UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS

RIESGO DE FRAUDE OPERATIVO BANCARIO EN EL ÁREA DE CAJA Y SU TRATAMIENTO A TRAVÉS DE LA AUDITORÍA INFORMÁTICA

TESIS

PRESENTADA A LA JUNTA DIRECTIVA DE LA FACULTAD DE CIENCIAS ECONÓMICAS

POR

OMAR GIOVANNI LUCERO COTTO

PREVIO A CONFERÍRSELE EL TÍTULO DE

CONTADOR PÚBLICO Y AUDITOR

EN EL GRADO ACADÉMICO DE

LICENCIADO

GUATEMALA, MARZO 2006

HONORABLE JUNTA DIRECTIVA
DE LA FACULTAD DE CIENCIAS ECONÓMICAS
DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Decano:	Lic. Eduardo Antonio Velásquez Carrera
Secretario:	Lic. Oscar Rolando Zetina Guerra
Vocal Primero:	Lic. Cantón Lee Villela
Vocal Segundo:	Lic. Albaro Joel Girón Barahona
Vocal Tercero:	Lic. Juan Antonio Gómez Monterroso
Vocal Cuarto:	P.C. Efrén Arturo Rosales Alvarez
Vocal Quinto:	B.C. José Abraham González Lemus

PROFESIONALES QUE PRACTICARON LOS EXAMENES
DE ÁREAS PRÁCTICAS BÁSICAS

Matemática y Estadística:	Lic. Oscar Noé López Cordón
Auditoria:	Lic. Jorge Luis Monzón Rodríguez
Contabilidad:	Lic. Mario Leonel Perdomo Salguero

PROFESIONALES QUE PRACTICARON EL
EXAMEN PRIVADO DE TESIS

Presidente:	Lic. Jorge Alberto Trujillo Corzo
Examinador:	Lic. Francisco Israel Ayala Morales
Examinador:	Lic. Beatriz Velásquez de Gatica

Guatemala, 8 de octubre de 2004

Señor Decano
Lic. Eduardo Antonio Velásquez Carrera
Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala

Estimado señor Decano:

En atención a la asignación efectuada por esa Decanatura de fecha 15 de Octubre del 2002, para asesorar al Perito Contador con especialidad en Computación Omar Giovanni Lucero Cotto, en el trabajo de Investigación denominado "RIESGO DE FRAUDE OPERATIVO BANCARIO EN EL AREA DE CAJA Y SU TRATAMIENTO A TRAVES DE LA AUDITORIA INFORMATICA", tengo el agrado de dirigirme a usted para informarle que he procedido a revisar y orientar al mencionado sustentante, sobre el contenido de dicho trabajo.

En ese sentido, el tema desarrollado plantea una fuente de consulta para las entidades bancarias ya que provee de los lineamientos necesarios para que puedan implementar los controles sobre el área de caja con el propósito de incrementar su control interno, por lo que en mi opinión reúne los requisitos exigidos por las Normas y regulaciones pertinentes, razón por la cual, recomiendo su aprobación para su discusión en el Examen Privado de Tesis, previo a optar al Título de Contador Público y Auditor en el grado académico de Licenciado.

"ID Y ENSEÑAD A TODOS"

Lic. Hugo Rodolfo Búcaro Pérez
Contador Público y Auditor
Colegiado Número 5624

ORDEN DE IMPRESIÓN

DEDICATORIA

A DIOS:	Por brindarme la oportunidad de alcanzar una meta más en mi vida, así como por la bendición de poder compartirlo con mis padres.
A MIS PADRES:	Idabel Lucero y Secundina Cotto de Lucero, por su constante dirección y apoyo espiritual, base de mi formación.
A MIS HERMANOS:	Por su apoyo moral
A MIS COMPAÑEROS Y AMIGOS:	Por su amistad.
A:	La Universidad de San Carlos de Guatemala y Docentes de la misma, por sus aportes en el proceso de enseñanza-aprendizaje en cada curso impartido.

ÍNDICE

CAPÍTULO II
Marco Legal, Técnico y Normativo en la Adaptación de Software en Auditoría

CAPÍTULO III
Transacciones Susceptibles de Fraude en el Área de Caja de un Banco Privado

CAPÍTULO IV
Riesgo de fraude Operativo Bancario en el Área de Caja y su Tratamiento a través de la Auditoría Informática

CAPÍTULO V

Caso Práctico Relativo a la Participación del Contador Público y Auditor Interno en la evaluación de Controles Internos para evitar fraudes en el Área de Caja por medios informáticos

INTRODUCCIÓN

Desde el surgimiento de las entidades bancarias, ha sido preponderante brindar información oportuna y exacta a sus cuenta habientes de las transacciones en ellas realizadas, por ejemplo: depósitos, pagos de cheques, transferencias cablegráficas, etc., tarea que se ha realizado con gran éxito con la implementación de sistemas informáticos en el procesamiento de dicha información.

Actualmente, el volumen de estas operaciones ha alcanzado grandes niveles y debido a ser la informática un área en constante evolución, igualmente se desarrollan paralelamente una serie de riesgos en dicho procesamiento, los cuales, deben de ser controlados; por otra parte, como consecuencia de los existentes fraudes de los que han sido sujeto algunos bancos de Guatemala, y tomando en cuenta que en la actualidad la mayoría de operaciones realizadas giran en derredor del área de caja, éstas entidades se han visto en la necesidad de implementar sistemas de control interno operacional tendientes a identificar, evitar y reducir tales anomalías.

Considerando también que prácticamente dichas transacciones se encuentran totalmente automatizadas, surge la necesidad de implementar controles que se acoplen al ambiente bajo el cual fueron creadas.

El presente trabajo se elaboró con el propósito de presentar una alternativa para la detección de fraude en el área de caja de una entidad bancaria, con el fin de fortalecer el sistema de control interno.

Para la mejor comprensión del tema el contenido se encuentra dividido en cinco capítulos: en los capítulos I y II se presentan aspectos generales teóricos y normativos que sirven de base para la importancia de lo que es la Auditoría Informática en la evaluación del sistema de control interno en una institución bancaria para el área de caja.

En el capítulo III se realiza una narración de la forma en que actualmente se desarrollan algunas transacciones en el área de caja en una institución bancaria y algunos controles internos existentes.

En el capítulo IV sobre la base de las mismas transacciones descritas en el capítulo III se muestran nuevas alternativas para el fortalecimiento del control interno con la ayuda de la Auditoría Informática.

Finalmente, el capítulo V da a conocer la adaptación de las herramientas descritas en el trabajo del Auditor, además muestra una estructura organizacional para la adopción de dichas técnicas.

CAPÍTULO I

Riesgo de Fraude Operativo en Entidades Bancarias

1.1 Antecedentes de las Entidades Bancarias

En la época del mercantilismo, entre los años 1450-1750, surgen los bancos propiamente dichos, quienes popularizan el uso de la letra de cambio, del pagaré y del giro cambiario, en sustitución del dinero, para efectuar pagos locales y otros lugares.

Guatemala ha experimentado tres reformas monetarias y bancarias importantes, la realizada entre los años 1924-1926, la iniciada en el año 1945 y la del año 2002. La primera tuvo como objetivos rehacer, estabilizar la moneda guatemalteca y consolidar un sistema bancario que tuviese como base un banco único emisor, El Banco Central de Guatemala. Esta primera reforma puso fin a un caos monetario, caracterizado por la popularidad de bancos emisores, por la inestabilidad de los cambios, por las especulaciones ilícitas y por la inmoralidad bancaria.

En virtud del funcionamiento la Junta Monetaria, una institución creada con el objeto de preparar la conversión de la moneda nacional y evitar fluctuaciones violentas de cambio, el país logró cierta estabilidad de la moneda, emitiéndose más tarde mediante el Decreto Legislativo No.1379, la Ley Monetaria y con ello, se creo “El Quetzal” como nueva moneda guatemalteca.

Como resultado de esta primera reforma, se creó también el Banco Central de Guatemala, con facultades de emisor único. Esta nueva institución se constituyó como una sociedad anónima mixta, aportando el Estado una parte para capitalización y dejando otra parte en manos de particulares, sin embargo, después de los cortos años de prosperidad de la economía guatemalteca, que siguieron a su fundación, vino la gran depresión económica de los años 1929-1933 la cual afectó a Guatemala, en una forma extraordinaria como país agrícola y de economía dependiente de un sólo producto de exportación (el café) y puso a prueba al ente emisor, cuya actuación se caracterizó por una política deflacionaria de crédito que impidió la recuperación de la actividad productiva del país.

La segunda reforma se inicia con el estudio de una nueva reforma monetaria y bancaria, más acorde con la realidad económica nacional. Al mismo tiempo, se crea el Ministerio de Economía, todo esto a principios del año 1945.

Esta reforma consistió en varios proyectos, siendo el primordial de ellos la creación de un sistema de Banca Central con un nuevo banco central (Banco de Guatemala) como institución netamente estatal con plena autonomía, con el objeto de que pudiera adaptar los medios de pago a las legítimas necesidades del país y promover la creación y el mantenimiento de las condiciones monetarias, cambiarias y crediticias más favorables al desarrollo ordenado de la economía guatemalteca.

Por otra parte, se reorganizó el Crédito Hipotecario Nacional para complementar la acción del Banco de Guatemala en el ejercicio de la actividad crediticia directa, especialmente en lo que se refiere al crédito agrícola industrial.

La tercera y última reforma de modernización del sistema financiero guatemalteco, se efectuó en el año 2002, con la promulgación de las siguientes leyes: Ley Orgánica del Banco de Guatemala (Decreto No. 16-2002), Ley Monetaria (Decreto No. 17-2002), Ley de Bancos y Grupos Financieros (Decreto No. 19-2002), Ley de Supervisión Financiera (Decreto No. 18-2002), Ley de Libre Negociación de Divisas (Decreto No. 94-2002) y Ley Contra el Lavado de Dinero u Otros Activos (Decreto No. 67-2001).

1.2 Banco

Los bancos autorizados conforme al Decreto 19-2002 del Congreso de la República, Ley de Bancos y Grupos Financieros, “podrán realizar intermediación financiera bancaria, consistente en la realización habitual, en forma pública o privada, de actividades que consistan en la captación de dinero, o cualquier instrumento representativo del mismo, del público, tales como la recepción de depósitos, colocación de bonos, títulos u otras obligaciones, destinándolo a financiamiento de cualquier naturaleza, sin importar la forma jurídica que adopten dichas captaciones y financiamientos; sus operaciones y servicios” (7:10) se dividen de la siguiente manera:

a) Operaciones Pasivas

1. Recibir depósitos monetarios
2. Recibir depósitos a plazo
3. Recibir depósitos de ahorro
4. Crear y negociar bonos y/o pagarés
5. Obtener financiamiento del Banco de Guatemala
6. Obtener créditos de bancos nacionales y extranjeros
7. Crear y negociar obligaciones convertibles
8. Crear y negociar obligaciones subordinadas
9. Realizar operaciones de reporto como reportado

b) Operaciones activas

1. Otorgar créditos
2. Realizar descuento de documentos
3. Otorgar en operaciones de cartas de crédito
4. Conceder anticipos para exportación
5. Emitir y operar tarjeta de crédito
6. Realizar arrendamiento financiero
7. Realizar factoraje
8. Invertir en títulos valores emitidos y/o garantizados por el Estado, bancos o entidades privadas

9. Adquirir y conservar la propiedad de bienes inmuebles o muebles
10. Constituir depósitos en otros bancos del país y en bancos extranjeros
11. Realizar operaciones de reporto como reportador

c) Operaciones de Confianza

1. Cobrar y pagar por cuenta ajena
2. Recibir depósitos con opción de inversiones financieras
3. Comprar y vender títulos valores por cuenta ajena
4. Servir de agente financiero, encargándose del servicio de la deuda, pago de intereses, comisiones y amortizaciones

d) Pasivos contingentes

1. Otorgar garantías
2. Prestar avales
3. Otorgar fianzas
4. Emitir o confirmar cartas de crédito

e) Servicios

1. Actuar como fiduciario
2. Comprar y vender moneda extranjera (efectivo y doctos.)

3.Apertura de cartas de crédito

4.Efectuar operaciones de cobranza

5.Realizar transferencia de fondos

6.Arrendar cajillas de seguridad

1.2.1 Institución de un Banco

Según la legislación de nuestro país, Decreto 19-2002 del Congreso de la República Ley de Bancos y Grupos Financieros, los bancos privados nacionales deben constituirse en forma de sociedades anónimas. La autorización de tales entidades se encuentra a cargo de la Junta Monetaria, quien se encarga de otorgar o denegar la solicitud para su establecimiento con base en el dictamen que para dicha gestión elabora la Superintendencia de Bancos.

Posteriormente, tanto el testimonio de la escritura constitutiva como la certificación de la resolución de la Junta Monetaria se presenta en el Registro Mercantil para su inscripción. Los bancos al contar con la autorización de la Superintendencia de Bancos deben iniciar operaciones a seis meses plazo seguidos de la fecha de la notificación de autorización para su constitución y/o establecimiento.

“El capital social con el que cuenta una entidad bancaria en el momento de su apertura, debe estar dividido y representado en acciones nominativas cuyo monto mínimo inicial será establecido o fijado siempre por la Superintendencia de Bancos

con base en un mecanismo aprobado por la Junta Monetaria y revisado por lo menos una vez al año" (7:17). Según resolución de Junta Monetaria JM-34-2005 de fecha 23 de enero de 2005, actualmente es de Q.102,000.000.00 para los bancos y sucursales de bancos extranjeros y Q.42,000.000.00 para los bancos de ahorro y préstamo para la vivienda familiar

1.2.2 Áreas en las que se encuentra dividido un Banco

De manera general los bancos en Guatemala se encuentran organizados de la siguiente manera:

- Gerencia General
  - Banca de Empresas
  - Tesorería
  - Banca de Personas
  - Mercadeo
  - Administración
  - Créditos
- Riesgos
  - Operaciones
    - Resolución Créditos
    - Operaciones (seguridad)
    - Contabilidad
  - Tarjeta de Crédito

- Informática

- Contraloría
  - Auditoría Interna
  - Cumplimiento

1.2.3 Área de Caja

Unidad concentradora de todas las transacciones relacionadas con valores, háblese por ejemplo de recepción de depósitos, retiros de ahorro, pagos de cheques, recepción cobros de terceros, notas de crédito y débito, pago de cheques de caja, entregas a bóveda, traslado de efectivo para la agencia central. Dividida principalmente en Caja propiamente dicha, Compensación (pagos de cheques, emisión de notas de débito, traslado de documentos a través de la cámara de compensación), Plataforma (emisión de cheques de caja, transferencias nacionales, apertura de cuentas) y Cajeros Automáticos (retiros de efectivo, pagos de terceros, transferencias).

1.3 Clasificación de las Entidades Bancarias

Con base en el Decreto 19-2002 del Congreso de la República, Ley de Bancos y Grupos Financieros, estos se clasifican de la siguiente forma:

- Bancos Privados Nacionales, son aquellas instituciones financieras de propiedad particular que realizan funciones de captación y financiamiento

de recursos, persiguiendo con ello una utilidad o beneficio como resultado del diferencial entre las tasas de interés activas –préstamos- y pasivas –cuentas de depósitos-.

- Bancos Extranjeros, están constituidos por el conjunto de entidades financieras cuyas oficinas matrices –centrales- radican en el exterior y cuya mayoría de capital pertenece a personas físicas o jurídicas no residentes en Guatemala.

1.4 Riesgo

El riesgo es inherente a las actividades de las entidades financieras, el área de Caja como parte importante de ellas, tiende a ser más vulnerable a la exposición de riesgos por concentrar un alto porcentaje de transacciones diariamente, las cuales, deben de ser evaluadas constantemente con el propósito de evitar ser utilizadas como áreas de fraude. Aunque lo importante es identificar las técnicas o mecanismos que nos permitan reducir esos niveles de riesgo, primero partiremos por entender ¿qué es un riesgo?.

“Posibilidad que sucedan eventos que puedan causar pérdidas en el futuro o variaciones en los ingresos futuros (ganancias o pérdidas)” (14:4).

“Agrupa una diversidad de conceptos que representan un riesgo para la entidad, como consecuencia de la posible ocurrencia de sucesos inesperados o fallos relacionados con la infraestructura operativa interna y externa. Incluye el riesgo

de que, debido al registro contable incorrecto de las operaciones se originen variaciones significativas en la información externa e interna facilitada" (14:5).

"Es aquel referido a las pérdidas directas e indirectas que resultan de procesos internos inadecuados o de los fallos en los mismos, humanos, de sistemas y como consecuencia de sucesos externos" (14:5).

1.5 Identificación del Riesgo

"El primer paso en un programa interno efectivo de administración de riesgo es distinguir los riesgos relevantes que un banco enfrenta, analizando su misión de negocios, actividades básicas y los principales procesos. Algunos de los riesgos genéricos más importantes frecuentemente identificados son aquellos relacionados con el crédito, liquidez, tasas de interés, tasa de cambio, precios de activos financieros sistemas y operaciones, contabilidad e información, actividad criminal, actividades fiduciarias, procesos gerenciales/administrativos, la estructura legal, reglamentaria y judicial, y la propia reputación del banco en el mercado. Estos tipos de riesgos no son mutuamente excluyentes y cualquier producto o servicio que el banco provee pueden exponerlo a múltiples riesgos" (7:3).

Estos riesgos pueden ser agrupados en categorías amplias, aunque cualquier intento por agrupar involucra un cierto grado de arbitrariedad. Por ejemplo, los riesgos de tasa de interés, cambiario y de liquidez esta cercanamente relacionados

con los riesgos de precios y frecuentemente se les categoriza como riesgos de mercado.

"Otra manera para identificar los riesgos es la siguiente:

Analizar los procesos críticos y sus recursos

- Identificación, documentación y evaluación (mejores prácticas)

Identificar los riesgos en cada proceso

- Analizando pérdidas históricas externas e internas
- Utilizando modelos estratégicos
- Siguiendo las "mejores prácticas" de la industria

Identificar los factores que afectan cada riesgo, por ejemplo:

- Volumen transaccional, complejidad (intrínseco y extrínseca), efecto del tiempo (día de la semana o temporada del año), impacto de los cambios, suficiencia de la Gerencia" (9:5)

1.6 Medición del Riesgo

"La medición del riesgo es un elemento crítico de un proceso efectivo de administración de riesgo. La medición permite a la gerencia priorizar, controlar y vigilar el riesgo. Los riesgos deben ser medidos de manera consistente, sin importar en qué parte del banco ocurran, sobre la base de estas dos variables: Potencial de Pérdidas y Frecuencia de las pérdidas. El potencial de pérdidas

representa la magnitud de la ocurrencia de una sola pérdida. La Frecuencia de las pérdidas mide la probabilidad de que ocurran pérdidas" (9:7).

1.7 Seguimiento del Riesgo

"El seguimiento del riesgo involucra la instrumentación de controles y sistemas adecuados que permitan a la gerencia monitorear de manera efectiva y continua los niveles de riesgo en cada área de negocios u operaciones.

El seguimiento del riesgo incluye una continua evaluación de la estabilidad de los riesgos y los niveles actuales de exposición. La exposición es la parte del riesgo que no ha sido cubierta o transferida. Las actividades de seguimiento pueden incluir comunicaciones formales e informales, revisión de datos apropiados e investigación de desviaciones respecto a la política establecida. Las actividades de seguimiento del riesgo deben estar apoyadas por sistemas de información que provean a la gerencia y el consejo de administración de reportes oportunos sobre la condición financiera, resultados operativos y exposición al riesgo de la organización en su conjunto" (9:7).

1.8 Control del Riesgo

"El control del riesgo incluye el establecimiento de procedimientos para mitigar los riesgos. Para determinar qué controles son necesarios para controlar un riesgo determinado, los gerentes deben ponderar el costo de mejores controles contra los beneficios de éstos. Existen varios métodos para lidiar con el riesgo, como el

reducirlo, asumirlo y transferirlo. El esquema de medición de riesgos del banco debe tener una herramienta de soporte para determinar el método apropiado. Los controles son los procedimientos establecidos para mitigar los riesgos.

Para cada riesgo importante que ha sido identificado, el banco debe establecer los controles clave asociados con ese riesgo. Deben establecerse directrices para asegurar que los controles funcionen de manera apropiada. Los controles deben ser revisados siempre que haya un cambio en los negocios u operaciones (p.e. nuevo producto). Por lo que el personal debe ser adecuadamente capacitado para asegurar que se sigan las políticas y procedimientos establecidos" (9:7).

1.9 Clasificación del Riesgo

Dentro de la clasificación más general tenemos la siguiente:

- Operacional
- Riesgo Bancario
  - De Crédito
  - Cambiario
  - De País y de Transferencia
  - De Mercado
  - Fiduciario
  - Estratégico Administración
  - De Tasa de Interés

  - De Liquidez
  - Contabilidad e información
  - De Precio
  - Legal, Reglamentario y Judicial
  - De Reputación
  - Criminal
- Riesgo Informático

Otros riesgos

- Riesgo de Fraude

1.10 Riesgo Operativo u Operacional

El riesgo de sistemas y operaciones (también conocido como riesgo de transacción) es el riesgo que enfrentan las ganancias o el capital que surge de problemas en la entrega de los servicios o productos. El riesgo involucra una amplia gama de asuntos tecnológicos, incluyendo el desarrollo de sistemas de procesamiento de información, capacidad y precisión de los sistemas, almacenamiento y entrega del procesamiento de datos, integridad y seguridad de los sistemas y administración de los acuerdos de subrogación de servicios. Este riesgo es función de los controles internos, sistemas de información, integridad de los empleados y procesos operativos.

Según el Comité de Basilea -organización formada en 1975, por los presidentes de los Bancos Centrales del Grupo de los Diez (Países), integrada por autoridades en

Supervisión Bancaria de los siguientes países: Bélgica, Canadá, Francia, Alemania, Italia, Japón, Luxemburgo, Holanda, Suecia, Suiza, Reino Unido y los Estados Unidos. Esta organización adopta el nombre de Comité de Basilea para la Supervisión Bancaria, ya que usualmente se reúne en el Banco de Regulaciones Internacionales en Basilea, donde se encuentra ubicada permanentemente su secretaría- acerca de la Administración del Riesgo Operacional, indica que tal riesgo se esta volviendo una característica importante de una práctica sólida de administración de riesgos en los mercados financieros modernos. Los tipos más importantes de riesgos operacionales involucran las evaluaciones de los controles internos y del gobierno corporativo. Tales evaluaciones pueden conducir a pérdidas financieras a través del error, el fraude, o el fracaso de rentabilidad en una forma oportuna o puede causar que los intereses de los bancos se vean comprometidos en alguna otra forma, por ejemplo, por sus casas de bolsa, oficiales de préstamos u otro personal que excedan su autoridad o que conduzcan los negocios en una forma no auténtica o riesgosa.

A pesar que dentro de la clasificación proporcionada existe dentro del riesgo bancario el riesgo operacional, se proporciona su explicación fuera del él, debido a que es el tema principal del presente trabajo, por lo que su definición no será descrita más adelante.

1.10.1 Administración de Riesgo Operativo

"Es el proceso continuo y sistemático de identificación del riesgo, su medición, análisis, control, prevención, reducción, evaluación y financiamiento.
Un programa global de administración del riesgo involucra la evaluación de los riesgos y controles para cada una de las unidades de negocios del banco, desarrollando planes para vigilar la actual efectividad de los controles y resolviendo las debilidades identificadas. Para que sea exitoso, el programa de administración de riesgos debe tener apoyo pleno de la gerencia ejecutiva y este compromiso debe extenderse a todo el banco. La administración del riesgo debe convertirse en una parte de la cultura del banco y un componente integral de la manera en que se realizan los negocios" (9:1).

Un programa global de administración de riesgos incluye cuatro componentes: a) Tolerancia de riesgo, que no es más que el deseo y la habilidad, o ambos, de asumir riesgos en algún tipo de actividad. En la banca, como en todo negocio, es necesario asumir algunos niveles de riesgo para poder obtener ganancias operativas. Es responsabilidad de la Gerencia Ejecutiva, establecer la tolerancia al riesgo del banco; b) Evaluación del riesgo, que consiste en una evaluación formal de los riesgos relevantes asociados a un producto, servicio u operación, a los controles ya establecidos para administrar esos riesgos dentro de los límites establecidos y a los mecanismos utilizados por la Gerencia para vigilar las

excepciones a estos límites; c) Vigilancia del riesgo y d) Evaluación de la administración del riesgo.

1.10.1.1 Monitoreo

Seguimiento de operaciones bancarias calificadas como críticas y cuya finalidad es controlar o reducir el riesgo de fraude operacional.

"La efectividad general de los sistemas de control interno del banco debe ser monitoreada en forma permanente. El monitoreo de riesgos claves debe ser parte de las actividades diarias del banco así como evaluaciones periódicas por línea de negocio y de la auditoría interna" (1:18).

1.10.1.2 Control

Según la Ley de Bancos y Grupos Financieros en su artículo 57 Control Interno, cita: "Los bancos y las empresas que integran grupos financieros deben mantener un sistema de control interno adecuado a la naturaleza y escala de sus negocios, que incluya disposiciones claras y definidas para la delegación de autoridad y responsabilidad, separación de funciones, desembolso de sus fondos, la contabilización de sus operaciones, salvaguarda de sus activos, y una apropiada auditoría interna y externa independiente, así como una unidad administrativa responsable de velar porque el personal cumpla estos controles y las leyes y disposiciones aplicables" (7:28).

1.10.1.3 Políticas y Procedimientos

En el momento de establecer el control a aplicar para el riesgo operacional se deben renovar o desarrollar nuevas políticas y procedimientos acorde a los objetivos.

1.11 Riesgo Bancario

El artículo 55 del Decreto 19-2002 Ley de Bancos y Grupos Financieros cita: "Los bancos y las empresas que integran grupos financieros deberán contar con procesos integrales que incluyan, según el caso, la administración de riesgos de crédito, de mercado de tasa de interés, de liquidez, cambiario, de transferencia, operacional y otros que estén expuestos que contengan sistemas de información y un comité de gestión de riesgos, todo ello con el propósito de identificar, medir, monitorear, controlar y prevenir los riesgos" (7:27).

1.11.1 Riesgos en Bancos

La banca, por su naturaleza, está vinculada a la toma de un amplio conjunto de riesgos. Los riesgos claves se comentan a continuación:

1.11.2 Riesgo de Crédito

"El riesgo de crédito es el riesgo que enfrentan las ganancias o el capital por las fallas de un acreditado para cumplir cualquier contrato con el banco, o para hacerlo como fuera acordado. El riesgo de crédito surge de todas las actividades

en que el éxito depende del comportamiento de una contraparte, de un emisor o de un deudor" (9:3).

"Grandes exposiciones en un solo prestatario o a un grupo de prestatarios relacionados, son causas comunes de problemas bancarios en los que representan una concentración de riesgo de crédito. Grandes concentraciones también pueden resultar con respecto a industrias particulares, sectores económicos, o regiones geográficas y por tener grupos de préstamos con otras características que les hacen vulnerables a los mismos factores económicos (por ejemplo, transacciones altamente apalancadas)"(4:16).

1.11.3 Riesgo Cambiario

"El riesgo cambiario es el riesgo que enfrentan las ganancias o el capital que se origina por movimientos en las tasas de cambio que afectan el valor de los activos o pasivos del banco. Este riesgo está asociado con la mayor parte de las actividades transfronterizas como fondeo, préstamos y actividades operativas de este tipo, aunque también está presente cuando los bancos entran al negocio de tomar depósitos o de dar préstamos a residentes domésticos, en moneda extranjera" (9:4).

También se puede entender como: la posibilidad de pérdidas por las variaciones en las tasas de cambio de las diferentes monedas, con las cuales, una institución

financiera realiza operaciones o tiene recursos invertidos. Por ejemplo, en Guatemala uno de los factores que influyen en la tendencia a la baja de la divisa es la abundante oferta de dólares producto del creciente ingreso de remesas familiares.

1.11.4 Riesgo de País y de Transferencia

En adición al riesgo inherente de crédito de la contraparte, los préstamos internacionales también incluyen el riesgo de país, que se refiere al riesgo asociado con el ambiente económico, social y político donde el prestatario tiene su domicilio.

"El riesgo del país es más evidente cuando se presta a otros gobiernos, considerando que tales préstamos no están típicamente asegurados, pero es importante considerar cuando se hacen préstamos o inversiones en el extranjero si estos se hacen a prestatarios públicos o privados. También existe un componente de riesgo de país llamado "riesgo de transferencia" que resulta cuando la obligación de un prestatario no esta denominada en la moneda local. La moneda de la obligación puede no estar disponible para el prestatario sin importar su particular condición financiera" (3:16).

1.11.5 Riesgo de Mercado

"Los bancos enfrentan el riesgo de pérdidas dentro y fuera del balance, resultantes de los movimientos de precios de mercado. Normas de contabilidad

causan que estos riesgos sean típicamente más visibles en las actividades de negociación (trading) de los bancos ya sea que involucren débitos o instrumentos líquidos, o cambio extranjero o posiciones de mercancías. Un elemento específico del riesgo de mercado es el riesgo de cambio extranjero" (9:16).

Sin lugar a dudas, los retos ante la firma del Tratado de Libre Comercio –TLC- son ejemplos de cómo puede afectar el mercado a una institución, por ejemplo, la competencia ante compañías internacionales con altos niveles de eficacia, tecnología, recurso humano altamente calificado, exigen inversiones en estas ramas.

1.11.6 Riesgo Fiduciario

"El riesgo fiduciario es el riesgo que enfrentan las ganancias o el capital que surge de la administración de cuentas de clientes y las actividades de inversión ejecutadas para los clientes del banco. Este riesgo involucra actividades tales como la administración de cuentas, administración de efectivo y custodia global cuando se hacen para clientes" (9:5).

1.11.7 Riesgo Estratégico / Administración

"Riesgo que enfrentan las ganancias o el capital por decisiones de negocios adversas o por la mala instrumentación de estas decisiones" (9:5).

1.11.8 Riesgo de Tasa de Interés

"El riesgo de tasa de interés es el riesgo que enfrentan las ganancias o el capital que se origina por movimientos en las tasas de interés. Este riesgo impacta tanto en las ganancias como en el valor económico de los activos de un banco, así como en los pasivos. Las formas primarias del riesgo de tasa de interés a los que típicamente están expuestos los bancos son: (1) el riesgo de reevaluación, que resulta de las diferencias de tiempo en el plazo de vencimiento (por tasa fija) y de la reasignación del precio (por tasa flotante) de los activos y pasivos del banco; (2) el riesgo de la curva de rendimiento, que resulta de cambios en la pendiente y forma de la curva de rendimiento (3) riesgo base, que resulta de la correlación imperfecta en el ajuste de las tasas ganadas y pagadas sobre diferentes instrumentos con otras características similares de reasignación de precios; y (4) opcionalidad que resulta de alternativas expresas o implícitas integradas en muchos activos y pasivos" (4:17).

1.11.9 Riesgo de Liquidez

"El riesgo de liquidez es el riesgo que enfrentan las ganancias o el capital por la incapacidad del banco para cumplir con sus obligaciones cuando éstas vencen, sin incurrir en pérdidas inaceptables y surge de la inhabilidad de un banco de acomodar las reducciones de sus pasivos o de respaldar incrementos en sus activos. Cuando un banco tiene una liquidez inadecuada, no obtiene suficientes fondos, ya sea incrementando sus pasivos o convirtiendo sus activos rápidamente,

con un costo razonable, afectando su rentabilidad. En casos extremos, una liquidez insuficiente puede ocasionar la insolvencia de un banco" (4:17).

1.11.10 Riesgo Contabilidad e información

"El riesgo financiero es el riesgo que enfrentan las ganancias o el capital debido a fallas en el cumplimiento con requerimientos transaccionales, de documentación o analíticos para obtener el tratamiento contable deseado. El riesgo financiero afecta la precisión, oportunidad y conveniencia de los datos utilizados para el análisis financiero y los reportes" (9:5).

1.11.11 Riesgo de Precio

"El riesgo de precio es el riesgo que enfrentan las ganancias o el capital que surge de cambios en el valor de carteras de instrumentos financieros (de deuda o capital) en el marco de actividades de negociación (creación de mercados, toma de posiciones, corretaje). Aunque los cambios de precios reflejan en gran parte cambios en las tasas de interés o en las tasas de cambio, otros factores como cambios en las leyes impositivas, eventos políticos, etc., también pueden afectar el precio de estos instrumentos" (9:6).

1.11.12 Riesgo Legal, reglamentario y judicial

"El riesgo legal y reglamentario (también conocido como riesgo de cumplimiento) es el riesgo que enfrentan las ganancias o el capital que surge de

violaciones o no cumplimiento con leyes, reglas, prácticas prescritas o estándares éticos" (4:17).

1.11.13 Riesgo de Reputación

"El riesgo de reputación surge de fallas operacionales, fallas en cumplir con leyes y regulaciones relevantes u otras fuentes. El riesgo de reputación es particularmente dañino para los bancos considerando que la naturaleza de su negocio requiere mantener la confianza de sus depositantes, acreedores y el mercado en general" (4:18).

1.11.14 Riesgo Criminal

"El riesgo criminal es el riesgo que enfrentan las ganancias o el capital debido a actividades criminales en contra del banco, dentro de estas tenemos la falsificación, el fraude, malversación, robo, transacciones de personas de adentro (insiders), vandalismo y extorsión" (9:5).

1.11.15 Riesgo de Fraude

"El fraude es la acción u omisión intencionada realizada con engaño, persigue el beneficio propio y es una de las consecuencias de riesgo operacional no cubierto y puede ser interno (empleados), externo o combinación de ambos; por sus peculiaridades, requiere tratamiento específico, pues es una función de

subriesgo de infidelidad (Recursos Humanos y de todos los demás subriesgos no cubiertos)" (9:9).

El fraude bancario, busca un beneficio propio mal habido utilizando el engaño, utilizando a la entidad y se divide en dos partes:

Fraude Interno, actos destinados a defraudar, usurpar la propiedad o evadir la regulación, la ley o las políticas de la empresa, regularmente involucra una parte interna. Ejemplos de ello incluyen: reportes de posiciones intencionalmente errados, defraudación de empleados, y negociación con información privilegiada por cuenta de un empleado.

Fraude Externo, actos por parte de terceros destinados a defraudar, usurpar la propiedad o evadir la ley. Ejemplos de ello incluyen: robo, falsificación y emisión de cheques sin fondos, falsificación de documentos.

De acuerdo a la legislación guatemalteca, fraude se define de la siguiente manera: "El funcionario o empleado público que, interviniendo por razón de su cargo en alguna comisión de suministros, contratos, ajustes, o liquidaciones de efectos de haberes públicos, se concertare con los interesados o especuladores, o usare de cualquier otro artificio para defraudar al Estado" (6:59).

Por último, la Norma Internacional de Auditoria –NIA- 240, establece: El término "fraude" se refiere a un acto intencional por parte de uno o más individuos de entre la administración, empleados, o terceras partes, que da como resultado una representación errónea de los estados financieros. El fraude puede implicar:

- Manipulación, falsificación o alteración de registros o documentos.
- Malversación de activos.
- Supresión u omisión de los efectos de transacciones en los registros o documentos.
- Registro de transacciones sin sustancia.
- Mala aplicación de políticas contables.

El riesgo de fraude deriva principalmente de los siguientes motivos:

- Cultura Corporativa: Falta de conocimiento con relación al fraude, desprecio del control, permisividad ante el fraude.
- Carencia de Controles: Falta de segregación de funciones, programas operativos mal diseñados, organismos de control inexistentes o ineficientes, carencia de políticas y normas.
- Gestión Recursos Humanos: Falta de objetividad en ascensos, falta de expectativas profesionales, sistemas de remuneración inadecuadas, mal clima laboral, selección de personal inadecuado.

Sin duda, las entidades bancarias se encuentran sujetas a distintos tipos de fraudes, debido a la tentación que existe como consecuencia del manejo del dinero.

1.11.15.1 Tendencias de Fraude

Actualmente se publican cifras que se extraen del mundo de las estadísticas en lo referente al fraude, este delito tiene la fuerza suficiente para alcanzar las mismas raíces de la solvencia de personas y empresas, y algunos han llegado a decir que podría quebrantar los cimientos del orden financiero internacional, si se le deja seguir avanzando sin oponerle adecuados mecanismos preventivos.

Hoy en día, la criminalidad económica que tiene mayor trascendencia es aquella que se apoya en medios fraudulentos. Estos se han ido adaptando paulatinamente a las nuevas formas de delinquir que han surgido con los medios técnicos (de forma particular en los informáticos).

1.11.15.2 Modalidades de Fraude

De una manera amplia, podemos citar las siguientes modalidades de defraudación.

- En forma solitaria o a través de una o más personas.
- Con participación de personal de la entidad, o no.

- Sucesivas acciones simultáneas por montos poco significativos o menores, o una acción única por un monto importante.
- A través de medios físicos, magnéticos y otros (línea telefónica).

1.12 Riesgo Informático

Los sistemas de información electrónica y el uso de la tecnología de la información, tienen riesgos que deben ser controlados efectivamente por parte de los bancos, en orden para evitar perturbaciones de negocios y pérdidas potenciales. Desde que el procesamiento de transacciones y las aplicaciones de negocios se han extendido más allá del uso de ambientes de grandes equipos de computación, a sistemas distribuidos de funciones de negocios de misiones críticas, la magnitud de los riesgos también se ha extendido.

1.13 Principios de Riesgo Generalmente Aceptados (GARP)

Los principios de riesgo generalmente aceptados GARP –Global Association of Risk Professionals-, fueron creados como respuestas al desafío del entorno actual y la necesidad de una estructura global y de control de riesgo. De manera general se encuentran basados en los siguientes aspectos:

"1°: La administración de riesgo es responsabilidad del Directorio, por lo tanto debe ser manejado desde la administración superior, por aquellos en el cual recae la responsabilidad de administrar el negocio.

2°: La estructura de administración de riesgo debe cubrir la totalidad de los riesgos existentes, incluidos aquellos, como por ejemplo, riesgos de operación, jurídicos, de imagen y de recursos humanos, los cuales no necesariamente se cuantifican o miden regularmente.

3°: Todas las funciones de apoyo y control, tales como, del front office (autorización, apoyo de decisión, experiencia de la contraparte, financiamiento, captación comercial), middle office y back office (valuaciones, informe de ganancias pérdidas, verificación de precios, procesamiento comercial, confirmación, liquidación, reconciliación, control activo), auditoría interna y legal, son integrantes de la estructura de riesgo.

4°: los objetivos de riesgo y las políticas deben ser conectadas a estrategias e implementados a través de procedimientos y controles sólidos" (16:6).

CAPÍTULO II

Marco Legal, Técnico y Normativo en la Adaptación de Software en Auditoría

2.1 Auditoría Interna

La auditoría interna es la denominación de una serie de procesos y técnicas, a través de las cuales se da una seguridad de primera mano a la dirección respecto a los empleados de su propia organización, a partir de la observación en el trabajo respecto a: si los controles establecidos por la dirección son mantenidos adecuada y efectivamente; si los registros e informes (financieros, contables o de otra naturaleza) reflejan las operaciones actuales y los resultados adecuada y rápidamente en cada división, departamento u otra unidad, y si éstos se están llevando fuera de los planes, políticas o procedimientos de los cuales la auditoría es responsable.

2.2 Auditoría Informática

"Evaluación de los recursos utilizados por el área de informática y de lo que se hace alrededor del computador. Realización total o parcial de un examen, aplicando normas, políticas y procedimientos de auditoría informática de aceptación general o de la organización con el propósito de emitir un juicio sobre la estructura de control de un sistema de aplicación específico o sobre aspectos generales relacionados con el área de informática. Utilizando para tal objetivo los siguientes recursos: Software, Hardware, Personal, Suministros" (10:1).

2.3 Auditoría en un Ambiente de Sistemas de Información por Computadora

Un ambiente de Sistemas de Información por Computadora –SIC-, existe cuando está involucrada una computadora de cualquier tipo o tamaño en el procesamiento por la entidad de información financiera de importancia para auditoría, ya sea operada por la entidad o por una tercera parte, esto según la Norma Internacional de Auditoría NIA 401.

El objetivo y alcance global de una auditoría no cambia en un ambiente SIC que es el de emitir opinión acerca de la posición financiera de la empresa. Sin embargo, el uso de una computadora cambia el procesamiento, almacenamiento y comunicación de la información financiera y puede afectar los sistemas de contabilidad y de control interno empleados por la entidad. Por consiguiente, un ambiente SIC puede afectar:

a) Los procedimientos seguidos por un auditor para obtener una compresión suficiente de los sistemas de contabilidad y de control interno.
b) La consideración del riesgo inherente y del riesgo de control a través de la cual el auditor llega a la evaluación del riesgo.
c) El diseño y desarrollo por el auditor de pruebas de control y procedimientos sustantivos apropiados para cumplir con el objetivo de la auditoría.

2.4 Regulaciones según NIA's

CODIFICACIÓN DE NORMAS INTERNACIONALES DE AUDITORÍA (NIAs) Y DECLARACIONES INTERNACIONALES DE AUDITORÍA

La aparición de las Normas Internacionales de Auditoria (NIAs) expedida por la Federación Internacional de Contadores (IFAC, por sus siglas en inglés), y las actualizaciones que realiza su Comité Internacional de Prácticas de Auditoria (AIPC) anualmente, denotan la presencia de una voluntad internacional orientada al desarrollo sostenido de la profesión contable, a fin de permitirle disponer de elementos técnicos uniformes y necesarios para brindar servicios de alta calidad para el interés público.

La aplicación de procedimientos de auditoría puede requerir que el auditor considere técnicas que usen la computadora como una herramienta de auditoría.

Estos diversos usos de la computadora son conocidos como Técnicas de Auditoría con Ayuda de Computadora (TAACs), a continuación un extracto de lo regulado por las Normas Internacionales de Auditoría al respecto.

1009 Técnicas de Auditoria con Ayuda de Computadora (TAACs)

La Norma Internacional de Auditoría (NIA) 1009, describe dos de los tipos más comunes de TAACs; software de auditoría y datos de prueba usados para propósitos de auditoría. Sin embargo, los lineamientos proporcionados en esta

norma aplican a todo tipo de TAACs. Para efectos del tema tratado se dará énfasis al primero.

2.4.1 Software de Auditoría

El software de auditoría consiste en programas de computadora usados por el auditor, como parte de sus procedimientos para procesar datos de importancia del sistema de contabilidad u operaciones de la entidad.

Puede consistir en programas de paquete, programas escritos para un propósito, y programas de utilería. Independientemente de la fuente de los programas, el auditor deberá verificar su validez para fines de auditoría antes de su uso.

- Los programas en paquete, son aplicaciones de computadora diseñadas para desempeñar funciones de procesamiento de datos que incluyen leer archivos de computadora, seleccionar información, realizar cálculos, crear archivos de datos e imprimir.

- Los programas escritos para un propósito, son aplicaciones de computadora diseñados para desempeñar tareas de auditoría en circunstancias específicas. Estos programas pueden ser preparados por el auditor, por la entidad, o por un programador externo contratado por el auditor.

- Los programas de utilería, son usados por la entidad para desempeñar funciones comunes de procesamiento de datos, como clasificación, creación

e impresión de archivos. Estos programas generalmente no están diseñados para propósitos de auditoría.

2.4.2 Consideraciones en el uso de TAACs

Al planear la auditoría, el auditor deberá considerar una combinación apropiada de técnicas de auditoría manuales y con ayuda de computadora. Al determinar si se usan TAACs, los factores a considerar incluyen:

- Conocimiento, pericia y experiencia del auditor en computadoras.
- Disponibilidad de TAACs e instalaciones adecuadas de computación.
- No factibilidad de pruebas manuales.
- Efectividad y eficiencia.
- Oportunidad.

La ventaja más relevante en el uso de TAACs radica en el factor tiempo, ya que el resultado o la respuesta del procesamiento de información a través de computadoras es más rápida que de forma manual. Otra ventaja, se centra en el alcance de las pruebas, ya que los volúmenes de información a verificar pueden ser más extensos con el uso de programas.

El uso de TAACs para el auditor, está estrechamente ligada con inversiones en equipo y programas que regularmente conllevan desembolsos significativos, los

cuales, deben de tomarse en cuenta para su aplicación.

2.4.3 Conocimiento, pericia y experiencia del auditor en computadoras

Específicamente, el auditor deberá tener suficiente conocimiento para planear, ejecutar y usar los resultados de las TAACs adoptadas. El nivel de conocimiento requerido depende de la complejidad y naturaleza de las TAACs y del sistema de contabilidad de la entidad. Consecuentemente, el auditor deberá estar consciente de que el uso de TAACs en ciertas circunstancias puede requerir de manera importante más conocimiento y pericia en computadoras.

2.4.4 Disponibilidad de TAACs e Instalaciones adecuadas de computación

El auditor deberá considerar la disponibilidad de TAACs, instalaciones adecuadas de computación y los necesarios archivos y sistemas basados en computadoras.

2.4.5 No factibilidad de pruebas manuales

Muchos sistemas de contabilidad computarizados realizan tareas para las que no hay evidencia visible disponible y, en estas circunstancias, puede no ser factible para el auditor realizar pruebas en forma manual. La falta de evidencia visible puede ocurrir en diferentes etapas del proceso operativo.

2.4.6 Efectividad y eficiencia

La efectividad y eficiencia de los procedimientos de auditoría puede mejorarse mediante el uso de TAACs al obtener y evaluar evidencia de auditoría, por ejemplo:

- Algunas transacciones pueden ser probadas más efectivamente por un nivel similar de costo, usando la computadora para examinar todas o un mayor número de transacciones que de otro modo serían seleccionadas.

2.4.7 Oportunidad

Ciertos archivos de computadora, como los archivos de transacciones detalladas, a menudo se conservan por sólo un tiempo corto, y pueden no estar disponibles en forma legible por la máquina cuando el auditor lo requiere. Así, el auditor necesitará hacer arreglos para la conservación de datos que él requiera, o puede necesitar alterar la programación de su trabajo que requiera de estos datos. Cuando el tiempo disponible para llevar a cabo una auditoría es limitado, el auditor puede planear usar unas TAACs porque satisfará sus requerimientos de tiempo mejor que otros procedimientos.

2.4.8 Utilización de TAACs

Los pasos principales que debe tomar el auditor en la aplicación de una TAACs, son:

(a) Fijar el objetivo de la aplicación de las TAACs.

(b) Determinar el contenido y accesibilidad de los archivos de la entidad.

(c) Definir los tipos de transacción que van a ser probados.

(d) Definir los procedimientos que se realizarán en los datos.

(e) Definir los requerimientos de datos de salida.

(f) Identificar al personal de auditoría y de computación que pueda participar en el diseño y aplicación de las TAACs.

(g) Refinar los estimados de costos y beneficios.

(h) Asegurarse de que el uso de las TAACs está controlado y documentado en forma apropiada.

(i) Organizar las actividades administrativas, incluyendo las habilidades necesarias y las instalaciones de computación.

(j) Ejecutar la aplicación de las TAACs.

(k) Evaluar los resultados.

2.4.9 Control de la aplicación de las TAACs

El uso de unas TAACs deberá ser controlado por el auditor para proporcionar razonable certeza de que los objetivos de auditoría y las especificaciones detalladas de las TAACs han sido satisfechos, y de que las TAACs no son manipuladas en forma inapropiada por el personal de la entidad. Los procedimientos específicos necesarios para controlar el uso de una TAAC dependerá de la aplicación particular.

Los procedimientos desempeñados por el auditor para controlar las aplicaciones del software de auditoría pueden incluir:

(a) Participar en el diseño y prueba de los programas de computadora.

(b) Verificar la codificación del programa para asegurar que está de acuerdo con las especificaciones detalladas del programa.

(c) Solicitar al personal de computación de la entidad que revise las instrucciones del sistema operativo para asegurar que el software correrá –funcionará- en la instalación de computación de la entidad.

(d) Correr el software de auditoría en pequeños archivos de prueba antes de correrlo en los archivos principales de datos.

(e) Asegurar que fueron usados los archivos correctos -por ejemplo, verificando con la evidencia externa, como totales de control conservados por el usuario.

(f) Obtener evidencia de que el software de auditoría funcionó como se planeaba -por ejemplo, revisando los datos de salida y la información de control-.

(g) Establecer medidas de seguridad apropiadas para salvaguardar contra la manipulación de los archivos de datos de la entidad.

La presencia del auditor no se requiere necesariamente en la instalación de computación durante la corrida de una TAAC para asegurar procedimientos de

control apropiados. Sin embargo, puede tener ventajas prácticas, como la posibilidad de controlar la distribución de los datos de salida y asegurar la corrección oportuna de errores -por ejemplo, si se fueran a usar archivos de entrada equivocados-.

Cuando utilice unas TAACs, el auditor puede requerir la cooperación del personal de la entidad que tenga amplio conocimiento de la instalación de computación. En tales circunstancias, el auditor deberá tener razonable certeza de que el personal de la entidad no influyó en forma inapropiada en los resultados de las TAACs.

2.4.10 Documentación

El estándar de papeles de trabajo y de procedimientos de retención de papeles de trabajo para una TAAC deberá ser consistente con el de la auditoría como un todo. Puede ser conveniente mantener los papeles técnicos que se refieren al uso de la TAAC separados de los otros papeles de trabajo de la auditoría. Los papeles de trabajo deberán contener suficiente documentación para describir la aplicación de la TAAC.

2.5 Regulaciones según CAATs

Los CAAT's (técnicas de auditoría asistidas por computador por sus siglas en inglés –Computer Assisted Audit Techniques-), emitidas por ISACA (Information Systems Audit and Control Association -Asociación de Auditoría y Control en

Sistemas de información-) son de suma importancia para el auditor cuando realiza una auditoría. Los CAAT's incluyen distintos tipos de herramientas y de técnicas, las que más se utilizan con los softwares de auditoría generalizado, software utilitario, los datos de prueba y sistemas expertos de auditoría. CAATs se pueden utilizar para realizar varios procedimientos de auditoría incluyendo: Prueba de los detalles de operaciones y saldos, procedimientos de revisión analíticos, pruebas de cumplimiento de los controles generales de sistemas de información, pruebas de cumplimiento de los controles de aplicación.

Los CAATs pueden generar otra gran parte de la evidencia de la auditoría que provienen de las auditorías de sistemas de información y como consecuencia, el auditor de sistemas de información debe planificar cuidadosamente y mostrar el cuidado profesional debido cuando se utilizan los CAATs. El ajustarse a esta guía no es obligatorio, pero el auditor de sistemas de información debe estar preparado para justificar cualquier incumplimiento a ésta.

2.5.1 Planificación.

Los factores a tomar en cuenta cuando se toma la decisión de utilizar CAATs cuando se planifica la auditoría, el auditor de sistemas de información debe considerar una combinación apropiada de las técnicas manuales y de auditoría asistidas por computador. Cuando se determina utilizar CAATs, los factores a considerar son los siguientes:

Conocimientos computacionales, pericia y experiencia del auditor de sistemas de información.

Eficiencia y efectividad de utilizar los CAATs en lugar de las técnicas manuales. Restricciones de tiempo.

2.5.2 Pasos para la planificación de los CAATs.

Los pasos más importantes que el auditor de sistemas de información debe considerar cuando prepara la aplicación de los CAATs seleccionados son los siguientes:

a) Establecer los objetivos de la auditoría de los CAATs, b) Determinar accesibilidad y disponibilidad de los sistemas de información, los programas/sistemas y datos de la organización. c) Definir los procedimientos a seguir (p. e. Una muestra estadística, recálculo, confirmación, etc.) d) Definir los requerimientos de recursos. e) Documentar los costos y los beneficios esperados, obtener accesos a las facilidades de los sistemas de información de la organización, sus programas/sistemas y sus datos. f) Documentar los CAATs a utilizar, incluyendo los objetivos, flujogramas de alto nivel y las instrucciones a ejecutar. g) Acuerdo con el cliente (auditado) los archivos de datos tanto como los archivos de operación detallados (transaccionales, por ejemplo), a menudo son guardados sólo por un período corto, por lo tanto, el auditor de sistemas de información debe arreglar que estos archivos sean guardados por el marco de tiempo de la auditoría. h) Ordenar el acceso a los sistemas de información de la

organización, programas/sistemas, y datos con anticipación para minimizar el efecto en el ambiente productivo de ésta.

El auditor de sistemas de información debe evaluar el efecto que los cambios a los programas/sistemas de producción puedan tener en el uso de los CAATs. Cuando el auditor de los sistemas de información lo hace, debe considerar el efecto de estos cambios en la integridad y utilidad de los CAATs, tanto como la integridad de los programas/sistema y los datos utilizados por el auditor de sistemas de información. Probando los CAATs el auditor de sistemas de información debe obtener una garantía razonable de la integridad, confiabilidad, utilidad y seguridad de los CAATs por medio de una planificación, diseño, prueba, procesamiento y revisión adecuados de la documentación. Esto debe ser hecho antes de depender de los CAATs. La naturaleza, el tiempo y extensión de las pruebas depende de la disponibilidad y la estabilidad de los CAATs.

2.5.3 Realización de la Auditoría.

2.5.3.1 Recolectar evidencia de la Auditoría.

El uso de los CAATs debe ser controlado por el auditor de sistemas de información para asegurar razonablemente que se cumple con los objetivos de la auditoría y las especificaciones detalladas de los CAATs.

El auditor debe: realizar una conciliación de los totales de control; realizar una revisión independiente de la lógica de los CAATs, realizar una revisión de los

controles generales de los sistemas de información de la organización que puedan contribuir a la integridad de los CAATs (p. e. Controles de los cambios en los programas y el acceso a los archivos del sistema, programas y/o datos).

2.5.3.2 El software de auditoría generalizado.

Cuando el auditor de sistemas de información utiliza el software de auditoría generalizado para acceder a los datos de producción, debe tomar las medidas apropiadas para proteger la integridad de los datos de la organización. Además, el auditor de sistemas de información tendrá que estar involucrado en el diseño del sistema y las técnicas que se utilizaron para el desarrollo y mantenimiento de los programas/sistemas de aplicación de la organización.

2.5.3.3 Software utilitario.

Cuando el auditor de sistemas de información utiliza el programa –software- utilitario debe confirmar que no tuvo lugar ninguna intervención no planificada durante el procesamiento y que este software ha sido obtenido desde la biblioteca de sistema apropiado, mediante una revisión del log de la consola –historial de usuarios- del sistema o de la información de contabilidad del sistema. El auditor de sistemas de información también debe tomar las medidas apropiadas para proteger la integridad del sistema y programas de la organización, puesto que estos utilitarios podrían fácilmente dañar el sistema y sus archivos.

2.5.3.4 Datos de prueba.

Cuando el auditor de sistemas de información utiliza los datos de prueba debe estar consciente de que puedan existir ciertos puntos potenciales de errores en el procesamiento, dado que esta técnica no evalúa los datos de producción en su ambiente real. El auditor de sistemas de información también debe estar consciente de que el análisis de los datos de prueba pueden resultar extremadamente complejos y extensos dependiendo del número de operaciones procesadas, el número de programas sujetos a pruebas y la complejidad de los programas/sistemas.

2.5.3.5 La documentación de los CAATs papeles de trabajo.

Una descripción del trabajo realizado, seguimiento y las conclusiones acerca de los resultados de los CAATs deben estar registrados en los papeles de trabajo de la auditoría. Las conclusiones acerca del funcionamiento del sistema de información y de la confiabilidad de los datos deben estar registrados en los papeles de trabajo de la auditoría. El proceso paso a paso de los CAATs debe estar documentado adecuadamente para permitir que el proceso se mantenga y se repita por otro auditor de sistemas de información. Específicamente los papeles de trabajo deben contener la documentación suficiente para describir la aplicación de los CAATs, incluyendo los detalles que se mencionan en los párrafos siguientes:

Planificación, la documentación debe incluir lo siguiente:

- Los objetivos y los CAATs a utilizar
- Los controles a implementar
- El personal involucrado
- El tiempo que tomará y los costos
- Ejecución.

La documentación en la ejecución debe incluir: Los procedimientos de la preparación y la prueba de los CAATs y los controles relacionados. Los detalles de las pruebas realizadas por los CAATs, los detalles de los input (ej. Los datos utilizados, esquema de archivos) el procesamiento (ej. Los flujogramas de alto nivel de los CAATs, la lógica) y los output (ej. Archivos log, reportes).

Evidencia de auditoría: la documentación debe incluir lo siguiente: el output producido, una descripción del trabajo de análisis de auditoría que se realizó para el output.

Resultado de la auditoría, conclusiones de la auditoría, otros, la documentación debe incluir lo siguiente: las recomendaciones de la auditoría.

2.6 Efectos del Procesamiento Electrónico de Datos (PED) en el Examen del Control Interno

El estudio del control interno incluye el análisis y la comprensión de los métodos que se utilizan para procesar la información financiera, con el objeto de determinar si las técnicas establecidas cumplen con los objetivos del control interno; por lo tanto, cuando el Procesamiento electrónico de datos –PED- forma parte del control interno y de éste se deriva información sujeta a examen, el auditor debe realizar su estudio y evaluación y como resultado de dicho trabajo, deberá documentar adecuadamente sus conclusiones sobre el efecto del PED en sus pruebas de auditoría.

El alcance al efectuar el examen del control interno establecido en el PED, dependerá de la importancia de las aplicaciones en el proceso de la información financiera.

El PED por su complejidad y su constante evolución, requiere para el estudio y evaluación de su control interno de personal con entrenamiento técnico y capacidad profesional adecuados.

El impacto que eventualmente puede tener una deficiencia o desviación del control interno en el área de PED puede ser menos evidente y, sin embargo, tener mayor repercusión en errores en los estados financieros que pasen inadvertidos; lo

anterior significa que el auditor está obligado a efectuar su revisión utilizando todos los elementos que le permitan asegurarse de que la información a dictaminar se procesa adecuadamente.

Cabe citar que este boletín se refiere únicamente al estudio y evaluación del control interno del PED llevado a cabo por el auditor para determinar la naturaleza, extensión y oportunidad que va dar a sus procedimientos de auditoría. No se refiere a los procedimientos específicos para evaluar la eficiencia en la operación del equipo de cómputo ni a las técnicas de auditoría utilizadas con ayuda del mismo computador para probar los sistemas (programas) y/o el contenido de los archivos.

Los objetivos de los controles establecidos en la empresa deben enfocarse a la creación, a través de las políticas y procedimientos adecuados, de un sistema que asegure que toda la información que deba ser procesada, se procese en forma correcta y oportuna y que dicho proceso se obtenga la información esperada. Los objetivos generales del control interno, son los siguientes:

Objetivos de autorización: Todas las operaciones deben realizarse de acuerdo con autorizaciones generales o específicas de la administración.

Objetivos de Procesamiento y clasificación de transacciones: Todas las operaciones deben registrarse para permitir que la preparación de estados

financieros de conformidad de principios de contabilidad generalmente aceptados o de cualquier otro criterio aplicable a dichos estados y para mantener en archivos apropiados datos relativos a los activos sujetos de custodia.

Objetivos de Salvaguarda física: El acceso a los activos sólo debe permitirse de acuerdo con autorizaciones de la administración, y

Objetivos de verificación y evaluación: Los datos registrados relativos a los activos sujetos a custodia deben compararse con los activos existentes a intervalos razonables y tomarse las medidas apropiadas respecto a las diferencias que existan. Asimismo, deben existir controles relativos a la verificación y evaluación periódica de los saldos que se informan en los estados financieros, ya que estos objetivos complementan en forma importante a los mencionados anteriormente.

CAPÍTULO III

Transacciones Susceptibles de Fraude en el Área de Caja de un Banco Privado

Las transacciones realizadas en el área de caja de un banco, involucran la mayor parte de productos o servicios que éste ofrece. Estas operaciones se encuentran enmarcadas dentro del riesgo operacional descrito en el capítulo dos y realizadas por personal contratado para estos propósitos.

Actualmente no existen controles de auditoria que cubran estas transacciones, que pudieran figurar dentro de los controles preventivos al área de caja específicamente. Estos se vuelven correctivos luego de identificarlos como parte de las revisiones periódicas que se realizan a dicha área o por reclamos de los clientes. A continuación se detallan las operaciones de caja susceptibles de fraude y la forma en que la auditoría actualmente las evalúa.

3.1 Funcionamiento actual del Área de Caja

3.1.1 Reversión de depósitos en efectivo en cuentas

Esta operación se origina luego que el cajero ha ingresado y certificado la transacción del cliente, éste realiza una reversión o extorno a la cuenta y se apropia del efectivo. El control para este tipo de operaciones por parte de la auditoría, es revisando el reporte de transacciones realizadas durante el día o en el momento que el cliente detecte el faltante. Es importante señalar que si se trata

de una empresa que realiza un número considerable de operaciones y la cantidad sustraída es relativamente baja puede pasar inadvertida.

3.1.2 Reversión de depósitos en efectivo y su posterior operación en cuenta de empleado.

Es similar a la anterior, con el agregado que el extorno se opera por parte del cajero en una cuenta de la cual es titular. El trabajo del auditor para detectar el fraude en este caso, es al cierre de cada día, verificando las cuentas de depósitos de cada uno de los empleados y cuestionar los depósitos en ellas operados, partiendo de la premisa que deben tener ingresos únicamente por su salario. Por otra parte, su trabajo puede empezar en el momento que el cliente se percate del faltante y presente un reclamo.

No todos los cuentahabientes realizan conciliaciones bancarias de sus cuentas, además, si tomamos en cuenta que los extornos son realizados a cuentas concentradoras por ejemplo: pago de teléfono, agua, luz, colegio, etc., la revisión se torna un tanto difícil y se complicaría aún más si los extornos fueran parciales.

3.1.3 Notas de crédito o depósitos a cuentas de empleados

Los créditos a las cuentas de empleados pueden presentarse también como una operación de notas de crédito ficticias a través del uso de la contraseña (password) de un empleado facultado para este tipo de transacciones. El auditor

en este tipo de casos, debe establecer dentro de sus revisiones, exámenes a cuentas de empleados, sobre movimientos sospechosos en sus cuentas de depósitos, pero el problema radica en: si se posee aún saldo en la cuenta luego de identificada la sustracción para recuperar el dinero; y, si el empleado aún tiene relación laboral con la entidad.

3.1.4 Notas de crédito o depósitos duplicados

Este caso se origina cuando por un error humano por parte del cajero o bien por un problema técnico en las comunicaciones entre la agencia y el computador que contiene la información de la cuenta -host del banco-, el cajero realiza dos veces una nota de crédito o un depósito a la cuenta de un cliente. Podemos deducir que la anomalía se corregirá en el momento del cuadre de la agencia, pero sucede que por fallas en los controles internos no se detecta o bien que debido a ser operada por otro cajero se duplicó la transacción, por lo que estaría cuadrada la jornada. El problema deriva cuando se detecte posteriormente y el cliente haya retirado los fondos e incluso cancelado la cuenta. Podemos nombrar a la operación como involuntaria a diferencia de la anteriores y sale de los alcances en las revisiones de la auditoría.

3.1.5 Retiros de ahorro sin libreta

Esta transacción posee la deficiencia que no se revisa el saldo de la cuenta por no contar con la libreta, por lo regular se solicita el aval (contraseña) del jefe

de la agencia para realizarla, sólo si el monto es significativo. Si un cajero conoce la contraseña y observa movimiento significativo en algunas cuentas, puede operarles un retiro con la esperanza que el cliente tarde unos días en detectarlo, tiempo en el cual, ya ha acumulado cierta cantidad y renuncia, burlando de esta manera, los controles a cuentas a empleados realizando depósitos a cuenta de un familiar. En este caso, la anomalía se detecta hasta que el cliente reclama los retiros.

3.1.6 Robo de libreta de ahorros de clientes

Cuando alguien realiza el robo de una libreta de ahorros e incluso roba o falsifica algún documento de identificación, puede realizar varios retiros por cantidades relativamente bajas para no llamar la atención, puede también, realizar las transacciones por medio de autobancos con el propósito de no levantar sospechas o que no se le identifique físicamente a través de cámaras por si el número de cédula no fuera acorde con la edad del supuesto cliente, burlando el control de la agencia. Otra alternativa a robos de libreta sería la impresión de estos documentos con características similares, datos que tienen que ser verificados en el instante sin perjudicar el servicio.

En los casos que se involucra a las libretas por retiros de dinero sin estos documentos o libretas robadas, las revisiones de auditoría son posteriores, revisando únicamente que en los retiros o depósitos a cuentas, se anoten los

correlativos de las libretas con el propósito de constatar que efectivamente se encuentren dentro de la numeración en circulación.

3.1.7 Retiros de ahorro a cuentas con poco movimiento

Un cajero puede establecer qué cuentas tienen poco movimiento o qué cuentahabiente realiza visitas periódicas para retirar efectivo, con el fin de manejar "auto préstamos". Aunque debe estar preparado por si existe un reclamo por parte del cliente y así registrar de inmediato la nota de crédito correspondiente. En casos como éste, se necesita la complicidad de más de una persona dentro de la agencia, con el propósito que no trascienda y se maneje dentro de ella, ya que en el momento de realizar los arqueos periódicos a su caja por parte del auditor o jefe de agencia, toda transacción se encuentre perfectamente documentada.

3.1.8 Retiro de ahorro en cuenta de cliente fallecido

El empleado de la agencia que tenga acceso a consultas generales de clientes, revisa diariamente los periódicos y establecer si personas fallecidas tienen cuenta en el banco, para luego realizar retiros sin libreta falsificando la firma del cuentahabiente. El proceso por parte de los familiares (si tiene, y si se encuentran enterados de la existencia de la cuenta) puede tardar algunas semanas, lo cual beneficiaría la sustracción de los fondos.

El control por parte de la auditoría es, realizar la misma tarea pero con el propósito de no permitir operaciones sobre la cuenta hasta que se presente alguien legalmente facultado para disponer de los fondos en ella depositados.

3.1.9 Retiros y depósitos en el mismo día y a la misma cuenta

Un cajero puede retirar a primera hora cierta cantidad de dinero de su caja para trabajarlo fuera de la agencia y obtener beneficios personales, al final del día registra el depósito con el dinero nuevamente en su poder y cuadra su caja no levantando ninguna sospecha. En este caso podemos pensar en arqueos sorpresas que pasarían a segundo plano de existir complicidad entre quien sustrajo el dinero y la persona encargada de realizarlos.

3.1.10 Depósitos menores repetitivos en cuentas de empleados

Puede darse el caso que el jefe de una agencia, cobre cantidades o tasas de interés, más altas de las autorizadas por servicios prestados, excedentes que deposita en su cuenta. Por ejemplo, en el caso de un sobregiro, cobra una cantidad más alta y prolonga la fecha de pago del sobregiro para que este no coincida con el depósito a su cuenta personal. Obviamente en este caso, si el pago por el servicio se realiza en efectivo, quedará únicamente por perseguir el cobro en exceso realizado al cliente, de lo contrario, quedará como otra operación de la agencia.

La auditoría puede revisar los cobros por servicios, pero estos no son generalmente cobrados, ya que por ejemplo en los cheques de caja, existen clientes que por su reciprocidad con la institución no se les cobra, razón por la cual, es complejo establecer omisiones o excesos en los cobros.

3.1.11 Pagos de cheques con firma falsificada y por montos elevados

La mayor parte de bancos, establecen límites para el pago de cheques, fuera de los cuales, existe una llamada telefónica al cliente con el propósito de confirmar su emisión. Actualmente, existen personas dentro de las entidades que alteran los datos y utilizan cheques falsos para que en el momento de realizar la llamada se marque un número en el que un tercero autoriza la transacción. Posterior al registro de la operación, se concreta el reclamo del cliente quien asegura no haber recibido la llamada de confirmación y el empleado bancario haberla realizado. Estos casos escapan de controles de auditoría.

3.1.12 Pagos de cheques con formas falsificadas

Existe la posibilidad que dentro del banco, exista una persona que teniendo acceso a firmas registradas para girar cheques de cuentas, robe talonarios de cheques a clientes y falsifique firmas registradas. Posteriormente, presenta cheques por denominaciones bajas para no despertar sospechas y los cobra en distintas agencias pero en un mismo día, con el propósito que ante el reclamo del cliente el dinero se encuentre totalmente en poder de los estafadores.

Es importante señalar que los pagos se realizan en efectivo y regularmente la identidad de los beneficiarios no es real. Las revisiones de la auditoria en pagos de cheques, se limitan a verificar características del cheque y firmas, por lo que la operación puede pasar inadvertida hasta un inminente reclamo.

3.1.13 Compra venta de divisas con tasas no autorizadas

Puede darse el caso que exista compra o venta de divisas con tasas o tipos de cambio por debajo de las autorizadas, ocasionando pérdidas para la institución; ya sea por errores o irregularidades por parte de las personas que prestan el servicio a los clientes, estableciendo tales deficiencias probablemente hasta cierres mensuales o revisiones periódicas de la auditoría.

3.1.14 Transacciones con tarjetas falsificadas de crédito y débito

Es secreto a todas voces que actualmente existen establecimientos y agrupaciones criminales que copian la banda magnética de las tarjetas de crédito o débito al realizar pagos o retiros de efectivo en establecimientos o cajeros automáticos respectivamente, las cuales, serán detectadas hasta que el cliente reciba su estado de cuenta al mes siguiente y solicite información sobre un sin número de compras o retiros realizados.

No es procedimiento de auditoría realizar revisiones sobre retiros o consumos con estas tarjetas.

3.1.15 Consultas de saldos a cuentas corrientes

Se ha descrito en numerales anteriores, la posibilidad que un empleado bancario tenga acceso a información de clientes que su clave de acceso al sistema no le permite consultar. Dependiendo de qué tan atractiva pueda resultar esta información, el empleado hará lo posible para que salga esta información de la institución y la cuenta sea sujeto de fraude. Es sabido que existen claves o niveles para el acceso a la información, pero también es cierto que dichas claves resultan no cumpliendo su cometido pues son de conocimiento generalizado dentro del personal de la agencia para "efectos prácticos" –agilizar el servicio al cliente, o realizar las tareas más rápido-.

En este caso, la auditoría no realiza revisiones sobre el historial de las consultas realizadas –bitácoras- y los motivos que las generaron.

3.1.16 Robo a través de autorización de un sobregiro a una cuenta

Puede darse el robo de una clave para la autorización de sobregiros en cuentas con saldos bajos o sin saldo, operaciones realizadas normalmente de una computadora distinta a la de la persona responsable, que regularmente es un funcionario de la entidad. Queda en este caso únicamente como prueba de auditoría, el historial de la bitácora del usuario que la autorizó, de todas formas no se descubrirá al responsable debido a que la clave es la autorizada.

3.1.17 Autorización de sobregiros a cuentas de empleados

Existen funcionarios con autorización para realizar esta operación, toma un curso diferente en el momento que se autoriza a sí mismo un sobregiro que pasa a ser un préstamo temporal, obviamente, a una tasa más baja de la autorizada, para no levantar sospechas y no llegar a extremos de no colocar tasas. Antes de llegar el vencimiento el responsable cubrirá el monto del sobregiro. Es importante por parte de la auditoría la revisión de sobregiros otorgados en las agencias, pero si se trata de una entidad grande, regularmente las visitas son anuales, lo cual permite sobregiros por periodos pequeños y burlar las revisiones o evaluaciones.

3.1.18 Liberación manual de reservas locales múltiples en el mismo día y en la misma cuenta

Un empleado, ex empleado o cliente, se presenta en varias agencias de un banco, aprovechando que tiene amistad con supervisores o jefes de agencia solicita la liberación de cheques ajenos depositados. Regularmente los montos son bajos para no levantar sospechas, pero en conjunto pueden llegar a ser significativos. Esta operación puede descubrirse hasta que se presenten los cheques a compensación, momentos en el que ya se ha retirado el dinero de la institución y estos resulten rechazados por falta de fondos.

3.1.19 Estafa a través de liberación manual de reservas del exterior por montos altos

Se trata de una modalidad de la anterior, pero se evidencia con el propósito de beneficiar al cliente o al mismo banco liberando –dar como disponibles fondos- montos de cheques del exterior. Dependiendo de las cantidades, se pueden correr riesgos muy altos que pueden perjudicar la estabilidad de la institución, si no se cuentan con controles sobre transacciones que usualmente escapan de una revisión periódica de la auditoría interna.

3.1.20 Ingreso de una contraseña que pertenece a un funcionario que ha reportado al sistema que se encuentra fuera del Banco

Definitivamente que para una auditoría tradicional, son aspectos que no se encuentran dentro de su alcance. Debido a que puede darse el caso, que un empleado aparte de conocer la clave para utilizarla cuando el responsable no se encuentre en su lugar de trabajo, puede manipularla simultáneamente y tener acceso a cambios en cualquier tipo de información en beneficio propio, lo cual, quedará registrado como culpable directo el responsable de la clave utilizada.

3.1.21 Pagos de nómina a empleados fantasma

Pueden existir pagos a empleados no existentes o aún no dados de baja en la planilla, con el propósito de realizar erogaciones perfectamente registradas contablemente y trasladarlas posteriormente a la cuenta del encargado de realizar

dichos desembolsos. Con un número considerable de empleados en una institución bancaria, la revisión quincenal de la correcta acreditación de empleados activos podría parecer impráctica si se contara con controles sobre los mismos.

3.1.22 Pagos de nómina duplicados

Puede verse como una variante de la anterior, pero en este caso se utilizan distintas formas de pago, aparte de la nota de crédito que comúnmente se emite catorcenal o mensualmente, surge un cheque por el mismo concepto, el cual, no podrá identificarse dentro del estado de cuenta del empleado con el mismo concepto.

3.2 Áreas cubiertas de riesgo de fraude

En la mayor parte de las transacciones citadas anteriormente, las pruebas realizadas por el auditor no tienen contemplado el control de riesgo de fraude, y las acciones son posteriores a la ocurrencia de la operación, si es que se tienen contempladas. Existen por ejemplo los sobregiros, que son sujeto de evaluaciones periódicas en agencias de una entidad bancaria, pero se hacen por lo menos una vez al año. Por lo que existe una brecha libre para realizar transacciones sin ser detectadas.

3.3 Áreas no cubiertas de riesgo de fraude

Las cuentas de depósitos de empleados por ejemplo, son sujeto difícilmente de evaluación por parte de la auditoría interna, en este sentido, es importante aclarar que nos referimos a su movimiento, ya que se pueden hacer revisiones sobre acreditaciones a una muestra seleccionada. No se presta también seguimiento a las transacciones realizadas por un usuario dentro de determinado período, pero se debe considerar lo indicado en el numeral 3.1.20, ya que puede existir robo de la misma.

Por otra parte, difícilmente se destinen evaluaciones para validar que efectivamente las formas emitidas por la institución se encuentren en circulación, con el propósito de detectar falsificaciones. Nos podemos enfocar principalmente en las libretas de depósito o cheques.

3.4 Controles existentes

Actualmente en las áreas descritas anteriormente, pueden existir controles que tengan como fin primordial salvaguardar a la institución. Por ejemplo: Se puede tener instituido que las operaciones en cuentas de ahorro se realicen estrictamente con la presentación de la libreta física y exista un listado de los números correlativos en circulación, revisiones mensuales de pagos de sueldos y/o cuentas de empleados, generar bitácoras de usuarios del sistema para analizar las operaciones realizadas, emitir reportes mensuales de sobregiros y verificar su

adecuada aplicación y autorización, emitir reportes de reversiones diarias de depósitos investigando cada uno de los motivos que las generaron así como la cuenta de destino final, etc. En términos generales se puede concluir que el resultado de dichos controles es posterior a la ocurrencia del hecho. Lo importante y novedoso para la auditoría, es realmente aplicar una evaluación o control preventivo y/o detectivo, entiéndase este en el tiempo que realmente sucede u ocurre.

Las operaciones en las cuales haya documentos falsificados, resultan prácticamente imposibles de controlar, si no existe una adecuada infraestructura tecnológica para ello, hablamos de libretas de depósito, cheques, tarjetas de débito y crédito. Sin lugar a duda un aspecto subjetivo que afectará todo tipo de transacciones será la intervención humana, ante la cual, es un tanto complejo actuar. Situaciones que simplemente serán contingencias para la institución y ante las cuales, tendrá que responder al cliente derivado de sus reclamos.

CAPÍTULO IV

Riesgo de Fraude Operativo Bancario en el Área de Caja y su Tratamiento a través de la Auditoría Informática

Todo lo detallado en el capítulo precedente, destaca la importancia para que se de seguimiento al riesgo de fraude operacional. Es importante señalar que la principal meta no es eliminar los riesgos de fraude operativo, sino ser proactivo en la identificación de este tipo de riesgo para obtener beneficios tangibles.

El avance de la tecnología y el consecuente abatimiento de los costos de los equipos de proceso electrónico de datos (PED), ha originado que cada vez sea mayor el número de bancos que utilizan estos equipos como una herramienta para el proceso de información. Por otro lado, los bancos que utilizan PED, debido a las ventajas que ofrece como son principalmente: velocidad, exactitud, oportunidad y manejo eficiente de grandes volúmenes de datos, tienden a incorporar al mayor número de sistemas al PED en las áreas susceptibles de automatizarse, tal como las hechas en el área de caja. Esto origina que la información producida por los centros de PED sea un elemento de suma importancia para la toma de decisiones en los bancos y para el control adecuado de muchas de sus operaciones.

Normalmente, los recursos económicos destinados a la actividad de PED representan cantidades importantes, lo cual hace indispensable que el rendimiento obtenido sobre dicha inversión deba ser satisfactorio, o sea, que el

aprovechamiento de la capacidad instalada en PED (personal y equipos) debe ser el máximo posible.

En consecuencia, las evaluaciones que la auditoría realice sobre áreas que utilicen PED deben ser acorde a las mismas, es decir, la auditoría debe destinar tanto personal capacitado en PED como utilizar equipo y programas informáticos que ayuden a dichos exámenes.

4.1 Aspectos a considerar en la utilización de aplicaciones o programas informáticos para el Monitoreo de Riesgos de Fraude en el área de Caja de una entidad Bancaria.

Considerando que la banca es dinámica y de rápida evolución, los bancos deben monitorear y evaluar continuamente sus sistemas de control interno, a la luz de las cambiantes condiciones internas y externas y deben mejorar esos sistemas según sea necesario para mantener su efectividad. En organizaciones multinacionales muy complejas, la administración superior debe asegurarse que la función de monitoreo se defina y estructure con propiedad dentro de la organización. El monitoreo de la efectividad de los controles internos puede ser hecha por personal de diferentes áreas, incluyendo la función de negocios por sí misma, el control superior el control financiero y la auditoría interna. Por esa razón, es importante que la administración superior aclare qué personal es responsable para cada función de monitoreo. El monitoreo debe ser parte de las

actividades diarias del banco pero también debe incluir evaluaciones periódicas separadas del proceso general del control interno. La frecuencia del monitoreo de diferentes actividades del banco debe ser determinada por la consideración de los riesgos involucrados y la frecuencia y naturaleza de los cambios que estén ocurriendo en el ambiente operativo. Las actividades de monitoreo permanentemente pueden ofrecer la ventaja de rápida detección y corrección de deficiencias en el sistema de control interno. Tal monitoreo es más efectivo cuando el sistema de control interno está integrado con el ambiente operativo y produce reportes regulares para revisión.

En contraste, las evaluaciones separadas, típicamente detectan problemas sólo después del hecho; sin embargo, dichas revisiones le permiten a la organización tomar una visión comprensiva y fresca de la efectividad del sistema de control interno y específicamente de la efectividad de las actividades del monitoreo. Las evaluaciones separadas del sistema de control interno, a menudo toman la forma de auto evaluaciones cuando las personas responsables de una función particular determinan la efectividad de los controles para sus actividades. La documentación y los resultados de la evaluaciones son entonces revisadas por la administración superior. Todos los niveles de revisión deben estar adecuadamente documentados y reportados sobre una base oportuna al nivel apropiado de administración.

La función de la auditoría interna es una parte importante del monitoreo permanente del sistema de controles internos, considerando que proporciona una

valuación independiente de la adecuación y cumplimiento de las políticas y procedimientos establecidos. Es importante que la función de auditoría interna sea independiente de las funciones del día a día del banco –operaciones descritas en el capítulo tres- y que tenga acceso a todas las actividades conducidas por la organización bancaria, incluyendo a sus sucursales y subsidiarias.

Al reportar directamente al comité de auditoría y a la administración superior, los auditores internos proporcionan información imparcial acerca de la línea de actividades. Debido a la importante naturaleza de su función, la auditoría interna debe estar conformada por individuos competentes y bien entrenados que tengan un claro entendimiento de su papel y responsabilidades. La frecuencia y alcance de las revisiones y pruebas de los controles internos por parte de la auditoría interna deben ser consistentes con la naturaleza, complejidad y riesgos de las actividades de la organización.

“Es importante que la auditoría interna reporte directamente a los más altos niveles de la organización bancaria, típicamente al Consejo de Administración o a su comité de auditoría superior. Esto permite el adecuado funcionamiento del gobierno corporativo a través de dar información al Consejo de Administración que no esté parcializada de ninguna manera por los niveles de administración que cubran los reportes. La junta también debe reforzar la independencia de los auditores internos a través de tener tales aspectos, así como sus recursos de

compensación y de presupuesto, determinados por el Consejo de Administración o por los más altos niveles de administración, en lugar de tenerlos determinados por parte de administradores que sean afectados por el trabajo de los auditores internos" (2:18).

Es importante señalar que paralelo a la parte administrativa, al implementar el seguimiento continuo o monitoreo al área de caja de una entidad bancaria, es conveniente considerar aspectos humanos, económicos y del hardware y software –equipo y programas- necesarios para obtener los resultados previstos.

En el caso del recurso humano, puede crearse dentro de la estructura organizacional de una entidad bancaria, una unidad destinada exclusivamente para salvaguardar a la institución ante los fraudes ya mencionados en el capítulo precedente, la cual, será responsable de ciertos riesgos y/o fraudes identificados en el área, para lo cual por ser tareas en algunos casos eminentemente operativas y hasta cierto punto mecánicas, no exigirán un nivel muy alto desde el punto de vista académico de las personas que realicen esta tarea. En tanto que las que requieran niveles de análisis profundos sean elevadas a la auditoría interna de la institución, en este sentido se da la posibilidad que exista por una parte un filtro para que la auditoría interna no descuide las tareas de una auditoría financiera e intervenga a través de auditorías operacionales en casos que por su magnitud e importancia lo requieran.

En segundo lugar, el hardware –elemento físico, computadoras, impresoras, etc.- y software –programas-, que aunque se considere que el gasto termina con la adquisición del programa o programas, no se debe obviar que dependiendo de los controles que se deseen establecer será el tamaño de éstos y las exigencias que demanden del hardware, por ejemplo: por la cantidad de información que éste maneje, se requiera un servidor independiente para no sobrecargar los ya existentes que manejan el corazón de la información para las áreas administrativas y red de agencias, por otra parte, las computadoras personales de los individuos que utilicen el programa o programas sean capaces de soportarlos, por ejemplo, limitaciones de memoria RAM –memoria de lectura o parte del computador que dependiendo de su tamaño puede procesar volúmenes significativos de información- y ambientes de sistemas operativos como Windows o Macintosh.

Por último y no menos importante es el factor económico, del cual, debe existir un exhaustivo análisis previo a la adquisición de los programas, que derivan en la obtención de herramientas adicionales que tal vez no se tienen previstas fuera de los ejemplos anteriormente citados, lo cual, varía de acuerdo a los alcances de los programas, por ejemplo, adquisición de cámaras, etc.

4.2 Principales aplicaciones para el Monitoreo de Riesgos de Fraude

4.2.1 Monitor e Inspector

Son softwares que utilizan información contenida en bases de datos con el propósito principalmente de monitorear o dar seguimiento a transacciones, las cuales, dependiendo de ciertas condicionantes (parametrizaciones), previamente establecidas por el usuario, envía alertas o mensajes cuando estas se cumplen, son también conocidos como programas de alerta temprana. Por ejemplo, si en una cuenta de empleado se registra un depósito adicional al de su sueldo, el programa se encuentra en la capacidad de identificar la transacción en tiempo real y hacerla del conocimiento de la Auditoría Interna.

Lo atractivo de estos programas, es justamente que a diferencia de cualquier modo tradicional de auditoría, se cuenta con la evidencia en el momento que esta ocurre y no luego de varios días dependiendo de las revisiones periódicas, si es que estas áreas se encuentran dentro de los programas anuales de revisión de la auditoría interna.

4.2.1.1 Forma de uso de la aplicación

Se puede enfocar desde dos puntos de vista, una persona que diseña las condicionantes (parametrizaciones) y la segunda que las utiliza e investiga.

En el primero de los casos, dependiendo de las transacciones que se deseen monitorear, el usuario cuenta con operadores lógicos (<, >, =, if, and, etc.) por medio de los cuales requiere al programa que informe en el momento que estas se cumplen. Por estas características, se pudiera pensar que es una actividad exclusiva para la auditoría de sistemas o el departamento de informática de la entidad, pero con la instrucción adecuada se pueden elaborar dichas condicionantes sin problema por el personal de auditoría. La complejidad y profundidad de las condicionantes dependerán de la creatividad de la persona que las elabore y de las facilidades para extraer la información de las bases de datos a utilizar.

4.2.1.2 Reportes

Cada una de estas herramientas, proporciona reportes diarios, semanales y mensuales de la actividad de las transacciones sujetas de monitoreo, las cuales, muestran irregularidades en su desarrollo o por lo menos a criterio de quienes formulan los parámetros en el software, estos reportes muestran el número de transacciones, el tipo de transacciones, el usuario que las efectuó, el monto por el que las realizó, la fecha y hora en que ocurrieron. Además, mantienen la historia de comentarios introducidos al programa durante el proceso de estudio y análisis de los resultados de los reportes, para que una persona de más alto nivel jerárquico decida si luego de las investigaciones realizadas es conveniente

profundizar más o brinda su visto bueno con el trabajo hasta ese momento realizado.

Estos reportes muestran los resultados en pantalla o impresora. Cuando hablamos de resultados en pantalla nos referimos a que se encuentra en capacidad de utilizar programas de correo electrónico como Microsoft Outlook o Microsoft Exchange, por ejemplo: en el momento que un evento parametrizado a través de los operadores lógicos descritos anteriormente se suscite, inmediatamente envía un mensaje de texto con el detalle de la transacción. Estos mensajes pueden ser clasificados para que sean dirigidos por tipo de transacción a una persona en especial de tal manera de no duplicar el estudio que se realice sobre ellas.

A pesar que actualmente el método de envío de avisos más utilizado es el correo electrónico, estos programas se encuentran en la capacidad de enviar mensajes a localizadores (beepers), fax o llamadas telefónicas, respetando en este último, el envío a distintas personas en la secuencia que se le indique. De tal manera, el programa se encontrará en la capacitad de informar o alertar al usuario cuando los eventos deseados se cumplan como se detalla a continuación:

4.2.1.2.1 Reversión de depósitos en efectivo en cuentas

El programa puede informar cuando: un cajero realice ilimitado número de reversiones, reversiones mayores a N cantidad, reversión y posterior operación

a cuenta que no es la originalmente operada, monto de la reversión no es igual al operado al inicio.

4.2.1.2.2 Reversión de depósitos en efectivo y su posterior operación en cuenta de empleado

El programa informa cuando la cuenta a la cual es operada la transacción, pertenece a un empleado.

4.2.1.2.3 Notas de crédito o depósitos a cuentas de empleados

Se obtienen mensajes de alerta, cuando la cuenta de un empleado ha recibido más de N notas de crédito o mayores a X monto.

4.2.1.2.4 Notas de crédito o depósitos duplicados

Si un depósito o nota de crédito se ha registrado más de una vez con el mismo número de documento, mismo número de cuenta, mismo monto y mismo cajero.

4.2.1.2.5 Retiros de ahorro sin libreta

Se realicen un N número de retiros sin libreta en el día o mes, número N de retiros que al final del día acumularon X cantidad, retiros a cuentas inactivas o embargadas, se realicen retiros a cuentas previamente consultadas.

4.2.1.2.6 Robo de libreta de ahorros de clientes

Cuando se realicen retiros de ahorro en distintas agencias a una misma cuenta en tiempo relativamente corto.

4.2.1.2.7 Retiros de ahorro a cuentas con poco movimiento

En el momento que existan retiros a cuentas sin movimiento o con estatus de inactivas, se realicen consultas de firmas en cuentas sin movimiento.

4.2.1.2.8 Retiro de ahorro en cuenta de cliente fallecido

Informa cuando se efectúen varios retiros a una misma cuenta por un mismo usuario y en un mismo día, o cuando se realicen retiros por más del 90% del saldo de la cuenta.

4.2.1.2.9 Retiros y depósitos en el mismo día y a la misma cuenta

Informa en el momento que se realice un retiro y posterior depósito ambos sin libreta a una misma cuenta.

4.2.1.2.10 Depósitos menores repetitivos en cuentas de empleados

Se realicen N número de depósitos a una cuenta que en conjunto suman X cantidad.

4.2.1.2.11 Pagos de cheques con firma falsificada y por montos elevados

Alerta en el momento de pagar un cheque por X cantidad, se haya consultado el saldo de la cuenta y posteriormente se pague el cheque.

4.2.1.2.12 Pagos de cheques con formas falsificadas

Se opere un cheque con numeración diferente al correlativo de cheques en circulación.

4.2.1.2.13 Compra-venta de divisas con tasas no autorizadas

Cuando se realicen transacciones de compra-venta de divisas con tasas no vigentes o sin el ingreso del código de aprobación de un funcionario que la autorice.

4.2.1.2.14 Transacciones con tarjetas falsificadas de crédito y débito

Transacciones en un período corto en distintos países, pagos en un mismo país pero en distinta localidad en períodos cortos, se realizan transacciones en establecimientos clasificados como alto riesgo. Catalogados de esta manera, debido a que no brindan medidas de seguridad en el momento de realizar pagos a través de tarjetas de crédito y débito, ya que copian las bandas magnéticas que contienen la información del cliente.

4.2.1.2.15 Consultas de saldos a cuentas corrientes

Se obtienen mensajes cuando un mismo usuario ha consultado una misma cuenta por N veces, consultas a saldos a cuentas con X monto o arriba de monto establecido, consultas cuentas en horario inhábil, consulta a una misma cuenta por distintos usuarios y la cuenta posee X monto, consultas a clientes VIP –clientes muy importantes, por sus siglas en inglés-, funcionarios, políticos, etc.

4.2.1.2.16 Robo a través de autorización de un sobregiro a una cuenta

Se encuentra en capacidad de informar cuando a una cuenta con tiempo relativamente corto de apertura se le ha autorizado un sobregiro, autorización de sobregiros con cuentas con saldos promedio bajos, autorizaciones de sobregiros mayores a X monto, cuando el sobregiro sea autorizado con la clave de un funcionario que se encuentra de vacaciones.

4.2.1.2.17 Autorización de sobregiros a cuentas de empleados

Identifica cuando ha sido autorizado un sobregiro a una cuenta de empleado.

4.2.1.2.18 Liberación manual de reservas locales múltiples en el mismo día y en la misma cuenta

Informa cuando existe más de una liberación manual de fondos en compensación a la misma cuenta en un mismo día.

4.2.1.2.19 Estafa a través de liberación manual de reservas del exterior por montos altos

Se autorice la liberación manual de fondos en compensación, por montos que sobrepasen X cantidad, y sean reservas locales o en moneda extranjera.

4.2.1.2.20 Ingreso de una contraseña que pertenece a un funcionario que ha reportado al sistema que se encuentra fuera del Banco

Cuando se introduzca la clave de un funcionario que se encuentra de vacaciones o se encuentre en el sistema dos veces un mismo usuario en distinta terminal de trabajo.

4.2.1.2.21 Pagos de nómina a empleados fantasmas

Se detecta cuando una cuenta de ahorros o cheques ha recibido más de N notas de crédito en el transcurso de un mes, o una cuenta que no es de empleado, recibe acreditación por pago de nómina.

4.2.1.2.22 Pagos de nómina duplicados

En el momento que una cuenta de ahorros o cheques de un empleado recibe más de cierto número de notas de crédito en pocos días, cuando una cuenta recibe pagos por dos vías ya sea a través de nota de crédito y a través de cheque propio o también, se establece que la cuenta no es de empleado y recibe acreditación de planilla.

4.2.1.3 Valor agregado de las herramientas de programas de monitoreo de riesgos

Reduce el esfuerzo y tiempo de la revisión, tal y como se citó en el capítulo anterior, este tipo de transacciones no son parte de una revisión constante por parte de la auditoría interna, por lo que en el momento de realizar estas evaluaciones se parte con la desventaja que la mayoría de los casos que entran dentro de la muestra seleccionada ya ocurrieron y es demasiado tarde para aplicar medidas que tiendan a su prevención sino sólo a su corrección. En este sentido estos programas abarcan el universo de los eventos identificándolos automáticamente y alertando a los responsables en tiempo real, por otra parte, brinda el beneficio de poder contar con los papeles de trabajo necesarios para documentar el trabajo realizado, por lo que después de varios días o meses luego de suscitadas las transacciones, se torna un tanto complejo reconstruir los hechos, lo que deviene en mayor tiempo y con resultados no tan precisos como sería estudiarlos en el mismo día que estos suceden.

Derivado de lo anterior, podemos deducir que otro aspecto con el cual contribuye la herramienta es la reducción de volúmenes de trabajo, ya que luego de varios días o meses de realizadas algunas transacciones se pueden aplicar pruebas que no sean las más acertadas ya que se parte de estándares para las muestras seleccionadas a diferencia de tomar caso por caso y evaluar en el momento qué medidas son las más acertadas y oportunas, por ejemplo, se puede partir con realizar entrevistas a empleados sobre el origen de un depósito especial, a diferencia que a través de la herramienta se tiene identificado que proviene de la reversión sobre una cuenta de un cliente.

En consecuencia, todo redunda en una mejora en el nivel de control, que a la larga es lo que se persigue, la actividad del análisis y la investigación son tareas diarias y no esporádicas o periódicas, por otra parte, no se trabaja sobre muestras seleccionadas o al azar sino sobre el universo de los eventos, ya que se cuenta con detalle de operaciones realizadas por funcionarios y empleados ante un posible fraude interno, además de supervisar el área de caja.

4.2.2 ACL, Excel o Works

4.2.2.1 Forma de uso de la aplicación

Antes de realizar un detalle de la forma de uso de estos programas, es necesario hacer una diferenciación con los descritos en el numeral 4.2.1.

Independientemente de los beneficios que éstas puedan brindar (como manejar grandes volúmenes de información y la facilidad de clasificarla acorde a nuestras necesidades), la ventaja de tener conocimiento de transacciones de fraude en tiempo real no es su principal bondad, ya que estos programas o aplicaciones, procesan información que ha sido registrada o sustraída a través de reportes del sistema para posteriormente clasificarla, siempre con la ayuda de operadores lógicos, además, sus procesos de análisis de la información no llegan a ser tan profundos como los mencionados en el numeral anterior, por ejemplo: En el caso de consultas y posteriores débitos a cuentas con saldos altos, para depositarlas en cuentas propias, estos programas nos llevan a manejar dos tipos de bases de datos, la primera de usuarios, filtrando las bitácoras y la segunda, de los maestros de cuentas de depósitos observando la cuenta afectada con el débito y confirmando la del empleado con el crédito respectivo. En tanto que con programas de alertas tempranas la información es procesada en fracción de segundos brindando todos los detalles de la operación.

Otro ejemplo serían las tarjetas de crédito, en el momento de realizar consumos en el extranjero o a nivel local, ya que se tendrían que generar reportes con cierta frecuencia y verificar los lugares en donde se realizaron los consumos, prestando especial atención a la hora y localidad e incluso y muy importante, observando el

negocio en donde se efectuó la operación, con el propósito de establecer que no se encuentre en lista de negocios fraudulentos.

El uso de estos programas como ya se puede inferir, consiste en manejar bases de datos, por lo regular bajo los formatos de texto (.txt) y manejarlas en los programas, de tal manera que el usuario decide qué tipo de información va a procesar. Sin lugar a dudas el programa ACL (Audit Command Language) es más avanzado que las hojas de cálculo citadas ya que brinda más estadísticas del trabajo realizado y ofrece facilidades como la selección de muestras de datos para las auditorías a realizar, ya que fue creado bajo este fin, ser una herramienta para el Contador Público y Auditor.

4.2.2.2 Reportes

Los reportes que emanan de estas herramientas siempre serán visualizados a nivel de archivos o impresiones, siempre con las depuraciones de información que el usuario haya seleccionado.

4.2.2.3 Valor agregado de la herramienta

El principal valor de estas herramientas radica en que se muestran como una alternativa ante la incapacidad de realizar grandes inversiones de dinero en programas más complejos de alertas tempranas, aunque es innegable que los resultados no serían los mismos, hablando en términos de tiempo y oportunidad.

CAPÍTULO V

Caso Práctico Relativo a la Participación del Contador Público y Auditor Interno en la evaluación de Controles Internos para evitar fraudes en el Área de Caja por medios informáticos

Luego de establecer un panorama acerca de la vulnerabilidad de las transacciones realizadas en el área de caja hacia el fraude y de las herramientas informáticas disponibles para mitigar los niveles de riesgo, expondré la participación que el Contador Público y Auditor tiene sobre la evaluación del riesgo de fraude operativo bancario en el área de caja.

Para el tema desarrollado, se hace la aclaración que de los medios existentes para la evaluación del control interno (explicación narrativa, cuestionarios y diagramas de flujo), nos inclinaremos por el cuestionario, pues se desea saber con detalle los controles sobre las operaciones de caja, las cuales, poseen características muy particulares.

5.1 Programa de Auditoría

El auditor interno revisa el sistema de control interno con el propósito de determinar su grado de fiabilidad como parte de un objetivo global, a no ser por estas revisiones siempre y cuando no revelen lo contrario la autenticidad de los registros es razonable, para el caso específico de fraudes se encuentra dentro de sus responsabilidades realizar exámenes para detectar errores e irregularidades que pudieran llegar a tener un efecto significativo sobre los estados financieros.

A continuación se presenta un programa de auditoría y cuestionario de control interno, con procedimientos que debe llevar a cabo el Contador Público y Auditor para evitar fraudes en el área de caja.

BANCO DE LA ASUNCIÓN, S.A.
AUDITORIA INTERNA
PROGRAMA DE AUDITORIA
AREA DE CAJA

Preparado Por:	**Omar Lucero**	**Fecha:**	**15-8-04**
Revisado Por:	**Juan Luis Mejía**	**Fecha:**	**20-08-04**

	PROCEDIMIENTO	Hecho Por:	Papel de Trabajo
I.	**PRESUNCIÓN DE RIESGOS** ➢ Ausencia de controles en operaciones en efectivo. ➢ Inadecuado seguimiento a reversión de operaciones, ya sean totales o parciales. ➢ Falta de revisión sobre cuentas inactivas o con poco movimiento que presentan movimientos significativos. ➢ Carencia de controles sobre los movimientos de cuentas de empleados. ➢ Ausencia de controles sobre la autenticidad de formas utilizadas para transacciones. ➢ Falta de controles sobre operaciones realizadas con tarjetas de crédito o débito.		

II.	**ALCANCE** Se evaluarán las operaciones de caja y derivado de sus niveles de riesgo se formularán condicionantes con la ayuda de operadores lógicos a través del programa Monitor.		
III.	**OBJETIVOS DEL TRABAJO Y PROCEDIMIENTOS A EJECUTAR** **OBJETIVOS** 1. Verificar que el sistema proporcione controles para operaciones en efectivo. 2. Elaborar controles en operaciones de cuentas de depósitos a través de un programa temprana, especialmente sobre las reversiones de depósitos en efectivo, tomando en consideración que estos pueden ser totales o parciales. 3. Identificar y crear controles sobre las cuentas que posean cierto tiempo de inactividad así como poco movimiento, para lo cual se debe verificar que existan bitácoras de la actividad o inactividad de cada cuenta. 4. Instituir controles sobre la liberación manual de reservas del país y extranjeras, valiéndose del sistema para regular quién, cuándo y cómo se realizó. 5. Establecer una base de datos con todas las cuentas de empleados de la institución y brindar seguimiento a las operaciones en ellas registradas. 6. Elaborar controles sobre las formas en blanco utilizadas por el banco y posteriormente entregadas a los clientes de manera que estas no sean susceptibles de copia o duplicación, el cual, tenga como centro de altas y bajas una base de datos del sistema. 7. Establecer controles para el correcto cobro de comisiones por servicios a clientes, los cuales, se encontrarán establecidos en el sistema.		

8. Crear controles sobre medidas de seguridad a nivle sitema para evitar clonación o duplicidad en tarjetas de crédito o débito.

9. Identificar los mecanismos de monitoreo con la ayuda de herramientas informáticas que permitan ampliar el alcance y oportunidad de los controles.

IV. PROCEDIMIENTOS

a) A través de mesas de trabajo, identificar las transacciones susceptibles de fraude.

b) Por medio de la técnica del cuestionario establecer el grado de control sobre del área de caja y con base a su resultado incorporar los controles correspondientes.

c) Participar en la formulación de las condicionantes que se desean implementar.

d) Traslado de las condicionantes al programa Monitor de alerta temprana.

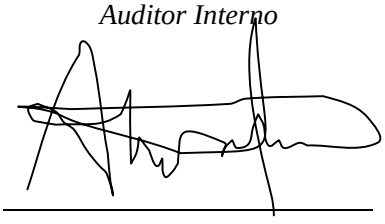
V. PRESUPUESTO DE TIEMPO Y PERSONAL ASIGNADO

Se estima utilizar un presupuesto de 28 horas de trabajo, distribuidas de la siguiente forma:

Personal	**Horas**
Auditor Interno	5
Auditor III	23
TOTAL	**28**

APROBACIÓN

Auditor Interno



Fecha: *21-08-04*

5.2 Cuestionario

BANCO DE LA ASUNCIÓN, S.A.
AUDITORIA INTERNA
CUESTIONARIO DE CONTROL INTERNO
AREA DE CAJA

Preparado Por:	**Omar Lucero**	**Fecha:**	**15-8-04**
Revisado Por:	**Juan Luis Mejía**	**Fecha:**	**20-08-04**

	SI	NO
1. Cuestiones Generales		
a. ¿Posee el banco un plan general para detectar casos de fraude?		
b. Si la respuesta es afirmativa, ¿cuáles son los medios utilizados para detección y control?		
c. ¿Existe un área dedicada al seguimiento y control de fraudes?		
d. Si la respuesta es afirmativa ¿a quién reporta?		
2. Operaciones de Caja		
a. ¿Se le brinda seguimiento a las operaciones realizadas diariamente y que son reversadas de manera total o parcial?		
b. Si la respuesta es afirmativa ¿se investiga la razón que motivó la reversión?		

c. ¿Existe inventario detallado sobre cheques y libretas de ahorro que se entregan a los clientes? d. ¿Poseen alguna medida de seguridad para evitar la falsificación de los mismos? e. ¿Para los cheques pagados mayores a Q.50,000.00 existe algún tipo de medida de seguridad antes de ser desembolsados? f. ¿Existe algún control sobre la liberación de reservas por parte de el personal de agencias ya sean del país o extranjeras? **3. Cuentas de Empleados** a. ¿Tiene identificada la institución las cuentas de cada uno de los empleados que en ella laboran? b. ¿Se le da algún tipo de seguimiento a los movimientos registrados en las cuentas de empleados con el propósito de indagar acerca de posibles movimientos significativos? c. ¿Se realizan pruebas periódicas sobre la correcta acreditación de sueldos hacia los empleados? d. ¿Existen políticas con relación a la autorización de sobregiros a empleados?		

4. Cuentas del público a. ¿Existe algún tipo de seguimiento a cuentas que no han presentado movimiento durante algún período y repentinamente realizan operaciones significativas con relación a sus saldos? b. ¿Cómo actúa la institución para resguardar fondos de personas fallecidas en tanto los fondos sean reclamados y no sean objeto de fraude? **5. Seguridad en los sistemas** a. ¿Se tienen asignadas claves de uso personal para cada uno de los usuarios del sistema? b. ¿El sistema posee la capacidad de guardar bitácoras de las operaciones realizadas? c. ¿Existen políticas para el correcto uso de claves dentro del personal de las agencias con el propósito de evitar su préstamo? d. ¿Existen restricciones a nivel sistema sobre consultas a saldos de clientes y la información personal de los mismos?, e. ¿Se exige se documente el motivo de las consultas? f. ¿Existe un responsable directo de los cambios que se realizan en el sistema?		

6. Tarjetas de débito o crédito a. ¿Cómo se le brinda seguridad al cliente sobre una posible clonación o duplicación de su tarjeta? b. ¿Existen controles sobre retitos de efectivo significativos o consumos en establecimientos o países identificados como peligrosos con relación a clonación de tarjetas? **7. Venta de productos o servicios** a. ¿Existen controles sobre la adecuada aplicación de tasas en compra venta de divisas? b. En la venta de servicios, como cheques de caja, ordenes de pago local, etc. ¿existen controles para las comisiones cobradas no sobrepasen las autorizadas? Nombre del funcionario encuestado:_____ Cargo: _____ Tel: _____ Fecha: _____.		

5.3 Cédulas de trabajo

Producto de las mesas de trabajo realizadas entre la auditoría y el área de informática, con el propósito de identificar transacciones susceptibles de fraude y elaborar los controles internos que contribuyan a que estas sean mitigadas a través del sistema de monitoreo. Es importante que el Contador Público y Auditor, documente por medio de papeles de trabajo la estructura de las condicionantes realizadas, como se muestra a continuación:

5.3.1 Reversión de depósitos en efectivo

Partiendo del supuesto que la reversión de transacciones registradas por parte de receptores pagadores, deben tener su origen en un 90% por errores en su registro u operación y el resto por solicitud del cliente, es importante brindar seguimiento a: la frecuencia de las reversiones, los montos usualmente sujeto de reversión y diferencias entre el monto depositado antes y después de la reversión.

Para este caso, se parte que la base de datos posee la ventaja de identificar las operaciones reversadas como NULL –anulada-, con lo cual, se establecerán dos controles. El primero, basado en reportes diarios de los motivos que generaron las reversiones, cuya cantidad se encontrará ya identificada por parte de la Auditoría Interna, debido a colocar un contador con un campo creado denominado rev_dep que brindará el número de estas operaciones dentro de una agencia por cada usuario.

CEDULA_____C-1_____

BANCO DE LA ASUNCIÓN, S.A. **FECHA: __22-08-04_____**
AUDITORIA INTERNA **HECHO POR:____OL_____**

TRANSACCIÓN

Número de reversiones de depósitos en efectivo en un mismo día.

OBJETIVO

Documentar los motivos de reversiones de operaciones en cuentas de depósitos.

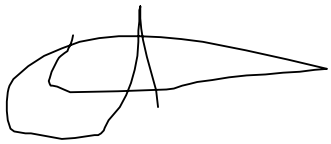
ANÁLISIS PREVIO

Tomando en consideración, que las transacciones cuyo registro no se ha concretado dentro del sistema quedan identificadas como NULL. Se procedió a establecer un contador al final del día que permita conocer el número de reversiones por agencia y usuario, las cuales, deben de estar lo suficientemente justificadas.

ESTRUCTURA DE LA ALERTA

La alerta enviará el resumen diario por agencia y usuario, conteniendo el total de transacciones, siempre y cuando se cumpla la condición que esta existe.

If rev_dep > 0



Hecho por: _____ Vo.Bo.:_____

Auditor III Auditor Interno

Estas reversiones pueden ser registradas posteriormente por cantidades menores a la reversada, sobre todo si los depósitos se realizan por montos altos. Por ejemplo, una cuenta recibe un depósito por Q.9,825.00, el receptor pagador reversa la operación y registra dos depósitos uno por Q.9,395.00 y otro por Q.430.00 a una cuenta diferente. Al final del día, en el cuadre de la jornada, la operación pasará inadvertida ya que el cuadre de depósitos a cuenta coincidirá en

monto. Obviamente el receptor pagador ya ha elaborado una boleta por cada depósito.

En este caso se establecerá un control que identifique este tipo de operaciones, para lo cual, se tomará el campo valor_credito que identifica la existencia de valores depositados, como se detalla a continuación:

CEDULA___C-2_____

BANCO DE LA ASUNCIÓN, S.A. **FECHA: __22-08-04_____**
AUDITORIA INTERNA **HECHO POR:____OL_____**

TRANSACCIÓN

Reversiones de operaciones con depósitos parciales en efectivo en un mismo día y a diferentes cuentas.

OBJETIVO

Establecer el destino de los depósitos parciales posteriores a la reversión de un depósito.

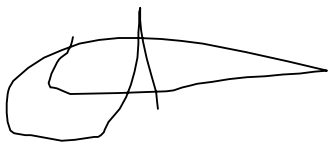
ANÁLISIS PREVIO

Partiendo que el sistema identifica las reversiones como NULL. Se establecerá un control sobre la cuenta reversada, y la operación posterior se determinará con revisiones sobre el movimiento de receptor pagador, no importando si la transacción fue secuencial a o al final del día. Este análisis se realizará fuera del programa de alerta temprana ya que el depósito puede tener como destino distintas cuentas, pero se tiene identificada la sustracción de fondos.

ESTRUCTURA DE LA ALERTA

La alerta identificará la reversión y posteriormente enviará el mensaje si la cuenta, recibió un depósito.

If rev_dep > 0 then display numero_de_cuenta and if valor_credito > 0



Hecho por: _____ Vo.Bo.:_____

Auditor III Auditor Interno

Por último, la reversión puede ser registrada a una cuenta de empleado o cuentas relacionadas a un empleado; para este control, previamente se debe contar con la

siguiente información: una base de datos conteniendo cuentas de empleados y relacionadas. El valor agregado en este caso, radica en que se establecerá de forma inmediata dicha relación sin esperar la consulta de listados de cuentas de empleados. Básicamente el aporte se puede medir en tiempo.

CEDULA____C-3_____

BANCO DE LA ASUNCIÓN, S.A. **FECHA: __22-08-04_____**
AUDITORIA INTERNA **HECHO POR:____OL_____**

TRANSACCIÓN

Reversiones de operaciones con depósito a cuenta de empleado.

OBJETIVO

Establecer si el destino de los depósitos es una cuenta de empleado.

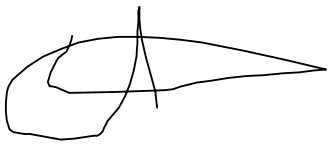
ANÁLISIS PREVIO

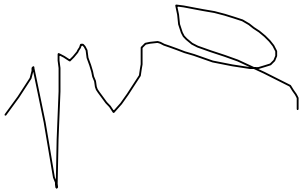
Sobre la base de la alerta de reversiones de operaciones con depósitos parciales en efectivo, en un mismo día y a diferentes cuentas, se adicionará una validación sobre la base de datos de cuentas de empleados, con el propósito de identificarlas y tomar las medidas correspondientes. Las cuentas de empleados dentro de la base de datos se identifican con el número 10.

ESTRUCTURA DE LA ALERTA

La alerta identificará la cuenta, que recibió el depósito.

If rev_dep > 0 then display numero_de_cuenta and if numero_de_cuenta = 10





Hecho por: _____ Vo.Bo.:_____

Auditor III Auditor Interno

5.3.2 Retiros de ahorro en cuenta sin movimiento

La base de datos que contiene las cuentas de depósitos, se encuentra en la capacidad de identificar las cuentas que por ejemplo tengan más de seis meses de inactividad. Lo cual, facilita su control a través de técnicas de auditoría asistidas por computador y una posible sustracción de fondos, procedimiento que con una revisión tradicional de auditoría sería compleja, debido a que el auditor tendría que solicitar reportes diarios de las cuentas con esta condición, con el propósito de establecer los motivos por los cuales algunas han salido de estos listados.

CEDULA____D-1_____

BANCO DE LA ASUNCIÓN, S.A. **FECHA: __22-08-04_____**
AUDITORIA INTERNA **HECHO POR:____OL_____**

TRANSACCIÓN

Retiro de ahorro en cuenta sin movimiento.

OBJETIVO

Identificar la sustracción de dinero en estas con un tiempo previamente establecido sin movimiento.

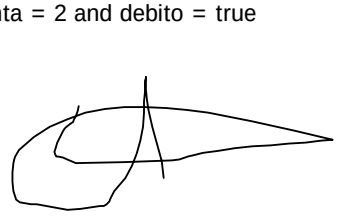
ANÁLISIS PREVIO

Se tomará el registro que cada cuenta posee en el momento de cumplir con la condición de inactiva y la alerta informará cuando se opere una transacción en ella. Una cuenta con movimiento posee estatus 1 y una inactiva 2, lo cual, se encuentra en el campo estatus_cuenta.

ESTRUCTURA DE LA ALERTA

Registro de transacciones en cuentas inactivas

If estatus_de_cuenta = 2 and debito = true



Hecho por: _____ Vo.Bo.:_____

Auditor III Auditor Interno

5.4 Estructura Organizacional

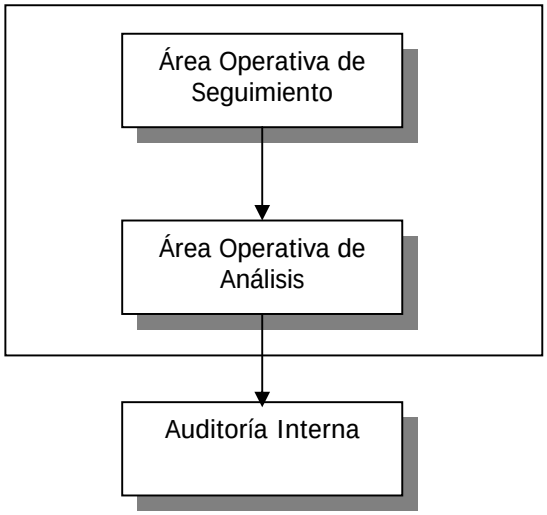
Pareciera que el presente tema en su orden de ideas, debe ser considerado primero para el control que se realice sobre el área de caja de una institución bancaria. Pero se desarrolla como tercero, con el propósito que se determinara o evidenciara inicialmente que, basándonos en algunos casos de los veintidós expuestos en los capítulos tres y cuatro, el límite de control tiene como base las posibles variantes de los fraudes u operaciones identificadas, desarrollados por la persona o personas encargadas de la elaboración o programación de las condicionantes.

Es importante señalar, que se debe poseer un área muy bien estructurada dentro de la entidad bancaria para los controles que se desean sobre el área de caja, y no se transforme en lo contrario. Por ejemplo, derivado del número de transacciones que una entidad posea puede llegar a manejar un número de transacciones significativa que puedan dar indicios de fraude, a las cuales, debe dar seguimiento. Por otra parte, tomando en cuenta lo citado al inicio del capítulo cuatro, el tema es dinámico por lo que se tiene que estar debidamente organizado para que prevalezca dicho control constantemente.

A continuación, se sugiere una estructura para la adecuada implementación y seguimiento de los casos de fraude identificados y las distintas maneras que tengan en el futuro.

CUADRO 1

Estructura Administrativa para la Detección e Investigación de los Casos de Fraude en el Área de Caja en una Entidad Bancaria



5.4.1 Área Operativa de Seguimiento

Será la encargada de recibir el cien por ciento de las alertas o mensajes debidamente parametrizados a través de los programas de alerta temprana, por ejemplo, puede recibir mensajes de fraude como retiros de cuentas de clientes fallecidos y posteriormente acreditados a cuentas de empleados.

El alcance de esta área servirá como el primer depurador de la información, ya que dependiendo de los datos que inicialmente se logren obtener, se decidirá si amerita elevarlo a otra instancia dentro de la estructura propuesta.

Partiendo del supuesto que efectivamente se produzcan operaciones no usuales y que pudieran generar fraude, el programa identifica que una cuenta de ahorro es sujeto de retiros y depósitos en un mismo día. La persona encargada de atender este tipo de alertas, dentro de las responsabilidades de su puesto de trabajo debe:

1°. Solicitar por escrito referencias a la agencia, esto con el propósito de tener evidencia.

2°. Si la instancia no es satisfactoria, se documenta el caso y se eleva a Área Operativa de Análisis.

Se puede pensar que con el hecho de solicitar referencias a la agencia, prácticamente se pone en sobre aviso a quienes se encuentran involucrados en el fraude, pero es justamente el propósito, que todos los empleados que laboran en el área de caja se encuentren enterados que las operaciones o transacciones de una agencia no sólo se encuentran bajo inspección de jefes de agencia, supervisores, revisiones periódicas de la Auditoría Interna; sino que, el círculo para cometer actos de fraude en beneficio propio prácticamente es nulo o cada vez más limitado.

Si dentro de la investigación se establece, en primer lugar que el cliente se identificó como un cambista el cual trabaja con una casa de cambio plenamente

reconocida y coincido con la información declarada en el momento de aperturar su cuenta, se procede siempre a dejar documentado el caso (entiéndase como se explicó en el capítulo IV dentro del mismo programa) y el proceso termina en ese momento. Como se puede apreciar, esta área se puede conformar con personas que no posean un alto nivel académico. Para poder realizar este tipo de procedimientos el banco deberá mantener información actualizada de sus cuentahabientes.

5.4.2 Área Operativa de Análisis

Sobre la base de la información ya recopilada, esta área examinará el caso, por ejemplo, hará revisiones de las bitácoras –historial de consultas- de los usuarios de la agencia, con el propósito de establecer si existen consultas a las cuentas del cliente y si dichos usuarios son los mismos que operan las transacciones; por otra parte, la periodicidad en que las operaciones se realizan.

Luego de los análisis practicados, se establece que se realizan autopréstamos con el propósito de trabajar el dinero y quedarse con los beneficios, actividad que con el propósito de no levantar sospechas en los saldos de las cuentas, se depositan en un mismo día, aprovechando que estos son altos y en un día no afectará si se le despoja de cierta cantidad. La cuenta obviamente, ya se encuentra plenamente estudiada. Para el personal que se encuentra en esta área, se requiere un nivel académico superior, ya que deben entender el funcionamiento de la entidad

bancaria para agotar varias alternativas o instancias para analizarlo, antes de hacerlo del conocimiento de la Auditoría Interna si procediera.

5.4.3 Auditoría Interna

Luego del análisis previo trasladado, la Auditoría Interna ya interviene con una revisión, con el propósito de recabar la evidencia documental necesaria para realizar las sugerencias del caso a la Gerencia correspondiente y comprobar la eficiencia de los controles establecidos, por ejemplo: se tendrán los retiros sin libreta con falsificación de firma y los respectivos depósitos con evidencias como: misma caligrafía en su redacción. Posteriormente se elaborarán informes a la Gerencia correspondiente acerca de la eficiencia en la supervisión del trabajo realizado por jefes y supervisores designados en agencias, a través de lo cual, se evidencian fortalezas y debilidades en su ejecución.

Es importante señalar que la Auditoría Interna haya o no transacciones que requieran su intervención, brindará seguimiento al desenvolvimiento de esta unidad de análisis con revisiones periódicas que evalúen los niveles de eficiencia, ya que es ajeno al establecimiento de controles en los cuales participa.

Para finalizar, se puede observar que con la estructura sugerida la auditoría interna entra en acción en casos concretos, de lo contrario, ocuparía su tiempo en aquellos que tal vez a pesar de ser identificados dentro de los mensajes parametrizados, no

son calificados como de fraude, sin descuidar que las áreas precedentes que le proveen de la información, deben de ser un área independiente siempre sujeta a evaluación, como se mencionó anteriormente.

CONCLUSIONES

1. El riesgo de fraude deriva principalmente de los siguientes motivos:
   - Cultura Corporativa: Falta de conocimiento con relación al fraude, desprecio del control, permisividad ante el fraude.
   - Carencia de Controles: Falta de segregación de funciones, programas operativos mal diseñados, organismos de control inexistentes o ineficientes, carencia de políticas y normas.
   - Gestión Recursos Humanos: Falta de objetividad en ascensos, falta de expectativas profesionales, sistemas de remuneración inadecuadas, mal clima laboral, selección de personal inadecuado.

2. La importancia en la adaptación de programas para el fortalecimiento del control interno en una entidad bancaria, redunda principalmente en: a) oportunidad, debido a que se tiene conocimiento del hecho en el momento que efectivamente se suscitaron las transacciones. b) alcance, ya que los procedimientos de análisis y verificación se centrarán en casos concretos y no sobre muestras que pueden contener información que no sea sujeto de fraude. c) seguimiento de los controles, en vista que los controles por si mismos no garantizan el éxito del establecimiento del control y permiten determinar posibles variantes a los fraudes identificados.

3. Las aplicaciones de auditoría, utilizadas para la detección de fraude operativo bancario son: a) los programas de alerta temprana, que son softwares que utilizan información contenida en bases de datos con el propósito principalmente de monitorear o dar seguimiento a transacciones, las cuales, dependiendo de ciertas condicionantes (parametrizaciones), previamente establecidas por el usuario, envían alertas o mensajes cuando éstas se cumplen, son también conocidos como programas de alerta temprana y b) los programas que manipulan bases de datos, son programas o aplicaciones que procesan información que ha sido sustraída a través de reportes del sistema para posteriormente clasificarla, siempre con la ayuda de operadores lógicos con el propósito de establecer muestras para realizar evaluaciones sobre dicha información.

4. Los aspectos a considerar en la adaptación de programas para el fortalecimiento de controles internos se resumen en:

- Determinación de qué área se encargará del monitoreo de riesgos, función orientadas específicamente a la auditoría interna, que es una parte importante del monitoreo permanente del sistema de controles internos.
- La frecuencia del monitoreo, va de la mano con el alcance de las revisiones y pruebas de los controles internos por parte de la auditoría interna, y deben de ser consistentes con la naturaleza, complejidad y riesgos de las actividades de la organización.

- Aspectos humanos, económicos y técnicos del hardware y software.

5. Los pasos para las evaluaciones de riesgos son: a) identificación del riesgo, distinguiendo los relevantes que un banco puede enfrentar, analizando su misión de negocios, actividades básicas y los principales procesos, b) medición del riesgo, que permite a la gerencia priorizar, controlar y vigilar el riesgo. Los riesgos deben ser medidos de manera consistente, sin importar en qué parte del banco ocurran, c) seguimiento del riesgo, involucra la instrumentación de controles y sistemas adecuados que permite a la gerencia monitorear de manera efectiva y continua los niveles de riesgo en cada área de negocios u operaciones, d) control del riesgo, el cual incluye el establecimiento de procedimientos para mitigar los riesgos. Determina qué controles son necesarios; por otra parte, los gerentes deben ponderar el costo de mejores controles contra los beneficios de éstos.

RECOMENDACIONES

1. Las Instituciones Bancarias cuyos controles internos relacionados al fraude no existan, se sugiere desarrollar una cultura de control dentro de la organización, así como, incorporar controles a las operaciones que en el área de caja se realicen, ya que pueden ser medios de fraude; además, fomentar la importancia de la supervisión en el desarrollo de las operaciones realizadas.

2. La Auditoría Interna de un banco que realiza revisiones periódicas en el área de caja para prevenir fraudes, se recomienda determinar el alcance y oportunidad de las pruebas de cumplimiento al realizar una auditoría informática.

3. La Auditoría Interna de una institución bancaria, en el momento de evaluar el control interno del área de caja a través de la auditoría informática, debe identificar y dar seguimiento oportuno a los posibles casos de fraude, para lo cual, es recomendable establecer una unidad que rastree diariamente dentro de las transacciones de la entidad cuáles son susceptibles de fraude para su debido análisis.

4. La Auditoría Interna que evalúe controles internos en el área de caja a través de herramientas informáticas, debe tener presente que el uso de

programas informáticos implica conocimientos técnicos de este campo, para lo cual, es conveniente considerar la ayuda de un especialista en la materia.

BIBLIOGRAFÍA

1. Bancafe, Manual Oficial de Cumplimiento, 2001
2. Comité de Basilea sobre Supervisión Bancaria, Administración de Riesgo Operacional, 2001
3. Comité de Basilea sobre Supervisión Bancaria, Marco de Referencia para los Sistemas de Control Interno en las Organizaciones Bancarias, Septiembre 1998.
4. Comité de Basilea sobre Supervisión Bancaria, Mejorando el Gobierno Corporativo para Organizaciones Bancarias, 1999
5. Comité de Basilea sobre Supervisión Bancaria, Principios Básicos para una Supervisión Bancaria Efectiva, Septiembre 1997
6. Congreso de la República de Guatemala, Decreto 17-73 Código Penal
7. Congreso de la República de Guatemala, Decreto 19-2002 Ley de Bancos y Grupos Financieros
8. Coopers & Lybrand, Los Nuevos Conceptos del Control Interno – Informe COSO-1997
9. Fondo Monetario Internacional, El Proceso de Administración de Riesgos: La Perspectiva de la Supervisión
10. GBM Guatemala, Auditoría en Informática, 1997
11. GBM Guatemala, Efectos del Procesamiento Electrónico de Datos (PED) en el Examen del Control Interno, 1997
12. IFAC, Codificación de Normas Internacionales de Auditoría (NIAS) y Declaraciones Internacionales de Auditoría

13. Instituto Guatemalteco de Contadores Públicos y Auditores, Introducción a los Principios de Basilea 2000
14. Monitor Byte, El Riesgo Operativo en el Siglo XXI, 2001
15. Océano/Centrum, Enciclopedia de la Auditoría, 1999
16. Principios de Riesgo Generalmente Aceptados (GARP)
17. Segundo Congreso Latinoamericano de Super Estrategias de Auditoría, Desarrollo Profesional Avanzado 1998
18. www.bis.org Comité de Basilea
19. www.lavadodinero.com Sitio de Prevención Lavado de Dinero
20. www.monografias.com Sitio de Consultas Temas Generales
21. www.montt.ucentral.cl Standares de Auditoría de Sistemas y Catas
22. www.respondanet.com Medición de Corrupción