



**PROYECTO DE INNOVACIÓN DE LA MICROEMPRESA (MICROSERVE)**

**Contrato No. PCE-0406-I-00-5034-01**

**MANUAL DE AUDITORÍA DE SISTEMAS PARA LA  
SUPERINTENDENCIA DE BANCOS**

**Orden de Entrega No. 3  
Orden de Tarea No. 27**

**por:  
Omar Sánchez  
Luis Ramírez**

**Presentado a:  
USAID Bolivia**

**Marzo 2002**

**MANUAL DE AUDITORÍA DE SISTEMAS PARA LA  
SUPERINTENDENCIA DE BANCOS**

por Omar Sánchez  
y  
Luis Ramírez

Orden de Entrega No. 3  
Orden de Tarea No. 27

PROYECTO DE INNOVACIÓN DE LA MICROEMPRESA (MICROSERVE)

Contrato No. PCE-0406-I-00-5034-01

Oficina de la Microempresa  
Centro de Desarrollo Económico

Agencia para el Desarrollo Internacional de los Estados Unidos  
Washington, D.C.

Esta obra recibió el apoyo de la Agencia para el Desarrollo Internacional de los Estados Unidos, La Paz, Bolivia, bajo compra por cuenta al Contrato de Cantidad Indefinida del Microserve No. PCE-0406-I-00-5034-01, cuyo contratista principal es Chemonics International Inc., 1133 20<sup>th</sup> Street, N.W., Washington, D.C., 20036; Tel. 202 955 5300; Fax 202 955 3400

## CONTENIDO

---

1.	Marco Teórico	2	
1.1	Conceptualización Del Sistema De Control Interno		1
1.2	Auditoría Informática		1
1.3	Marco Conceptual		1
1.4	Control Interno		3
1.5	Metodología de Auditoría Informática		6
2.	Realización del Trabajo de Auditoría Informática		8
2.1.	Evaluación Global		8
2.2.	Evaluación Detallada		12
2.3.	Documentación del Trabajo Realizado		16
Anexo No. 1	Responsabilidades de los Auditores Interno y Externo		17
Anexo No. 2	Definición y Evaluación del Riesgo		21
Anexo No. 3	Planeación de Auditoría		25
Anexo No. 4	Naturaleza de las Pruebas de Auditoría		27
Anexo No. 5	Esquema de Trabajo		29
Anexo No. 6	Evaluación Global: Programa de Auditoría para el Área de Sistemas		31
Anexo No. 7	Informe del Trabajo de Auditoría		35
Anexo No. 8	Evaluación Detallada: Programa de Auditoría para Aplicaciones Significativas		38

# Manual de Auditoría para la Superintendencia de Bancos

## 1. Marco Teórico

### 1.1 Conceptualización del Sistema de Control Interno

### 1.2 Auditoría Informática

Esta guía se referirá específicamente a la Auditoría Informática. No obstante, es importante destacar que “... *conceptualmente la auditoría, cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas*”<sup>1</sup>.

Si se busca dentro de las diversas teorías un concepto específico de auditoría informática, se concluye que ésta es una parte integrante de la auditoría en general con un objetivo específico, que es el de una revisión de la propia informática y de su entorno con el fin de proteger los activos y recursos, determinar si contribuye al desarrollo del objeto social de la entidad, verificar si sus actividades se desarrollan eficientemente en concordancia con la normatividad vigente (interna y externa) y validar la efectividad del control interno.

Dado lo anterior, es necesario que se cumplan los siguientes requisitos:

- Que los auditores de sistemas conozcan con suficiencia los procedimientos operativos relacionados con el negocio de la entidad auditada, ya que será este conocimiento lo que les permitirá evaluar el impacto de las inconsistencias detectadas en el funcionamiento de los sistemas de información y, al final, emitir un juicio profesional sobre el área de sistemas de una entidad.
- Que los equipos que se conformen para la realización de la auditoría estén integrados por expertos conocedores de la tecnología empleada por los supervisados, así como de los procedimientos más adecuados que podría aplicar en cada caso en particular. En caso de que participen auditores sin la suficiente experiencia, se recomienda que éstos deben ser apoyados por expertos, así como un mayor grado de supervisión del trabajo.

### 1.3 Marco Conceptual

COSO<sup>2</sup> define Control como “*Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos*”.

---

<sup>1</sup> Piattini Mario G., Auditoría Informática

<sup>2</sup> Committee of Sponsoring Organisations of the Treadway Commission. Internal Control-Integrated Framework.

Como requerimientos del negocio en materia de información y debido a que la auditoría informática es parte importante dentro del Sistema de Control Interno, se adoptan los criterios de la metodología COBIT<sup>3</sup> respecto de los conceptos establecidos por ésta. COBIT combina los principios contenidos en los modelos referenciales (como COSO) y determina que la auditoría informática debe contemplar los siguientes requisitos:

### **Requerimientos de Calidad**

*Calidad.* La información que se procesa debe ser de tal calidad que el resultado sean datos que permitan la adecuada toma de decisiones.

*Costo.* Los costos de procesamiento deben ser óptimos.

*Entrega.* Calidad no es suficiente, es necesario que la información sea oportuna.

### **Requerimientos Fiduciarios (COSO)**

Efectividad y eficiencia de operaciones.

Confiabilidad y suficiencia de la información.

Cumplimiento de las leyes y regulaciones.

### **Requerimientos de Seguridad**

Confidencialidad.

Integridad.

Disponibilidad.

Adicionalmente, COBIT ha incorporado los conceptos que se enfocan hacia la información y sus características, para lo cual presenta las siguientes definiciones, que hoy día son de aceptación mundial en el área de la Auditoría Informática:

### **Efectividad**

Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

### **Eficiencia**

Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

### **Confidencialidad**

Se refiere a la protección de información sensible contra divulgación no autorizada.

### **Integridad**

Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

### **Disponibilidad**

Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

---

<sup>3</sup> COBIT Objetivos de Control para la Información y la Tecnología Relacionada

**Cumplimiento**

Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.

**Confiabilidad de la Información**

Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Teniendo como referencia el presente marco teórico, la auditoría informática permite evaluar o determinar tres aspectos básicos, los cuales incluyen:

- Si el área de sistemas de la entidad realiza con eficacia y efectividad sus operaciones básicas, entre las que se incluyen la relacionada con la valoración de los riesgos del negocio.
- Si el área de sistemas de la entidad brinda suficiencia y confiabilidad sobre la información que procesa.
- Si los procedimientos están implementados en concordancia con las normas internas y externas que rigen a la entidad.

**1.4 Control Interno**

El área de sistemas de cualquier organización, constituye un elemento importante en el cumplimiento de la Misión y el logro de la Visión institucional.

Por ésta razón, debe hacerse una breve referencia del verdadero alcance del sistema de control interno de una organización, de manera que se ubique en el contexto del área de sistemas y, por ende, en su supervisión o auditoría.

**1.4.1 Definición de control interno**

Hoy día el control interno se define como un proceso realizado por la junta directiva, los administradores y demás personal de una entidad, diseñado para proporcionar seguridad razonable en la búsqueda del cumplimiento de los objetivos en las siguientes categorías que si bien son distintas entre sí, se encuentran íntimamente relacionadas. Estas son:

- La efectividad y eficiencia de las operaciones, esto es, el cumplimiento de los objetivos básicos de la entidad, salvaguardando los recursos de la misma; es decir, los activos de la empresa y los bienes de terceros que se encuentran en poder de la entidad,
- La suficiencia y confiabilidad de la información financiera, así como de la preparación de toda la información; y,
- Cumplimiento de toda la regulación aplicable a la institución.

Así, el control interno se considera efectivo cuando proporciona a la administración y a los supervisores seguridad razonable sobre los siguientes aspectos:

- la extensión en la cual se están consiguiendo los objetivos de las operaciones de la entidad;
- la confiabilidad en la preparación de la información financiera y contable;
- el cumplimiento de las leyes y regulaciones aplicables, y
- los procedimientos operativos diseñados.

#### **1.4.2 Componentes del control interno**

En toda organización se dan los siguientes elementos que componen un sistema de control interno. El área de sistemas de alguna u otra manera está presente en todos y cada uno de ellos.

##### **1.4.2.1 El entorno de control: La estructura general de control interno**

El diseño de un sistema de control interno exige la elaboración y adopción formal de unos códigos éticos y reglas de conducta que generen conciencia y cultura del control interno entre los empleados de la organización. Este entorno constituye la base del control interno y es el objetivo hacia el cual los administradores deben dirigir gran parte de sus esfuerzos.

Este componente sirve como fundamento para los demás componentes del control, pues busca proporcionar la disciplina y estructura necesaria para la valoración de riesgos en aras de la consecución de los objetivos específicos trazados por la entidad.

Este entorno busca que la entidad cuente con una estructura general de control interno, para lo cual deben establecerse no solo unos principios y reglas de conducta que definan la orientación del proceso mismo, sino para que se establezcan los elementos humanos y las políticas de entrenamiento y permanente actualización frente a las estrategias y a la forma de desarrollar adecuadamente esos procesos; se busca que la organización desarrolle y solidifique una cultura de autocontrol.

De ésta forma se logra implementar las actividades de control y modificarlas cuando las condiciones lo justifiquen, así como capturar y comunicar la información relevante a través de la organización.

##### **1.4.2.2 Medición, evaluación y limitación de riesgos**

Las entidades deben identificar y medir los riesgos a que se ven expuestas en el desarrollo de su actividad, pues sólo con unos procedimientos claros de medición de riesgos se podrá tener una adecuada administración de los mismos. A consecuencia, es indispensable establecer objetivos tanto globales de la organización como de actividades relevantes; para obtener una base sobre la cual sean identificados y analizados los factores que amenazan su propio cumplimiento.

En la evaluación de los riesgos, las entidades deben definir unos objetivos y unos límites, de forma que su trabajo se oriente al logro de los mismos y bajo criterios de prudencia. Igualmente, dado que las condiciones económicas, financieras, regulatorias y operativas son fluctuantes,

deben mantener mecanismos que además sirvan para identificar y tratar los riesgos asociados con los cambios. Esta evaluación debe cubrir todos los diversos riesgos que enfrentan las instituciones, tales como riesgo de crédito, país y de transferencia, mercado, tasa de interés, liquidez, operacional, legal y riesgo de depuración.

#### **1.4.2.3 Control de actividades**

Esto se refiere básicamente al cumplimiento de las actividades diarias asignadas, expresadas en las políticas y procedimientos establecidos por la entidad.

Es indispensable que las entidades implementen la ejecución de las políticas a través de toda la organización, en todos los niveles y en todas las funciones e incluye el establecimiento de unos procedimientos obligatorios para todas las actividades, tales como revisiones de los altos mandos, actividades de control apropiadas para diferentes departamentos o divisiones, controles físicos, chequeos periódicos de conformidad con los límites de las exposiciones, un sistema de aprobaciones y autorizaciones, y un sistema de verificación y conciliación.

La entidad debe asegurar que exista una segregación adecuada de tareas y que al personal no le sean asignadas responsabilidades contrapuestas. Las áreas de potenciales conflictos de interés deben ser identificadas, minimizadas, y cuidadosamente monitoreadas.

Estas actividades pueden ser manuales o computarizadas, administrativas u operacionales, generales o específicas, preventivas o detectivas, cuyo principal objetivo es la identificación, prevención y administración de los riesgos (potenciales o reales).

#### **1.4.2.4 Entorno de información y comunicación**

La información operacional, financiera, jurídica y de cumplimiento que hace posible conducir y controlar la organización debe identificarse, capturarse y difundirse ampliamente hacia todas las áreas de la entidad. Esta difusión debe dirigirse a todos los niveles, hacia y desde todos los entes, que tengan interés o se relacionen con la información correspondiente.

Para ello se debe contar con los medios necesarios para identificarla, procesarla y comunicarla, los cuales a su vez deben ser objeto de permanente monitoreo por parte de la administración, a fin de que la información se dé a conocer en forma adecuada y oportuna, de manera que le permita al personal afectado cumplir con sus responsabilidades.

#### **1.4.2.5 Monitoreo o Supervisión**

Las entidades deben monitorear continuamente la eficacia general de los controles internos para ayudar a lograr el objetivo organizacional. En tal sentido, es importante que se establezcan controles automáticos o “alarmas” tanto en los sistemas computacionales como en los manuales, de manera que permanentemente se valore la calidad y el desempeño del sistema en el tiempo, pues ello equivale a una actividad de supervisión y administración. Para ello, dicho monitoreo se debe realizar en todas las etapas del proceso y en tiempo real en el curso de las operaciones.

La evaluación a veces toma la forma de auto evaluación, en la que el personal responsable de una sección o dependencia determina la efectividad y razonabilidad de los controles para sus actividades. Dicha valoración a su vez será evaluada en su conjunto con las de las demás secciones por parte de la administración.

Adicionalmente, los auditores internos realizan evaluaciones del control interno y efectúan recomendaciones para su mejoramiento como parte de sus obligaciones. Dicho monitoreo debe cubrir el examen, la evaluación adecuada y la efectividad del control interno de la entidad y la calidad y cumplimiento en el desempeño en la realización de las responsabilidades asignadas. Esta revisión debe ser llevada a cabo por personal competente y entrenado adecuadamente.

### 1.5 Metodología de auditoría informática

Cuando un auditor de informática evalúa los sistemas de control en el ambiente de informática de una entidad, debe tener claro que sólo un sistema de control interno eficaz le ayuda a la entidad a alcanzar las metas y los objetivos, y a mantener un sistema confiable de información financiera y administrativa. Además, sólo en un ambiente de control interno confiable podrá tener seguridad razonable de que la entidad cumplirá con las leyes y regulaciones aplicables, así como con las políticas, planes y procedimientos internos.

Por lo tanto, la metodología empleada para el desarrollo del trabajo depende en gran medida de la naturaleza, la complejidad y los riesgos de las operaciones que efectúa una entidad, pero debe ser apropiada para lograr identificar factores internos y externos que puedan afectar la calidad de la información procesada y, por ende, el logro de objetivos institucionales.

En general, las metodologías conducen a realizar una evaluación global de las entidades financieras supervisadas lo que permite identificar toda la estructura del área de sistemas, determinando debilidades y fortalezas de su ambiente de control, proceso que se realiza con entrevistas y análisis de la documentación del departamento de sistemas. Un ejemplo de un análisis DOFA:

<p style="text-align: center;"><b>DEBILIDADES</b></p> <ul style="list-style-type: none"> <li>• Desaprovechamiento de la tecnología implementada y disponible en la entidad</li> <li>• Exceso de carga de trabajo por la complejidad de algunas actividades</li> <li>• La demanda de soporte técnico supera la estructura instalada</li> </ul>	<p style="text-align: center;"><b>OPORTUNIDADES</b></p> <ul style="list-style-type: none"> <li>• Apoyo administrativo en el desarrollo de proyectos</li> <li>• Tecnología de Punta en el mercado</li> <li>• Liberación de software a bajo costo o sin costo (Linux , Start-office)</li> </ul>
<p style="text-align: center;"><b>FORTALEZAS</b></p> <ul style="list-style-type: none"> <li>• Talento humano calificado</li> <li>• Infraestructura física del área de sistemas</li> <li>• Metodologías claramente definidas de desarrollo de aplicaciones y liberación de versiones</li> <li>• Claras políticas de administración y utilización de recursos técnicos</li> <li>• Definiciones bien establecidas de los proyectos</li> </ul>	<p style="text-align: center;"><b>AMENAZAS</b></p> <ul style="list-style-type: none"> <li>• Limitaciones económicas de la entidad para inversión en tecnología</li> <li>• Bajo perfil de los usuarios de las aplicaciones o falta de capacitación en las herramientas</li> <li>• Desconocimiento de los proyectos de sistematización</li> <li>• Baja capacidad de manejo de información</li> </ul>

No obstante cualquiera sea la metodología empleada, es necesario que una vez concluida esta primera fase se tenga claridad sobre:

- El grado en que la entidad tiene computarizado el procesamiento de la información para las principales áreas del negocio.
- La complejidad relativa de los sistemas computarizados que la entidad emplea.
- La eficiencia de la estructura organizacional de los sistemas computarizados y su administración.
- La medida en que el auditado depende de las aplicaciones que tiene operando.
- El software y aplicaciones que puedan permitir cambios no autorizados a programas o a los datos.

Como producto de la evaluación global, además de identificar los controles generales, se deben determinar los riesgos inherentes y de control que enfrenta la entidad, con el fin de realizar la planeación de nuevas visitas de auditoría enfocadas a realizar pruebas específicas (de control o sustantivas) a los diferentes componentes del área de sistemas. Algunos ejemplos de evaluación, que se derivan del análisis global, pueden ser: evaluar el riesgo crediticio trimestralmente, monitorear riesgos de liquidez mensualmente, evaluar confiabilidad en riesgos de transferencia de información anualmente, evaluación de consistencia de la información, etc.

Dado que la información que se genera para la entidad es proporcionada a través del empleo de recursos de tecnología informática, la metodología empleada permite enfocar, implementar y monitorear medidas de control adecuadas para evaluar:

- Los datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados.
- Las aplicaciones, es decir, los procedimientos programados o manuales que desarrolla la entidad.
- La tecnología que cubre tanto hardware como software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
- Las instalaciones y los recursos para alojar y dar soporte a los sistemas de información.
- Las habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

Esto con el fin de asegurar que los requerimientos de información de los usuarios de la entidad son satisfechos. A continuación, el numeral 2. Realización del trabajo de Auditoría Informática, detalla cómo realizar la evaluación para cubrir todos los aspectos del área de informática.

## 2. Realización del Trabajo de Auditoría Informática

El trabajo de auditoría informática se enfoca en determinar las áreas básicas de evaluación para emitir una opinión sobre si el área de sistemas de la entidad auditada cumple los requerimientos mínimos para soportar las operaciones de ésta y si su enfoque permite soportar y apoyar el cumplimiento de los planes estratégicos.

El trabajo de auditoría se divide entonces en dos grandes fases, a saber:

- La primera, denominada **Evaluación Global**, donde se identifican los objetivos de la entidad, las estrategias que han diseñado para lograrlos y el esquema organizacional del área de sistemas. También se determina la debida concordancia entre las necesidades de la entidad y el recurso tecnológico disponible, es decir, la medida en que el área de sistemas cubre y apoya suficientemente las actividades críticas y los riesgos importantes.
- La segunda, denominada **Evaluación Detallada**, enfocada a medir, en las áreas determinadas como de mayor riesgo, los procesos y los controles implementados, con el fin de determinar si son adecuados y fomentar un apropiado ambiente de control.

### 2.1. Evaluación global

#### 2.1.1. Conocimiento de la entidad financiera supervisada

El auditor de informática debe identificar claramente la actividad económica para la cual fue constituida la entidad, lo cual le permite determinar si el soporte de sistemas es suficiente para el logro de objetivos, si se encuentra sobredimensionado y si apoya el crecimiento de la entidad en un futuro cercano.

Es necesario realizar una evaluación efectiva del riesgo considerando factores internos (como la naturaleza de las actividades de la entidad, la calidad y habilidad del personal, la capacidad de manejar el negocio, etc.) así como factores externos (condiciones fluctuantes de la economía y de los mercados, avances tecnológicos, soporte de los proveedores y el tiempo que éstos la garantizan, etc.) que puedan afectar el logro de los objetivos plasmados en el plan estratégico de la entidad.

En este proceso se debe contar con, al menos, la siguiente información:

- a. **Plan estratégico.** El cual debe estar por escrito y debe ser conocido por las diferentes áreas de la entidad. Esto con el fin de identificar los objetivos institucionales, sus actividades críticas y sus riesgos relevantes, de manera que frente a ellos se evalúe si el área de sistemas sostiene estos aspectos.
- b. **Organigrama.** En donde se describan claramente los niveles de jerarquía y la relación existente entre el área de sistemas y las demás áreas que conforman la entidad. Este permitirá identificar los dueños y responsables de la información, así como la estructura del área de sistemas frente a la administración.

- c. **Manual de Funciones.** Donde se identifique claramente las responsabilidades de cada cargo, con el fin de definir si éste tiene concordancia con el Organigrama planteado; además permitirá medir el nivel de organización y claridad que se tiene frente al talento humano disponible.

En general, la información que permita al auditor identificar claramente el objeto social de la entidad y sus objetivos a corto, mediano y largo plazo, con el fin de validar si el área de sistemas mantiene adecuadamente éstas proyecciones.

## 2.1.2 Conocimiento del área de sistemas

Al entrar al área de sistemas, el conocimiento se inicia identificando con mayor detalle la estructura del área (algunas veces lo que dice el organigrama no refleja lo que está sucediendo en la práctica) y los objetivos del área se deben comparar frente al plan estratégico global (muchas veces los objetivos del área no se encuentran escritos, pero se puede evidenciar la concordancia entre sus planes y actividades y los objetivos de la entidad).

### 2.1.2.1 Plataforma “Hardware”

Una vez definidos la estructura y los objetivos, se procede a identificar los componentes del área de sistemas de la entidad, para lo cual se tendrán en cuenta aspectos tales como:

- a. *Los servidores existentes.* Tipo, número, lugar y/o ubicación de las principales unidades de procesamiento (servidores). Esto le permitirá al auditor definir cuántos centros de cómputo existen y la necesidad de visitarlos independientemente.
- b. *Si los servidores están interconectados y determinar el tipo de procesamiento de datos.* Centralizado o distribuido. Determinando si el tipo de procesamiento implementado está acorde con las necesidades de la entidad, ya que se puede encontrar un proceso centralizado que implique sobrecarga en los procesos de cierre, inadecuado manejo de los procesos de interfase, subutilización de equipos, etc., razón por la cual podría recomendarse un ajuste a procesamiento distribuido.
- c. *Determinar cuántos lugares de procesamiento de información existen.* Es importante definir claramente cuáles áreas de la entidad realizan procesamiento de información, ya que éstas implican la definición de tipos de pruebas (sustantivas o de control) a realizar en éstas áreas.
- d. *Para cada equipo determinar localización y características (configuración actual y máxima, con el fin de medir el crecimiento).* Tener en cuenta los proyectos de adquisición de máquinas o cambio de las actualmente instaladas. Esto le permite al auditor opinar respecto de la subutilización, o adecuado dimensionamiento del área sistemas.
- e. *Contratos vigentes de compra, alquiler y servicio de mantenimiento.* Esto le permite medir los costos que incurre la entidad para el mantenimiento del área de sistemas.
- f. *Contratos de seguros.* A efectos de validar si las pólizas vigentes están cubriendo adecuadamente los activos.
- g. *Área de comunicaciones.* Este análisis requiere de un alto grado de detalle. Debe evaluarse la capacidad de intercambio de información, distribución de información y los diferentes pasos que siguen los datos hasta presentar el producto final, por ejemplo, informe de liquidez, informe de morosidad de cartera, extractos bancarios, etc.

- h. *Convenios que se tienen con otras instalaciones para procesamiento de datos o mantenimiento de copias de seguridad.*
- i. *Ambiente de Microcomputación.*
- j. *Políticas de operación "front" y "back office", ya que se puede encontrar que éstas son desarrolladas por la misma persona (ejemplos: aprobación de desembolsos y entrega de los mismos; autorización de límites y realización de las operaciones con cupos; etc.)*

### **2.1.2.2 Plataforma "Software"**

Para identificar la complejidad de las aplicaciones instaladas es necesario tener en cuenta aspectos tales como:

- a. Descripción general de las aplicaciones instaladas, en producción, y de los que están por instalarse, incluyendo "software" de sistemas operacionales.
- b. Fechas de instalación de los aplicativos con el fin de determinar su obsolescencia (tener en cuenta que muchas veces las aplicaciones más antiguas son también las más probadas).
- c. Determinar si se lleva control de las modificaciones más significativas realizadas a las aplicaciones, lo cual implica que existe un adecuado control entre los ambientes de producción y desarrollo. Es necesario validar si están claramente definidos los planes de liberación de versiones, identificando las principales razones de cambio de versión.
- d. Definir claramente las interfases entre las aplicaciones, determinando si son automáticas o manuales. Es importante identificar la periodicidad con que se efectúan los cierres de operaciones y el tiempo que se tarda el sistema en enviar información para el análisis y la toma de decisiones.
- e. Volumen aproximado de transacciones procesadas por el aplicativo con el fin de medir su capacidad y determinar necesidades de técnicas especiales de auditoría sobre los mismos.
- f. Documentación de los paquetes de software adquiridos por la entidad.
- g. Tipo de procesamiento de datos, identificando si es independiente o distribuido por redes a fin de evaluar la suficiencia del procesamiento frente a la infraestructura del hardware.
- h. Manuales de usuario, de formatos y técnicos.
- i. Informes de Auditoría Interna relacionados con el área de sistemas.
- j. Proyectos de Instalación de nuevas aplicaciones.
- k. Aplicaciones procesadas en microcomputadores.

### **2.1.2.3 Plataforma de seguridad**

Entre los aspectos del área de sistemas que deben ser considerados y que están relacionados con la seguridad, se encuentran:

- a. Administración, Seguridad y Control en los centros de cómputo. A fin de determinar si existen políticas claras de recuperación del negocio ante un desastre en el centro de cómputo. En una entidad lo más importante es determinar la forma de continuar sus operaciones.
- b. Independencia entre los sistemas de aplicación que se encuentran en producción y los que están en desarrollo, con el fin de medir los controles al acceso a programas fuente y a las Bases de Datos.
- c. Segregación de funciones.

- d. Suficiencia de las aplicaciones para reportar a sus usuarios la información requerida, aspecto que se lograra evidenciar evaluando en áreas diferentes a sistemas, indagando cómo ven los usuarios el soporte que esta área brinda.

#### **2.1.2.4 Evaluación de los procesos de adquisición de tecnología (*hardware* y *software*)**

Incluye un diagnóstico del área de sistemas frente a los requerimientos de la organización y el grado en que el área cubre y apoya las necesidades generales o específicas del negocio, para lo cual se determinará si se realizan, como mínimo, las siguientes actividades:

- a. Si se analizan los requerimientos de “hardware” y “software” y se estima la duración de la implementación.
- b. Si se estudian las diferentes propuestas y se efectúan las recomendaciones pertinentes buscando el mayor grado de satisfacción a los requerimientos formulados.
- c. Si se verifica que la administración de sistemas haya elaborado un plan de implementación con su correspondiente cronograma, en donde se incluyan responsables, tareas y fechas de entrega.
- d. Si durante el proyecto se adelanto un monitoreo permanente al proceso, con el fin de asegurar que se dio cumplimiento al plan y el proveedor suministro lo convenido.

#### **2.1.3 Conclusiones de la evaluación global**

La información obtenida por el auditor, mediante sus programas de trabajo, debe permitirle expresar una conclusión con respecto a:

- a. Si el departamento de informática soporta adecuadamente las operaciones de la entidad y sus estructuras logística y física le permiten mantener ese soporte ante un crecimiento previsto en el plan estratégico de la misma. Además de validar si el “hardware” instalado corresponde a los inventarios, si se encuentran correctamente instalados, si se mantienen adecuadamente y si dan el rendimiento requerido.
- b. Si existen políticas y procedimientos de control que permanentemente estén evaluando las medidas de control implementadas y si atienden apropiadamente cualquier riesgo no identificado previamente.
- c. Si existe información adecuada y comprensible en áreas como finanzas, operaciones de cartera de créditos, captaciones, etc. Además si es confiable, oportuna y está soportada adecuadamente la información, mediante control de acceso a aplicaciones y restricciones a operaciones de los aplicativos.
- d. Si las aplicaciones existentes funcionan adecuadamente para los productos tradicionales y para soportar los nuevos productos que la entidad tenga previsto instalar (el término productos hace referencia a ahorro a la vista, ahorro programado, tarjeta de crédito, crédito por diversas líneas, etc.), además de validar si se dispone de las licencias correspondientes.
- e. El análisis de transmisión de información y de la forma en que las diferentes áreas de la entidad la obtienen debe permitir al auditor identificar riesgos de información financiera no confiable, esto ayuda en la medición de los límites que asume la entidad respecto a su exposición al riesgo con el fin de cumplir metas.
- f. La estructura organizacional del área sistemas, permitirá determinar si los procedimientos operativos garantizan un ambiente de procesamiento de datos apropiado para preparar

información confiable. Es decir, si existe una adecuada segregación de funciones en el departamento de sistemas. De igual forma, si existen controles y procedimientos operativos tales como manuales de operación y controles operativos diarios, supervisión de usuarios privilegiados, control sobre “software” sensitivo, y el desarrollo de sistemas, políticas, procedimientos y lineamientos de seguridad, función de administración de seguridad, y entrenamiento a los empleados en seguridad.

- g. Si las necesidades y productos que ofrece la entidad están adecuadamente cubiertos con el inventario físico y lógico del área sistemas, es decir, si la plataforma sobre la cual corren las diferentes aplicaciones soportan de forma efectiva las operaciones y metas que tiene prevista la empresa.

Vale agregar que la experiencia, el conocimiento y el instinto (olfato) del auditor le permitirá concluir cuáles aplicaciones requieren un trabajo detallado de auditoría. Por ejemplo, en la evaluación global se identifican aplicaciones, procesos o datos que están presentando errores, aparentemente no relacionados, lo que pone de manifiesto la necesidad de evaluar parámetros, diseño y mantenimiento de aplicaciones específicas en forma más detallada. Además, el volumen de información que procesen determinadas aplicaciones ayudará a dictar la necesidad de llevar a cabo pruebas sustantivas sobre las mismas.

Por último, y a partir de las conclusiones, el auditor decide sobre el enfoque (qué revisa), el alcance (cuánto revisa), la oportunidad (cuándo se revisa), las pruebas a realizar (cómo revisa), los perfiles de las personas para ejecutarlas (quién revisa), el inventario de medios necesarios (con qué revisa), así como el tiempo estimado para adelantar la evaluación detallada.

## **2.2 Evaluación Detallada**

Como se observó en el análisis global, las entidades no cuentan con una única aplicación que soporte todas sus operaciones. Lo que normalmente se encuentra es que un producto o servicio es tratado por varias aplicaciones. Por esta razón el auditor debe identificar para cada proceso la exactitud de los datos recibidos y la concordancia con los datos enviados, midiendo así la confiabilidad que existe entre las diferentes interfases implementadas.

### **2.2.1 Auditoría a las aplicaciones**

#### **2.2.1.1 Auditoría a los riesgos de las aplicaciones**

El alcance del examen de auditoría sobre las aplicaciones que se encuentran implementadas en la entidad, debe como mínimo incluir los siguientes riesgos:

#### **Riesgo 1: Acceso a funciones de procesamiento**

Personas no autorizadas pueden tener acceso a las funciones de procesamiento de transacciones de los programas de aplicación, permitiéndoles leer, modificar, agregar o eliminar datos o ingresar transacciones no autorizadas para su procesamiento. Algunos medios de control para minimizar este riesgo serían:

- segregación de funciones; y,

- medios de control de acceso: identificadores de usuario, perfiles de acceso, menús, acceso a los datos por programas, dispositivos de acceso para los datos/programas a través de restricciones lógicas de las terminales, dispositivos de seguridad de terminales (incluyendo dispositivos de acceso personalizado o tarjetas de banda magnética).

### **Riesgo 2: Ingreso de datos**

Los datos permanentes y de transacciones ingresadas para el procesamiento pueden ser imprecisos, incompletos o ingresados más de una vez. Algunos medios de control para este riesgo son:

- controles de edición y validación;
- controles de lote; y,
- doble digitación de campos críticos.

### **Riesgo 3: Items rechazados o en suspenso:**

Los datos rechazados y las partidas en suspenso pueden no ser identificadas, analizadas y corregidas. Algunos medios de control para este riesgo son:

- controles programados; y,
- controles del usuario.

### **Riesgo 4: Procesamiento**

Las transacciones reales ingresadas para su procesamiento o generadas por el sistema pueden perderse o ser procesadas o registradas en forma incompleta, inexacta o en el período contable incorrecto. Algunos medios de control para este riesgo son:

- formularios prenumerados y rutinas de control de secuencia;
- controles de balanceo programados;
- controles de lote;
- controles de rótulos de archivos;
- controles de transmisión de datos; y,
- procedimientos de reenganche y recuperación.

### **Riesgo 5: Cambios a los programas**

Los programadores pueden realizar cambios incorrectos no autorizados en el “software” de aplicación que reducen la integridad de la información procesada a través del sistema. Algunos medios de control para este riesgo son:

- procedimientos de iniciación, aprobación y documentación de los cambios a los programas;
- intervención de los usuarios;

- procedimientos de catalogación y mantenimiento;
- procedimientos de prueba;
- supervisión efectiva; y,
- procedimientos de implantación.

#### **Riesgo 6: Acceso General**

Personas no autorizadas (empleados o terceros) pueden tener acceso directo a los archivos de datos o programas de aplicación utilizados para procesar transacciones permitiéndoles realizar cambios no autorizados a los datos o programas. Algunos medios de control para este riesgo son:

- software de control de acceso;
- análisis de logros e informes gerenciales;
- control de acceso físico; y,
- protección de datos.

#### **Riesgo 7: Continuidad de operaciones**

Imposibilidad de recuperar la capacidad de procedimientos de información ante una interrupción temporal o definitiva, puede ocasionar pérdidas significativas de tiempo de procesamiento, destrucción parcial o total de información y suspensión del servicio a los clientes (empleados o terceros). Algunos medios de control para este riesgo son:

- desarrollo y documentación de un plan de contingencias;
- depósito externo de seguridad;
- procedimientos de copias de respaldo;
- contratos de mantenimiento;
- documentación actualizada de aplicaciones;
- utilización de UPS; y,
- habilidad y capacidad de los Usuarios.

#### **2.2.1.2 Auditoría a las aplicaciones claves**

Los aspectos señalados en el numeral anterior, deben ser más amplios en aplicaciones como cartera de créditos, captaciones (a la vista, a términos fijo, etc.), reporte de información a los entes externos, aplicaciones de tesorería, reportes de relación de solvencia o capital adecuado, etc. Que corresponden a las aplicaciones que soportan las operaciones básicas de la entidad.

En este tipo de auditoría o análisis detallado se puede determinar con claridad la disponibilidad de la entidad para generar información en medio magnético que permita la ejecución de pruebas asistidas por computador.

#### **2.2.2. Auditoría a los datos**

Realizar pruebas sustantivas le permite al auditor evaluar la integridad y confiabilidad de la información que emplea la entidad en la toma de decisiones; este tipo de auditoría está orientado

a detectar la presencia o ausencia de errores en procesos automáticos que por el volumen de información es más complejo validar en forma manual.

Estas pruebas están orientadas a detectar diferentes irregularidades, tales como:

- Operaciones omitidas, no registradas en el sistema;
- Operaciones duplicadas;
- Operaciones inexistentes o incluidas en forma anormal;
- Clasificación incorrecta de los datos; y,
- Operaciones con información incompleta, como por ejemplo: en un registro de desembolso de dinero podrían faltar fechas, identificación de terceros, clase de operación, etc.

Cuando el auditor de informática solicita archivos con las bases de datos correspondientes a un producto, estos son el soporte de las cifras financieras que reporta la entidad (tanto a sus usuarios internos como externos), por tanto su trabajo debe incluir:

- conciliaciones con partidas financieras de las cuales este archivo es el soporte; ejemplo: un archivo de cartera de créditos con un corte específico deberá cruzar con la cifra que se revela en el balance general, de no ser así se debe profundizar en el análisis para evidenciar la existencia de fallas de la aplicación o de los usuarios de la misma; y,
- cálculos independientes de las aplicaciones de la entidad para realizar comparativos con informes generados por sus sistemas; por ejemplo: a un archivo con la información de las inversiones de la entidad se le pueden hacer cálculos sobre los márgenes de utilidad que generan éstas en un período determinado, que al ser comparados con los informes del área financiera podrá indicar al auditor la suficiencia en la información y el correcto procesamiento de la misma.

El auditor debe tener presente los rastros de auditoría que las aplicaciones generan, estos archivos le permiten identificar el acceso autorizado a la aplicación, el control de las operaciones que deban ser restringidas (ejemplo: autorización de desembolsos a cajeros, autorización de sobregiro, etc.), las fechas y horas de alimentación del sistema, etc. Esta pista de auditoría brinda la confianza de auditoría o se constituye en un indicio claro de la necesidad de implementar mecanismos de control más fuertes.

### **2.2.3 Conclusiones de la evaluación detallada**

La información obtenida por el auditor le permite expresar una opinión con respecto a:

- a. Si los diferentes riesgos a que se expone la entidad se encuentran cubiertos. Tales riesgos pueden ser, riesgos de transferencia de información, riesgos operacionales, riesgos de manipulación de datos (la tasa de interés, el plazo, fechas de vencimiento, etc.)
- b. Si se registra fielmente la información que genera cada operación llevada a cabo por la entidad, descripciones, atributos, identificación de los entes que intervienen, nombres, dirección, valores, etc.

- c. Si los procesos de cálculo y edición implementados garantizan la integridad de los datos y, por ende, generan informes que sirven a la organización, presentando información adecuada y en forma oportuna.
- d. Si los controles previstos ante riesgos de fallo en dispositivos periféricos como el servidor, líneas de transmisión de datos, etc. están controlando y minimizando el riesgo existente.
- e. Si la plataforma sobre la cual está operando la aplicación brinda la integridad, confidencialidad y características requeridas por la información.

### **2.3. Documentación del Trabajo Realizado**

El auditor, mediante papeles de trabajo, debe dejar constancia de las labores realizadas. Estos papeles de trabajo (que pueden constar en medio magnético o en papel) le sirven al auditor para:

- a) facilitar la preparación del informe;
- b) comprobar y explicar en detalle las opiniones y conclusiones resumidas en el informe;
- c) proporcionar información para los organismos de control y vigilancia del Estado;
- d) coordinar y organizar todas las fases del trabajo;
- e) proveer un registro histórico permanente de la información examinada y los procedimientos de auditoría aplicados; y,
- f) servir de guía en revisiones subsecuentes.

Los papeles de trabajo deben reflejar en forma clara los datos significativos contenidos en los registros, los métodos de comprobación utilizados y la evidencia adicional necesaria para la formación de una opinión y preparación del informe. Además, deben identificar claramente las expresiones informativas y los elementos de juicio o criterio utilizados.

Los papeles de trabajo no están limitados a información cuantitativa, por consiguiente, se deben incluir en ellos notas y explicaciones que registren en forma completa el trabajo efectuado por el auditor, las razones que le asistieron para seguir ciertos procedimientos y omitir otros y su opinión respecto de lo examinado.

Los papeles de trabajo deben ser revisados por los supervisores para determinar lo adecuado y eficiente del trabajo del talento humano sujeto a supervisión. En tales revisiones, los papeles de trabajo deben estar completos, legibles y organizados sistemáticamente, de tal manera que no sean necesarias informaciones suplementarias e interpretaciones por parte de quien los preparó.

## ANEXO NO. 1

---

### Responsabilidades de los Auditores Interno y Externo

#### LA AUDITORÍA INTERNA

La auditoría interna se considera como un control de alto nivel potencial dentro de una organización, y sus responsabilidades incluyen la evaluación y prueba de los sistemas de la entidad.

La competencia y objetividad de los auditores internos depende fundamentalmente de los siguientes factores:

- El grado de independencia dentro de la organización
- Su competencia y experiencia
- La importancia de su trabajo dentro de la organización
- Lo adecuado de sus papeles de trabajo y sus informes
- La forma en que las acciones originadas como consecuencia de sus informes son objeto de seguimiento e implementadas

#### Independencia dentro de la organización

Los auditores internos son empleados de la entidad y por consiguiente, no pueden ser considerados independientes en la misma forma que los auditores externos. No obstante, según el nivel jerárquico de la auditoría interna dentro de la organización de la entidad y el apoyo que recibe de la gerencia superior, los auditores pueden mantener un grado razonable de objetividad. Un indicio de tal independencia sería que el jefe de la auditoría interna dependiera del nivel más alto de la gerencia y que tuviera acceso directo a la Junta Directiva o al comité de auditoría. Si los auditores internos están estrechamente controlados por la gerencia, es probable que sus actividades sean dirigidas a objetivos muy limitados y no contribuyan a fortalecer los sistemas de control.

La auditoría interna es una actividad apreciativa, independiente de los sectores objeto de revisión. Por lo tanto, ésta debería reportar a los máximos niveles de la organización y depender de ellos. La auditoría interna tiene por objeto la revisión de las operaciones para servir de base a la administración. Por este motivo, es un control que se describe como independiente pues mide y evalúa la eficacia de otros controles.

#### Competencia y experiencia

Los auditores internos deben poseer antecedentes educacionales y experiencia de trabajo compatibles con sus responsabilidades. Además de poseer conocimientos contables, de auditoría y de los sistemas de información, deben entender también las responsabilidades de la gerencia y las operaciones de la entidad. Los programas formales de capacitación interna o una oportuna participación en cursos externos de capacitación permite asegurar que todo el personal de auditoría interna conozca su trabajo y que se mantenga informado sobre nuevas técnicas e ideas.

### **Importancia de su trabajo dentro de la organización.**

Los objetivos de los auditores internos puede recaer primordialmente en los sistemas de control, en la eficiencia de las operaciones o en la supervisión de las transacciones de las sucursales, sin embargo, su participación en la identificación y administración de los riesgos a los cuales está expuesta la entidad de manera sistemática y permanente, le dará mayor importancia al equipo de auditoría.

### **Sus funciones incluyen:**

- Revisión de las operaciones para verificar la autenticidad, exactitud y concordancia con las políticas y procedimientos establecidos por la organización.
- Control de los activos a través de los registros contables y comprobaciones físicas.
- Revisión de las políticas y procedimientos para evaluar su efectividad.
- Auditoría de otras organizaciones con las que existen relaciones contractuales a cumplir u otras vinculaciones económicas.

La auditoría interna trabaja en forma separada a las operaciones de la organización. En síntesis la auditoría interna es un mecanismo de control selectivo e independiente de los engranajes de control interno habituales que hacen a la operatoria de la empresa.

### **Sus papeles de trabajo y sus informes**

Los auditores internos deben documentar su trabajo adecuadamente. Sus papeles de trabajo deben incluir programas de auditoría que presenten un claro registro del alcance del trabajo realizado y un adecuado respaldo para las conclusiones obtenidas. Los papeles de trabajo y los informes deben ser revisados por la gerencia o dirección de auditoría interna. Sin la documentación apropiada que proporcione evidencia del trabajo realizado, el esfuerzo de la auditoría interna no poseerá mucho valor.

Los informes de auditoría interna deben ser considerados por la gerencia superior correspondiente que no está directamente involucrada en las áreas sujetas a la auditoría, quienes deben actuar con presteza en respuesta a las recomendaciones.

También deben existir procedimientos que aseguren un adecuado seguimiento de las recomendaciones realizadas por los auditores internos.

## **Seguimiento e implementación de las acciones originadas como consecuencia de los informes de auditoría interna**

Un departamento de auditoría bien organizado y provisto de personal competente puede ser un importante elemento de los sistemas de control de una entidad y su efectividad aumenta en la medida en que sus informes sean atendidos y sus recomendaciones sean oportunamente implementadas. Un seguimiento continuo de los sistemas de control realizado por ese grupo y una demostrada atención permitirá reducir la frecuencia y alcance de la Supervisión en una entidad.

## **LA AUDITORÍA EXTERNA**

### **Independencia dentro de la organización**

Como su nombre indica es una función de carácter externo. Una de las funciones más comunes de la auditoría externa es brindar una opinión sobre las manifestaciones de la administración incluidas en la información contable emitida por el ente económico. Esta función es conocida como auditoría de estados financieros o información financiera. Sin embargo, el auditor externo está capacitado para brindar cualquier servicio que implique el examen de información, operaciones, procedimientos, actividades, proyecciones, etc., que necesiten de un juicio profesional dentro del marco de competencia del contador público.

El requerimiento más común de la auditoría externa es la opinión sobre los estados financieros que emite una entidad, para lo cual se dedica a examinar cada una de las cifras que componen dichos estados financieros, a evaluar el sistema de control interno existente en la entidad y a determinar si el mismo le da garantía a las afirmaciones relacionadas con los estados financieros tales como existencia, integridad, derechos y obligaciones, valuación y presentación y revelación.

Sus actividades no son permanentes en la entidad y casi siempre su trabajo se realiza en dos o tres visitas, a lo sumo.

El contador público en el ejercicio de las funciones de auditor externo no es responsable de los actos administrativos de las empresas o personas a las cuales presta sus servicios.

### **Importancia de su trabajo dentro de la organización y sus informes.**

El resultado del trabajo del auditor externo se ve plasmado principalmente en la opinión que emita según sus compromisos con la entidad; sin embargo, de su trabajo se obtienen recomendaciones que buscan fortalecer el sistema de control interno, pero por su permanencia, no tienen el mismo alcance que le podría brindar la auditoría interna.

El auditor externo no es responsable con la administración de la calidad del sistema de control interno y es a ésta última a quien le corresponde adoptar o implementar las recomendaciones que emita el auditor externo.

## **Competencia y experiencia**

La labor de auditoría externa implica una competencia profesional singular, caracterizada por una serie de atributos tales como independencia, educación y conocimientos especializados, dedicación al servicio, y matriculación en los cuerpos encargados del control del ejercicio profesional.

Además, por sobre todo ello, deben existir aspectos de ética profesional a ser tenidos en cuenta durante el desarrollo de la labor y durante todo el transcurso de la vinculación profesional.

## **Sus papeles de trabajo**

Los auditores externos deben documentar su trabajo adecuadamente. Sus papeles de trabajo deben incluir la planeación con el enfoque, el alcance y la oportunidad de sus actividades, los programas de auditoría con las decisiones preliminares o relación de actividades a ejecutar, e un claro registro del alcance del trabajo y un adecuado respaldo para las conclusiones obtenidas. Los papeles de trabajo del auditor se constituyen en la evidencia que respalda su opinión.

### **Definición y Evaluación del Riesgo**

#### **Riesgo Inherente**

El riesgo inherente es la susceptibilidad de un ente económico a la existencia de errores o irregularidades significativos antes de considerar la efectividad de los sistemas de control.

El riesgo inherente está totalmente fuera de control por parte de quienes administran un ente económico. Difícilmente se pueden tomar acciones que tiendan a eliminarlo porque es propio de la operación del ente.

Por ejemplo, en una entidad financiera supervisada con alta tecnología el riesgo inherente será mayor que el nivel de riesgo que se determine en una entidad financiera supervisada con tecnología estándar. Por qué es así?. El riesgo que existe en la valuación de alta tecnología lleva implícito el problema de la obsolescencia que es de relevante importancia y difícilmente puede identificarse, reducirse o tratarse aisladamente, cualquiera sea el sistema de control que la entidad establezca.

#### **Factores que determinan el Riesgo Inherente**

Entre los factores que determinan la existencia de un riesgo inherente se pueden mencionar:

- La naturaleza del negocio del ente: el tipo de operaciones que se realizan y el riesgo propio de esas operaciones; la naturaleza de sus productos y volumen de transacciones;
- La situación económica y financiera del ente;
- El riesgo de auditoría de una pujante entidad con altos niveles de ganancias y sólida posición económico financiera no será el mismo que el de una entidad con graves problemas financieros y baja rentabilidad económica que comprometa la vigencia del principio de empresa en marcha;
- La organización gerencial y sus recursos humanos y materiales; la integridad de la gerencia y la calidad de los recursos que el ente posee; y,
- La predisposición de los niveles gerenciales a establecer adecuados y formales sistemas de control; su nivel técnico y la capacidad demostrada en el personaje clave, son elementos que deben evaluarse al medir el riesgo inherente.

## **Riesgo de Control**

El riesgo de control es el riesgo en que los sistemas de control están incapacitados para detectar o evitar errores o irregularidades significativas en forma oportuna.

Por ejemplo, dentro del componente de ingresos por intereses por servicios financieros, el nivel de riesgo de control de una entidad con un complejo sistema de verificación de créditos a los clientes antes de continuar el otorgamiento de crédito es distinto al de otra que no realiza estos controles y, por lo tanto, está más expuesta a que sus cuentas por cobrar por concepto de intereses puedan ser consideradas incobrables.

Este tipo de riesgo también está fuera del control de los auditores, pero por otro lado, las recomendaciones resultantes del análisis y evaluación de los sistemas de información, contabilidad y control que se realicen van a ayudar a mejorar los niveles de riesgo en la medida en que se adopten tales recomendaciones.

Además, la existencia de bajos niveles de riesgo de control, lo cual implica que existen buenos procedimientos en los sistemas de información, contabilidad y control, puede ayudar a mitigar el nivel de riesgo inherente evaluado en una etapa anterior.

## **Factores que Determinan el Riesgo de Control**

Los factores que determinan el riesgo de control están presentes en el sistema de información, contabilidad y control. La tarea de evaluación del riesgo de control está íntimamente relacionada con el análisis de estos sistemas.

La existencia de puntos débiles de control implicaría "a priori" la existencia de factores que incrementan el riesgo de control y, al contrario, puntos fuertes de control serían factores que reducen el nivel de este riesgo.

## **EVALUACION DEL RIESGO**

La evaluación del riesgo es el proceso por el cual, a partir del análisis de la existencia e intensidad de los factores de riesgo, se mide el nivel de riesgo presente en cada caso.

El nivel del riesgos suele medirse en cuatro grados posibles, éstos son:

- Mínimo
- Bajo
- Medio
- Alto

En algunas circunstancias quizá resulte poco clara esta clasificación, por lo que muchas veces la evaluación del nivel de riesgo se limita a determinar un riesgo alto o bajo.

La tarea de evaluación está presente en dos momentos de la planificación de auditoría.

- **Planificación estratégica:** En esta etapa se evalúa el riesgo global de auditoría relacionado con el conjunto de los estados contables y, además, se evalúa el riesgo inherente y de control de cada componente en particular.
- **Planificación detallada:** En esta etapa se evalúa el riesgo inherente y de control específico para cada afirmación en particular, dentro de cada componente.

La evaluación del nivel de riesgo es un proceso totalmente subjetivo y depende exclusivamente del criterio, capacidad y experiencia del auditor. Además, es la base para la determinación del enfoque de auditoría a aplicar y la cantidad de satisfacción de auditoría a obtener. Por lo tanto, debe ser un proceso cuidadoso y realizado por quienes posean la mayor capacidad y experiencia en un equipo de trabajo.

No obstante ser un proceso subjetivo, hay formas de tratar de estandarizar o disminuir esa subjetividad. En ese sentido, se tratan de medir tres elementos que, combinados, son herramientas a utilizar en el proceso de evaluación.

- La significatividad del componente (saldos y transacciones).
- La existencia de factores de riesgo y su importancia relativa.
- La probabilidad de ocurrencia de errores o irregularidades básicamente obtenida del conocimiento y la experiencia anterior de ese ente.

La combinación de los posibles estados de estos tres elementos brindan un marco para evaluar el riesgo.

Un nivel de riesgo mínimo estaría conformado cuando en un componente poco significativo no existan factores de riesgo y donde la probabilidad de ocurrencia de errores o irregularidades sea remota.

Cuando en un componente significativo existan factores de riesgo pero no demasiado importante y la probabilidad de existencia de errores o irregularidades sea baja improbable, ese componente tendrá una evaluación de riesgo bajo.

Por último, un componente tendrá un nivel de riesgo alto cuando sea claramente significativo, con varios factores de riesgo, algunos de ellos muy importantes y donde sea totalmente probable que existan errores o irregularidades. La tabla siguiente esquematiza estos conceptos:

Nivel de riesgo	Significatividad	Factores de riesgo	Probabilidad de ocurrencia de errores
Mínimo	No significativo	No existen	Remota
Bajo	Significativo	Existen alguno pero poco importantes	Improbable
Medio	Muy significativo	Existen algunos	Posible
Alto	Muy significativo	Existen varios y son importantes	Probable

El proceso de evaluación tratará de ubicar a cada componente en alguna de estas categorías. Es claro entender que seguramente algún componente reúna las tres categorías presentadas, pero no todas del mismo nivel.

Por ejemplo, la cartera de créditos suele ser un componente claramente significativo para los estados financieros en su conjunto pero, normalmente, no presenta muchos factores de riesgo y la probabilidad de existencia de errores es improbable o remota.

En el otro extremo, los saldos de anticipos de sueldos pueden ser muy poco significativos pero estar muy mal controlados, siendo la posibilidad de existencia de errores totalmente probable.

En estas circunstancias, como en muchas otras, debe apelarse al criterio del auditor, es el único que en cada caso particular determinará que nivel de riesgo corresponde medir.

## ANEXO NO. 3

---

### Planeación de Auditoría

#### Objetivos

1. Evaluar, mediante el conocimiento global de la entidad financiera supervisada, si el sistema de información:
  - salvaguarda los activos;
  - mantiene la integridad de los datos;
  - lleva a cabo eficazmente las operaciones de la entidad; y,
  - utiliza eficientemente los recursos.
2. Determinar las áreas de mayor riesgo dentro de la entidad, en materia de procesamiento de información, identificando cada uno de los aplicativos que soportan las operaciones de la entidad.
3. Evaluar si el área de sistemas de la entidad realiza con eficacia y efectividad sus operaciones básicas, entre las que se incluyen la relacionada con la valoración de los riesgos del negocio.
4. Plantear, elaborar y formalizar una serie de proyectos de corto, mediano y largo plazo orientados a monitorear la calidad y control de los elementos relacionados con los recursos de informática, mediante la evaluación y revisión oportuna de todos sus componentes, según prioridades determinadas en el conocimiento de la entidad financiera supervisada.

#### Desarrollo del Trabajo

##### Evaluación global

1. Analizar aspectos organizacionales:
  - a. Plan estratégico: Donde se identifican los objetivos y procesos corporativos y se considera el uso de las diversas tecnologías de información.
  - b. Plan de informática: En el cual se determinan proyectos específicos que cubren las necesidades de la entidad para el logro de sus objetivos.
  - c. Plan de contingencias: Con el cual se garantizan la confidencialidad, integridad y disponibilidad tanto de la información como de los sistemas ante eventos sorpresivos.
  - d. Organigrama general y de sistemas: Con el cual se evalúa la independencia de los departamentos usuarios del área de sistemas y se evidencia si existe una adecuada segregación de funciones.

2. Analizar aspectos de control en sistemas:
  - a. Planificación y gestión de los recursos, identificando el presupuesto, planes de adquisición y gestión de la capacidad de los equipos;
  - b. Controles para usar de manera efectiva los recursos físicos y lógicos implementados en la entidad;
  - c. Controles físicos y lógicos para asegurar que el acceso a la información quede restringido únicamente a los usuarios autorizados; y,
  - d. Controles de tratamiento de datos para garantizar la integridad de los mismos y el procesamiento de la totalidad de los mismos.
3. Identificar inventarios físicos y lógicos en el área de sistemas.
4. Determinar próximas visitas de auditoría.
5. Efectuar informe de deficiencias para la administración.

### **Evaluación Detallada**

Las actividades que el auditor debe desarrollar en cada una de las aplicaciones o en las diferentes áreas del departamento de informática se derivan del conocimiento global de la entidad financiera supervisada, donde se han identificado el tipo de riesgos existentes durante el procesamiento de información o cuando se determine que los controles previstos pueden ser débiles.

En general, una planeación detallada debe efectuarse cuando:

- a. Los componentes son de alto riesgo o muy significativos para la auditoría en su conjunto.
- b. Los componentes han sido afectados por cambios significativos en los sistemas de información contable y de control.
- c. Las modificaciones del plan son convenientes para la eficiencia en la auditoría.
- d. Planeamos un trabajo de auditoría por primera vez.

## ANEXO NO. 4

---

### **Naturaleza de las Pruebas de Auditoría**

Existen, en forma general, dos clasificaciones de pruebas de auditoría: los que proporcionan evidencia de control, denominados pruebas de cumplimiento; y los que proporcionan evidencia sustantiva, denominados pruebas sustantivas. En la práctica, resulta difícil clasificarlos ya que muchos cumplen un doble propósito. Las pruebas que proporcionan evidencia de control también pueden proporcionar evidencia sustantiva acerca de las transacciones y saldos individuales examinados. En forma similar, las pruebas que proporcionan evidencia sustantiva generalmente permiten inferir la existencia y efectividad de los controles relacionados.

#### **Pruebas de Cumplimiento (o de control)**

Las pruebas de cumplimiento proporcionan evidencia de que los controles clave existen y de que son aplicados efectiva y uniformemente. Las pruebas de cumplimiento para los controles:

- aseguran o confirman nuestra comprensión de los sistemas del cliente, particularmente de los controles clave dentro de los sistemas; y,
- corroboran la efectividad de los controles clave durante el período de confianza.

Las pruebas de cumplimiento para las funciones de procesamiento computarizados también apuntan a corroborar que esas funciones han operado durante el período de confianza. Esto implicaría asegurarse de que la función de procesamiento computarizada opera adecuadamente en un punto en el tiempo y obtener evidencia de que los controles sobre los cambios a estos sistemas, sean y hayan sido efectivos. En otros casos, podemos enfrentar el riesgo de cambio no autorizado o inadecuado de las funciones de procesamiento computarizados, aplicando pruebas sustantivas.

Las pruebas que pueden utilizarse para obtener evidencia de control incluyen:

- Indagaciones y manifestaciones de la entidad
- Observaciones
- Procedimientos de diagnóstico
- Actualizaciones de sistemas
- Inspección de la documentación del sistema
- Técnicas de datos de prueba
- Pruebas detalladas de transacciones y saldos a través de:
  - Inspección de documentos que respaldan las transacciones y otros registros
  - Reproducción

## **Pruebas Sustantivas**

Las pruebas sustantivas proporcionan evidencia directa sobre la validez de las transacciones y los saldos incluidos en los registros contables o estados financieros y por consiguiente, sobre la validez de las afirmaciones importantes.

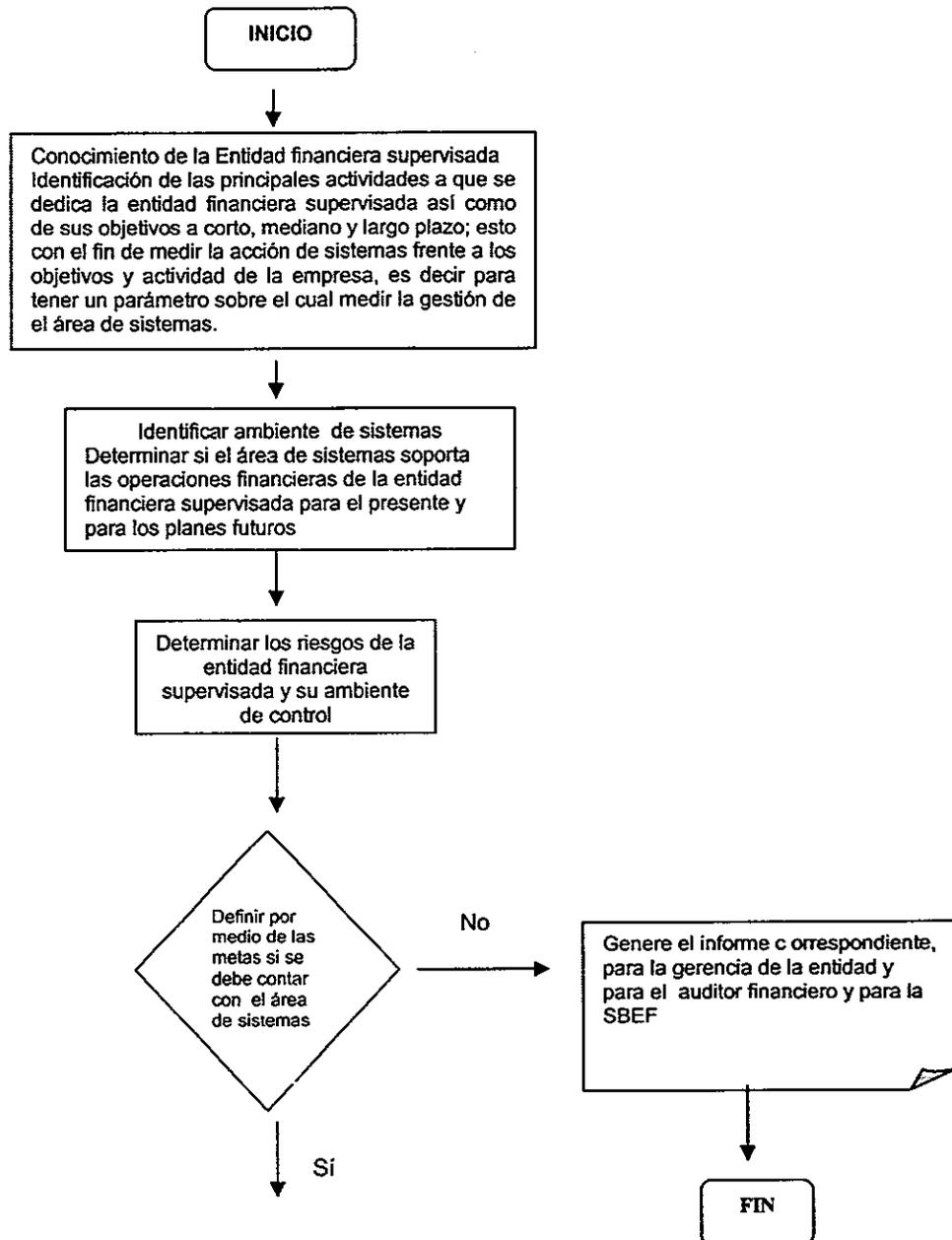
Las pruebas sustantivas incluyen:

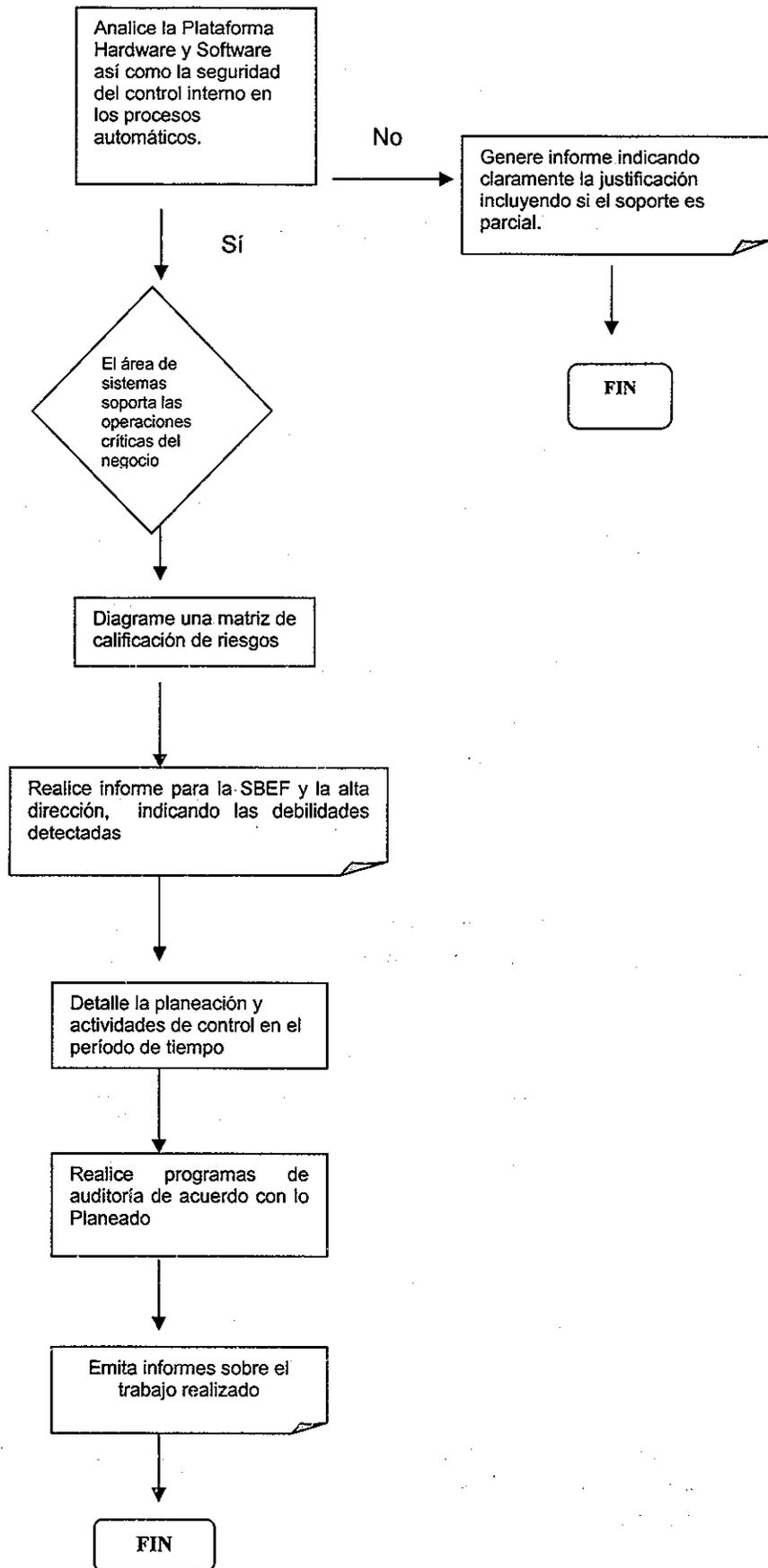
- Indagaciones y manifestaciones de la entidad
- Procedimientos analíticos
- Pruebas detalladas de transacciones y saldos a través de:
  - Inspección de los documentos respaldatorios y otros registros contables
  - Observación física
  - Confirmaciones externas
  - Reproducción

## ANEXO NO. 5

**Esquema de Trabajo**

El siguiente esquema muestra los pasos básicos para establecer el trabajo de auditoría de sistemas en entidades financieras, desde la óptica de la Superintendencia de Bancos y Entidades Financieras:





## ANEXO NO. 6

---

### Evaluación Global: Programa de Auditoría para el Área de Sistemas

El siguiente programa muestra los aspectos básicos que se deben tener en cuenta al realizar la evaluación global de la entidad financiera supervisada con el fin de determinar el enfoque, el alcance y la oportunidad de la evaluación detallada.

Esta guía es genérica, por ende es importante que se adapte a las necesidades de cada entidad financiera supervisada.

#### Estudio Inicial

El auditor debe solicitar los siguientes documentos para análisis:

- 1) *Organigrama*  
El organigrama expresa la estructura de la entidad.  
Se presentan casos en los que existe un organigrama diferente al oficial, lo que se pondrá de manifiesto en los informes de auditoría.
- 2) *Departamentos*  
Se entiende como departamento a los órganos o estamentos que siguen inmediatamente a la dirección. El auditor identificará cada uno de ellos a fin de validar la relación de estos con el área de sistemas.
- 3) *Relaciones jerárquicas y funcionales entre órganos de la organización*  
El auditor verifica si se cumplen las relaciones funcionales y jerárquicas previstas por el organigrama, o por el contrario detecta, por ejemplo, si algún empleado tiene dos o más jefes.
- 4) *Flujos de Información*  
Además de las corrientes verticales entre los departamentos, la estructura organizacional, cualquiera que sea, produce corrientes de información horizontales y oblicuas; es necesario identificar claramente estos flujos de información entre los grupos de una organización para medir su eficiente gestión, y si son acordes al organigrama.

En ocasiones, las entidades crean canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa.

- 5) *Número de puestos de trabajo*  
El auditor comprobará que los nombres de los puestos de trabajo de la organización corresponden a las funciones reales. Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes.
- 6) *Número de personas por puesto de trabajo*  
Es un parámetro que los auditores informáticos deben considerar. La inadecuada segregación de funciones se puede dar por un número de personas que realizan las mismas funciones y rara vez se nota en la estructura general de la entidad.

### **Entorno Operacional**

Es importante que de la evaluación global se tenga claridad respecto al entorno operacional de la entidad, por lo cual es necesario identificar:

- a) *Situación geográfica de los sistemas*  
Se determinará la ubicación geográfica de los distintos centros de sistemas en la entidad y verificar la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.
- b) *Arquitectura y configuración de hardware y software*  
Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas esta muy ligada a las políticas de seguridad de la entidad vigilada. Por lo tanto, es necesario que el auditor identifique claramente la distribución e interconexión de los equipos.
- c) *Inventario de "Hardware" y "Software":*  
El auditor solicitará información escrita, en donde figuren todos los elementos físicos y lógicos del área. En cuanto a "Hardware", figurarán las CPU, unidades de control local y remotas, periféricos de todo tipo, etc.

El inventario de "software" debe contener todos los productos lógicos del sistema, desde el "software" básico hasta los programas de utilidad adquiridos o desarrollados internamente.

- d) *Comunicación y redes de comunicación*  
En el estudio inicial se debe identificar el número, situación y características principales de las líneas de comunicación, así como de los accesos a la red pública de comunicaciones si existe.

Igualmente se solicitará información sobre las redes locales implementadas en la entidad supervisada.

## Aplicaciones, bases de datos y archivos

El estudio global de la entidad financiera supervisada debe incluir una idea general de los procesos informáticos realizados en la entidad auditada. Para ello deberá conocer lo siguiente:

- a) *Volumen, antigüedad y complejidad de las aplicaciones*
- b) *Metodología del diseño*  
Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizados varias a lo largo del tiempo se pondrá en los papeles de trabajo
- c) *Documentación*  
La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.

La no documentación de programas disminuye gravemente el mantenimiento de los mismos.

- d) *Cantidad y complejidad de las bases de datos y los archivos*  
Información de tamaño y características de las bases de datos, clasificándolas en relación y jerarquías, buscando identificar el volumen de información que manejan con el fin de obtener una visión aceptable de las características de la carga informática.

Al identificar los volúmenes de información que las aplicaciones manejan, se identifica la estructura relacional de las base de datos (o archivos); este punto permite que el auditor identifique claramente la estructura relacional de datos para cada aplicación, a fin de poder opinar respecto a la suficiencia y capacidad de control y almacenamiento de información de las diferentes aplicaciones.

## Determinación de recursos de la Auditoría Informática

Una vez recolectada toda la información y realizado un análisis de la misma, se procede a determinar las áreas y componentes que requieren de un mayor grado de estudio para evaluar sus mecanismos de control, para lo cual el auditor debe definir si empleará:

- a) Programas propios de la auditoría adquiridos, es decir, la Superintendencia puede contar con herramientas de auditoría de tipo comercial y que podrían ser empleadas para las pruebas de auditoría;
- b) Programas de auditoría diseñados para la entidad financiera supervisada. Algunas veces las aplicaciones comerciales no son tan flexibles a todas las entidades, por esta razón es necesario hacer desarrollos propios y ajustados a los requerimientos de la entidad donde se ejecutaran las pruebas de auditoría;
- c) Logs de auditoría generados por las propias aplicaciones. Estos son más efectivos cuando se trata de pruebas de cumplimiento, por tanto, es importante que el auditor identifique las posibilidades de las aplicaciones en generación de Logs de auditoría y se valga de ellos en las pruebas que efectúe.

El empleo de dichos recursos implicará analizar la necesidad de generar procesos en los servidores, por lo cual debe solicitar a la entidad financiera supervisada tiempo de máquina, espacio de disco, impresoras, etc.

**ATENCIÓN:** Cuando se realice el trabajo de auditoría detallada, es importante tener claridad sobre el tipo de procesamiento de la información: centralizada o distribuida, *batch*\*, o en tiempo real \*, o aplicaciones de teleproceso que están permanentemente activas.

*\*Batch y Tiempo Real:*

Las aplicaciones que son *batch* son aplicaciones que cargan mucha información durante el día y durante la noche se corren los procesos de cálculo para actualizar los datos. Es decir, recolecta información durante el día, pero el refresco de los datos se realiza a una hora específica para arrancar al día siguiente.

Las aplicaciones que son tiempo real u *on-line*, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son sistemas que actualizan los datos de inmediato.

## ANEXO NO. 7

---

### Informe del Trabajo de Auditoría

De la evaluación global de la entidad financiera supervisada, se desprenden tres informes: uno para la SBEF, otro para las directivas de la entidad y otro interno indicando la planeación de la auditoría detallada y definiendo cuáles son las áreas que requieren una auditoría detallada.

#### 1. Aspectos a destacar en el informe para la Dirección

Este informe debe enunciar a la alta dirección las debilidades más representativas. La conclusión de la evaluación global debe enfocar su análisis a identificar si la estructura del área de sistemas soporta las principales operaciones de la entidad, por tanto el informe deberá contener los siguientes aspectos:

##### a. Debilidades de coordinación y organización

- No coinciden los objetivos de la informática con los de la entidad, por ende, los planes de proyección en el área informática no soportan el actual número de operaciones ni el crecimiento de la entidad, de acuerdo con las metas planteadas, o bien existe sobredimensionamiento en los planes de sistemas respecto al número de operaciones a desarrollar.
- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente, es decir, la producción de información genera un alto grado de errores o es presentada en forma inoportuna; esto puede obedecer a mejoras en las aplicaciones que no fueron probadas apropiadamente o a una reestructuración fallida de alguna área o en la modificación de alguna norma importante.

##### b. Debilidades en el servicio prestado por sistemas a los diferentes usuarios

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios o actualización de “software” en las terminales de los usuarios, refresco de paneles, variación de los archivos que deben tener diariamente a su disposición, etc.
- No se reparan las averías de “hardware” ni se resuelven inconsistencias de red en plazos razonables, lo cual hace que el usuario sienta desatención permanente.
- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Esta inoportunidad en la información puede causar importantes desajustes en la toma de decisiones, en especial en los resultados de aplicaciones críticas y sensibles como tesorería, cartera de créditos, módulo gerencial, etc.

### **c. Debilidades en la administración del área de sistemas**

- Incrementos inesperados en los costos del área, sin justificación, lo que se puede evaluar a través del análisis de los presupuestos establecidos para el área.
- Escasa o nula justificación en las inversiones informáticas, lo que se evalúa al analizar los planes de acción y los proyectos que el departamento de sistemas tiene planeados en el corto plazo
- Desviaciones presupuestales significativas, que pueden estar mostrando falta de planeación o planeación que no está en concordancia con los objetivos de la entidad.
- Debilidades en la definición, organización y ejecución de los nuevos proyectos de sistematización (aclaramos que debe auditarse simultáneamente al área de sistemas por el desarrollo de proyectos, así como al departamento que realizó la petición).

### **d. Debilidades en la Seguridad**

- Resultados de la evaluación del nivel de riesgos en los siguientes aspectos:  
Seguridad Lógica  
Seguridad Física  
Confidencialidad

La evaluación de los riesgos la debe hacer el equipo de auditoría mediante la priorización de cada uno de los riesgos detectados y la posibilidad de su ocurrencia; además, es importante que se identifique la incidencia de los riesgos en aplicaciones de las cuales la entidad depende o por los cuales maneja un alto volumen de información.

- Continuidad del servicio, teniendo en cuenta que este concepto establece las estrategias de continuidad de las operaciones ante fallo locales o totales de las aplicaciones o computadores. Destacar el hecho de que no existan planes de contingencia apropiados para minimizar la ocurrencia de un siniestro.
- Area de procesamiento de datos fuera de control, es decir, mala organización de la información, falta de controles a programas propios o adquiridos, inadecuada distribución de equipos y puestos de trabajo, etc.

La identificación de los controles que deben existir en cada aplicación surge del análisis del flujo de la información a través de la Entidad; de acuerdo a los procesos de control establecidos por las áreas y una vez el auditor los ha analizado podrá, de acuerdo a su criterio profesional, emitir una opinión respecto a la necesidad de mayores controles o la suficiencia de los existentes.

## **2. Aspectos a Destacar en el Informe para la Planeación Detallada**

Este informe debe enunciar a la **SBEF** el detalle de las aplicaciones que soportan las operaciones representativas en la entidad, identificando para cada una de estas el tipo de auditoría sugerido (pruebas de control o pruebas sustantivas), así como la periodicidad con que este tipo de trabajo deberá realizarse. Por lo anterior, el informe deberá contener los siguientes aspectos:

### a. Detalle de las Aplicaciones Significativas

Para cada una de las aplicaciones consideradas como significativas es necesario documentar:

- especificaciones detalladas del programa;
- diagrama de flujo que aclare estructura de la aplicación;
- detalle que defina si el módulo es desarrollo propio o adquirido así como la facilidad de obtener fuentes;
- tipo de procesamiento del programa; y,
- resultados del procesamiento determinar claramente que genera la aplicación, por ejemplo, si ésta genera únicamente listados o además genera archivos planos que son interfase a otras aplicaciones, o genera información para terceros, etc.

### b. Detalle de la Pruebas a realizar en las Aplicaciones Significativas

Preparar un cronograma de trabajo indicando fechas y tipo de pruebas a realizar en cada una de las aplicaciones significativas de acuerdo al nivel de riesgo calificado en el conocimiento global de la entidad financiera supervisada.

Es importante que en este detalle del trabajo a realizar se incluyan comentarios sobre las posibles complicaciones al efectuar auditoría más detallada, aspectos que se deberían tener en cuenta, como los siguientes:

- Apoyo limitado o inexistente dentro del área de sistemas
- Apoyo limitado o inexistencia en la entidad auditada
- “Hardware” incompatible
- Disponibilidad limitada de tiempo en el computador
- Archivo de entrada con gran volumen de datos
- Dispositivos de entrada/salida extremadamente lentos
- Necesidad de efectuar procedimientos de conciliación extensos o complicados
- Dificultad de la metodología de cálculos
- Existencia y retención de todos los archivos requeridos
- Información o informe de conciliación definido entre lo generado por las aplicaciones y los informes a los usuarios internos o externos

## ANEXO NO. 8

---

### **Evaluación Detallada: Programa de Auditoría para Aplicaciones Significativas**

El siguiente programa muestra los aspectos básicos que se deben tener en cuenta al realizar la evaluación detallada de la entidad financiera supervisada con el fin de determinar la suficiencia de las aplicaciones para garantizar que la información procesada sea exacta, oportuna, confiable medible, etc.

Esta guía es genérica, por ende es importante que se adapte a las necesidades de cada entidad financiera supervisada.

#### **Planeación:**

Definir un programa de trabajo que permita identificar los siguientes aspectos (tenga en cuenta que esta información puede estar muy clara en los papeles de trabajo de la evaluación global):

- Objetivo de la aplicación y usuarios
- Análisis de la plataforma "hardware" sobre la cual está instalada la aplicación
- Identificación de las herramientas motor de base de datos
- Lenguajes de programación, sistema operacional, etc
- Grado de satisfacción de los usuarios
- Requerimientos no satisfechos
- Costo/beneficio del software actual
- Software por legalizar

#### **Programa de trabajo - prueba sustantiva:**

A continuación se detalla un modelo de programa de trabajo para una aplicación que controle la cartera de créditos de una entidad vigilada por la Superintendencia, donde previamente se ha determinado que la prueba que se debe realizar es de tipo SUSTANTIVA.

<b>Entidad financiera supervisada: COOPERATIVA DE AHORRO Y CREDITO XXXX</b> <b>Prueba : CARTERA DE CREDITOS LINEA CONSUMO</b> <b>Norma : Circular 100 y 039/99 Superintendencia Bancaria</b> <b>Corte : Noviembre 30 de 1999</b>
---

**Objetivo** Evaluar la cartera de consumo de **COOPERATIVA DE AHORRO Y CREDITO XXXX** con corte noviembre 30 de 1999, determinando totalidad, calidad de la información que es soporte de los estados financieros y los montos de provisión registrados por la entidad en cumplimiento de las normas de la Superintendencia Bancaria.

## Desarrollo del Trabajo

1. Solicitar archivo plano a la entidad financiera supervisada, con los siguientes datos:
  - Código del negocio
  - RUT de la entidad financiera supervisada
  - Tipo de crédito (Línea 1= Comercial    Línea 2= Consumo)
  - Valor del crédito
  - Tipo de garantía (1= Admisible    2= No admisible)
  - Número de cuotas
  - Fecha último pago
  - Periodicidad de las cuotas
  - Saldo capital
  - Días de mora
  - Intereses corrientes causados
  - Intereses de mora causados
  - Valor garantía
  
2. Ejecutar pruebas de auditoría para:
  - validar la consistencia de la información suministrada.
  - validar la totalidad de la información respecto de los informes suministrados a entes de control o directivos de la entidad.
  - calificar el crédito de acuerdo al número de días en mora teniendo en cuenta la normatividad emitida por la Superintendencia Bancaria.
  - calcular el monto de la provisión de acuerdo a la calificación dada a la base de datos de cartera de créditos.
  
3. Documentar con papeles de trabajo los resultados obtenidos.
  
4. Preparar informe.

### Programa de trabajo – prueba de control:

A continuación se detalla un modelo de programa de trabajo para una aplicación que controle la cartera de créditos de una entidad vigilada por la Superintendencia Bancaria, donde previamente se ha determinado que la prueba que se debe realizar es de CONTROL.

Entidad financiera supervisada: **COOPERATIVA DE AHORRO Y CREDITO XXXX**  
 Prueba: **CARTERA DE CREDITOS LINEA CONSUMO**  
 Norma: **Circular 100 Y 039/99 Superintendencia Bancaria**  
 Corte: **Noviembre 30 de 1999**

## Desarrollo del Trabajo

1. Solicitar entrevistas con usuarios del departamento de cartera de créditos que manejan la aplicación SICOOP++.
2. Desarrollar un programa de trabajo que valide como mínimo los siguientes aspectos:
  - Ingreso de usuarios autorizados y tipo de control para minimizar el riesgo
  - Ingreso de datos consistentes y totalmente, ejemplo: que las fechas se registren en los formatos correctos, que existan máscaras para el registro de códigos y números, que se digite la totalidad de la información solicitada, etc
  - Controles en las interfases para paso de información entre aplicaciones
  - Exactitud en los cálculos
  - Evaluación del tipo de procesamiento, de acuerdo al volumen de ítems que ingresa y genera la aplicación
  - Controles en el área de sistemas a las liberaciones de versiones y ajustes que modifiquen la estructura de la aplicación
  - Manuales Técnico y de Usuario que minimicen la dependencia de expertos o desarrolladores de la aplicación
  - Procesos para copias de respaldo tanto de datos como de la aplicación
  - Si la aplicación es adquirida, evalúe el soporte que el proveedor brinda a la misma.
3. Documentar con Papeles de Trabajo los resultados obtenidos
4. Presentar Informe