar metodologías estándar.

### **2. En la fase de implantación y puesta a punto:**

Realización de pruebas exhaustivas con todos los programas, utilizando juegos de ensayos completos.

Formalizar los procedimientos de puesta en explotación de las aplicaciones, separando claramente las librerías de programas en explotación de las que están en desarrollo.

### **3. En la fase de explotación:**

Controlar el estricto cumplimiento de la normativa y procedimientos de operación establecidos.

Realización de copias de seguridad o "backup", conservándolas en zonas protegidas contra acciones perjudiciales.

Establecer y controlar los canales de distribución de documentación.

Limitar el acceso del personal al Centro de Proceso de Datos en función de sus tareas.

Definir los niveles de importancia y de confidencialidad de los datos para establecer el acceso a las librerías y a las Bases de Datos.

Preparar procedimientos automáticos de explotación que reduzcan al máximo la intervención de los operadores y sus posibles errores.

Mantener actualizado un registro de incidencias surgidas en la utilización del sistema.

Registro por parte del sistema de todas las acciones realizadas por cada terminal y usuario.

Establecer diferentes niveles de acceso a la información.

Utilización de claves de acceso a la información o "pass-word".

Encriptar la información de alto valor.

Revisar periódicamente la seguridad de los enlaces de telecomunicaciones.

Este último aspecto, se refiere a las redes de transmisión de datos que precisan de un sistema especial de seguridad, complementario del comentado en los anteriores apartados. Tanto según su forma de diseño (estrella, bus o anillo) como en función del software utilizado, la seguridad en cada tipo de red tendrá unas características distintivas.

El objetivo de un sistema de seguridad para redes es el de garantizar el acceso controlado desde el terminal a la aplicación, la integridad en la transmisión de información por red y la confidencialidad de los datos transmitidos por la misma.

Entre el riesgo de carácter específico que afecta especialmente a las redes de comunicación está la posibilidad de accesos no autorizados desde el exterior. De esta manera podrían entrar virus en el sistema, o simplemente acceder al mismo "piratas" (hackers) que, para obtener beneficio o por simple diversión, consulten, alteren o destruyan datos o programas sensibles.

Al hablar de seguridad en redes locales, es preciso hacer una especial

referencia a los problemas específicos del trabajo en red, y más concretamente al control que se ejerza sobre el acceso a las comunicaciones. En este sentido, se pueden destacar una serie de medidas para la correcta operatividad de la red de área local: limitar los niveles de acceso a la red, estableciendo los controles oportunos; criptografiar los datos confidenciales que circulen por la red y proteger físicamente la red contra conexiones no autorizadas (pinchazos).

En casos extremos se podría considerar la posibilidad de introducir un ordenador intermedio como "filtro" o llave de acceso; o bien aislar el ordenador conectado al exterior del resto de la red interna.

Finalmente, no quiero dejar de señalar la existencia de una actividad, que no se ciñe únicamente al área de los sistemas de información, y que nace de la estrategia empresarial basada en la reducción drástica de los costes fijos en las empresas, con el propósito de mejorar su competitividad. Es la contratación de servicios externos, el llamado OUTSOURCING en el ámbito informático, que puede ser origen y motivo de importantes riesgos.

Hay servicios primarios con responsabilidades muy concretas, en donde esta contratación puede no ser aconsejable o albergar bastantes riesgos. Otros servicios, en cambio, tras un cuidadoso análisis de riesgos, al ser menores podría asumirse dicha contratación.

Desde el punto de vista de la Auditoría Interna es preciso analizar con rigor aquello que puede contratarse externamente y lo que no; y de lo que se estima que se puede contratar hasta donde se puede; y hasta donde pueden llegar las responsabilidades; y hasta qué punto se deben asumir los riesgos.

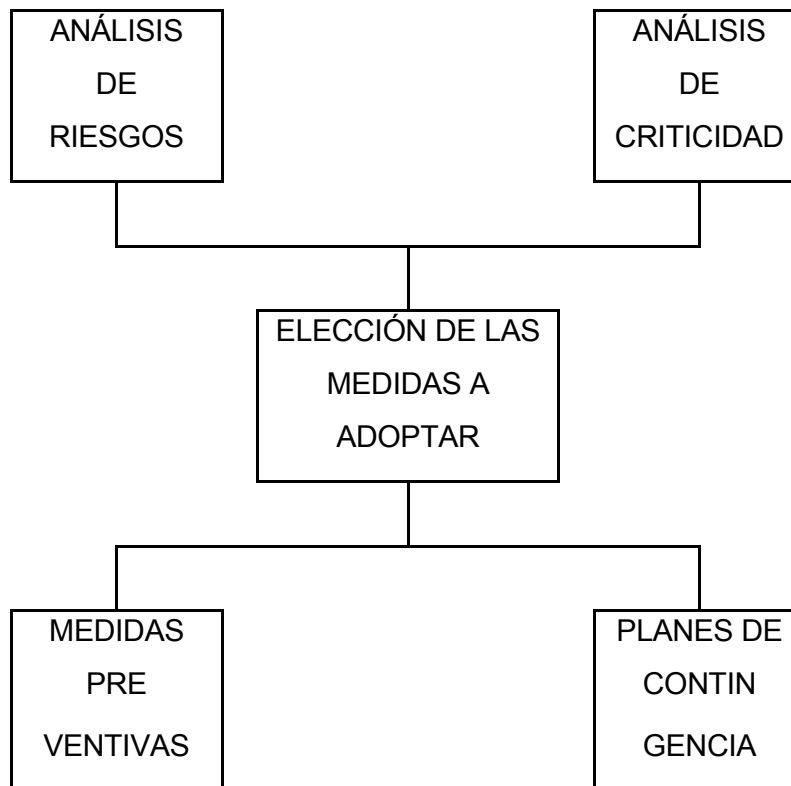
En el caso de contratación externa, las actuaciones del personal contratado debe estar controlado por personal propio, el cual aplicando estrictos

y eficaces procedimientos debe dirigir todas las actuaciones de dicho personal, revisando que sus procedimientos y métodos de trabajo se ajustan a lo establecido en nuestras propias normas y procedimientos.

De acuerdo con todo lo que acabamos de ver, la seguridad informática se establece como un compromiso entre la necesaria operatividad del sistema, frente a los diversos riesgos potenciales y los diferentes mecanismos y procedimientos que permiten minimizar la probabilidad de aparición de incidentes, o reducir sus efectos.

Cada uno de estos procedimientos supone un coste (directo e indirecto) para el funcionamiento del sistema que habrá que tomar en consideración. Ello nos lleva a considerar a la seguridad informática como un problema de carácter económico, en el que se tratan de alcanzar unos objetivos o resultados determinados mediante la asignación eficiente de unos recursos, que tienen un coste. En consecuencia, la seguridad de un sistema de información debe ser, por tanto, cuidadosamente planificada y presupuestada, determinándose los niveles aceptables de seguridad para la organización y su coste, así como los medios más idóneos para conseguirlos.

Las tareas a llevar a cabo con esta finalidad, se pueden resumir en el esquema siguiente:



### a) Análisis de riesgos

La primera tarea consiste, por una parte, en la determinación de los riesgos a los que pueden estar expuestos los sistemas de información de la organización. Por otra parte, se deberá tratar de estimar la probabilidad de ocurrencia de cada uno de los riesgos detectados, teniendo en cuenta que no existen riesgos y probabilidades asociables de modo estándar, sino que ambos varían con las características de cada instalación. Algunas de éstas probabilidades se pueden determinar mediante el conocimiento de la frecuencia con que se presentan determinados sucesos, o recurriendo a las estadísticas propias de la instalación.

## **b) Análisis de criticidad**

Se trata, en primer lugar, de establecer una lista de elementos críticos (Bases de Datos, aplicaciones, sistemas operativos, equipos centrales, de comunicaciones, periféricos, etc.) según el impacto que su carencia o mal funcionamiento causaría en la operatividad del sistema de información. Para ello, a cada uno de estos elementos se les asigna un tiempo durante el cual sería posible para la empresa, asumir su falta de funcionamiento, ordenándolos de menor a mayor tiempo. Los elementos críticos aparecerán en los primeros lugares.

Una vez realizado lo anterior, se puede comenzar con la determinación de lo que podríamos denominar como nivel aceptable de seguridad. Se trata, para ello, de encontrar un punto de equilibrio entre las técnicas y procedimientos a emplear y su coste, frente a los beneficios que a partir de estas medidas se pueden derivar. En consecuencia, es necesario tratar de cuantificar dos tipos de magnitudes: por un lado, los daños que se pueden ocasionar en el sistema y una estimación de los costes derivados de dichos daños; y por otro, los costes de implantación y mantenimiento de las medidas apropiadas para su minimización.

## **c) Elección de medidas a adoptar**

El apartado de medidas a adoptar comprende un conjunto de acciones y decisiones, así como la asignación de recursos (de personal, equipos, software, etc.) para tratar de evitar los riesgos tanto de origen accidental como intencionado. Se suelen contemplar dos categorías fundamentales de medidas:

De Prevención: engloba a todas aquellas medidas dirigidas a minimizar la probabilidad de ocurrencia de incidentes.

De Corrección: aquéllas que tratan de corregir los daños ocasionados una vez producido el incidente. Estas medidas vendrán recogidas en el Plan de Contingencias, cuyos objetivos se pueden resumir en los siguientes puntos:

- Minimizar las interrupciones en la operación normal.
- Limitar la extensión de las interrupciones y de los daños que produzcan.
- Posibilitar una vuelta al servicio rápida y sencilla.
- Ofrecer a los empleados unas normas de actuación frente a casos de emergencia.
- Proveer de medios alternativos de proceso en caso de catástrofe.

El Plan de Contingencias debe recoger, en forma de planes unitarios, las respuestas a los diferentes problemas que pueden surgir. Cada uno de estos planes unitarios contendrá al menos, los siguientes bloques:

- El Plan de Emergencia. Será la guía en la que se fijen las acciones a realizar inmediatamente después de cada fallo o daño. El plan debe contener unas acciones inmediatas y otras posteriores, y además reflejar la asignación de responsabilidades al personal.
- El Plan de Recuperación. Debe contemplar las normas de actuación a emprender para reiniciar todas las actividades de proceso interrumpidas.

La otra actividad necesaria para conseguir evitar o minimizar la probabilidad de ocurrencia de riesgos en los sistemas de información corresponde a las que realiza la Auditoría Informática Interna. Como es bien sabido, es una función de valoración independiente establecida por la dirección,

que tiene como misión principal la de velar por la integridad y eficiencia de los sistemas de información, así como de evaluar el alcance y la eficacia de los sistemas de control interno y de seguridad informática establecidos en relación con dichos sistemas, en cumplimiento de las políticas y principios dispuestos por la dirección. Sobre las actuaciones específicas de la Auditoría Informática Interna tuve ocasión de exponer, en la pasada reunión de Brasil, mi propuesta sobre la concepción y las actuaciones de la misma.

En consecuencia, no voy a extenderme más sobre este aspecto, remitiéndoles a dicho documento, por lo que, seguidamente, paso a comentar otro tipo de riesgo que nos afecta directamente a los auditores: el riesgo de auditoría.

#### **IV. EL RIESGO DE AUDITORÍA**

Uno de los temas más importantes que los auditores externos e internos han de tener en cuenta, tanto en la planificación de la auditoría como en la ejecución de la misma y en el informe posterior, es el riesgo de emitir un informe erróneo.

El riesgo de auditoría consiste en el error que puede producirse en el informe como consecuencia de no disponer de una evidencia completa sobre aquellos hechos analizados que se relacionan con el objeto de la auditoría, bien por no haber podido realizar todas las pruebas que el auditor considerase necesarias o porque del resultado de éstas no consiga de forma completa la certeza moral necesaria.

Un auditor nunca podrá tener una seguridad absoluta al expresar una opinión. Cada dictamen representa la adquisición de un riesgo, que debe ser estimado y mantenido dentro de límites razonables.

El modelo de riesgo de auditoría propuesto por la normativa internacional para los auditores externos relaciona el riesgo de auditoría con los tres componentes siguientes: el riesgo inherente, el riesgo de control y el riesgo de detección. Las definiciones de estos componentes figuran en las normas internacionales de auditoría (NIA número 25):

"El **riesgo inherente** es la posibilidad de que un saldo de una cuenta o un tipo de transacción contenga errores significativos, individualmente o agregados con otros similares, asumiendo que no están relacionados con el control interno."

"El **riesgo de control** es el riesgo de que los saldos de las cuentas o una clase de transacciones puedan contener errores significativos, individualmente o cuando se agreguen con otros errores similares, siendo la característica de este riesgo que no puede ser prevenido o detectado oportunamente por el sistema de control interno."

"El **riesgo de detección** es el riesgo de que un procedimiento de auditoría no detecte un error que exista en un saldo de una cuenta o en una clase de transacción, que pueda ser significativo, individualmente considerado o cuando se agregue a errores similares. El nivel de riesgo de detección se relaciona directamente con los procedimientos de auditoría."

Los riesgos inherente y de control difieren del de detección en que su existencia es independiente de la auditoría y no tienen nada que ver con el auditor externo, éste ha de aceptarlos porque son intrínsecos a la empresa. El auditor no puede controlarlos, pero si evaluarlos o estimarlos, y a partir de aquí, establecer el nivel de riesgo de detección que esté dispuesto a aceptar y así reducir el riesgo de auditoría deseado a un nivel aceptablemente bajo. Por tanto,

el riesgo de auditoría propiamente dicho es el de detección, el que fija el auditor ateniéndose a en qué medida ha asumido los otros dos riesgos.

Si aplicamos este mismo modelo a la Auditoría Interna, los riesgos inherente y de control deberían ser perfectamente conocidos y evaluados por la misma, al ser, como se ha dicho, riesgos propios de cada empresa.

En cumplimiento de su misión, la Auditoría Interna debería conocer cuáles son las áreas más críticas y cuáles son las operaciones más usuales de su propia empresa, por lo que podría determinar con un pequeño margen de error el riesgo inherente asumido. Asimismo, la evaluación, calidad y eficacia del control interno de la empresa es una de las funciones principales de la Auditoría Interna y, en consecuencia, al objeto de cumplir de forma eficaz su misión, la Auditoría Interna debería conseguir minimizar el riesgo de control e, incluso, procurar anularlo.

Quedaría el riesgo de detección, que, como se ha dicho anteriormente, el auditor puede manejar o fijar en función de mejorar la eficacia de los procedimientos de auditoría y aumentar el alcance de los mismos.

El aumento en la eficacia de los métodos y procedimientos de auditoría está en función de la mejora constante de los procedimientos de análisis de la Auditoría Interna, según la naturaleza y calidad de dichos métodos, la confiabilidad de los datos a los que se aplican los procedimientos y el nivel de detalle en que estén disponibles dichos datos.

En el aspecto del alcance de los procedimientos de auditoría, el error puede surgir del nivel o representatividad de la muestra examinada, que al aplicar a la misma las pruebas substantivas de auditoría podría llevar al auditor a conclusiones inadecuadas, por no haberse aplicado el muestreo preciso o haber

comprobado toda la población. La clave para reducir este tipo de riesgo es aplicar un procedimiento adecuado de muestreo o, en ocasiones, puede ser necesario comprobar toda la población.

Son los criterios de importancia relativa y de riesgo probable los que deben orientar al auditor en orden a definir la suficiencia y adecuación de la evidencia. Ambos conceptos se influyen mutuamente y, por ello, deben ser considerados de forma conjunta al establecer el juicio de valor correspondiente.

El concepto de importancia relativa y riesgo probable no afecta exclusivamente a la obtención de la evidencia, sino también a otros aspectos del trabajo de la Auditoría Interna, como, por ejemplo, a la elaboración del informe.

Por otra parte, no resulta sencillo realizar una calificación de ambos conceptos por la propia indeterminación que representan. Existen informaciones que tienen importancia con relación a otras, aunque no la tengan en sí mismas, y viceversa. En otras ocasiones, ciertas informaciones, por demasiado prolijas o detalladas, pueden oscurecer el proceso de auditoría o el informe. Por ello, no existen reglas fijas en relación a este tema que queda en función de la calificación que establezca el propio auditor.

Finalmente, señalar que en el riesgo de auditoría que se adopte se ha de tener en cuenta la interrelación entre el coste que supone el incrementar las pruebas de evidencia y el riesgo de error que esté dispuesta a asumir la Auditoría Interna. En el término medio está la prudencia y quizás el mejor nivel de riesgo de auditoría.

Madrid, 1 de junio de 1998