

# IV REUNION DE AUDITORES INTERNOS DE BANCA CENTRAL

CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS – CEMLA

Cartagena de Indias, Colombia 6 al 10 de julio de 1998

---

## CONCLUSIONES Y RECOMENDACIONES

### TEMA 1: AUDITORIA DE LA INVERSION DE LAS RESERVAS INTERNACIONALES

1. Para realizar una adecuada auditoria de las reservas internacionales el auditor interno debe obtener el entrenamiento necesario en los aspectos relacionados con la administración de las reservas. Tener conocimiento de la legislación que afecta las operaciones internacionales y las políticas y procedimientos operativos del banco central en cuanto al manejo de las reservas.
2. La auditoria debe apoyar a la administración en la identificación de riesgos, detección de debilidades y fijación de controles en el manejo de las reservas internacionales para ello debe contar con las herramientas que permitan efectuar la evaluación de las distintas estrategias de inversión, entre otros el portafolio benchmark.
3. En los contratos con agentes externos (custodios o administradores) para el manejo de las reservas internacionales se debe considerar los requerimientos de control que la auditoria interna plantee.
4. Por lo menos una vez al año se deberán realizar auditorías a los custodios y administradores externos.
5. La auditoria debería participar en calidad de observador en los comités de inversiones de reservas para tener un conocimiento más cercano del proceso de toma de decisiones.
6. La auditoría debería utilizar tecnología automatizada en la revisión de las reservas con el propósito de ser más eficientes y oportunos.
7. Con la finalidad de que las auditorias internas de los bancos centrales cuenten con personal especializado en operaciones con reservas internacionales se requiere que se programen cursos sobre el manejo de reservas internacionales para el personal de las auditorias.

### TEMA 2: RIESGOS

1. El Riesgo es la probabilidad de que un evento o acción afecte adversamente a la entidad impidiendo el cumplimiento de sus objetivos y metas.
2. El manejo de riesgos es una responsabilidad de la administración, implica la identificación, evaluación y gestión de los riesgos. Es muy importante fijar objetivos claros para identificar los *factores críticos de riesgo* con el propósito de establecer parámetros para medirlos y prevenir su posible ocurrencia a través de mecanismos de control e información. Es esencial que los bancos centrales adopten metodologías para la identificación, valoración y gestión de riesgos.
3. La auditoria interna debe adaptar sus metodologías de trabajo hacia la identificación, medición y priorización de riesgos con el objeto de dirigir sus esfuerzos hacia las áreas críticas y minimizar el riesgo de auditoria. Así mismo, es conveniente que para la planificación de auditoría también se tenga en cuenta la evaluación de riesgos que realice la administración.

### TEMA 3: AUDITORIA INFORMATICA

1. La auditoría, consciente de los rápidos cambios tecnológicos, debe trabajar en un proceso de mejoramiento continuo y evaluar periódicamente las metodologías utilizadas para llevar a cabo la auditoría de informática. Como instrumento de fundamental importancia en el apoyo de la auditoría se recomienda el uso de metodologías estándares tales como: COSO y Cobit.
2. La auditoría de la gestión de la labor de informática debe incluir la evaluación de los planes de largo plazo de la tecnología de información, los cuales deben ser consistentes con los planes estratégicos de la institución.
3. Un elemento clave en la evaluación de la adquisición y desarrollo de sistemas de información es la utilización de una sana metodología para el ciclo de vida del desarrollo del sistema. Igualmente lo es la participación y compromiso de los usuarios en todo el proyecto, como responsables de determinar los requerimientos funcionales, de seguridad y de control que deben ser implementados en la aplicación que se está desarrollando o que se adquiere.
  - El auditor debe tener en cuenta los asuntos del proyecto y del negocio a través de los procesos de planeación, diseño y aprobación. La auditoría debe participar en los equipos de trabajo y seguimiento con el propósito de asegurar el cumplimiento de la metodología y la fortaleza de los controles, así como la inclusión de los requerimientos de los usuarios.
  - El auditor también debe verificar el desarrollo de controles manuales y automatizados en el sistema de aplicación, así como que el sistema implementado cumpla con los requerimientos funcionales, de seguridad y control para asegurar la calidad y seguridad de la información y ver si cumple con los objetivos del negocio.
4. Al auditar las aplicaciones del negocio se debe considerar que la aplicación es un elemento integral de la función del negocio. Por esta razón, los riesgos de aplicación funcionales y los controles relacionados con los mismos deben ser considerados en su conjunto.
5. Para asegurar la capacidad de los auditores para enfrentar los retos de tecnología de información, los siguientes puntos son críticos para la efectividad de la función de auditoría:
  - Tener los recursos apropiados de hardware y software, así como los programas de capacitación necesarios.
  - El equipo específico de auditoría debe estar organizado como un todo para lograr el nivel óptimo de habilidades y mezcla de las disciplinas que se requieran.
6. la administración debe estar consciente de los objetivos de control para la tecnología de información y debe asegurar una suficiente comprensión de estos conceptos.
7. Es importante considerar dentro del plan de continuidad del negocio aquellos aspectos que atañen al cambio del milenio, definiendo procedimientos alternativos para operar.