

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONOMICAS

**“EL CONTROL INTERNO EN EL MANEJO DE LAS OPERACIONES
DE LAS CUENTAS DE DEPÓSITO REALIZADAS A TRAVÉS DE
REDES ELECTRONICAS”**

TESIS

PRESENTADA A LA JUNTA DIRECTIVA DE LA
FACULTAD DE CIENCIAS ECONOMICAS

POR

ERICK ALFONSO DAVILA ALVAREZ

PREVIO A CONFERIRSELE EL TITULO DE

CONTADOR PUBLICO Y AUDITOR

EN EL GRADO ACADEMICO DE

LICENCIADO

GUATEMALA, NOVIEMBRE DE 1998

**MIEMBROS DE LA JUNTA DIRECTIVA DE LA
FACULTAD DE CIENCIAS ECONOMICAS
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**

Decano:	Lic. Miguel Angel Lira Trujillo
Secretario:	Lic. Eduardo Antonio Velásquez Carrera
Vocal I:	Lic. Jorge Eduardo Soto
Vocal II:	Lic. Andrés Guillermo Castillo Nowell
Vocal III:	Lic. Víctor Hugo Recinos Salas
Vocal IV:	P.C. Julissa Marisol Pinelo Machorro
Vocal V:	P.C. Miguel Angel Tzoc Morales

EXONERADO DEL EXAMEN DE AREAS PRACTICAS

Conforme al artículo 15 del Reglamento para Evaluación Final de Exámenes de Areas Prácticas y Examen Privado de Tesis y al numeral 5.1 del Punto Quinto, del Acta No. 6-96, de la sesión celebrada por la Junta Directiva de la Facultad de Ciencias Económicas, el 14 de marzo de 1996.

**JURADO QUE PRACTICO
EL EXAMEN PRIVADO DE TESIS**

Presidente:	Lic. Rubén Eduardo del Aguila Rafael
Examinador:	Lic. David Porfirio Díaz López
Examinador:	Lic. Salvador Giovanni Garrido Valdez



Guatemala, 11 de mayo de 1998

Licenciado
Donato Monzón Villatoro
Decano de la Facultad
de Ciencias Económicas
Universidad de San Carlos de Guatemala
Su Despacho

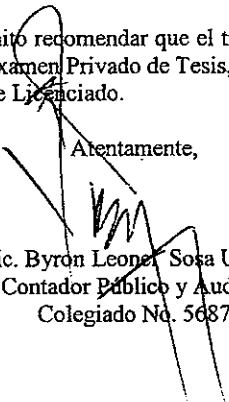
Señor Decano:

Atendiendo la designación que se me hiciera oportunamente, he procedido a asesorar al señor **ERICK ALFONSO DÁVILA ALVAREZ** en la preparación de su proyecto de tesis titulado **"EL CONTROL INTERNO EN EL MANEJO DE LAS OPERACIONES DE LAS CUENTAS DE DEPÓSITO REALIZADAS A TRAVÉS DE REDES ELECTRÓNICAS"**.

En opinión del suscrito, este trabajo constituye un importante aporte para la Contaduría Pública y Auditoría, así como para todo aquel estudiante o profesional interesado en el tema, ya que abarca lo concerniente a la identificación de los riesgos financieros a que están expuestos los recursos en una institución bancaria y que tienen relación con el establecimiento de un adecuado sistema de control interno en los sistemas de redes electrónicas.

Por lo anterior, me permito recomendar que el trabajo presentado por el sustentante se acepte para discusión en el Examen Privado de Tesis, previo a optar al título de Contador Público y Auditor en el grado de Licenciado.

Atentamente,



Lic. Byron Leonel Sosa Urbina
Contador Público y Auditor
Colegiado No. 5687



FACULTAD DE CIENCIAS
ECONOMICAS

DECANATO DE LA FACULTAD DE CIENCIAS ECONOMICAS. GUATEMALA,
DOCE DE NOVIEMBRE DE MIL NOVECIENTOS NOVENTA Y OCHO.

Con base en lo estipulado en el Artículo 23°. Del Reglamento de Evaluación Final de Exámenes de Areas Prácticas y Examen Privado de Tesis y el Acta AUD. 42-98, donde consta que el estudiante ERICK ALFONSO DAVILA ALVAREZ, ha aprobado su Examen Privado de Tesis, se le autoriza la impresión del Trabajo de Tesis, denominado: "EL CONTROL INTERNO EN EL MANEJO DE LAS OPERACIONES DE LAS CUENTAS DE DEPOSITO REALIZADAS A TRAVES DE REDES ELECTRONICAS".

Atentamente,

"ID Y ENSEÑAD A TODOS"

LIC. EDUARDO ANTONIO VELASQUEZ CARRERA
SECRETARIO



LIC. MIGUEL ANGEL LIRA TRUJILLO
DECANO



DEDICATORIA

A DIOS

Por haberme permitido alcanzar este objetivo

A MIS PADRES

Sara Leticia Alvarez de Navas, y
Armando Navas Hernández,
como recompensa a sus esfuerzos

A MI ESPOSA

Karina Benítez Villatoro de Dávila,
como agradecimiento y muestra de mi amor eterno

A MIS ABUELITOS

Alfonso Alvarez Rodríguez (Q.E.P.D.) y
Hortencia Cárdenas de Alvarez (Q.E.P.D.),
como símbolo de gratitud y amor

A TODA MI FAMILIA

Por haberme apoyado y alentado a seguir adelante

A MIS AMIGOS DE PROMOCION

Como símbolo de nuestros mutuos esfuerzos

A MI ASESOR DE TESIS

Lic. Byron Leonel Sosa Urbina,
por haberme guiado en esta ardua tarea

A LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Por haber dado luz a mis conocimientos

A LA SUPERINTENDENCIA DE BANCOS

Por brindarme la oportunidad de poner en práctica los conocimientos
adquiridos y aprender

INDICE

Página

INTRODUCCION

CAPITULO I EL CONTROL INTERNO

1.1	Definición	1
1.2	Clasificación de los controles internos	2
1.2.1	El control administrativo	2
1.2.2	El control contable	2
1.3	Características del control interno fiable	3
1.3.1	Plan de organización	4
1.3.2	La estructura contable	5
1.3.3	Auditoría Interna	6
1.3.4	Calidad del personal	7
1.3.5	Control interno en un sistema electrónico de datos	7
1.4	El control interno y la dirección	8
1.4.1	El papel de la dirección	8
1.4.2	El fraude administrativo	9

CAPITULO II OPERACIONES BANCARIAS EN CUENTAS DE DEPOSITO A LA VISTA GIRABLES CON CHEQUE

2.1	Generalidades sobre el sistema bancario guatemalteco	11
2.1.1	Definición	12
2.1.2	Clasificación	12
2.1.2.1	Bancos Comerciales	13
2.1.2.2	Bancos Hipotecarios	13
2.1.2.3	Bancos de Capitalización	14
2.1.2.4	Bancos Comerciales e Hipotecarios	14
2.1.3	Servicios que prestan las entidades bancarias	15
2.2	Cuentas de depósito a la vista girables con cheque	16
2.2.1	Definición	17
2.2.2	Importancia	17
2.2.3	Clasificación	17
2.2.4	Procedimientos de ejecución de depósitos a la vista	18

CAPITULO III REDES ELECTRONICAS

3.1	Definición	20
-----	------------	----

3.2	Utilidad y ventajas de las redes electrónicas	21
3.2.1	La importancia de la tecnología de la informática para los bancos	22
3.3	Clasificación de las redes electrónicas	25
3.3.1	Por su localización	25
3.3.2	Por su propietario	26
3.3.3	Por su topología	27
3.4	Partes de que constan las redes electrónicas	35
3.4.1	Equipo terminal de datos (ETD)	36
3.4.2	Equipo de terminación del circuito de datos (ETCD)	36
3.4.3	Equipos de conmutación de datos (ECD)	36
3.4.4	Protocolos	36
3.4.5	Repeaters	37
3.4.6	Bridges	37
3.4.7	Routers	37
3.4.8	Computadora	37
3.4.9	Tecnología	38

CAPITULO IV

EL CONTROL INTERNO EN OPERACIONES DE CUENTAS DE DEPOSITO A LA VISTA GIRABLES CON CHEQUE, REALIZADAS A TRAVES DE REDES ELECTRONICAS

		39
4.1	Terminología relacionada con el riesgo y el peligro	40
4.2	Identificación de riesgos genéricos, desde el punto de vista financiero	41
4.2.1	Delitos cometidos en contra del patrimonio de las instituciones bancarias y cuenta-habientes	42
4.2.2	Multas y sanciones	44
4.2.3	Errores, omisiones e irregularidades que ocasionan ineficiencia en el servicio bancario	46
4.2.4	Incendios, explosiones, pérdidas y extravíos	49
4.3	Administración de riesgos	49
4.3.1	Eliminar	50
4.3.2	Tolerar	50
4.3.3	Transferir	51
4.3.4	Tratar	52
4.4	Naturaleza del control interno bancario	52
4.4.1	Estudio y evaluación del control interno bancario	53
4.5	Elementos necesarios a considerar para el establecimiento de un sistema de control interno en un sistema de redes electrónicas	53
4.5.1	Cultura organizacional	54
4.5.2	Educación permanente	54
4.5.3	Políticas de seguridad	55
4.5.3.1	Política de seguridad del sitio	56
4.5.3.2	Cómo asegurar la responsabilidad de una política de seguridad	57
4.5.4	Normas y procedimientos que conforman el sistema de control interno para una red de transmisión electrónica de datos	57
4.5.4.1	Análisis de riesgos	60

4.5.4.2	Cómo identificar recursos	64
4.5.4.3	Cómo identificar las amenazas	64
4.5.4.4	Cómo identificar a quién se le debe permitir utilizar los recursos de la red	65
4.5.4.5	Plan de acción cuando la política de seguridad ha sido violada	67
4.5.4.6	Cómo responder a las violaciones de la política	68
4.5.4.7	Cómo vigilar el uso del sistema	70
4.5.4.8	Cómo utilizar la encriptación para proteger la red	70
4.6	Clasificación de controles internos	71
4.6.1	Según su cobertura	71
4.6.2	Según su naturaleza	72
4.6.3	Según su propósito	72
4.6.4	Según su estado	73
4.7	Tipos de control interno en el proceso de datos	74
4.7.1	Controles en los datos de entrada	75
4.7.2	Controles de transmisión	75
4.7.3	Controles de procesamiento	76
4.7.4	Controles de almacenamiento de datos	77
4.7.5	Controles de la información de salida	78

CAPITULO V

PARTICIPACION DE AUDITORIA INTERNA EN LA IMPLANTACION Y EVALUACION DEL CONTROL INTERNO DE LAS OPERACIONES DE DEPOSITO A LA VISTA, GIRABLES CON CHEQUE A TRAVES DE UNA RED ELECTRONICA

5.1	Actuación del auditor interno en la implantación de un sistema de redes electrónicas	80
5.1.1	Responsabilidad	81
5.1.2	Oportunidad	81
5.1.2.1	Inicio	82
5.1.2.2	Análisis	
5.1.2.3	Diseño del sistema	87
5.1.2.4	Desarrollo del sistema	87
5.1.2.5	Implantación del sistema	88
5.2	Preparación y capacitación del auditor interno en redes electrónicas	92
5.3	Técnicas y procedimientos de auditoría	92
5.3.1	Prueba del proceso y resultados de una operación en una cuenta de depósitos monetarios, a través de la red electrónica, con datos del auditor	93
5.3.2	Utilización de sistemas de software para realizar pruebas de auditoría en un sistema de redes electrónicas	94
5.3.3	Método de rastreo de una operación realizada en la red	95
5.3.4	Otras técnicas	96
5.4	Características de un sistema de redes electrónicas que influyen en una auditoría	96
5.5	El uso de especialistas en redes electrónicas	97
5.6	Ejemplos de papeles de trabajo	99



CONCLUSIONES	123
RECOMENDACIONES	125
BIBLIOGRAFIA	128

INTRODUCCION

A consecuencia de los acelerados cambios tecnológicos, dentro de los cuales se incluyen las comunicaciones a nivel mundial, del incremento de la competencia en la economía global y del cambio en las actitudes de los consumidores, quienes han pasado a ser más exigentes y menos fieles; las organizaciones tienen que enfrentar estándares de competitividad cada vez más altos. Para hacer frente a estos desafíos, las empresas tienen que examinar todos los aspectos de sus negocios y tecnificar la mayor cantidad posible de ellos, a fin de sobrevivir en el mercado.

El campo financiero no ha sido inmune a estos cambios, por el contrario, la globalización de los mercados financieros se está abriendo camino sofisticada y aceleradamente. Como resultado de las corrientes de liberalización de los mercados en todo el mundo, los bancos están en la búsqueda de lograr economías de escala favorables, tratan de aumentar su cobertura geográfica, tanto a nivel local como internacional y ofrecer diversos productos y servicios que facilitan las actividades financieras de sus clientes.

Hoy en día, los bancos invierten sumas importantes en tecnología para el procesamiento electrónico de datos de sus operaciones, han reconocido que es un factor clave en el éxito de su negocio, debido a que los clientes desean productos actualizados, completos e integrados que se realicen con un gran nivel de servicio en un corto período de tiempo.

En el negocio bancario es necesario contar con información diaria de sus operaciones, principalmente en lo que se refiere a sus cuentas de depósitos girables con cheque, ya que de ello dependen los niveles diarios de liquidez de una institución bancaria, por consiguiente son indispensables sistemas de información confiables que garanticen la efectiva gestión y funcionamiento de la institución.

Ningún sistema, procesado por medios manuales, mecánicos o electromecánicos, brinda una protección o garantía absoluta contra los riesgos inherentes al mismo. Los sistemas de redes electrónicas no aumentan el nivel de los riesgos, pero los mismos constituyen una poderosa

herramienta que, por las funciones que concentran, los volúmenes de información y datos que se procesan, requieren mayores controles por parte del auditor.

Es por ello que el interés de la presente investigación gira en torno a *“El Control Interno en el Manejo de las Operaciones de las Cuentas de Depósito Realizadas a través de Redes Electrónicas”*. En el mismo se desarrollan tópicos relacionados con la identificación de los riesgos financieros resultantes de la ocurrencia o materialización de los peligros potenciales a que están expuestos los recursos en una institución bancaria y el establecimiento de elementos necesarios, para un adecuado sistema de control interno que permita prever controles en los sistemas de redes electrónicas.

La investigación se llevó a cabo con base en los siguientes objetivos generales:

1. Analizar la aplicación y funcionalidad de un sistema de redes electrónicas en relación con el ejercicio profesional del Contador Público y Auditor.
2. Profundizar en el estudio de un sistema de control interno fiable en las operaciones bancarias, realizadas a través de redes electrónicas.
3. Brindar a las instituciones bancarias elementos de apoyo que puedan utilizarse en la aplicación de controles internos, a través de redes electrónicas.

Para el efecto, es necesario dar a conocer en forma general los componentes de una red electrónica, establecer los riesgos desde el punto de vista financiero en las operaciones de las cuentas de depósito a la vista girables con cheque y que se realizan a través de redes electrónicas, con el fin de identificar los aspectos a considerar para el establecimiento de un sistema fiable de control interno, y por último, determinar los procedimientos estándares que podría utilizar el Auditor en la evaluación del control interno de dichas operaciones.

Para el logro de tales objetivos, la investigación se dividió en cinco capítulos. El primero de ellos analiza el control interno, su definición, clasificación y características principales.

El segundo capítulo establece generalidades sobre el sistema bancario guatemalteco y la definición, importancia y clasificación de las cuentas de depósito a la vista girables con cheque.

En el tercer capítulo se define una red electrónica, su clasificación, componentes, utilidad, ventajas y desventajas que representa el uso de la misma.

En el cuarto capítulo se estudia la terminología relacionada con el riesgo, se identifican riesgos genéricos desde el punto de vista financiero y se proporcionan algunos lineamientos generales sobre la administración de los riesgos. Asimismo, se da a conocer la naturaleza del control interno bancario, los elementos necesarios para el establecimiento de un sistema de control interno en redes electrónicas, la clasificación de controles internos y los tipos de control interno en las diferentes fases del procesamiento electrónico de datos.

El quinto capítulo, considerado como el más importante de esta tesis, versa sobre la participación de auditoría interna en la implantación y evaluación del control interno en las operaciones de depósitos a la vista, a través de redes electrónicas. En este capítulo se analiza la actuación, preparación y capacitación del auditor interno en la implantación de un sistema de redes, se detallan técnicas y procedimientos de auditoría, así como las características de la redes electrónicas que influyen en el examen de un sistema de redes. Como un apoyo en este tipo de auditorías se plantea la participación de especialistas y se presentan ejemplos de papeles de trabajo.

Las últimas secciones de la investigación corresponden a las conclusiones derivadas de los temas desarrollados, las recomendaciones planteadas y la bibliografía utilizada para el efecto.

Es importante mencionar que los sistemas desarrollados con controles bien concebidos e implementados adecuadamente, ofrecen un grado razonable de confianza a las instituciones bancarias; es decir, sólo mediante una constante modernización y sistematización de las operaciones que se realizan en una entidad bancaria, resguardadas por un adecuado control



interno, se podrán desarrollar nuevos servicios y enfocar múltiples retos del próximo siglo y en todo ello, el Contador Público y Auditor tiene un papel determinante.

Finalmente se desea mencionar, que otro objetivo que motivó este trabajo es que el mismo sea de utilidad a las instituciones bancarias, estudiantes, profesionales de la auditoría y para todo aquel investigador cuyo interés gire alrededor de actividades financieras.

CAPITULO I

EL CONTROL INTERNO

Muchas personas interpretan el término control interno como los pasos que da un negocio para evitar los fraudes del personal. En realidad tales medidas son más bien una pequeña parte del control interno. El propósito básico de éste es promover la operación eficiente de la organización.

En ese sentido, los administradores de las instituciones bancarias deben comprender que el control interno es más que salvaguardar los activos de las compañías. Para efecto que se comprenda la importancia del mismo, seguidamente se define lo que es el control interno y posteriormente se exponen algunos temas básicos para todo sistema de esta naturaleza.

.1 DEFINICION

“El control interno abarca el plan de organización, los métodos coordinados y medidas adoptadas dentro de la empresa para salvaguardar sus activos, verificar la adecuación y fiabilidad de la información de la contabilidad, promover la eficacia operacional y fomentar la adherencia a las políticas establecidas de dirección”¹

En otras palabras, el control interno está formado por todas las medidas que se toman para suministrar a la administración la seguridad razonable de que todo está funcionando conforme las políticas de la Dirección, por lo que incluye métodos por medio de los cuales se delega autoridad y se asigna responsabilidades para funciones tales como ventas, compras, contabilidad y otros. El control interno también incluye programas para preparar, verificar y distribuir a los diversos niveles de supervisión, informes y análisis comunes que capacitan al ejecutivo para la toma de decisiones y para mantener el control sobre la variedad de actividades y funciones dentro de la organización.

¹ James A. Cashin, Paul D. Neuwirth, John F. Levy, Enciclopedia de la Auditoría, Tomo I, pág. 278

1.2 CLASIFICACION DE LOS CONTROLES INTERNOS

El Comité de Principios Contables del Instituto Americano de Contadores Públicos Titulados (AICPA), mediante la declaración No. 1 sobre Normas de Auditoría, clasificó los controles internos en contables y administrativos, por lo que seguidamente se entra a considerar dicha clasificación:

1.2.1 EL CONTROL ADMINISTRATIVO

"Este incluye, aunque no queda limitado al ámbito del mismo, el plan de organización, los procedimientos y registros relacionados con los procesos de decisión y autorización de las transacciones por parte de la dirección. Toda autorización representa una función de dirección, asociada con la responsabilidad de alcanzar los objetivos de la organización, y constituye el punto de partida para el establecimiento del control contable de las transacciones"².

1.2.2 EL CONTROL CONTABLE

"Consiste en el plan de organización, procedimientos y registros referentes a la salvaguarda de los activos y confiabilidad en la información financiera"³. Este se ha diseñado para proporcionar una seguridad razonable de que:

- a. Las transacciones se efectúan de acuerdo con la autorización general o específica de la dirección.
- b. Las transacciones se registran de manera de que permitan la preparación de estados financieros de acuerdo con los principios de contabilidad generalmente aceptados y el control sobre los activos.
- c. El acceso a ciertos activos estará permitido únicamente con la autorización de la dirección.

² Normas Profesionales del Comité de Principios Contables, del Instituto Americano de Contadores Públicos Titulados, pág. 248.

³ IBID, pág. 248.

- d. El activo contabilizado se compara con el existente a intervalos de tiempo razonable y que se adopten las medidas correspondientes en el caso de que existan diferencias.

Las definiciones descritas no son mutuamente excluyentes; el propósito de las mismas es delimitar el alcance de cada tipo de control.

1.3 CARACTERÍSTICAS DEL CONTROL INTERNO FIABLE

Los sistemas de control interno varían significativamente de una organización a otra. Las características específicas del control en cualquier sistema dependen de factores tales como el tamaño, la estructura, la naturaleza de las operaciones y los objetivos de la organización para los cuales fue diseñado el sistema.

Sin embargo, ciertos factores son esenciales para que un control interno sea satisfactorio en casi cualquier organización en gran escala. En la publicación de la Declaración sobre Procedimientos de Auditoría -SAP- (Statement on Auditing Procedures)" No. 33, se enumeran cuatro características a considerar. Estas son:

1. "Un plan de organización que facilite la división adecuada de las responsabilidades y funciones.
2. Una eficiente estructura contable.
3. Una labor oportuna de Auditoría Interna.
4. La calidad y el entrenamiento del personal que integra y se relaciona con la organización".⁴

Jack C. Robertson en su obra Auditing, añadió una quinta característica, la cual contempla operaciones realizadas a través de redes electrónicas, y expone:

⁴ Instituto Americano de Contadores Públicos Titulados Op. Cit., 279

“Un sistema fiable de control interno funciona en realidad de forma eficaz, para detectar y corregir los errores en un sistema electrónico de datos”.⁵ Nótese la importancia relevante que le da al primero respecto al segundo.

1.3.1 PLAN DE ORGANIZACION

Un plan de organización se refiere a la división de autoridad, responsabilidad y obligaciones entre los miembros de una organización. El mismo deberá dar la seguridad de que las transacciones se llevan a cabo de conformidad con las políticas de la compañía, de que se acrecienta la eficiencia en las operaciones, se resguardan los activos y se promueve la confianza en los datos contables.

En gran parte, estos objetivos pueden lograrse por medio de la separación adecuada de las responsabilidades para: a) la iniciación o aprobación de las transacciones, b) la custodia de los activos y c) los registros contables que se llevan.

a. ***Control Interno sobre las Transacciones.***

Un principio fundamental de control contable es que ninguna persona o departamento deberá manejar todos los aspectos de una transacción de inicio a fin. Cada transacción se debe llevar a cabo mediante cuatro pasos: *deberá estar autorizada, aprobada, ejecutada y registrada*. El control contable se mejora si cada uno de estos pasos se llevara a cabo por empleados o departamentos relativamente independientes. De esa manera, ningún departamento estará en la posibilidad de completar una transacción que no haya sido revisada, aprobada y registrada por otras dependencias.

b. ***Responsabilidad de los Activos.***

Otro principio para lograr un adecuado control interno contable es la separación de la función de contabilidad de la custodia de los activos. Cuando los departamentos de contabilidad y de custodia son independientes, el trabajo de cada departamento sirve para

⁵ Robertson, Jack C., Auditing, pág. 191

comprobar la precisión del otro. Estas comparaciones deberán hacerse periódicamente, entre los registros contables y los activos físicos en existencia. La investigación de la causa de cualquier discrepancia descubrirá la ineficiencia, ya sea en el procedimiento para salvaguardar los activos, o en el mantenimiento de los asientos contables relacionados. Si no hubiera independencia entre lo contabilizado y la custodia de los activos, se podrían manipular los registros para ocultar el desperdicio, la pérdida o el robo de los mismos.

Registros Contables.

El departamento de contabilidad, es responsable de que todas las funciones de registro, diseño e implementación del control interno contable, sean adecuadas. Respecto a la actividad financiera, este departamento se encarga de que las transacciones se registren oportunamente, pero no maneja los activos financieros. Los registros contables establecen la responsabilidad sobre los activos, así como proporcionan la información necesaria de los movimientos financieros, declaraciones de impuesto y las decisiones operativas diarias.

.3.2 LA ESTRUCTURA CONTABLE

Al diseñar el sistema, es importante que los formatos y procedimientos establecidos permitan la revisión y autorización de todas las transacciones antes de que éstas queden registradas. Los formatos deben permitir el correcto registro de tales revisiones y autorizaciones iniciales, firma, nombre o código del encargado) para establecer la responsabilidad plena de las acciones realizadas por los individuos ejecutores. Estos deberán estar prenumerados y registrados para asegurarse de que quedan incluidas todas las transacciones ejecutadas por la empresa en el sistema de contabilidad.

El catálogo de cuentas y el manual de contabilidad constituyen también unos componentes esenciales del sistema. El primero constituye un marco básico del sistema de contabilidad y facilita la recopilación y clasificación de las diversas transacciones. El segundo, describe conceptos de autoridad, responsabilidad, obligaciones y muestra el método de trabajo para alcanzar los objetivos en forma eficaz y económica.



En resumen, un sistema contable deberá tener la capacidad de medir la actuación y eficiencia de las unidades individuales de las organizaciones, permitiendo obtener la siguiente información mínima:

1. Una documentación interna adecuada para enfocar la responsabilidad.
2. Un cuadro de cuentas, clasificado de acuerdo con las responsabilidades de los supervisores individuales y de los empleados clave.
3. Un manual de políticas y procedimientos contables y unos cuadros de flujo que describan los métodos establecidos para procesar las transacciones.
4. Un pronóstico financiero que consiste en un plan detallado de las operaciones, con estipulaciones para informes y análisis oportunos de las variaciones entre la situación real y los estándares presupuestales.
5. Un sistema de costos de fabricación, si es adecuado para el tipo de actividad que desarrolla la organización.

1.3.3 AUDITORIA INTERNA

Otro componente básico de un control interno eficaz es el personal de auditoría interna. El trabajo de los auditores internos consiste en evaluar el sistema de control interno y la eficiencia con la que las diversas unidades de la organización están realizando las funciones que se les han asignado. En una empresa pequeña, el gerente o propietario puede investigar personalmente cada fase de las operaciones y determinar si se están desarrollando conforme lo planificado. Sin embargo, en una organización grande, la alta gerencia establece un gran número de departamentos, divisiones u otras unidades de la organización, asignando un gerente a cada dependencia. Esta descentralización de autoridad, determina el escenario de los auditores internos. Su función es visitar, asesorar y valorizar los problemas y la actuación de cada departamento de la compañía. Como representantes de la alta gerencia, los auditores internos se interesarán por determinar si cada sucursal o departamento comprende claramente su trabajo, cuenta con el personal necesario, lleva adecuadamente los registros, protege el efectivo, los inventarios y otros activos, y en general si desempeña de manera efectiva la función que le señala el plan general de la organización del negocio.

1.3.4 CALIDAD DEL PERSONAL

Indudablemente, los requerimientos descritos con anterioridad no pueden cumplirse sin que los altos cargos y empleados clave de la empresa sean competentes para cumplir con sus obligaciones de manera eficaz y eficiente. Por lo tanto, la calidad debe incluir la ética, inteligencia, dedicación y responsabilidad de un individuo. El auditor cuenta con unos medios limitados para juzgar en un principio esta característica, pero con el tiempo, puede efectuarse una valoración razonable observando y examinando el trabajo realizado por el personal clave. Disponer de un grado de calidad en proporción a las responsabilidades, debería cotejarse periódicamente.

1.3.5 CONTROL INTERNO EN UN SISTEMA ELECTRONICO DE DATOS

Debido a la importancia de las implicaciones de los sistemas electrónicos de datos en los conceptos tradicionales de control, el AICPA emitió el SAS (Statement on Auditing Standards) No. 3, al cual denominó: "*Los Efectos del Procesamiento Electrónico de Información (PEI), en el Estudio del Auditor y la Evaluación del Control Interno*".

En ese texto se clasifican los controles internos en las dos siguientes categorías: *Controles Generales y Controles de Aplicación*. Los controles generales se relacionan con todas las aplicaciones del procesamiento electrónico de información e incluyen consideraciones tales como: a) organización del departamento de informática; b) los procedimientos para la documentación, prueba y aprobación del sistema original y cambios posteriores; c) controles interconstruidos en el equipo y d) seguridad para los archivos y equipo.

Los controles de aplicación, son aquellos que se relacionan con tareas específicas ejecutadas por el procesamiento electrónico de datos, tales como la preparación de las nóminas, facturación, contabilidad, otros. Los controles de esta naturaleza incluyen las medidas que tienen como finalidad asegurar la confiabilidad del insumo, mediante controles sobre el procesamiento y controles sobre el producto. Estos controles suelen estar implantados en el software de aplicaciones, el cual se refiere a

los programas que son escritos, para o por usuarios, con el objeto de realizar en la computadora una tarea específica.

Por aparte, también se definió que un sistema electrónico de datos puede interactuar de dos maneras en el control interno. La primera es servir de herramienta para llevar a cabo un adecuado control interno y la segunda es tener un control interno del área y/o departamento de informática. En el primer caso, la evaluación del control interno de una organización se lleva a cabo utilizando el equipo físico (hardware) y las instrucciones detalladas, previamente programadas (software), como herramientas que auxiliarán en el logro de los objetivos. En el segundo caso, se debe proteger adecuadamente los activos de la organización por medio del control, con el objeto de obtener la información en forma veraz, oportuna y confiable, para mejorar con ello la operación de la organización mediante la ejecución de las operaciones de informática y cumplir de esa manera con las políticas establecidas por la administración.

1.4 EL CONTROL INTERNO Y LA DIRECCION

Para comprender de una manera más amplia el papel que juega la Dirección en relación al control interno, y como ésta puede en un momento determinado pasar por encima de las normas establecidas en dicho sistema, se presenta a continuación los dos siguientes temas:

1.4.1 EL PAPEL DE LA DIRECCION

La dirección tiene la responsabilidad de tener un sistema coherente con las características mencionadas anteriormente, las cuales sirvan de base para proteger los activos de la empresa y que, entre otras cosas, permitan asegurar que los estados financieros sean razonables y correctos. Además, debe cerciorarse del cumplimiento de los procedimientos establecidos, de que se tienen en cuenta los cambios en la situación operacional y que se adoptan las medidas correctoras oportunas cuando existan anomalías en el sistema. Para el efecto puede delegar parte de esta función, al departamento de auditoría interna.

4.2 EL FRAUDE ADMINISTRATIVO

Al considerar la responsabilidad de los auditores en el descubrimiento de fraudes, ayuda a diferenciar el fraude ajeno a la administración, del fraude administrativo. El fraude ajeno a la administración consiste en acciones deshonestas que ocurren dentro de una compañía, a pesar de los esfuerzos de la gerencia para evitar tales actos. Como se expuso anteriormente, un sistema eficaz de control interno da protección contra los fraudes ajenos a la administración. La función del auditor para evitar el fraude ajeno a la administración consiste en estudiar y evaluar el sistema de control interno y hacer recomendaciones para el mejoramiento del mismo.

El fraude administrativo ocurre solamente cuando los altos ejecutivos de una compañía engañan deliberadamente a los accionistas, a los acreedores y a los auditores. Generalmente el propósito del fraude administrativo es el de publicar estados financieros engañosos que exageran las utilidades de la empresa y su fortaleza financiera, todo ello para recibir aumentos en salarios, bonificaciones, beneficiarse con opciones de acciones o precios más altos por su propiedad de valores de la compañía. También puede estar implicado el robo de activos.

Los casos de fraude de la administración han figurado en encabezados de periódicos durante meses en algunas ocasiones, y quizás han llevado a algunas personas a creer que el fraude interviene en cada fracaso espectacular de los negocios. Sin embargo, ello no siempre es así, ya que tales fracasos pueden tener como origen la depresión en las condiciones económicas, la inflación, la lucha laboral, los errores de juicio de la administración y muchas otras causas que no implican fraude.

El auditor puede reconocer que existe un ambiente que conduce al fraude, cuando el grupo de contabilidad carece de suficiente personal competente y se retrasa en su trabajo, cuando los controles internos son débiles, cuando ocurren transacciones importantes entre la compañía y sus funcionarios o cuando la junta directiva no es activa ni está interesada.

Al haber tenido a la vista los temas esenciales respecto al control interno (definición, clasificación, características y el papel de la dirección), se está en la posibilidad de entender la

|



importancia que tiene el mismo en la ejecución de todo tipo de transacciones que se realicen dentro de una organización y se tiene una base para comprender el control interno de las operaciones bancarias en cuentas de depósitos a la vista girables con cheque, lo cual se expone en los capítulos siguientes.

CAPITULO II

OPERACIONES BANCARIAS EN CUENTAS DE DEPOSITO A LA VISTA GIRABLES CON CHEQUE

En el capítulo anterior se expuso lo referente al control interno. Siguientemente se exponen los aspectos más importantes a considerar para comprender las operaciones que realizan las instituciones bancarias con respecto a las cuentas de depósito a la vista girables con cheque.

Como un preámbulo al desarrollo de este capítulo, es de mencionar que los bancos desempeñan un papel importante en la transferencia de medios de pago dentro de la economía de un país, pues una de sus funciones principales es la de servir de intermediarios entre personas que cuentan con capitales ociosos o improductivos, los cuales dejan en depósito, y personas que lo necesitan en el campo de la producción. Es en esa práctica de tomar y dar prestado, en ese flujo y reflujo de dinero, es donde los bancos impulsan grandemente el comercio, la industria, la agricultura y otras actividades del hombre.

2.1 GENERALIDADES SOBRE EL SISTEMA BANCARIO GUATEMALTECO

Los sistemas bancarios de los diversos países, han tendido a gravitar alrededor de los sistemas de banca central, cuyo modelo es el inglés, el cual tiene tres partes: El banco central, los bancos comerciales y varias instituciones auxiliares que se dedican a ciertos negocios relacionados con el crédito. Este es el modelo que se ha seguido en Guatemala.

La distinción entre bancos centrales y comerciales radica por esencia en sus objetivos. El banco comercial persigue obtener utilidades, en tanto que al banco central le interesan los efectos que produzcan las operaciones de los bancos comerciales en el sistema económico del país donde radica. Es de señalar que los bancos centrales son los únicos que pueden *emitir* dinero, pero los bancos comerciales son *creadores* de dinero, por la intermediación financiera que realizan. Los bancos comerciales pueden ser pocos o muchos; negocian con el público en general y tienen

accionistas, quienes pretenden obtener la máxima rentabilidad posible de los capitales que invirtieron. El banco central es uno en cada país, los negocios que hace con el público son con el propósito de corregir variaciones anormales en indicadores macroeconómicos (medios de pago, inflación, tipo de cambio y otros).

2.1.1 DEFINICION

Tradicionalmente se han concebido a los bancos, como aquellas instituciones cuya función primordial o fundamental era la de servir de intermediarios entre oferentes y demandantes de capital.

Actualmente esta definición se ha quedado corta, debido al desarrollo constante de la sociedad y las necesidades que nacen del mismo desarrollo. En ese sentido el sistema bancario ha tenido entre otros objetivos, el multiplicar la oferta de productos y servicios financieros para mejorar sus oportunidades en el mercado y propiciar su mayor competitividad a nivel nacional e internacional.

Con este nuevo enfoque, un banco es una institución que sirve de intermediaria en operaciones de crédito, vende productos y servicios financieros y coadyuva al desarrollo del sistema productivo de un país.

En Guatemala, el funcionamiento de los bancos del sistema está regido principalmente por la Ley de Bancos, Decreto 315 del Congreso de la República; Ley Monetaria, Decreto 203 del Congreso de la República, Ley Orgánica del Banco de Guatemala, Decreto 215 del Congreso de la República y Disposiciones Reglamentarias emitidas por Junta Monetaria y por el Superintendente de Bancos.

2.1.2 CLASIFICACION

De acuerdo con el artículo 34 de la Ley de Bancos, la clasificación de las entidades bancarias en Guatemala está determinada por las operaciones que éstas realizan, por lo que las

ismas se encuentran agrupadas de la siguiente manera:

1.2.1 BANCOS COMERCIALES

Son las instituciones de crédito que reciben depósitos monetarios y a plazo, con el objeto de invertir los recursos captados en operaciones de corto y mediano término. Asimismo, ofrecen servicio de descuento de letras y pagarés, cuyo vencimiento no exceda de un año. También realizan otras operaciones dentro de las que se pueden mencionar, la emisión de cartas de crédito a plazos que no excedan de un año, compra de valores o títulos tanto nacionales o extranjeros y otras. Es importante destacar que las operaciones que realizan en moneda extranjera requieren la autorización previa de la Junta Monetaria, por el hecho de que ese tipo de operaciones influyen en la determinación del tipo de cambio.

1.2.2 BANCOS HIPOTECARIOS

Estos bancos se caracterizan porque su operación activa principal es la concesión de préstamos con garantía de bienes inmuebles hipotecarios, mientras que su principal operación pasiva es la emisión de bonos hipotecarios y prendarios, así como la recepción de depósitos de ahorro y de plazo mayor.

Dentro de las operaciones más importantes que proporcionan los Bancos Hipotecarios se mencionan: Créditos de avío a plazo no mayor de un año, para financiar las labores productivas de las propiedades hipotecadas a su favor, con garantía prendaria de sus respectivos productos; créditos a plazo no mayor de cinco años, para financiar compras y operaciones útiles o productivas de mediano término con garantía prendaria, hipotecarias o mixta; créditos a plazo mayor, de hasta veinticinco años, para financiar operaciones productivas, compras de largo término o para refinanciar obligaciones análogas ya existentes con garantía hipotecaria.

Por otra parte los bancos hipotecarios también pueden adquirir Bonos y Títulos de Crédito de reconocida solidez, emitidos o garantizados por el Estado, así como de entidades públicas y privadas cuyas emisiones sean calificadas como de primer orden por la Comisión de Valores.

Financia sus operaciones con capital propio y reservas de capital, con recursos obtenidos de depósitos de ahorro y a plazo mayor, con la emisión de Bonos Hipotecarios y Prendarios, con empréstitos en el país y en el extranjero (previa autorización de la Junta Monetaria) y también podrán obtener recursos del Banco de Guatemala en operaciones autorizadas por la Institución.

2.1.2.3 BANCOS DE CAPITALIZACION

Son instituciones de crédito que emiten títulos de capitalización y reciben, en calidad de primas de ahorro, pequeñas sumas del público, con el objeto de invertir su producto en distintas operaciones de plazos que concuerden con los de las obligaciones contraídas, lo cual se puede comparar con los préstamos sobre pólizas de seguro de vida. Estos bancos promueven la construcción de casas, cuyo valor será pagado por el sistema de cuotas fijas.

Dentro de las operaciones que están autorizadas a realizar se encuentran: Hacer adelantos con garantía de las primas de ahorro recibidas al amparo de sus contratos de capitalización, adquirir bonos y otros títulos de crédito en las mismas condiciones de los bancos hipotecarios en cuanto les fueren aplicables, otorgar préstamos a otras instituciones de crédito, adquirir predios urbanizados y construir casas con el objeto de colocar en el público lotes o viviendas urbanas mediante ventas o contratos de arrendamiento con promesas de venta.

Los Bancos de Capitalización financian sus operaciones con capital propio y reservas de capital, además con recursos provenientes de: Recepción de primas de ahorro, bajo las condiciones de sus contratos de capitalización; obtención de empréstitos en el país o en el extranjero previa autorización de la Junta Monetaria.

2.1.2.4 BANCOS COMERCIALES E HIPOTECARIOS

A estos bancos también se les denomina "Bancos Mixtos", ya que están autorizados a realizar en forma indirecta operaciones de Bancos Comerciales como de Bancos Hipotecarios, ambos mencionados con anterioridad.

2.1.3 SERVICIOS QUE PRESTAN LAS ENTIDADES BANCARIAS

La creciente competencia, la desregularización de los mercados y la siempre creciente sofisticación entre clientes, ha dado como resultado la rápida evolución del sector bancario. Al igual que se busca disminuir los costos y mejorar la eficiencia, se está haciendo énfasis en la calidad del servicio al cliente y en ampliar la gama de productos y servicios. La velocidad a la cual se está dando este cambio se ha acelerado, en parte, debido a los servicios mejorados a través de redes y los métodos de entrega del producto.

En ese sentido, una de las características que presenta en la actualidad el mercado bancario guatemalteco, es la tendencia a la formación del sistema de banca múltiple, pues se presenta como una opción para superar la demanda de servicios financieros que afrontan las entidades bancarias. La banca múltiple se define como un centro en el que se puede adquirir cualquier producto o servicio financiero disponible en el mercado, con responsabilidad unitaria frente a la clientela, los accionistas y el gobierno.

En otras palabras, la banca múltiple, conocida también como: banca universal, banca corporativa, banca de servicios generales y supermercado financiero, es aquella que ofrece servicios de banca comercial, hipotecaria, financiera y fiduciaria, asimismo ofrece productos y servicios propios de empresas almacenadoras, aseguradoras, afianzadoras, arrendadoras y en sí todas aquellas negociaciones de índole financiero o de apoyo a las mismas, tales como factoraje, asistencia en sistemas de información basados en tecnología electrónica, evaluación de proyectos, asesoría de finanzas y auditorías, etc.

En septiembre de 1993, con el programa de modernización financiera, impulsado tanto por el sector financiero como por la banca central, se reconocieron mediante acuerdos, aquellas operaciones que puedan realizar los bancos y que no están explícitamente previstas, tanto de naturaleza activa, pasiva o bien como indiferenciadas, con el fin de diversificar la oferta de productos y servicios bancarios conforme a las prácticas financieras más modernas.

Dentro de estas operaciones, se encuentran el servicio de cajero automático, la concesión de tarjetas de débito en cuentas de depósitos, la conexión de redes electrónicas entre las computadoras de los clientes y las del propio banco, afin de que se puedan realizar sus operaciones desde el hogar y otras.

2.2 CUENTAS DE DEPOSITO A LA VISTA GIRABLES CON CHEQUE

Los contratos pueden ser “reales” o “consensuales”. Los primeros son aquellos que para perfeccionarse, requieren la entrega material de una cosa; mientras que los segundos se perfeccionan por el simple consentimiento de las partes contractuales.

En el ámbito bancario, la operación de Depósito figura entre los primeros y se define así: “Es un contrato real por medio del cual una persona recibe de otra determinados valores para su custodia, quedando obligada a devolverlos cuando se los reclame esta última.”⁶ La persona que recibe los bienes en depósito se denomina “depositario”, y la que los entrega se denomina “depositante”.

En cuanto a la clasificación, los depósitos bancarios se dividen en “regulares” e “irregulares”. Los regulares corresponden a títulos, alhajas y otros valores muebles, en donde el que actúa como depositario tiene que devolver forzosamente los mismos objetos que recibió. En los depósitos irregulares, que por lo general versan sobre dinero, el banco que recibe el depósito no devuelve precisamente los mismos billetes y monedas recibidos, sino otros de la misma clase. Los depósitos de dinero (billetes y monedas) también se les denomina Depósitos de Fondos, los cuales no permanecen ociosos sino que los bancos los invierten en préstamos, compra de valores y otras inversiones.

6 Ernesto R. Molina, Contabilidad Bancaria, pág 60

1.2.1 DEFINICION

Las cuentas de depósitos a la vista girables con cheque es una de las diferentes modalidades que tienen las entidades bancarias para captar recursos financieros, que les permite actuar como intermediarios financieros. Estas cuentas son exigibles a simple requerimiento del depositante por medio de cheques.

En este tipo de depósito el cliente se presenta a la institución bancaria para abrir su cuenta, a que le proporciona una chequera (y una tarjeta de débito, en los bancos donde se cuenta con este servicio) para realizar los retiros cuando la persona lo necesite. Cada fin de mes el cliente recibe un estado de cuenta para verificar los depósitos y retiros realizados durante el mismo, a fin de que el depositante pueda conciliar su saldo con el del banco.

1.2.2 IMPORTANCIA

Dentro de los aspectos más importantes se pueden mencionar los siguientes:

Como medio de pago, ya que por medio de cheque o tarjetas de débito se pueden realizar diferentes transacciones comerciales (compras o pagos) entre entes económicos.

Depósito de valor, debido a que constituyen un activo que mantienen los depositantes en una entidad bancaria.

Como activo que surge para cubrir futuras eventualidades (motivo de precaución).

Como medio de control sobre el uso del numerario de una persona o empresa.

1.2.3 CLASIFICACION

La clasificación de los depósitos según determinados requisitos para su constitución y evolución, es la siguiente:

1. **Depósito Condicional.** Es aquel que versa sobre valores que han de devolverse sólo hasta que se cumpla determinada condición señalada por el depositante, por ejemplo un depósito

a la orden de un menor, cuya condición sea entregárselo únicamente hasta que muera el padre.

- b. **Depósito Judicial.** Es aquel que se refiere a valores o fondos que el banco separa por orden de un juez, y cuya condición de entrega es una orden de la misma autoridad.
- c. **Depósito a la Orden.** Este se trata de dinero que el banco recibe para ser entregado a terceras personas.
- d. **Depósito en Garantía.** Es aquel que recibe el banco para garantizar una operación, como ejemplo se puede mencionar el depósito que un cliente deja como garantía de una carta de crédito que solicita.

2.2.4 PROCEDIMIENTOS DE EJECUCION DE DEPOSITOS A LA VISTA

La operación de recibir depósitos para un banco es de carácter pasivo. Conforme la técnica contable, siempre que aumente ese pasivo se abonará la cuenta que corresponda, al disminuir por retiros de los depositantes se cargará la misma.

De manera que es necesario tomar en cuenta que una persona o empresa puede depositar en su cuenta de depósitos a la vista cualquiera de los siguientes valores:

- Billetes y monedas nacionales
- Cheques del propio banco, girados contra depósitos de otras cuentas
- Cheques de Gerencia o de Caja
- Cheques de otros bancos locales, y otros.

Por otra parte, es de señalar que una persona puede girar un cheque a favor del mismo banco en que ha constituido sus depósitos, y ello podría ser por cualquiera de los motivos siguientes:

Para retirar dinero
Para abonarle o cancelarle al banco un préstamo
Para comprar bienes al banco
Para comprarle cheques de viajero o monedas extranjeras
Para comprarle bonos
Para comprarle un giro o una transferencia
Para pagarle un documento que fue librado a su cargo
Para cubrirle el valor parcial o total de cartas de crédito
Para pagar el alquiler de cajillas de seguridad u otro servicio que le presta el banco
Para pagarle al banco intereses o comisiones
Para pagarle cualquier adeudo diferente al de préstamos, y otros.

Como se puede apreciar, son variados y distintos los motivos por los cuales se gira un cheque.

Para efectos de observar en forma gráfica los pasos que se realizan en las cuentas de depósitos monetarios, en el *Capítulo V*, denominado *Participación de la Auditoría Interna en la Implantación y Evaluación del Control Interno en las Operaciones de Depósito a la Vista Girables con Cheque, a través de una Red Electrónica*, se incluyen diferentes operaciones con algunos flujogramas, los cuales se enumeran a continuación:

1. Apertura de una cuenta de depósitos a la vista girables con cheque
2. Investigación de cuentas nuevas
3. Denegación de apertura de cuenta
4. Captura de firmas
5. Entrega de chequeras
6. Pagos de cheques.

CAPITULO III

REDES ELECTRONICAS

Debido al gran volumen de transacciones que se manejan actualmente en las operaciones bancarias, las instituciones financieras se han visto en la necesidad de utilizar los avances en materia de sistemas de procesamiento electrónico de datos, como una de las herramientas esenciales, para hacerle frente al constante desarrollo de la sociedad. Dentro de este marco, se encuentra el uso de los sistemas de redes electrónicas, de los cuales se ha valido las entidades bancarias para ofrecer un mejor servicio en las operaciones de las cuentas de depósito a la vista irrevocables con cheque.

1.1 DEFINICION

Durante la última década, las computadoras y las redes informáticas han producido en nuestra sociedad un impacto de enormes consecuencias. Se dice que se ha entrado en la "Era de la Información". Lo cierto es que estas herramientas revolucionarias han multiplicado la productividad en el trabajo, tanto para las empresas como para los usuarios individuales.

Pero, ¿Qué es una red electrónica de computadoras? Son varias las definiciones aceptadas por la industria; de las más sencillas se presentan las siguientes:

"Un sistema de redes electrónicas se define como una colección interconectada de computadoras autónomas. Se dice que dos computadoras están interconectadas si éstas son capaces de intercambiar información."⁷

La conexión puede hacerse a través de medios físicos como cables, mediante satélites de comunicación, microondas, etc. Al decir que son autónomas se refiere a que no existe una dependencia de una computadora sobre otra.

Tanenbaum, Andrew S., Redes de Ordenadores, Pág. 2.

Otra definición presenta: "Una red electrónica es un grupo de computadoras (y terminales, en general) interconectadas a través de uno o varios caminos o medios de transmisión. La mayoría de las veces, este medio de transmisión es la línea telefónica, debido a su fácil accesibilidad."⁸

En estas dos definiciones destaca la finalidad concreta que tienen las redes electrónicas: transferir e intercambiar datos entre computadoras y terminales. Es el intercambio de datos lo que hoy permite funcionar a múltiples servicios, los cuales se consideran parte de la vida cotidiana del ser humano, tales como: cajeros automáticos, terminales de punto de venta y otros.

3.2 UTILIDAD Y VENTAJAS DE LAS REDES ELECTRONICAS

Día a día, infinidad de usuarios acuden a las redes informáticas para atender sus necesidades privadas o comerciales. Esta tendencia se acentúa a medida que las empresas y los usuarios van descubriendo la potencia de estos medios. En la actualidad, las computadoras registran periódicamente las transacciones que se realizan, se ocupan de las operaciones bancarias, gestionan las reservaciones de los hoteles y realizan muchas otras actividades económicas que dependen por completo de las redes electrónicas.

Esto demuestra que las redes electrónicas presentan varias ventajas importantes a los usuarios, ya sean empresas o particulares, estando entre otras las siguientes:

1. Las organizaciones modernas suelen estar expandidas, incluyen empresas distribuidas en varios puntos de un país o extendidas por todo el mundo. Muchas de las computadoras y terminales situados en los distintos lugares necesitan intercambiar datos e información, con frecuencia ese intercambio ha de ser diario. Mediante una red puede conseguirse que todas esas computadoras se intercambien información y que los programas y datos necesarios estén al alcance de todos los miembros de la organización.
2. La interconexión de computadoras permite que varias máquinas compartan los mismos

⁸ Uylless Black, Redes de Computadoras, Protocolos, Normas e Interfaces. Pág. 1

recursos. Por ejemplo, si una computadora se satura por estar sometida a una carga excesiva de trabajo, se puede utilizar la red para que otra computadora se ocupe de este trabajo, con lo cual se consigue un mejor aprovechamiento de los recursos.

3. Las redes pueden resolver también un problema de especial importancia: la tolerancia ante fallos. En caso de que una computadora falle, otra puede asumir sus funciones y su carga de trabajo, algo de particular importancia en los sistemas de control del tráfico aéreo. Si una computadora falla, las computadoras de reserva entran en funcionamiento rápidamente y toman el mando de todas las operaciones de control, sin que en ningún momento llegue a existir peligro para los pasajeros.
4. El uso de redes confiere una gran flexibilidad en el ámbito laboral. Los empleados pueden trabajar desde sus hogares, al utilizar terminales conectados con la computadora de la oficina. Hoy en día es frecuente ver personas que viajan con su computadora portátil, y la conectan a la red de su empresa a través de la línea telefónica situada en la habitación del hotel. Otros usuarios que viajan a oficinas alejadas, emplean los teléfonos y las redes para transmitir y recibir información decisiva, como informes de ventas o datos administrativos, y para extraer datos de las computadoras centrales de su empresa.
5. El factor económico en la utilización de una red, consiste en compartir recursos entre sí, ahorrando con ello la adquisición de información por cada terminal.

La sociedad de nuestros días emplea la información para reducir los costos de producción de los bienes que se consumen y en general para mejorar la calidad de vida. Gracias a los sistemas de comunicaciones y a las redes electrónicas, hoy es posible el intercambio rápido de información residente en computadoras esparcidas por todo un país.

3.2.1 LA IMPORTANCIA DE LA TECNOLOGIA DE LA INFORMATICA PARA LOS BANCOS

Como resultado de la mejora en las comunicaciones, la liberalización de los mercados y la

supresión de las barreras comerciales, cada vez más, los bancos tienen que enfrentarse a la competencia tanto nacional como internacional. Para hacer frente a estos desafíos, estas instituciones tienen que examinar todos los aspectos de sus negocios, siendo uno de los más importantes, la necesidad de *Tecnología de la Informática*.

Sin duda, las mejoras en los medios de transporte y comunicación han ayudado a crear un mercado global. La globalización de los mercados financieros se está abriendo camino en la industria de los servicios financieros a pasos agigantados.

En los principios de la filosofía económica se están arraigando conceptos tales como el libre comercio, libre circulación de capital y condiciones de libre mercado. El libre mercado se está expandiendo y diversificando sobre una base global. Como resultado de la liberalización de los mercados en todo el mundo, los bancos están entrando de forma agresiva en los nuevos mercados, principalmente mediante fusiones y adquisiciones. Estas nuevas oportunidades hacen que los bancos consigan economías de escala favorables, que aumenten su esfera geográfica, que incrementen su penetración en el mercado de su interés y que aprovechen el creciente número de acuerdos comerciales internacionales y transacciones financieras. Al entrar en nuevos mercados, a su vez, los bancos reducen su dependencia de los caudales económicos de un determinado mercado regional o nacional.

En este entorno, los bancos se enfrentan a nuevos desafíos a medida que se adaptan a esta nueva esfera comercial globalizada.

Tanto los clientes individuales como corporativos desean productos actualizados, completos e integrados, que se realicen con un gran nivel de servicio, en un corto período de tiempo. Existe una necesidad creciente de más y mejor información que sea de fácil acceso para el usuario final. Los bancos están haciendo frente a un incremento exponencial en la variedad y complejidad de sus productos. Necesitan sistemas capaces de informar, comerciar y liquidar. La gestión necesita información para sopesar el riesgo y la rentabilidad.

En la actualidad, los bancos tienen que hacer frente a la competencia de instituciones que

no pertenecen al sector de la banca en la nueva esfera financiera global. Los clientes pueden ahora adquirir productos financieros y servicios, que anteriormente eran el núcleo de las operaciones e ingresos de los bancos, en instituciones que no son bancarias. Es así, que compañías internacionales de corredores de bolsa ofrecen cuentas con dinero de mercado, cuentas para jubilaciones personalizadas e incluso préstamos hipotecarios. Por otra parte, las compañías de seguros tradicionales, cooperativas, uniones de crédito y sociedades de préstamos hipotecarios, también compiten con la banca minorista aumentando su gama de productos y servicios.

Los bancos además se enfrentan a otras amenazas de competencia. Fabricantes de automóviles ofrecen tratos especiales para el financiamiento en la adquisición de nuevos carros. Por ejemplo, General Motors ha lanzado una tarjeta Visa de la compañía que está teniendo gran aceptación en todo el mundo. Los grandes almacenes promocionan los beneficios de sus propias tarjetas de crédito y muchas corporaciones como Shell, Esso, Pro inversiones y otras, tienen sus propias divisiones de financiamiento al consumidor.

A medida que la demarcación de la línea entre bancos e instituciones no bancarias se hace todavía más confusa, los bancos deben reaccionar introduciendo nuevos productos y ofreciendo mejores servicios, si quieren mantener sus clientes y atraer nuevos.

Como herramienta básica para conseguir lo anterior, las instituciones bancarias se han valido de los avances tecnológicos en los sistemas electrónicos de datos. Las tremendas innovaciones y cambios que se han realizado en la forma en que se dirige un banco se debe a estos avances, lo cual ha hecho posible el cambio. La tecnología de la informática ha jugado un papel esencial en la creación de mercados globales y fue un factor importante con el que los gobiernos contaron a la hora de tomar decisiones para liberalizar los mercados financieros. La información es esencial en la banca, por lo tanto, es importante contar con buenos sistemas de esta índole para la efectiva gestión y funcionamiento de un banco.

Originalmente, la tecnología de la informática se introdujo para reducir costos, pero en la actualidad este concepto ha cambiado a favor de brindar un mejor servicio. Las instituciones financieras apuntan hacia la tecnología de la informática para hacer frente a los retos de la nueva

esfera de negocios, ya que es la única forma de conseguir la base de la gestión global.

3.3 CLASIFICACION DE LAS REDES ELECTRONICAS

Las redes electrónicas se pueden clasificar de la siguiente forma:

- Por su Localización.
- Por su Propietario.
- Por su Topología.

A continuación se exponen los aspectos más importantes de cada una de ellas.

3.3.1 POR SU LOCALIZACION

Por su localización las redes electrónicas se pueden clasificar así:

- a) LAN (Local Area Network)
- b) MAN (Metropolitan Area Network)
- c) WAN (Wide Area Network)

a) LAN (LOCAL AREA NETWORK)

Las redes de área local son aquellas que “cubren un área geográfica limitada, es decir que debe ser local en extensión geográfica, aunque el término *local* podría referirse desde una oficina, un edificio grande o hasta una instalación educativa o industrial de múltiples edificios”.⁹

Este tipo de redes está diseñado para compartir datos entre estaciones de trabajo. Algunas de las características de las redes de área local son:

- Ofrece conectividad con distintos tipos de computadoras.
- Soportan comunicaciones de datos a alta velocidad.

⁹ Decynar Estuardo León, Interconexión de Redes Remotas, Pág. 10

b) MAN (METROPOLITAN AREA NETWORK)

La red de área metropolitana está por delante de la red de área local. En este tipo de red se pueden realizar comunicaciones a alta velocidad a distancias más largas. Dentro de sus principales características se encuentran las siguientes:

- Dan lugar a esquemas de transmisión de señales rápidas.
- Hacen posible el establecimiento de redes privadas virtuales dentro de la misma red.
- Asegura la alta confiabilidad, disponibilidad y facilidad de mantenimiento de la red.

c) WAN (WIDE AREA NETWORK)

Este tipo de red de área extendida utiliza enlaces punto a punto. Las WAN abarcan países enteros y pertenecen a múltiples organizaciones. Los diseñadores de redes WAN están casi siempre obligados por razones de tipo económico y político, a utilizar las redes públicas de teléfonos existentes, sin importar su conveniencia técnica. Debe considerarse al utilizar este tipo de red el margen de error debido a la baja fiabilidad de los medios utilizados para la telecomunicación, existiendo para ello, algoritmos de verificación de error de transmisión.

3.3.2 POR SU PROPIETARIO

En este tipo de redes electrónicas se encuentran las siguientes:

- a) Redes Públicas
- b) Redes Privadas

a) REDES PUBLICAS

Las compañías privadas o los gobiernos de varios países han comenzado a ofrecer servicios de redes a cualquier organización que desee suscribirse a ellas. La conexión física es propiedad de la compañía operadora de redes, proporcionan un servicio de comunicación para los

|



clientes y terminales quienes obtienen un costo más bajo al utilizar este servicio. A este tipo de sistema se le llama *RED PUBLICA* y es análoga o frecuentemente forma parte del sistema telefónico público.

b) REDES PRIVADAS

Análoga a las redes públicas existen implementaciones de redes dentro de una empresa o corporación. Estas redes prestan servicios específicos para los departamentos o empresas de la corporación, a este tipo de redes se les llama *REDES PRIVADAS*. Los medios de comunicación utilizados en este tipo de red varían del servicio telefónico, ya que emplean un sistema propio de cableado, radio frecuencia, etc. Las redes privadas prestan servicio exclusivo a la empresa o filiales; es decir, que no prestan servicio de transmisión de información a terceras personas.

En la práctica una red privada puede llegar a formar parte de una red pública, con el objetivo de ampliar su rango de comunicación e intercambio de información.

3.3.3 POR SU TOPOLOGIA

La configuración de una red suele conocerse como topología de la misma. La topología es la forma (la conectividad física) de la red. El término "topología" es un concepto geométrico con el que se alude al aspecto de una cosa.

A la hora de implantar la topología de una red, el diseñador ha de plantearse tres objetivos principales:

1. Proporcionar la máxima fiabilidad posible, para garantizar la recepción correcta de todo el tráfico (encaminamiento alternativo).
2. Encaminar el tráfico entre el equipo terminal de datos (ETD), transmisor y receptor, a través del camino más económico dentro de la red (aunque, si se consideran más importantes otros factores, como fiabilidad, este camino de costo mínimo puede no ser el

más conveniente). El equipo terminal de datos (ETD) se puede definir como la máquina que emplea el usuario final en una red, ejemplo: cajeros automáticos, terminales punto de venta de un almacén, computadoras personales instalados en oficinas y otros.

- Proporcionar al usuario final un tiempo de respuesta óptimo y un caudal eficaz máximo.

Cuando se habla de fiabilidad de una red, se refiere a la capacidad que tiene la misma para transportar los datos correctamente (sin errores) de un equipo terminal de datos a otro. Ello incluye también la capacidad de recuperación de errores o datos perdidos en la red, ya sea por fallo del canal, el ETD, el equipo de terminación del circuito de datos, ETCD (Su misión es conectar los ETD a la línea de comunicaciones, ejemplo: los Módems) o del equipo de conmutación de datos (ECD), cuya función principal es encaminar los datos del usuario hasta su destino final a través de la red, lo cual evita los dispositivos y canales ocupados o fuera de servicio. La fiabilidad está relacionada también con el mantenimiento del sistema en el que se incluyen las comprobaciones diarias, el mantenimiento preventivo que se ocupa de relevar de sus áreas a los componentes averiados o de funcionamiento incorrecto, o bien, el aislamiento de los focos de averías. Cuando un componente crea problemas, el sistema de diagnóstico de la red ha de ser capaz de identificar y localizar el error, aislar la avería y, si es preciso, aislar del resto de la red el componente defectuoso.

El segundo objetivo a cumplir a la hora de establecer una topología para la red consiste en proporcionar a los procesos de aplicación que residen en los ETD el camino más económico posible. Para ello es necesario:

- Minimizar la longitud del canal que une los componentes, lo cual suele implicar el encaminamiento de los datos del usuario a través del menor número posible de componentes intermedios.
- Proporcionar el canal más económico para cada actividad concreta; por ejemplo, transmitir los datos de baja prioridad a través de un enlace de baja velocidad por línea telefónica normal, lo cual es más barato que transmitir esos mismos datos a través de un canal vía

satélite de alta velocidad.

El tercer objetivo es obtener un tiempo de respuesta mínimo y un caudal eficaz lo más elevado posible. Para reducir al mínimo el tiempo de respuesta hay que acortar el retardo entre la transmisión y la recepción de los datos de un ETD a otro. En aplicaciones interactivas, por ejemplo, es fundamental conseguir un tiempo de respuesta bajo. El caudal efectivo o eficaz expresa la cantidad máxima de datos de usuario que es posible transmitir en un determinado período de tiempo.

Ya visto los objetivos que se deben de perseguir a la hora de diseñar una red, es necesario conocer las formas más comunes en las que se podrían organizar las redes según su configuración, siendo éstas:

- a) Topología Jerárquica (Arbol)
- b) Topología Horizontal (De bus o Ethernet)
- c) Topología en Estrella (Centralizada)
- d) Topología en Malla
- e) Topología de Anillo
- f) Redes Token Ring de IBM

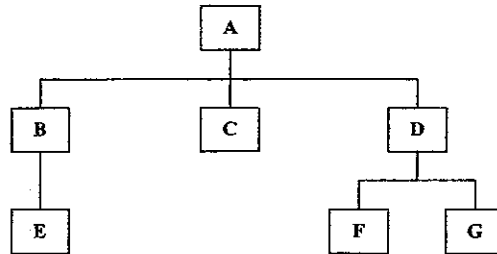
a) TOPOLOGIA JERARQUICA (ARBOL)

La estructura jerárquica es una de las más extendidas en la actualidad. El software que controla la red es relativamente simple y la topología proporciona un punto de concentración de las tareas de control y de resolución de errores.

“Esta topología se encuentra integrada por una computadora central, la cual controla y dirige la transmisión e intercambio de datos entre las distintas terminales. La computadora central se encuentra situado en el nivel más elevado de la jerarquía que controla la red. Sin embargo, muchos fabricantes incorporan a esta topología un cierto carácter distribuido, dotando a ciertas terminales un control directo sobre otras computadoras situadas en niveles inferiores dentro de la

jerarquía, lo cual reduce la carga de trabajo de la computadora central".¹⁰

Las redes con topología jerárquica se conocen también como redes verticales o en árbol. La palabra "árbol" alude al hecho de que su estructura se parece bastante a un árbol cuyas ramas van abriéndose desde el nivel superior hasta el más bajo. A continuación se presenta un diagrama que representa a esta topología:



a.1) DESVENTAJAS DE LA TOPOLOGIA JERARQUICA

Aunque la topología jerárquica resulta interesante por ser fácil de controlar, puede presentar ciertos problemas en cuanto a la posibilidad de aparición de cuellos de botella. En determinadas situaciones, la computadora central, ha de controlar todo el tráfico entre los distintas terminales. Este hecho no sólo puede crear saturaciones de datos, sino que además plantea serios problemas de fiabilidad. Si la computadora central falla, toda la red deja de funcionar, a no ser que exista otra computadora de reserva capaz de hacerse cargo de todas las funciones de la computadora averiada. Pese a todo, las topologías jerárquicas se han venido usando ampliamente desde hace bastantes años, y seguirán empleándose durante mucho tiempo, ya que permiten la evolución gradual hacia una red más compleja, puesto que la adición de nuevas terminales es relativamente sencilla.

Si se para a pensar un poco, se encontrará claros ejemplos de topologías en árbol en numerosas actividades de la vida diaria. Un caso evidente es el organigrama de personal de una

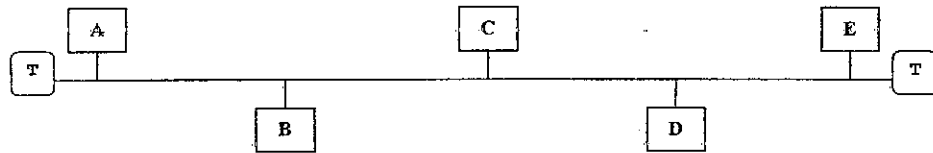
¹⁰ Uylees Black, Op. Cit. Pág. 8

empresa. Como es lógico, las ventajas y desventajas de una red vertical de comunicaciones son más o menos las mismas que las de una empresa estructurada jerárquicamente, con líneas de autoridad muy claras, con cuellos de botella frecuentes en los niveles superiores y a menudo una insuficiente delegación de responsabilidades.

b) TOPOLOGÍA HORIZONTAL (DE BUS O ETHERNET)

Esta estructura es frecuente en las redes de área local y es relativamente fácil controlar el flujo de tráfico entre las distintas terminales. “La topología está configurada con derivaciones o ramales que se extienden desde un sistema central. Cuando una transacción atraviesa el bus (normalmente un cable coaxial, de fibra óptica o dúplex trenzado) todas y cada una de las conexiones escuchan la señal que lleva consigo una designación de dirección. Este tipo de redes posee terminadores a los extremos de la red, los cuales le indican donde termina la misma”.¹¹

Para efectos de ilustración, a continuación se presenta un diagrama:



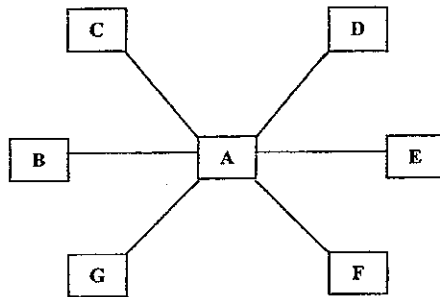
b.1) DESVENTAJAS DE LA TOPOLOGÍA HORIZONTAL

La principal limitación de una topología horizontal está en el hecho de que suele existir un sólo canal de comunicaciones para todos los dispositivos de la red. En consecuencia, si el canal de comunicaciones falla, toda la red deja de funcionar. Algunos fabricantes proporcionan canales completamente redundantes por si falla el canal principal. Otro inconveniente de esta configuración estriba en la dificultad de aislar las averías de los componentes individuales conectados al bus. La falta de puntos de concentración complica la resolución de este tipo de problemas.

¹¹ Deeynar Estuardo León, op. cit., pág. 30

b) TOPOLOGIA EN ESTRELLA (CENTRALIZADA)

Esta topología era una de las más empleadas en los sistemas de comunicación de datos a lo largo de los años sesenta y a principios de los setenta, derivado de que resultaba fácil de controlar, ya que el software no es complicado y su flujo de tráfico es sencillo. Todo el tráfico mana del núcleo de la estrella. La computadora central posee el control de las operaciones de cómputo primarias, en donde todas las estaciones distantes alimentan de información a la central. La configuración en estrella es por tanto, una estructura muy similar a la de la topología jerárquica, aunque su capacidad de procesamiento distribuido es limitada. A continuación se presenta un diagrama que presenta esta topología:

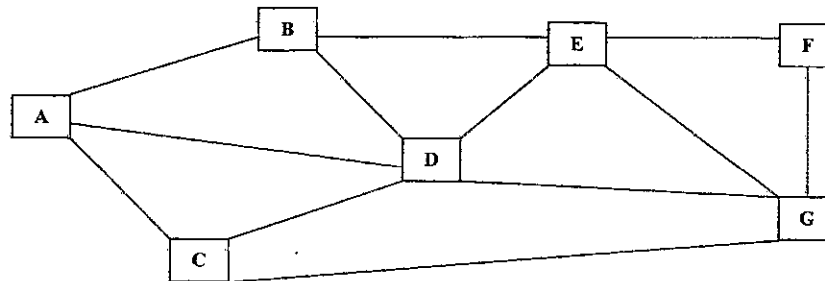


c.1) DESVENTAJAS DE LA TOPOLOGIA EN ESTRELLA

La computadora central es responsable de distribuir la información de datos hacia el resto de los componentes; se encarga además, de localizar las averías. Esta tarea es relativamente sencilla en el caso de una topología en estrella, ya que es posible aislar las líneas para identificar el problema. Sin embargo, y al igual que en la estructura jerárquica, una red en estrella puede sufrir saturaciones y problemas en caso de avería de la computadora central.

d) **TOPOLOGIA EN MALLA**

La topología en malla se ha venido empleando en los últimos años. Lo que la hace atractiva es su relativa inmunidad a los problemas de embotellamiento y averías. Gracias a la multiplicidad de caminos que ofrece a través de las distintas estaciones de trabajo, es posible orientar el tráfico por trayectorias alternativas en caso de que alguna terminal esté averiada u ocupada, ya que estas estaciones se pueden conectar con líneas independientes de comunicación a las de la computadora central. Para efectos de ilustrar esta topología, se presenta el siguiente diagrama:



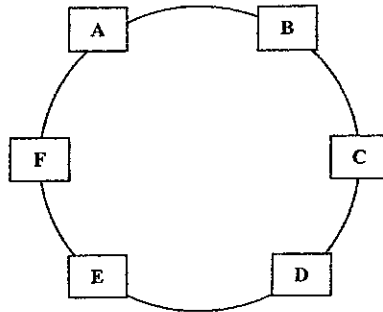
d.1) **DESVENTAJAS DE LA TOPOLOGIA EN MALLA**

A pesar de que la realización de este método es compleja y cara (para proporcionar estas funciones especiales, la lógica de control de los protocolos de una red en malla puede llegar a ser sumamente complicada), muchos usuarios prefieren la fiabilidad de una red en malla a otras alternativas.

e) **TOPOLOGIA EN ANILLO**

Este tipo de configuración es bastante extendida. La topología en anillo se llama así por el aspecto circular del flujo de datos. En la mayoría de los casos, los datos fluyen en una sola dirección, en donde cada estación recibe la señal y la retransmite a la siguiente, en anillo. Este tipo de organización resulta atractivo, ya que en él son bastante raros los embotellamientos, tan

frecuentes en los sistemas en estrella o en árbol. Además, la lógica necesaria para poner en marcha este tipo de red, es relativamente simple, ya que cada componente llevará a cabo una serie de tareas muy sencillas: aceptar los datos y enviarlos a la estación conectada al anillo o retransmitirlos al próximo componente del mismo. La gráfica que se presenta a continuación muestra la manera en que este tipo de topología opera:



e.1) DESVENTAJAS DE LA TOPOLOGIA EN ANILLO

Como todo tipo de redes, ésta posee algunos defectos. El problema más importante es que todos los componentes del anillo están unidos por un mismo canal. Si falla el canal, toda la red se interrumpe. Por eso, algunos fabricantes han ideado diseños especiales que incluyen canales de seguridad, por si se produce la pérdida de algún canal. Otros, por aparte, construyen conmutadores que dirigen los datos automáticamente, saltándose la estación averiada hasta la siguiente, con el fin de evitar que el fallo afecte toda la red.

f) REDES TOKEN RING DE IBM

La compañía IBM ha dado un gran apoyo al estándar de red con paso de testigo de anillo. En ese sentido, esta topología incluye una función de monitorización del testigo (llámese así a la cantidad de información que se transporta en un momento determinado), es decir, que en cada anillo existe una unidad de interfaz que se encarga de vigilar el testigo activo, por si es necesario

recuperar datos perdidos o testigos extraviados.

“En el campo del control físico, existe un bit que hace de bandera para motorizar la información. La estación de vigilancia de la información usa esta bandera para detectar la circulación continua de un testigo ocupado. Cuando una estación obtiene el control del anillo, coloca una cabecera a la información que se va a enviar. Al hacerlo, el campo de monitorización del testigo se activa. Cuando la información regresa a la estación que lo envió, después de atravesar todo el anillo, ésta lo extrae de la red. Si por cualquier razón la computadora emisora ha funcionado mal, el testigo ocupado pasará de largo y volverá a llegar a la estación de vigilancia, la cual observará que la bandera de monitorización sigue activa; esto hará que se llegue a la conclusión de que la estación transmisora ha funcionado mal, extrayendo el testigo ocupado de la red para insertar uno libre, tras lo cual la red continuará funcionando de manera normal.

Otra posibilidad es que la información se pierda, entendiéndose por ello que una unidad de interfaz con el anillo reciba el testigo, pero tenga algún impedimento para regenerarlo y colocarlo de nuevo en el anillo. También puede ocurrir que el testigo quede dañado por algún problema eléctrico en el circuito y que, como consecuencia de ello, resulte indescifrable. Sea cual sea el motivo de la pérdida del testigo, el módulo activo de vigilancia maneja la situación mediante un temporizador que se activa cada vez que pasa un testigo, ya sea libre u ocupado. Si el temporizador llega al final de su cuenta antes de que el testigo en circulación haya regresado a la estación de vigilancia, ésta deberá reinicializar el anillo insertando en el otro testigo libre”.¹²

3.4 PARTES DE QUE CONSTAN LAS REDES ELECTRONICAS

Para que las computadoras y terminales puedan comunicarse entre sí existen ciertos dispositivos comunes para las diferentes topologías de redes, que permiten intercambiar información entre computadoras autónomas. Entre los diversos componentes, seguidamente se definen los que se consideran prioritarios:

¹² Uylless Black, op. Cit., pág. 143

3.4.1 EQUIPO TERMINAL DE DATOS (ETD)

Esta definición suele emplearse de forma genérica para aludir a la máquina que emplea el usuario final. Un equipo terminal de datos puede ser desde una gran computadora, del tipo de los IBM, o una máquina pequeña, como una terminal o una computadora personal.

3.4.2 EQUIPO DE TERMINACION DEL CIRCUITO DE DATOS (ETCD)

Es también llamado "*Equipo de Comunicación de Datos*". Su misión es conectar los equipos ETD a la línea o canal de comunicaciones. Los ETCD diseñados en los años sesenta y setenta, eran dispositivos exclusivamente de comunicaciones. Sin embargo, en los últimos años estos equipos han ido incorporando más funciones de usuario, hoy en día algunos ETCD contienen parte de los procesos de aplicación. Un ejemplo de este equipo es un simple módem.

3.4.3 EQUIPOS DE CONMUTACION DE DATOS (ECD)

La función principal de este equipo es conmutar o encaminar el tráfico (datos de usuario) hasta su destino final a través de la red. El ECD proporciona las funciones vitales de encaminamiento por la red, evitando los dispositivos y canales ocupados o fuera de servicio. Asimismo, el ECD puede dirigir los datos hacia su destino final a través de componentes intermedios que pueden ser a su vez otros equipos de conmutación.

3.4.4 PROTOCOLOS

Los protocolos son acuerdos acerca de la forma en que se comunican entre sí los ETD y los dispositivos de comunicaciones, pueden incluir regulaciones concretas que recomienden u obliguen a aplicar una técnica o convenio determinado. Por lo general, son varios los niveles de interfaces y protocolos que necesitan las aplicaciones de usuario para funcionar.

En la actualidad se están llevando a cabo esfuerzos considerables a nivel mundial, con el fin de publicar normas y recomendaciones que sean independientes del fabricante. Siguiendo esta

tendencia, muchas organizaciones están adoptando interfaces y protocolos comunes.

3.4.5 REPEATERS

Los repetidores son elementos de comunicación que permiten extender la longitud de cable físico y poder ampliar el número de estaciones utilizadas en la red. Los repetidores amplifican la señal original de transmisión en el medio utilizado. El uso de repetidores es dependiente de dos variables: La arquitectura de la red y el tipo de medio de transmisión utilizado.

3.4.6 BRIDGES

Los Bridges son elementos de comunicación que permiten segmentar el tráfico de la red. La segmentación de la red permite restringir la cantidad de tráfico que fluye sobre toda la red, lo cual propicia un mejor rendimiento sobre ella.

3.4.7 ROUTERS

Dispositivo que segmenta el tráfico de la red y utiliza la dirección o destino del mensaje. Es dependiente del protocolo de la capa de red, así como de la topología de la misma. Opera en base a una jerarquía de direcciones que son definidas por el protocolo y es comúnmente utilizada para comunicaciones entre redes. Un buen ejemplo de un sistema jerárquico de direcciones es el número telefónico, el cual está dividido en cuatro secciones: código del país, código del área, código de oficina central y número de línea.

3.4.8 COMPUTADORA

Dispositivo que recibe, procesa y presenta los datos resultantes. Máquina de propósito general que procesa datos de acuerdo a un conjunto de instrucciones que se almacenan internamente, ya sea temporal o permanentemente. La computadora y todo el equipo conectado a éste se denomina *hardware*. Las instrucciones que le dicen qué debe hacer se llaman *software*.

Una computadora procesa datos capturándolos desde el teclado, disco o canal de comunicaciones hacia la memoria (RAM), calculándolos, comparándolos y copiándolos. Luego genera la salida de los resultados a la pantalla, los salva en disco o quizá los transmite nuevamente a través de un canal de comunicaciones. A la computadora también se le denomina *Ordenador* (máquina para el procesamiento de datos).

3.4.9 TECNOLOGIA

Conjunto de los conocimientos técnicos y científicos aplicados a la industria. El término "*tecnología*" en su etimología griega, significó originalmente discurso de las artes, tanto estéticas como aplicadas. La readopción del vocablo en el siglo XVII le asoció una relación única con las artes aplicadas, aunque su espectro semántico se amplió progresivamente hasta designar en los inicios del siglo XX a los métodos, procesos e ideas ligados a la obtención de herramientas y máquinas. En la segunda mitad del siglo, la tecnología se definió como el conjunto de medios y actividades mediante los que el hombre persigue la alteración y manipulación de su entorno.

Una vez expuesto lo relativo al control interno, cuentas de depósito a la vista y el marco general de lo que es una red electrónica, el siguiente paso es el de conjugar estos temas, afin de establecer un control interno adecuado, en operaciones de cuentas de depósito a la vista girables con cheque, realizadas a través de redes electrónicas, tema que será tratado en el siguiente capítulo.

CAPITULO IV
**EL CONTROL INTERNO EN OPERACIONES DE CUENTAS DE
DEPOSITO A LA VISTA GIRABLES CON CHEQUE, REALIZADAS A
TRAVES DE REDES ELECTRONICAS**

En los capítulos anteriores se ha visto en su orden, el marco conceptual de lo que es el control interno, sus características y el papel que desempeña la Dirección en relación al establecimiento de un sistema coherente que promueva la operación eficiente de la organización. El segundo capítulo se refirió a las operaciones que se realizan en las cuentas de depósito a la vista girables con cheque, desarrollándose en él algunas generalidades acerca del sistema bancario guatemalteco. Después, en el tercer capítulo, se definió lo que son redes electrónicas, su importancia y clasificación.

En el presente apartado se establece la relación de los anteriores temas, afin de obtener un adecuado control interno que promueva la eficacia y eficiencia de las operaciones que se realicen en la cuentas de depósito a la vista girables con cheque, a través de un sistema de redes electrónicas.

Pero, ¿cómo obtener un adecuado sistema de control interno que promueva la eficacia y eficiencia en este tipo de operaciones a través de un medio electrónico?

El primer procedimiento será determinar la identificación de la presencia y naturaleza de los riesgos puros o exposiciones a posibles efectos adversos en la actividad que se ha de desarrollar, afin de evitar las condiciones peligrosas que materialicen la ocurrencia de alguna pérdida.

Sin embargo, previa identificación de los riesgos en las operaciones realizadas a través de un sistema en red, en las cuentas de depósito a la vista girables con cheque, es necesario familiarizarse con la terminología relacionada con el riesgo y peligro.

4.1 TERMINOLOGIA RELACIONADA CON EL RIESGO Y EL PELIGRO

La definición de riesgo se debe entender como la posibilidad de pérdida. Por aparte, hay que saber diferenciar el **riesgo especulativo**, el cual puede dar como resultado un efecto favorable (ganancia) o un efecto desfavorable (pérdida), del **riesgo puro** que sólo puede dar como resultado un efecto adverso o no.

Intimamente relacionado con el riesgo se encuentra el **peligro**, el cual se define como la “condición que puede producir efectos adversos sobre la mejor utilización de los recursos humanos y materiales”¹³.

En relación a cada una de las actividades realizadas por el ser humano en sus diferentes acepciones, tanto de las más genéricas a las más concretas, llevan implícitas riesgos que al ejercerlas, puede que den algún resultado adverso o no, es decir que pueden dar lugar a **riesgos puros** como los siguientes:

- Accidentes de trabajo, deportivos, domésticos, de circulación.
- Enfermedades especiales o comunes.
- Incendios y explosiones.
- Robos, hurtos, atentados y sabotajes.

Esta es una descripción genérica de algunos riesgos puros que pueden estar presentes en las actividades humanas, lo cierto es que si no se pueden describir condiciones adversas (porque no existe la posibilidad de pérdida) no se está ante la presencia de riesgos puros. Por lo tanto, evitar los riesgos puros significaría que se pretende eliminar todas y cada una de las posibilidades de tener pérdidas como las descritas, lo cual resultaría prácticamente imposible.

¹³ José Adolfo Calderón, Seguridad Bancaria, pág. 60

Dentro de las operaciones de las cuentas de depósito a la vista girables con cheque, realizadas a través de redes electrónicas, como en otras actividades, eliminar la posibilidad de que existan eventos desfavorables es poco menos que imposible, por lo que se debe convenir que no es correcto hablar de eliminación de riesgos en su concepción habitual. No se trata de favorecer que subsistan las pérdidas sino todo lo contrario, se pretende señalar los caminos eficaces para evitar las mismas y clarificar, con un cierto rigor técnico, las posibilidades reales.

En ese sentido, es necesario establecer las condiciones peligrosas, tanto materiales como sociales, para poder definir la situación de peligro concreto. Una **condición peligrosa** se determina cuando se establecen las causas de los peligros y agentes involucrados en los mismos, los cuales conducen a una posibilidad de pérdida. El control de riesgos se basa precisamente en evitar condiciones peligrosas, en reducir y eliminar peligros, es la lucha contra lo concreto, en contraposición a los esfuerzos por anular lo abstracto. El auténtico conocimiento de estos hechos generadores ha de permitir la mejor aplicación de la técnicas adecuadas para evitar consecuencias desagradables.

El reconocimiento de estos conceptos básicos es lo que permitirá en determinado momento dar soluciones adecuadas a una estructura organizativa. Ignorarlos conduce a resultados desfavorables.

4.2 IDENTIFICACION DE RIESGOS GENERICOS, DESDE EL PUNTO DE VISTA FINANCIERO

Al estar ya familiarizados con la terminología relacionada con el riesgo y el peligro, el primer paso para el auditor en lo que se refiere a la implantación de un adecuado sistema de control interno, es como se dijo anteriormente, identificar la presencia y naturaleza de riesgos puros o exposiciones a posibles efectos adversos, en el entendido que una vez confeccionada la lista o inventario, no ha finalizado el proceso de identificación. Esta función debe tener un carácter dinámico en el desarrollo de la actividad de la empresa.

Al llevarse a cabo las operaciones de las cuentas de depósito a través de una comunicación en línea, se puede visionar una serie de riesgos genéricos puros, percibidos desde el punto de vista financiero, que pueden afectar el buen desarrollo de dichas operaciones. Estos riesgos genéricos se clasifican de la siguiente manera:

1. Delitos cometidos en contra del patrimonio de las instituciones bancarias y cuenta-habientes.
2. Multa y sanciones.
3. Errores, omisiones o irregularidades que ocasionan ineficiencia en el servicio bancario.
4. Incendios, explosiones, pérdidas y extravíos.

4.2.1 DELITOS COMETIDOS EN CONTRA DEL PATRIMONIO DE LAS INSTITUCIONES BANCARIAS Y CUENTA-HABIENTES.

Las pérdidas que se producen a consecuencia de los delitos y las que se seguirán produciendo si no se toman las medidas de control adecuadas, son superiores a lo que generalmente se reconoce y publica. El vocablo delito deviene del latín *delictum*, el cual significa culpa, crimen, quebrantamiento de la ley. Otras definiciones señalan al delito como: “un acto prohibido, porque produce más mal que bien, esto es, más mal para el paciente que bien para su autor; la violación de un deber exigible, hecha en perjuicio de la sociedad o de los individuos; la lesión de un derecho”.¹⁴

El delito informático se debe entender como aquel hecho, el cual además de provocar un daño, se utiliza cualquier componente de un sistema electrónico de datos para conseguir un fin. Sin embargo éste no ha sido bien entendido, se piensa, como en el caso de la seguridad de incendio o robo que, “eso no le puede suceder a la empresa donde uno labora, o es poco probable que suceda aquí”. En ese sentido, muchos bancos no son conscientes de su nivel real de vulnerabilidad, se tiene la idea que los sistemas no pueden ser violados si no se entra al centro de

¹⁴ Ignacio de Casso y Francisco Cervera, *Diccionario de Derecho Privado*, Editorial Labor, pág. 1390.

ómputo, olvidándose de los riesgos a que están sujetos por el uso de terminales y sistemas remotos de teleproceso.

Es por eso que se ha tomado al delito como un riesgo genérico que puede provocar grandes pérdidas a una institución bancaria. En el código penal, en el título VI, se encuentran tipificado las siguientes clases de delitos en contra del patrimonio:

- a) **Hurto:** Es aquel acto que se realiza al tomar sin la debida autorización, cosa mueble, total o parcialmente ajena.
- b) **Robo:** Quien sin la debida autorización y con violencia anterior, simultánea o posterior a la aprehensión, tomare cosa mueble, total o parcialmente ajena.
- c) **Usurpación:** Comete usurpación quien mediante violencia, engaño, abuso de confianza o clandestinamente, con fines de apoderamiento o de aprovechamiento ilícito, despojare o pretendiere despojar a otro de la posesión o tenencia de un bien inmueble o de un derecho real constituido sobre el mismo, ya sea invadiendo el inmueble, manteniéndose en él o expulsando a sus ocupantes.
- d) **Extorsión:** Quien para procurar un lucro injusto o para defraudarlo obligare a otro, con violencia a firmar, suscribir, otorgar, destruir o entregar algún documento, a contraer una obligación, a condonarla o a renunciar a algún derecho.
- e) **Chantaje:** Comete delito de chantaje quien exigiere a otro, dinero, recompensa o efectos, bajo amenaza directa o encubierta de imputaciones contra su honor o prestigio, o de violación o divulgación de secretos, en perjuicio del mismo, de su familia o de la entidad en cuya gestión intervenga o tenga interés.
- f) **Estafa:** Comete estafa quien induciendo a error a otro, mediante artificio o engaño lo defraudare en su patrimonio en perjuicio propio o ajeno.
- g) **Apropiaciones y Retenciones Indebidas:** Quien en perjuicio de otro, se apropiare o distrajere dinero, efectos o cualquier otro bien mueble que hubiere recibido en depósito, comisión o administración, o por cualquier otra causa que produzca obligación de entregarlos o devolverlos.
- h) **Violación a Derechos de Autor:** Incurrirá a este delito quien fabricare, pusiere en venta o introdujere en la República artículos que, por su nombre, marca, patente,

envoltura, presentación o apariencia, puedan ser confundidos fácilmente con productos similares, patentados o registrados a nombre de otro.

- i) **Daño:** Se comete el delito de daño quien de propósito, destruyere, inutilizare, hiciere desaparecer o de cualquier modo deteriorare, parcial o totalmente, un bien de ajena pertenencia.

Los delitos de hurto, robo, estafa, o en su caso, apropiación irregular, se tendrán por consumados en el momento en que el delincuente tenga el bien bajo su control, después de haber realizado la aprehensión y el desplazamiento respectivo, aun cuando lo abandonare o lo desapoderen de él.

4.2.2 MULTAS Y SANCIONES

Dentro del marco legal guatemalteco, las actividades de una institución bancaria se encuentran regidas principalmente por la Ley de Bancos, Ley Orgánica del Banco de Guatemala, acuerdos de Junta Monetaria y Resoluciones del Superintendente de Bancos.

Bajo esos preceptos, se encuentran reguladas las operaciones de las cuentas de depósito a la vista girables con cheque, principalmente en lo que se refiere al encaje bancario. Este se encuentra definido en el artículo 63 de la Ley Orgánica del Banco de Guatemala, Decreto 215 del Congreso de la República. Dicha definición expone: *Los Bancos estarán obligados a mantener constantemente en el Banco de Guatemala, en forma de depósitos de inmediata disponibilidad, una reserva proporcional a las obligaciones depositarias que tuvieren a su cargo. Dicha reserva, sumada a los fondos en efectivo que los Bancos mantuvieren en Caja, tanto en sus oficinas, principales como en sus sucursales y agencias, constituirá el "Encaje Bancario".*

Los "Encajes Bancarios" deberán alcanzar por lo menos los montos mínimos que establezca la Junta Monetaria, conforme a los preceptos que fije la Ley. Los fondos en efectivo de los bancos de que se ha hecho referencia, en ningún caso podrán representar para los efectos del encaje, una cantidad que exceda del 25% del monto total a que ascienda el encaje requerido.

Dentro de las obligaciones depositarias, sujetas a encaje, que tienen a su cargo las entidades bancarias se encuentran los Depósitos Monetarios, los cuales son definidos en el numeral romano I, inciso a) del artículo 67 de la Ley Orgánica del Banco de Guatemala, como aquellos depósitos que son exigibles a simple requerimiento del depositante por medio de cheques.

En ese sentido, los depósitos monetarios que se manejan a través de redes electrónicas, pueden presentar las siguientes infracciones en relación al encaje:

- a) **Sobregiro en la Cuenta de Encaje:** Este se dará cuando, en las operaciones de un día, el valor total de los cheques emitidos por los clientes de una institución bancaria, regularizado por las operaciones a favor de éstos en la Cámara de Compensación, es superior a lo que el banco tiene depositado en el Banco de Guatemala. El riesgo está en la ocurrencia del sobregiro, si en un día (principalmente en fin de mes) no hubiera comunicación en red y derivado de ello no se pudiera determinar con exactitud el total de los cheques recibidos de otros bancos; además, si se recibieran más cheques en contra de lo normal, los cuales en total sean mayores que las disponibilidades que se tenga en el Banco de Guatemala, ocurriría un sobregiro en la cuenta de encaje del banco de que se trate.
- b) **Posición Negativa de Encaje en el Mes:** El artículo 70 de la Ley Orgánica del Banco de Guatemala, en relación a este tema, describe: *“La posición de encaje de los bancos se establecerá con base en el monto de los encajes computables y de las obligaciones afectas al encaje al fin de cada día. Para los efectos de esta ley, la posición mensual de encaje se define como la suma algebraica de los excesos y las deficiencias de encaje que ocurrieren en cada uno de los días del mes, dividida entre el número de días del mismo mes. Normalmente se aplicará esta definición y, en consecuencia, se permitirá a los bancos compensar cualquier deficiencia en los encajes en uno o más días del mes con los excesos de encaje en los demás días del mismo mes.*

Sin embargo, si dentro del periodo mensual el número de días con deficiencia fuera excesivo, a juicio de la Junta Monetaria, ésta podrá negar a cualquier banco la facultad de compensar las deficiencias con los excesos de encaje; y considerar como posición de encaje la suma de las deficiencias diarias dividida entre el número de días del mes”.

Ahora bien, debido a que los bancos se les permite compensar deficiencias de encaje con excesos, dentro de un mismo mes, los banqueros han adoptado como práctica mantener como encaje únicamente lo necesario, ya que ese es un tipo de reserva no remunerada para los mismos. Por consiguiente, debido a los márgenes bajos que por ese concepto se manejan, los bancos se exponen al riesgo de que por problemas en sus redes electrónicas de comunicación, dejen de operar transacciones que aumenten sus requerimientos de encaje, hasta el punto de que posteriormente se determine que el banco infringió con lo que a ese respecto establece la ley. Esto hará que se le imponga a la institución bancaria una multa sobre el importe de la deficiencia, equivalente a la aplicación de una vez y media la tasa máxima de interés anual que los bancos estén autorizadas a cobrar en sus operaciones activas.

4.2.3 ERRORES, OMISIONES E IRREGULARIDADES QUE OCASIONAN INEFICIENCIA EN EL SERVICIO BANCARIO

La diferencia que existe entre un error y una irregularidad es la intención. Según el Diccionario de la Real Academia Española, error se define como: “Vicio del consentimiento causado por equivocación de buena fe, que anula el acto jurídico si afecta a lo esencial del mismo o de su objeto.”¹⁵ Asimismo, el Diccionario define a la Irregularidad como: “Malversación, desfalco, cohecho u otra inmoralidad en la gestión o administración pública, o en la privada”.¹⁶

¹⁵ Diccionario de la Real Academia Española, decimoctava edición, pág. 555

¹⁶ IBID, pág. 762

Por aparte se dice que hay omisión cuando se ha dejado de hacer algo necesario o conveniente, en la ejecución de una actividad.

Dentro de los errores y omisiones cometidos que se relacionan con una red se encuentran los siguientes:

- a) **Fallos en el Hardware o Software:** Grabar en un disco dañado, caída del sistema de comunicación en línea, falla de un programa operacional, bloqueo de una terminal remota.
- b) **Accidentes:** Incendio no intencional, ruptura de un tubo, explosión, corto circuito.
- c) **Humanos:** Error al digitar el número de cuenta en un depósito, montar la versión equivocada de un programa, utilizar un archivo no actualizado, realizar una rutina que calcule los intereses de los depósitos con error, transmitir información al usuario equivocado.

Asimismo, dentro de las irregularidades más comunes se encuentran las siguientes:

- a) **Fraudes:** Dentro de los actos intencionales, los fraudes son los actos más comunes y perjudiciales. Sus características son la intencionalidad y el engaño. La primera característica es la frontera o diferencia entre el error y el fraude. Quien hace el fraude tiene la intención de engañar, va a diseñar algunos procesos o formas muy particulares, para esconder su acción y para que parezca como error del sistema, o se le impute a otra persona. Siempre aparecen fraudes nuevos. Algunos de los métodos actuales, utilizados para la realización de fraudes son los siguientes: **Caballo de Troya:** Se colocan instrucciones adicionales y/o se modifican las existentes, en un programa, para que además de las funciones propias, efectúe una función no autorizada. Se puede hacer en el software aplicativo u operativo. Es fácil de esconder entre los cientos de instrucciones de un programa. Las instrucciones son introducidas preferencialmente, adicionando el cambio no autorizado al momento de implantar un cambio autorizado. **Técnica del Salami:** Esta técnica se caracteriza por el robo de pequeñas cantidades

desde un gran número de registros, alterando el programa. Los fondos así obtenidos se aplican a una cuenta especial y los totales de control no cambian. A esta técnica se le puede llamar también el caso del redondeo. **La Bomba Lógica:** Con este método se programa una condición o estado específico. Hasta cuando esa condición o estado no se cumpla, el programa funciona conforme a lo autorizado. Cuando la condición o estado se presenta, entonces una rutina o módulo fraudulento realiza la acción no autorizada. Un ejemplo claro de esto, puede ser el problema del año 2,000, ya que es una situación que va a suceder en el futuro. **Trampas-Puertas:** Los sistemas operacionales tienen puertas de acceso, definidas para adaptarlos a las condiciones particulares en una aplicación de un programa. También tienen salidas que permiten transferir el control a un programa escrito por el usuario. Las puertas pueden ser utilizadas para introducir modificaciones no autorizadas, por personal experto en ese software. Las salidas para transferir el control del programa fraudulento. **Intercepción:** Es llamada también captura de la información. La intervención se puede realizar en cualquiera de los circuitos de comunicación, en cualquier punto, como ejemplo se tienen los siguientes: entre terminales y concentradores, entre terminales y computadores, entre computadores y computadores, etc. La intercepción puede realizarse a través de: El cable físico, fibra óptica, microondas, satélite, otros.

- b) **Virus:** Un virus de computador es un programa desarrollado intencionalmente destructivo, escrito a propósito, diseñado para permanecer invisible hasta que se ejecuta. Esto puede dar lugar a extorsión, a través de la venta de la vacuna que venga a remediar el daño hecho por el virus.
- c) **Piratería:** Dentro del campo de la informática, se dice que hay piratería cuando una persona roba o destruye software o hardware a otra. Como ejemplo se puede mencionar el siguiente: Una institución bancaria contrata a un programador para desarrollar un sistema para el cálculo diario de intereses en las cuentas de depósitos monetarios. Posteriormente, se retira algún empleado que tenga acceso a los programas y se los lleva para implementarlos en otro banco.

- d) **Vandalismo:** Dentro de este concepto cabe mencionar todos los delitos en contra del patrimonio de las instituciones bancarias y cuenta-habientes, definidos anteriormente y aplicados a las operaciones a través de redes electrónicas.

4.2.4 INCENDIOS, EXPLOSIONES, PERDIDAS Y EXTRAVIOS

Estos tipos de riesgos son probables que ocurran en cualquier tipo de actividad que se realice y pueden ser causados ya sea por la naturaleza o por el hombre. Los riesgos de pérdida ocasionados por la naturaleza pueden ser: Inundaciones, terremotos, rayos, huracanes, condiciones ambientales extremas y otros. Por otra parte, los hechos realizados por el hombre, en relación al tema de referencia, pueden ser intencionales o no, es decir que pueden convertirse en errores o irregularidades. La falta de un plan de seguridad a la hora de que suceda una catástrofe y la falta de un seguro de computación, puede producir consecuencias desastrosas. Dentro del plan de seguridad se puede incluir lo siguiente: capacitar al personal de una empresa en el uso de extinguidores, indicar rutas de evacuación para casos de emergencia, otros.

Por otro lado, un problema en la transferencia de datos mediante redes electrónicas, se puede suscitar cuando, por algún motivo, se pierda un canal que sirva para tal propósito; sin embargo, en este caso, se deben de tener otras rutas alternas que cumplan con el objetivo deseado. Además habrá que tomar en cuenta que por alguna falla del sistema se puede perder toda la información, por lo que el uso de Back-ups resulta un procedimiento muy importante.

4.3 ADMINISTRACION DE RIESGOS

Una vez identificados y evaluados los riesgos, se encuentra ante la metodología de administrarlos. Para ello se tienen varias alternativas que sucesivamente se comentan:



4.3.1 ELIMINAR

Es una alternativa poco factible para utilizarse con frecuencia ante riesgos de carácter genérico (porque la única forma de evitar todos los riesgos de una empresa es dejar de ser empresa), sin embargo, cabe la posibilidad de que hay ocasiones concretas en que de forma parcial, los riesgos pueden ser evitados.

Se debe recordar que no debe confundirse la prevención de riesgos con la eliminación de riesgos. **La prevención es una actitud ante el riesgo y la eliminación es un método de administrar riesgos.**

4.3.2 TOLERAR

El método de tolerar, consentir, aceptar o mantener, implica correr con ciertos riesgos de forma consciente tras un buen trabajo de análisis de decisiones por parte de la gerencia. Significa que este método resulta difícilmente aplicable con responsabilidad sin una rigurosa evaluación del riesgo.

Normalmente las decisiones de tolerar, recaen en riesgos con muy bajos valores de gravedad. El mantenimiento de este método ante ciertos riesgos hace necesaria una permanente y total atención a los parámetros de probabilidad de que existan pérdidas, tiempos de exposición o presencia de condiciones peligrosas y sus posibles consecuencias. Cualquier variación substancial en estos factores puede aconsejar una decisión diferente a la de tolerar el riesgo.

Tener asumido un riesgo en forma voluntaria es por tanto, una herramienta posible del auditor. Sin embargo, lo que no se puede admitir es la presencia del riesgo de una forma inconsciente o inadvertida.

En ocasiones puede ser aplicada una variante a este método. Es la que podríamos llamar "seguro propio" o creación de un fondo de previsión, el cual se destinaría a absorber las pérdidas si éstas aparecen.

De todas formas, es conveniente que antes de decidir tolerar un riesgo, se considere los siguientes aspectos:

- No arriesgar más de lo que pueda permitirse perder.
- No arriesgar mucho a cambio de poco.
- No decidir sin considerar las posibilidades.

Son preceptos básicos, derivados de lo único seguro que tiene el riesgo: su incertidumbre.

4.3.3 TRANSFERIR

La forma más común de transferencia de riesgos es el contrato de seguro, aunque también existe la posibilidad de las firmas individuales de compromiso.

Para muchos responsables y directivos de empresas, poco preocupados por la previsión y su actitud ante los riesgos, la solución de transferir el riesgo ha sido la única metodología que han recurrido. Cualquier alternativa que se les pudiera brindar para hacer frente a los riesgos podría chocar con esta respuesta: ¡Si ya estamos asegurados!

Esta posición subsiste por el desconocimiento de que normalmente, es la forma más cara de gestionar un riesgo, considerada aisladamente que el seguro no evita la consecuencia, aunque puede disminuir en muchos casos la gravedad de las mismas. Sin embargo, habrá que considerar las cláusulas de la póliza de seguro, principalmente lo referente a los bienes y riesgos excluidos, ya que por falta de conocimiento de las mismas, se podrá estar expuesto a una pérdida no asegurada.

La transferencia del riesgo es indispensable en muchas ocasiones (hasta obligatoria a veces) porque son muy escasas las posibilidades de aplicación del método de eliminar los riesgos (si fuese generalizada esa posibilidad, mal futuro se auguraría a los aseguradores, porque “sin riesgo no hay seguro”) y porque tolerarlos es una solución limitada. Además, no todas las medidas de control al alcance son eficaces al ciento por ciento.

Es un método a considerar, pero es una solución honerosa, siéndolo más cuanto mayor sea el porcentaje de gravedad del riesgo. De ahí la conveniencia de actuar simultáneamente con otros métodos, en busca de la mayor rentabilidad del conjunto de acciones. Son típicos riesgos transferibles los propios fenómenos naturales (catástrofes), los de vida y responsabilidad civil.

4.3.4 TRATAR

La previsión de riesgos y la consiguiente reducción de pérdidas, es el método más eficaz de administrar los riesgos. Consiste en adoptar los medios y los sistemas para tener un adecuado control interno.

La gestión profesional del control interno en el trabajo, es el sistema que ha de dar una adecuada respuesta al auditor para el tratamiento de los riesgos. La planificación, organización, dirección y control, así como las correspondientes actividades asociadas a cada una de esas funciones, tienen su aplicación práctica en el desarrollo del método de tratar los riesgos donde, se incluyen las técnicas para el tratamiento de los mismos.

4.4 NATURALEZA DEL CONTROL INTERNO BANCARIO

El control interno en un banco debe estar adecuado con la naturaleza y escala del negocio. Estos deben incluir disposiciones claras para la delegación de autoridad y responsabilidad, separación de funciones que envuelven el compromiso de la propia entidad bancaria (el reembolso de los depósitos que tengan a su cargo, la contabilización de sus activos y pasivos), una

conciliación de estos procesos, salvaguarda de sus activos, una apropiada auditoría interna y externa independiente, así como velar por el cumplimiento de las leyes y regulaciones aplicables al giro bancario.

En ese sentido, la necesidad de controles en el sistema bancario está vinculada con el propósito de reducir los riesgos a que están sujetas sus operaciones; es decir, que se requiere que el control interno prevenga, detecte y corrija, cuando ocurran, los errores o irregularidades a que están sujetas las operaciones realizadas por éstas instituciones financieras.

4.4.1 ESTUDIO Y EVALUACION DEL CONTROL INTERNO BANCARIO

Para la correcta planificación de la auditoría bancaria, es indispensable que se evalúe el control interno existente, como base para determinar los procedimientos que se van a realizar. De acuerdo con las normas de auditoría en vigor, dicha evaluación permite conocer las operaciones del banco que se examinarán y asimismo, medir el grado de dificultad que se encontrará para desarrollar un trabajo satisfactorio de auditoría. Además permite establecer el grado de confiabilidad que se puede asumir en relación con los procedimientos seguidos por el banco para obtener la información sujeta al examen.

4.5 ELEMENTOS NECESARIOS A CONSIDERAR PARA EL ESTABLECIMIENTO DE UN SISTEMA DE CONTROL INTERNO EN UN SISTEMA DE REDES ELECTRONICAS

De igual forma que en los sistemas procesados por medio no electrónicos, al establecer un sistema de red, se debe tener en cuenta los aspectos teóricos que conforman un sistema adecuado de control interno, a fin de que se incorporen sus elementos en el desarrollo de cualquier actividad.



En ese sentido, el procedimiento a seguir, después de haber identificado los riesgos, será el de establecer un "*Programa Integral de Protección en red*". Este programa se debe llevar a cabo, de acuerdo al siguiente orden:

1. Establecer una cultura organizacional que genere un alto grado de conciencia a todos los niveles involucrados en el sistema, desde los altos ejecutivos hasta el personal operativo.
2. Desarrollar una educación permanente que refuerce a la cultura organizacional. Esta educación permanente hará a la vez que el personal adquiera un compromiso más fuerte hacia el buen funcionamiento del nuevo sistema implantado.
3. Implantación de políticas y estándares de seguridad de red efectivos, que puedan proteger la inversión y recursos de información del banco.
4. Establecimiento de normas y procedimientos que conformen el sistema de control interno que proporcione una efectiva y eficaz seguridad a la institución bancaria en las operaciones realizadas en red.

4.5.1 CULTURA ORGANIZACIONAL

Colocar seguridades y controles en un ambiente en red, sin crear antes una cultura organizacional, es como colocar puertas de acero cuando las paredes son de papel. Es por ello que este es un aspecto vital para el desarrollo de cualquier sistema, ya que a través de que se lleve a cabo una formación integral del personal de una institución, eliminando aspectos negativos como: prepotencia, mala comunicación, incertidumbre, miedo, actitud negativa y otros, se conseguirá de una forma eficaz y efectiva, cualquier objetivo que planea la organización.

4.5.2 EDUCACION PERMANENTE

Además de hacer entender al personal, acerca de la necesidad del control y crear en ellos una filosofía, es importante hacer participar al personal. Sin embargo, para que esa participación sea efectiva, es necesario capacitar a la gente, a fin de que su aporte sea mucho más técnico y preciso. Dicha capacitación hará a la vez, que el personal desarrolle un compromiso más fuerte

con la institución, ya que en la medida que el individuo vaya aprendiendo, asimismo, se le podrá exigir un trabajo más técnico y especializado.

Por otra parte, habrá que tomar en cuenta el costo-beneficio de la capacitación, ya que se puede dar el caso de que se esté capacitando al personal, en beneficio para la competencia. Por consiguiente, la capacitación debe ser parte de un plan de desarrollo integral del recurso humano.

4.5.3 POLITICAS DE SEGURIDAD

Una política de seguridad es indispensable para proteger los recursos e información que tienen las entidades bancarias en las redes. “Una política de red, es un documento que describe los asuntos de seguridad de red de una organización”¹⁷, es el tercer procedimiento efectivo para construir barreras de protección efectivas.

La mayoría de las organizaciones tienen información sensible y secretos importantes en sus redes. Esta información deberá ser protegida contra el vandalismo del mismo modo que otros bienes valiosos.

La mayoría de diseñadores de redes, por lo general, empiezan con la implantación de soluciones de barreras de protección antes de que ningún problema de seguridad de red haya sido identificado en forma acertada. Tal vez una razón para esto sea que, establecer una política efectiva de seguridad de red, signifique formular algunas preguntas difíciles con relación a qué tipos de servicios de trabajo y recursos va a permitir que tengan acceso los usuarios, y cuáles tendrá que restringir debido a los riesgos de seguridad.

Se deberá tener presente que la política de red que se use no disminuya la capacidad del servicio a los clientes de la entidad bancaria. Una política de red que evita que los usuarios cumplan con sus tareas en forma efectiva, puede tener consecuencias indeseables.

¹⁷ Karanjit Siyan y Chris Hare, Internet y Seguridad en Redes, Pág. 89

Existen diferentes tipos de políticas que se pueden implantar, sin embargo la más común es la Política de Seguridad del Sitio.

4.5.3.1 POLITICA DE SEGURIDAD DEL SITIO

Un banco puede tener muchos sitios y cada uno contar con sus propias redes. Si la institución bancaria es grande, es muy probable que los sitios tengan diferentes administradores de red, con diferentes metas alineadas a un solo objetivo. Si estos sitios no están conectados por medio de una red interna, cada uno de ellos podrá tener sus propias políticas de seguridad de red. Sin embargo, si los sitios están conectados por una red interna, la política de red deberá agrupar las metas de todos los sitios que están interconectados. En general, un sitio es cualquier parte del banco que posee computadoras y recursos relacionados con la red. Dichos recursos incluyen, pero no se limitan a los siguientes:

- ◆ Estaciones de trabajo.
- ◆ Computadoras anfitrión y servidores.
- ◆ Dispositivos de Interconexión: compuertas, enrutadores, puentes, repetidoras.
- ◆ Servidores de terminal
- ◆ Software para red y aplicaciones.
- ◆ Cables de red.
- ◆ Información en archivos y bases de datos.
- ◆ Cajeros automáticos.

La política de seguridad del sitio debe tomar en cuenta la protección de estos recursos. Puesto que el sitio está conectado con otras redes, la política de seguridad del sitio debe considerar las necesidades y requerimientos de todas las redes interconectadas. Esto es importante, porque es posible lograr una política de seguridad de red que salvaguarde los intereses de unos cuantos, pero que puede ser perjudicial para otros.

4.5.3.2 COMO ASEGURAR LA RESPONSABILIDAD DE UNA POLITICA DE SEGURIDAD

Un aspecto importante de la política de seguridad de red es asegurar que todos saben cuál es su responsabilidad para manejar la seguridad. Es difícil para una política de seguridad de red anticipar todas las amenazas posibles. La política puede, sin embargo, garantizar que cada tipo de problemas tiene a alguien que puede manejarlo de manera responsable. Asimismo, pueden existir varios niveles de responsabilidad asociados con una política de seguridad de red. Cada usuario de la red, por ejemplo, deberá ser responsable de guardar su contraseña. Un usuario que pone en riesgo su cuenta, aumenta la probabilidad de comprometer otras cuentas y recursos. Por otro lado, los administradores de red y de sistema, son responsables de mantener la seguridad general de la red. Como un ejemplo aplicado a las operaciones bancarias en cuentas de depósitos, se pueden mencionar las siguientes:

- ◆ La política que define a los responsables y quiénes tienen acceso de autorizar sobregiros en cuentas de cheques, en el sistema en red.
- ◆ Definir quiénes tienen acceso a liberar la reserva de cobro que se aplica a los cheques de otros bancos que se reciben para depositar en cuentas de depósitos monetarios .

4.5.4 NORMAS Y PROCEDIMIENTOS QUE CONFORMAN EL SISTEMA DE CONTROL INTERNO PARA UNA RED DE TRANSMISION ELECTRONICA DE DATOS

Definir un sistema de control interno en red para una institución bancaria, significa desarrollar normas y procedimientos que salvaguarden los recursos de la red contra pérdidas y daños. Un planteamiento posible para desarrollar este sistema es el análisis de lo siguiente:

- ◆ ¿Qué recursos se deben proteger?
- ◆ ¿De qué personas se necesita proteger a los recursos?
- ◆ ¿Qué tan reales son las amenazas?



- ◆ ¿Qué tan importante es el recurso?
- ◆ ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?
- ◆ Examinar con frecuencia su sistema de control interno de red para verificar si sus objetivos y circunstancias en la red han cambiado.

El siguiente cuadro, muestra una hoja de trabajo que se puede emplear para ordenar las ideas respecto a estos planteamientos:

HOJA DE TRABAJO PARA DESARROLLAR UN PLANTEAMIENTO DE SEGURIDAD

Recursos de la Red			Tipo de Usuarios Indeseables	Posibilidad de una Amenaza	Medidas a Implantar para Proteger los Recursos de Red
Número	Nombre	Importancia del Recurso			

- ◆ La columna "*Número de Recursos de la Red*" es un número de red de identificación interna de los recursos a ser protegidos (si es que se aplica), por ejemplo: el número de inventario del recurso que se examina.
- ◆ La columna "*Nombre de los Recursos de la Red*" es una descripción de los recursos, por ejemplo: un servidor que archiva los datos de las cuentas de depósitos monetarios.
- ◆ La columna "*La Importancia del Recurso de la Red*" puede estar en una escala numérica del cero al diez, o en expresiones tales como: bajo, medio, alto, muy alto, otros.
- ◆ La columna "*Tipo de Usuarios Indeseables*" puede tener calificativos como interno, externo, huésped, o nombres de grupo como usuarios de cuenta, asistentes corporativos, otros. Ejemplo: Los encargados de Servicio y Atención al Público, que no tengan acceso al menú de pago de cheques o depósitos, los cuales tienen acceso los receptores-pagadores.
- ◆ La columna "*Posibilidad de una amenaza*" puede estar en una escala numérica de cero a diez, o en expresiones tales como: baja, media, alta, muy alta, otros.
- ◆ Y la columna "*Medidas a Implantar para Proteger los recursos de Red*" puede tener valores como *permisos del sistema operativo* para archivos y directorios, *pistas/alertas de auditoría* para servicios de red, *enrutadores de selección* y *barreras de protección* para anfitriones y dispositivos de red, o cualquier otra descripción del tipo de control de seguridad.

En general, el costo de proteger una red de una amenaza debe ser menor que el costo de la recuperación, si es que se ve afectado por la amenaza de seguridad. Si no se tiene el conocimiento suficiente de lo que desea proteger y de las fuentes de la amenaza, lograr un nivel aceptable de seguridad podrá ser difícil. El auditor no debe dudar en emplear la ayuda de otros usuarios con conocimiento especializado, con relación a los bienes de la red que se desee proteger y las posibles amenazas en contra de ésta.

Por ello, es importante involucrar al tipo adecuado de personas en el diseño del sistema de control interno que proporcione seguridad a la red y dentro de éste, sin lugar a dudas, debe participar el auditor. Este grupo de personas, podrían incluir a aquellos involucrados en las

siguientes ramas: Auditoría, grupos de sistemas de información de campo y organizaciones relacionadas con la seguridad física. Si se desea un soporte universal del sistema de control interno en red, es importante involucrar a estos grupos para contar con su cooperación y aceptación del sistema de seguridad de red que se desea implantar.

4.5.4.1 ANALISIS DE RIESGOS

Al crear un sistema de control interno de red, es importante entender que la razón para crear una medida es, en primer lugar, establecer que los esfuerzos invertidos en la seguridad son costeables. Esto significa que se debe entender cuáles recursos de la red vale la pena proteger, y que algunos recursos son más importantes que otros, por ejemplo: el servidor que contiene todos los archivos de todas las cuentas de depósitos monetarios, frente a una terminal de una agencia, que posee únicamente una determinada cantidad de firmas. También se deberá identificar la fuente de amenaza de la que se protege a los recursos. A pesar de la cantidad de publicidad sobre intrusos en una red, varias encuestas indican que para la mayoría de las organizaciones, la pérdida real que proviene de los “miembros internos” es mucho mayor.

El análisis de riesgos implica determinar lo siguiente:

- ◆ Qué necesita proteger.
- ◆ De quién debe protegerlo.
- ◆ Cómo Protegerlo.

Los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso. “Según los autores Karanjit Siyan y Chris Hare, en su libro: Internet y Seguridad en Redes, en el análisis de riesgos, es necesario determinar los siguientes factores:

1. Estimación del riesgo de pérdida del recurso (Ri).
2. Estimación de la importancia del recurso (Wi).

Como un paso hacia la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico. Por ejemplo, al riesgo (R_i) de perder un recurso se le asigna un valor de cero a diez, donde cero indica que no hay riesgo y diez es el riesgo más alto. De manera similar, a la importancia de un recurso (W_i) también se le puede asignar un valor de cero a diez, donde cero significa que no tiene importancia y diez es la importancia más alta. La evaluación general del riesgo será entonces el producto numérico del valor del riesgo y su importancia (también, llamado el peso). Esto puede escribirse como sigue:

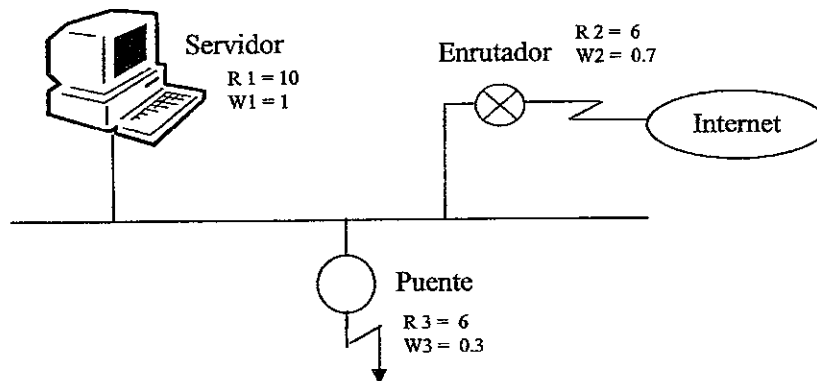
$$WR_i = R_i * W_i$$

W_i = Peso del riesgo del recurso

R_i = Riesgo del recurso

W_i = Importancia de Recurso¹⁸

En la presente figura se muestra una red simplificada, con un servidor, un enrutador y un puente. Los administradores de sistemas han producido las estimaciones siguientes para el riesgo y la importancia de los dispositivos en la red.



¹⁸ IBID, pág. 94

Servidor = 1	Enrutador = 2	Puente = 3
R1 = 10	R2 = 6	R3 = 6
W1 = 1	W2 = 0.7	W3 = 0.3

El cálculo de los riesgos evaluados de estos dispositivos se muestra a continuación:

Servidor:

$$WR1 = R1 * W1 = 10 * 1 = 10$$

Enrutador:

$$WR2 = R2 * W2 = 6 * 0.7 = 4.2$$

Puente:

$$WR3 = R3 * W3 = 6 * 0.3 = 1.8$$

El siguiente cuadro muestra una hoja de trabajo que el auditor puede utilizar para registrar los cálculos previos:

HOJA DE TRABAJO PARA EL ANALISIS DE RIESGO DE SEGURIDAD EN LA RED

Recurso de Red		Riesgos de los Recursos de Red (Ri)	Importancia del Recurso (Wi)	Riesgo Evaluado (Ri*Wi)
Número	Nombre			
1	Servidor	10	1	10
2	Enrutador	6	0.7	4.2
3	Puente	6	0.3	1.8

- ◆ La columna “*Numero de Recursos en Red*” es un número para identificación interna del recurso en la red (si aplica).
- ◆ La columna “*Nombre de los Recursos de Red*” es una descripción de los recursos.
- ◆ La columna “*Riesgo para los recursos de Red (Ri)*” puede estar en una escala numérica del cero al diez, o en expresiones como: bajo, medio, alto, muy alto, otros.
- ◆ De manera similar, la columna “*Importancia del Recurso (Wi)*” puede estar en una escala numérica del cero al diez, o en expresiones como bajo, medio, alto, muy alto, otros.
- ◆ Si utiliza valores numéricos para las columnas de riesgo e importancia, puede calcular el valor en la columna “*Riesgo Evaluado (Ri*Wi)*” como el producto de los valores riesgo e importancia.

“Con la siguiente fórmula es posible calcular el riesgo general de los recursos de la red:

$$WR = (R1*W1 + R2*W2 + \dots + Rn*Wn) / (W1 + W2 + \dots + Wn)^{19}$$

Para el ejemplo anteriormente visto, el cálculo del riesgo general es el siguiente:

$$WR = (R1*W1 + R2*W2 + R3*W3) / (W1 + W2 + W3)$$

$$WR = (10 + 4.2 + 1.8) / (1 + 0.7 + 0.3)$$

$$WR = 16 / 2$$

$$WR = 8$$

Otros factores que se deben considerar para el análisis del riesgo de un recurso de red son su disponibilidad, su integridad y su carácter confidencial. La disponibilidad de un recurso es la medida de qué tan importante es tenerlo disponible todo el tiempo. La integridad de un recurso es la medida de qué tan importante es que éste o los datos del mismo sean consistentes. Esto es de particular trascendencia para los recursos de bases de datos. El hecho de ser confidenciales se aplica a los recursos, como archivos de datos, a los cuales se desea restringir el acceso.

¹⁹ IBID, pág. 96

4.5.4.2 COMO IDENTIFICAR RECURSOS

Al realizar un análisis de riesgo, se debe identificar los recursos cuya seguridad esté en posibilidad de ser quebrantada. Recursos como el hardware, están obviamente en lista, pero recursos como las personas que utilizan los sistemas, con frecuencia se ignoran. Es importante identificar todos los recursos de la red que podrían ser afectados por un problema de seguridad.

A continuación se hace una lista de algunos recursos de red que deben ser considerados al estimar las amenazas a la seguridad general, o que podrían interrumpir los servicios que proporciona una institución bancaria (la misma no tiene carácter restrictivo):

1. **Hardware:** Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores de terminal, enrutadores.
2. **Software:** Programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicación.
3. **Datos:** Durante la ejecución, almacenados en línea, archivados fuera de línea, apoyos, bitácoras de auditoría, bases de datos, en tránsito sobre medios de comunicación.
4. **Humanos:** Usuarios, personas para operar sistemas.
5. **Documentación:** Sobre programas, hardware, sistemas, procedimientos administrativos locales.
6. **Accesorios:** Papel, formas, cintas, información grabada.

4.5.4.3 COMO IDENTIFICAR LAS AMENAZAS

Una vez identificados los recursos que necesitan protección, se deben identificar cuáles son las amenazas a tales recursos. Así, las amenazas podrán examinarse para determinar qué potencial de pérdida existe.

A continuación se describe algunos tipos de amenazas:

- a) **Definición de Acceso no Autorizado:** Sólo se permite el acceso a los recursos de red a usuarios autorizados. Una amenaza común es el acceso no autorizado a los recursos de cómputo, el cual puede ser de diversas formas, como utilizar la identificación de otro usuario para obtener acceso a la red y sus recursos. La gravedad de esta amenaza depende del sitio y la naturaleza de la pérdida potencial, ya que para algunos sitios el hecho de permitir acceso a un usuario no autorizado podrá causar daños irreparables, ante la falta de seguridad para cubrir los medios.
- b) **Riesgos de Divulgar Información:** La divulgación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza. Se deberá determinar el valor o sensibilidad de la información guardada en las computadoras. Las instituciones financieras mantienen información confidencial, su divulgación podría ser dañina a sus clientes y para la reputación misma de la organización. La gente a menudo supone que las intrusiones a la red y a las computadoras son hechas por individuos que trabajan de manera independiente. Esto no siempre es así. Los peligros del espionaje industrial y gubernamental sistemático son hechos reales.
- c) **Servicio Denegado:** Las redes enlazan recursos valiosos como computadoras y bases de datos, proporcionan servicios de los cuales depende una organización. La mayoría de los usuarios de esas redes confía en estos servicios para realizar de manera eficiente su trabajo. Si estos servicios no están disponibles, hay una pérdida de productividad. Un ejemplo clásico es cuando no hay comunicación en los bancos, y se tienen que esperar varias horas para realizar una operación sencilla, como lo es el cambio de un cheque.

4.5.4.4 COMO IDENTIFICAR A QUIEN SE LE DEBE PERMITIR UTILIZAR LOS RECURSOS DE LA RED

Para ello debe hacerse una lista de los usuarios que requieran ingresar a los recursos de la red, sin embargo no será necesario tomar en cuenta a cada usuario en particular, sino se deben identificar grupos de usuarios, tales como: Jefes de Agencia, Jefes de Departamento, Receptores-Pagadores, Visas de Cheques, otros. Hay que tomar en cuenta que se deberá incluir una clase de

usuarios externos. Estos son los usuarios que pueden tener acceso a la red desde cualquier parte, como las estaciones individuales de trabajo u otras redes, o bien clientes, para que puedan realizar operaciones y consultas a sus cuentas de depósitos, desde sus oficinas u hogares.

Por aparte, se tendrá que tomar en cuenta las siguientes consideraciones acerca de este tema:

- a) **Identificar el Uso Correcto de un Recurso:** Después de determinar a cuáles usuarios se les permite ingresar a los recursos de la red, posteriormente se tendrá que proveer guías para el uso aceptable de estos recursos. La política debe establecer qué tipos de uso de red son aceptables e inaceptables, y qué tipo de uso será restringido. Asimismo, deberá decir con claridad que los usuarios individuales son responsables por sus acciones. La responsabilidad de cada usuario existe además de los mecanismos de seguridad implantados. No tiene sentido construir mecanismos de seguridad de barreras de protección costosas, si un usuario puede divulgar la información mediante la copia de archivos en disco duro o cinta, y haciendo disponibles los datos para individuos no autorizados.
- b) **Identificar quién esta Autorizado a Otorgar Acceso y a Aprobar el Uso:** Por otra parte, también se deberá identificar a quien se le autorizará otorgar acceso a sus servicios, así como qué tipo de acceso podrán otorgar estos individuos. El reto es balancear el acceso restringido con privilegios especiales para hacer frente a la red más segura, esto es, darle acceso a la gente que necesita estos privilegios para llevar a cabo su trabajo. En general, se deberá otorgar sólo el privilegio necesario para desempeñar las tareas necesarias. Si a la gente que se le otorga privilegios, no son sujetos legales ni responsables, se corre el riesgo de crear lagunas en el sistema y otorgamiento inconsistente de permisos a usuarios. Estos sistemas son invariablemente difíciles de manejar.
- c) **Determinar la Responsabilidad del Usuario:** El sistema de control interno, deberá definir los derechos y responsabilidades de los usuarios al utilizar los recursos y servicios de la red.

- d) **Determinar las Responsabilidades de los Administradores del Sistema:** El administrador de sistemas con frecuencia necesita recabar información de los archivos en los directorios privados de los usuarios para diagnosticar problemas del sistema. Los usuarios, por otro lado, tienen derecho de mantener su privacidad. Las normas internas deberán especificar el límite hasta dónde los administradores del sistema podrán examinar los directorios y archivos privados del usuario para el diagnóstico de problemas del sistema, y para investigar las violaciones de seguridad. Si la seguridad está en riesgo, la política deberá permitir a los administradores mayor flexibilidad para que se corrija los problemas de esta índole.
- e) **Que Hacer con la información delicada:** Desde el punto de vista de seguridad, los datos delicados en extremo, deberían restringirse a algunos anfitriones y administradores del sistema. Antes de otorgar el acceso a los usuarios a un servicio en un anfitrión, es necesario considerar qué servicios e información existen y a los cuales puede ingresar un usuario. Si el usuario no tiene necesidad de manejar los datos delicados, entonces no debería tener una cuenta en un sistema que contiene dicho material.

5.4.5 PLAN DE ACCION CUANDO LA POLITICA DE SEGURIDAD HA SIDO VIOLADA

Cada vez que se viola la política de seguridad, el sistema se abre a amenazas de pérdida. La política de seguridad y su implantación deben evitar obstruir el sistema, en lo posible. Si la política de seguridad es demasiado restrictiva o no está bien explicada, es muy posible que sea violada.

Cuando se detecte una violación a la política de seguridad, se debe clasificar si la violación ocurrió por una negligencia personal, un accidente o error, ignorancia de la política actual o ignorancia deliberada a la política. En este último caso, la violación pudo haber sido realizada no sólo por un individuo, sino por un grupo, que realizan conscientemente un acto de violación directa de una política de seguridad. En cada una de esas circunstancias, la política de

seguridad debe ofrecer guías sobre las medidas a tomar de inmediato. Es razonable esperar que el tipo y severidad de la acción corresponda a la severidad de la violación.

4.5.4.6 COMO RESPONDER A LAS VIOLACIONES DE LA POLITICA

Cuando una violación sucede, la respuesta depende del tipo de usuario que causó la violación, ya que éstos pueden ser locales o externos. La diferencia entre ello se basa más que nada en límites de red, administrativos, legales o políticos.

Es necesario definir acciones basadas en el tipo de violación. Los usuarios internos y externos de la red deben conocer la política de seguridad. Si existen usuarios externos que utilizan la red de manera legal, es responsabilidad de la institución verificar que estos individuos tengan un conocimiento general de las políticas establecidas.

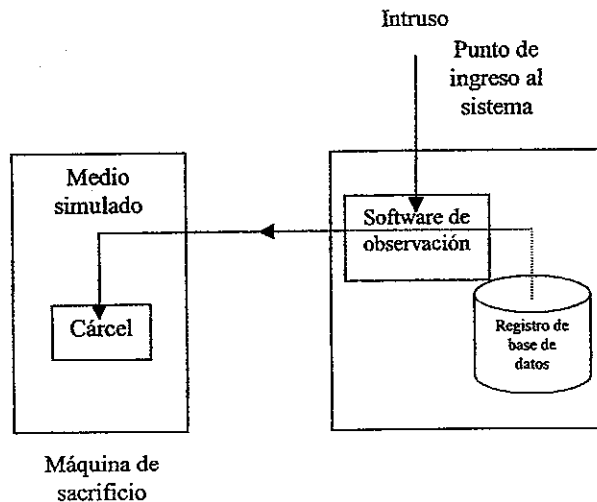
Hay dos tipos de respuestas a incidentes de seguridad: proteger y proceder, perseguir y procesar. Si los administradores de seguridad sienten que la red del banco es bastante vulnerable, podrán elegir la estrategia de proteger y proceder. La meta de esta política es proteger de manera inmediata la red y restaurarla a su estado normal para que los usuarios puedan seguir utilizándola. A veces no es posible restaurar la red de manera inmediata a su operación normal, por lo que se deberá aislar segmentos de la red y cerrar sistemas, con el objeto de prevenir mayor acceso no autorizado al sistema. Una desventaja de esto es que los intrusos saben que han sido detectados e iniciarán acciones para evitar ser rastreados. También el intruso podrá reaccionar a su estrategia de protección mediante el ataque al sitio con una estrategia diferente; por lo menos, el intruso continuará su destrucción en otra parte.

El segundo enfoque (perseguir y procesar) adopta la estrategia de que la mejor meta es permitir a los intrusos seguir con sus acciones mientras se observan sus actividades. Esto deberá hacerse tan disimuladamente como sea posible, para que los intrusos no se den cuenta de que están siendo observados. Las actividades del intruso deberán registrarse, para que existan pruebas disponibles en la fase de acusación de la estrategia. Este procedimiento es el que recomiendan las

agencias de la ley y fiscales, porque esto genera pruebas que esas agencias pueden usar en el procesamiento de los intrusos. La desventaja de esto es que el intruso continuará robando información o haciendo otros daños y la empresa será vulnerable a las demandas que resulten del daño al sistema y la pérdida de información.

Una forma posible de vigilar a los intrusos sin causar daño al sistema es construir una "cárcel". Una cárcel, en este caso, es un medio simulado para que lo utilice el intruso y para que sus actividades puedan ser observadas. El medio simulado presenta datos falsos, pero el sistema se prepara de tal forma que las actividades del intruso sean detectadas.

Para construir una cárcel, es necesario tener acceso al código fuente del sistema operativo y talento de programación de la compañía que pueda simular este medio. Es más seguro construir la cárcel con el uso de una máquina de sacrificio en un segmento aislado de la red para minimizar el riesgo de contaminar otros segmentos de ésta y sistemas por las actividades del intruso. También es posible construir la cárcel mediante el uso de un medio simulado de software, aunque esto es más difícil de preparar. A continuación se muestra una figura que permite tener una idea general para construir una cárcel:



4.5.4.7 COMO VIGILAR EL USO DEL SISTEMA

El administrador del sistema puede realizar periódicamente la vigilancia de la red. De la misma manera, es posible utilizar un software creado para la vigilancia del sistema que incluye la observación de varias de sus partes y la búsqueda de algo inusual.

Esta deberá hacerse en forma regular. No es suficiente hacerla cada mes o cada semana, pues esto dejaría una brecha en la seguridad sin ser detectada por un largo tiempo. Algunas brechas de seguridad pueden ser detectadas unas horas después de que suceden, en cuyo caso la vigilancia semanal o mensual no servirá de mucho. La meta de la vigilancia es detectar la brecha en la seguridad con oportunidad para responder de manera apropiada.

Algunos de los métodos que se pueden utilizar son los siguientes:

- a) Comparar la lista de usuarios registrados con historiales de registros anteriores. Acá se podrá detectar si un usuario muestra actividad de registro fuera de las horas normales, lo cual será motivo de alerta.
- b) Examinar los historiales de cuentas con propósitos de cobranza y detectar patrones de uso inusual en el sistema.
- c) Las compuertas de las barreras de protección pueden utilizarse para obtener un registro de acceso a la red, el cual deberá ser vigilado con frecuencia.
- d) Si tiene recursos especiales que desee vigilar, se podrá construir herramientas propias de vigilancia con el uso de utilerías estándares del sistema operativo.

4.5.4.8 COMO UTILIZAR LA ENCRIPCIÓN PARA PROTEGER LA RED

La encriptación puede utilizar los datos en tránsito así como los datos guardados. Algunos vendedores ofrecen dispositivos de encriptación de hardware que pueden emplearse para encriptar y desencriptar datos en conexiones de punto a punto.

La encriptación puede definirse como “el proceso de tomar información que existe de manera legible y convertirlo en una forma que otros no puedan entender”²⁰

Si el receptor de los datos encriptados desea leer los datos originales, éste deberá convertirlos al original mediante un proceso llamado descryptación. La descryptación es el proceso inverso de la encriptación. Para realizar la conversión de los datos, el receptor debe poseer una pieza especial llamada clave. Es necesario guardar y distribuir la clave con cuidado.

La ventaja al usar la encriptación es que, aunque otros métodos para proteger sus datos (listas de control de acceso, permiso de archivo, contraseñas, etc.) fueran vencidos por un intruso, sus datos todavía carecerán de significado para él.

6 CLASIFICACION DE CONTROLES INTERNOS

El objetivo principal de una evaluación de auditoría, es la identificación de los controles requeridos para proteger los recursos que están comprometidos en el sistema operativo analizado. En ese sentido, se analizarán a continuación la clasificación de los controles internos, aplicados a las operaciones de las cuentas de depósito monetario realizadas a través de redes electrónicas.

6.1 SEGUN SU COBERTURA

Controles Generales: Son los que se aplican a más de un sistema operativo. Un ejemplo sería la política de red que deberá agrupar las metas de todos los sitios que están interconectados por una red interna, en donde cada sitio tiene un diferente administrador de red.

Controles Particulares: Son los que se aplican a un determinado sistema operativo. Un ejemplo sería la utilización del mecanismo *chroot*, en un sistema Unix para hacer una

IBID, pág. 132

cárcel. Con este mecanismo se evita el acceso hacia los archivos de los dispositivos y a archivo real de contraseñas (/etc/passwd).

Controles Específicos: Son los que se refieren a un determinado recurso o grupo de recursos en un sistema operativo. Su aplicación puede citarse en el control interno que lleva una persona que otorga el acceso a un sistema operativo.

4.6.2 SEGUN SU NATURALEZA

Controles Manuales: Son los que deben ser aplicados por los recursos humanos que participan en la administración del sistema operativo. Como ejemplo se puede mencionar la política de seguridad en la red que debe definir los derechos y responsabilidades de los usuarios al utilizar los recursos y servicios de la misma.

Controles Automáticos: Normalmente son los controles incorporados en los programas del computador. Una aplicación de este control es la generación de copias de seguridad automáticas que resguardan los archivos matrices en caso de posibles pérdidas.

4.6.3 SEGUN SU PROPOSITO

Controles Disuasivos: Son medidas orientadas a desanimar a las personas para que no lleven a cabo acciones que podrían transformarse en amenazas para los recursos protegidos. Un ejemplo lo constituye la encriptación que puede utilizarse para proteger los datos en tránsito así como los datos guardados. La ventaja de este método es que si fueran vencidos otros controles (lista de control de acceso, contraseñas, etc.) los datos carecerían de significado para el intruso.

Controles Preventivos: Son las medidas encaminadas a evitar una amenaza. Están ubicados de tal forma que entran en operación cuando los controles disuasivos no han funcionado, teniendo la característica de ser los controles de menor costo. A manera de

referencia puede citarse la segregación de funciones que debe existir entre la responsabilidad de la custodia y el manejo del procesamiento de la información.

Controles Detectivos: Son las medidas orientadas a detectar la presencia de las amenazas y pueden impedir la continuidad de un proceso. No impiden que ocurra un error, pero dan la alarma después que ha ocurrido. Requieren de ciertos gastos operativos moderados. Puede hacerse referencia al dígito verificador en una cuenta de depósitos monetarios consistente en un número, generalmente el último de un campo de identificación, que es una función matemática de todos los demás dígitos en el campo. La validez de todo el campo se comprueba al calcular con base en los demás dígitos, el dígito verificador, y se compara con el número consignado en el campo.

Controles Correctivos: Son las medidas aplicables en el momento en que se haya materializado una amenaza, o sea, cuando ya se está ante la ocurrencia del riesgo. Ayudan a la investigación y corrección de las causas de los errores detectados. Por ejemplo, las estrategias de respuesta que se pueden utilizar cuando un usuario, interno o externo, se introduce sin autorización a un programa en la red. Dichas estrategias a incidentes de seguridad son, en síntesis, proteger y proceder o perseguir y procesar, como se mencionó con anterioridad.

Controles Recuperativos: Como su nombre lo indica son las medidas orientadas a recuperar o compensar las consecuencias de los riesgos acaecidos. Los back-ups que deben realizarse con alguna frecuencia, constituyen un ejemplo de este tipo de control.

4.6.4 SEGUN SU ESTADO

Controles Implantados: Son las medidas resultantes de la evaluación, aceptadas por los administradores del sistema y efectivamente puestas en práctica.

Controles por Implantar: Son las medidas resultantes de la evaluación de auditoría, aceptadas por los administradores del sistema y que están en proceso de implantación.

Controles Descartados: Son aquellos controles que luego de su análisis, la administración del área operativa decide no implantar. El hecho de que la administración descarte un determinado control no significa que el auditor deba acogerse a esta decisión, si fuera el caso la auditoría deberá insistir en su recomendación. Es importante que se tenga una documentación permanente de estos controles para evidenciar las recomendaciones en caso de que llegaran a materializarse las amenazas o riesgos que se pretendían proteger.

Por otra parte, es importante tomar en cuenta el costo que significa proteger las redes de una amenaza, la cual debe ser menor que el costo de su recuperación (relación costo-beneficio).

4.7 TIPOS DE CONTROL INTERNO EN EL PROCESO DE DATOS

Los controles internos se implantan durante el ciclo del procesamiento electrónico de datos; es decir, cuando los datos se ingresan en la red, se realiza la transmisión al computador central, se ejecuta el proceso para el cual se ingresaron los datos, generando una actualización de los mismos, y se finaliza con el resultado o salida de la información deseada.

En síntesis, se detallan a continuación los tipos de control interno en el procesamiento de datos:

- Origen o entrada de la transacción
- Transmisión
- Procesamiento

- Almacenamiento de datos y acceso
- Salida

.1 CONTROLES EN LOS DATOS DE ENTRADA

Estos controles se diseñan para proporcionar una seguridad razonable de que todos los datos recibidos han sido debidamente autorizados, convertidos a un formato y lenguaje comprensible por el equipo, e identificados para que los mismos no se pierdan, supriman, dupliquen, dupliquen o cambien en forma inadecuada. Dentro de estos controles se encuentran:

- El uso de una clave de acceso.*** La primera defensa en contra del acceso no autorizado a un sistema en red es el archivo de claves de entrada al sistema (password). Este consiste en identificar efectivamente a cada usuario en la red, así como restringir el acceso a la información, monitorear las actividades de acceso y prevenir la revelación y/o modificación no autorizada de datos. Sin embargo, éste puede ser el punto más débil si no se toman las medidas preventivas necesarias, a fin de que dicho control cumpla su cometido. Algunas medidas preventivas pueden ser: que la clave cuente con un mínimo de ocho caracteres, que sea de naturaleza alfanumérica, cambiarla periódicamente, no debe ser almacenada en la memoria del computador ni ser mostrada o impresa cuando se digita en la terminal.
- Dígito verificador.*** Este control es de gran utilidad sobre todo cuando deben manejarse gran cantidad de cuentas y movimientos, tal es el caso de las cuentas de depósitos monetarios. El uso del mismo constituye un método adecuado para evitar cambios de números entre cuentas.

1.2 CONTROLES DE TRANSMISION

Son necesarios para asegurar la integridad de la transmisión y detectar errores que afectan tiempo de respuesta. Algunos de estos controles son:

[



- a) **Identificación de terminal.** Las direcciones individuales de la terminal serán usadas para asegurar solamente terminales autorizadas que están conectadas a la aplicación usada en conjunción con la identificación del usuario y el software de control de acceso.
- b) **Identificación de usuario.** El uso de palabras claves, tarjetas o verificación de firma sirven para asegurar que solamente los individuos autorizados tienen acceso permitido a la red y a la aplicación.
- c) **Tablas de autorización de usuarios.** Consiste en una lista de usuarios autorizados para acceder a la red, en sus distintas funciones y archivos.
- d) **Encriptación.** Reduce el riesgo de descubrimiento y alteración de la información.
- e) **Circuitos Dedicados.** Es una línea de transmisión de un punto a otro que es usada para transmitir datos entre dos lugares, lo cual es más seguro que un circuito de discado o conmutado.
- f) **Respaldo de la red.** Consiste en establecer una línea alterna en caso de que falle la línea principal que comunica a la red.

4.7.3 CONTROLES DE PROCESAMIENTO

Estos controles están diseñados para proporcionar seguridad razonable de que el procesamiento de datos se ha llevado a cabo como lo planeado respecto a una aplicación específica; es decir, todas las transacciones son procesadas como fueron autorizadas, en otros términos, las transacciones autorizadas se incluyen y las no autorizadas se omiten. Entre las técnicas de control de proceso se encuentran:

- a) **Control de totales.** Consiste en cotejar totales de datos de entrada contra totales de procesamiento.
- b) **Marcas identificadoras de archivo.** Estas pueden ser externas (como etiquetas) e internas, las que son incorporadas dentro de los archivos para ser cotejadas contra las instrucciones del programa, condición para iniciar o finalizar un proceso.

- c) **Verificación de límites y grados de razonabilidad.** Este proceso determinará que la información se encuentre dentro de los límites establecidos y los datos sean razonables.
- d) **Verificación de fechas.** Por medio de las fechas de ejecución que ingresa el operador al computador se pueden comprobar que los datos son válidos. Por ejemplo, si se quiere consultar el movimiento registrado en una cuenta de depósitos monetarios de un día determinado, se accesa a la cuenta en la red y se indica la fecha que se desea consultar.
- e) **Expiración de archivos.** Consiste en resguardar archivos, que por considerarse de importancia, deben mantenerse por determinados períodos de tiempo. Este control puede implementarse en el software de cada aplicación en forma automática.

4.7.4 CONTROLES DE ALMACENAMIENTO DE DATOS

Estos controles son aplicados a la información que es procesada. Dentro de los mismos figuran:

- a) **Back-ups.** Esta técnica indica que los archivos deben estar respaldados por lo menos por dos copias de la versión en uso, para permitir en determinado momento su recuperación. La retención de los archivos vigentes de datos, archivos maestros más antiguos y archivos de transacciones necesarios para ponerlos al día, son importantes para continuar el procesamiento en caso de un desastre, accidente, imprevistos u otra eventualidad.
- b) **Respaldo de los procedimientos.** Los manuales de procedimientos también son necesarios, por lo tanto, copias de todos los procedimientos relacionados con un sistema de red deben estar almacenados en un lugar seguro. Estos incluyen, entre otros, manuales sobre los sistemas y normas de programación, biblioteca de documentación y de archivos, procedimientos de control de datos y procedimientos que señalan los planes para las operaciones de red durante las emergencias.

- c) *Respaldo de los programas.* El respaldo de los programas consiste en dos áreas básicas: el software del sistema operativo y el software de las aplicaciones. Este respaldo debe estar por lo menos en dos copias de la versión en uso, una copia debe estar almacenada en la biblioteca de cintas y discos (llamada también Cintoteca) para que esté inmediatamente disponible en caso de que se dañe la que está en uso, y la otra copia debe estar en un sitio seguro en otro local (usualmente son los programas originales).

4.7.5 CONTROLES DE LA INFORMACION DE SALIDA

Estos controles están diseñados para asegurar la corrección del resultado del procesamiento y que solamente el personal autorizado pueda recibir la información. La corrección de los resultados del procesamiento incluyen tanto archivos actualizados como informes impresos. Este objetivo se puede satisfacer conciliando los totales de entrada con los totales de salida, y comparando la información con los documentos fuente. Como parte de estos controles se encuentran:

- a) *Respecto a las salidas del proceso:*
- Verificación del total de registros leídos contra el total de grabados, más rechazos si existen.
 - Conciliación de los totales o cifras de control de los datos de entrada contra los totales de la información de salida.
 - Comprobación de que el saldo inicial de una cuenta sea igual al saldo final del proceso anterior.
 - Revisión de que la información de salida esté completa, en formularios correctos y adecuadamente impresa.
 - Que los reportes sean los que corresponden y que fueron solicitados.
- b) *Verificación de detalle.* Es la que se ejerce con aquellos datos o informaciones relevantes, haciéndose verificaciones con procedimientos manuales y de punteo de

los datos principales. Un ejemplo lo constituye el cuadro que se debe realizar en las operaciones de las cuentas de depósitos monetarios; entre los reportes del procesamiento electrónico de datos, los saldos que refleja contabilidad y los documentos fuente (depósitos y cheques).

- c) **Pruebas integradas.** Permiten verificar que los controles establecidos por medio de programas funcionan adecuadamente y de acuerdo a lo previsto. Estas pruebas se llevan a cabo a través del equipo y constituyen un procedimiento de control muy eficaz para evaluar los controles programados.

Con este último tema se analizaron los elementos necesarios a considerar para el establecimiento de un sistema de control interno en una red de procesamiento electrónico de datos. Estos factores deben formalizarse en una política que le ayude a una institución bancaria a identificar las amenazas de seguridad, realizar análisis de riesgos y determinar cómo proteger los recursos en la red a través de la realización de operaciones en cuentas de depósitos monetarios.

En el siguiente capítulo se analizarán directrices que permitirán evaluar el control interno en dichas operaciones, realizadas a través de una red electrónica, con la participación del auditor.

CAPITULO V
PARTICIPACION DE AUDITORIA INTERNA
EN LA IMPLANTACION Y EVALUACION DEL CONTROL INTERNO
DE LAS OPERACIONES DE DEPOSITO A LA VISTA,
GIRABLES CON CHEQUE
A TRAVES DE UNA RED ELECTRONICA

Uno de los objetivos del Auditor Interno es velar que el control interno implantado sea efectivo, de manera que cualquier irregularidad no pueda existir por un tiempo prolongado sin ser detectada. Normalmente, los Auditores Internos deben estar siempre alerta ante la posibilidad de los fraudes. La confabulación de dos o más empleados puede ocultar el fraude por un tiempo, pero es responsabilidad del Auditor Interno hacer que los controles detecten las desviaciones de los procedimientos preestablecidos.

5.1 ACTUACION DEL AUDITOR INTERNO EN LA IMPLANTACION DE UN SISTEMA DE REDES ELECTRONICAS

En el pasado se consideraba que la participación de Auditoría Interna se limitaba a la revisión de los sistemas hasta que éstos se encontraban implantados y funcionando, se pensaba que si participaba activamente en su desarrollo podría en determinado momento, comprometer su independencia y objetividad.

Hoy en día esta actitud ha cambiado, se ha comprobado a través de la práctica que la participación temprana de Auditoría Interna ha sido importante, en el sentido de asegurar que se incluyan los controles necesarios en los nuevos sistemas. Sin embargo, el hecho de que participe en el desarrollo de un sistema, no elimina la necesidad de que se hagan revisiones posteriores, con total independencia, una vez el sistema esté funcionando.

5.1.1 RESPONSABILIDAD

El Auditor Interno es por excelencia un experto en el control interno, por lo que está en las mejores condiciones de participar activamente, como una tarea inherente a su función que realiza, en el desarrollo de un sistema de redes electrónicas que permita optimizar las operaciones de depósitos monetarios, a través de una comunicación en línea. En ese sentido, su contribución se orientará a asegurar, en forma razonable, que las aplicaciones computarizadas incluyen controles sólidos, confiables y oportunos, por lo que su responsabilidad se concreta principalmente, sobre la calidad del sistema que se desarrolla y sobre los controles que se incorporen en el sistema, en el momento de su construcción.

Debe quedar claro en la mente de la administración, que la participación de Auditoría Interna en el desarrollo de un sistema de redes electrónicas se concreta a emitir su opinión sobre la documentación que se refiere a la inclusión o no de controles razonablemente adecuados y que, consecuentemente, esta unidad debe estar en libertad de efectuar revisiones con total independencia, después de implantado el sistema.

Para que Auditoría Interna esté en condiciones de hacer un trabajo efectivo, es necesario considerar los siguientes aspectos:

- a) Que exista un respaldo total de la administración.
- b) Que haya una comunicación fluida y permanente con el Departamento de Procesamiento Electrónico de Datos y la empresa (si es que se contrata) encargada de instalar y desarrollar la red.
- c) Que el Personal de Auditoría Interna cuente con suficientes conocimientos en relación a un sistema de redes electrónicas.

5.1.2 OPORTUNIDAD

Como ya se indicó, la participación del Auditor Interno, en el desarrollo de un sistema de redes electrónicas, debe darse precisamente desde el inicio en que se desarrolla el mismo, a efecto

e que los controles que se consideren necesarios, sean incorporados en las diferentes fases o etapas del desarrollo, ya que una vez esté funcionando el sistema, es más difícil y costoso efectuar las modificaciones.

Normalmente la metodología utilizada para el desarrollo de sistemas consiste en dividir el esfuerzo en la construcción del sistema, en etapas o fases que permitan analizar, evaluar, respuestar y controlar el proyecto total, en una forma sencilla y segura. Tales fases o etapas laramente definidas, pueden clasificarse así:

- a) Inicio
- b) Análisis
- c) Diseño
- d) Desarrollo
- e) Implantación

.1.2.1 INICIO

Cuando se habla de la necesidad de poner en marcha un proyecto de comunicación en línea a través de redes electrónicas y de ofrecer ciertos atractivos que justifiquen su implementación, se inicia en ese momento la planificación de un sistema. La fase del inicio de un proyecto consiste en la planeación de las tareas que se irán a realizar para llevar a cabo dicho proyecto. Es decir que en esta etapa se incluyen los estudios del sistema, desde su identificación y preparación, hasta el análisis que servirá para la ejecución de las actividades planificadas. Los estudios deben realizarse con visión futurista; es decir, visualizando la ejecución y operación del sistema. Cada estudio necesita una evaluación, en la cual se decide la conveniencia de seguir adelante con el sistema. Esta etapa se puede desarrollar de la siguiente manera:

a) **Investigación Preliminar**

Lo importante de esta etapa es identificar las causas y consecuencias del problema de no tener instalado un sistema de comunicación a través de redes electrónicas

que permita manipular las diferentes operaciones en las cuentas de depósito a la vista girables con cheque. Para ello se analizará entre otras cosas, lo siguiente:

- Los síntomas existentes al no contar con un sistema en red.
- La magnitud del problema.
- La necesidad de solución inmediata.
- Identificar las posibles causas del problema.
- Analizar la posibilidad de solucionar el problema al tratar los síntomas, o atacar sus causas.
- Señalar las condiciones que están manteniendo o agravando el problema.
- Estudiar la conveniencia de implantar el sistema de redes electrónicas, en su totalidad, o en partes.

En este paso las personas que participarán en una forma más directa y profunda serán: el personal operativo relacionado con el manejo de los depósitos monetarios, o usuarios (personal de apertura de cuentas, receptores-pagadores, verificadores de operaciones y personal que realiza el cuadro) y el personal del Departamento de Procesamiento de Datos. En este sentido, la participación de auditoría interna será la de evaluar los anteriores cuestionamientos, a fin de emitir su opinión en relación a la forma objetiva en que se abordará el problema.

Definidos los problemas prioritarios, deben plantearse los objetivos por alcanzar. En función de ellos se identifican y analizan las diferentes opciones para solucionar los problemas. Auditoría Interna se encargará de analizar la posibilidad de cumplir los objetivos planteados, a fin de señalar si los mismos son razonables o inalcanzables, de acuerdo a la situación en que se encuentre la institución bancaria. Asimismo, recopilará todos los objetivos trazados, para posteriormente verificar si éstos se cumplieron.

b) Estudio de Factibilidad

Este estudio consistirá en el perfeccionamiento de la idea del proyecto, incluyendo una estimación de sus beneficios y costos. Para el caso del cual se está tratando, "Implantación de un sistema de comunicación en línea a través de redes electrónicas en las operaciones de los depósitos a la vista girables con cheque", la intervención de Auditoría Interna se orientará a analizar si el sistema es susceptible de realizarse, cuál es el resultado de la relación beneficio – costo y si es conveniente que se realice.

Para ello, la Departamento de Auditoría Interna deberá solicitar el estudio de factibilidad de los diferentes sistemas que se encuentren en operación, así como los que estén en la fase de análisis para evaluar si se considera la disponibilidad y características del equipo, los sistemas operativos y lenguajes disponibles, las necesidades de los usuarios, las formas de utilización del sistema en red, el costo y los beneficios que reportará el sistema, el efecto que producirá en quienes lo usarán, el efecto que éstos tendrán sobre el sistema y la congruencia de los diferentes programas.

Para investigar el costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compilaciones, programas, pruebas, paralelos), tiempo, personal y operación, cuestión que en la práctica se definen como: costos directos, indirectos y de operación.

Los beneficios que justifiquen el desarrollo de un sistema pueden ser: el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema, mayor exactitud, mejor servicio, una mejoría en los procedimientos de control, mayor confiabilidad y seguridad.

Del análisis de las opciones del proyecto, se selecciona el que tenga la mayor posibilidad de satisfacer parcial o totalmente las necesidades detectadas, tomando siempre en cuenta la disponibilidad limitada de recursos, así como los criterios

técnicos, económicos y sociales pertinentes. Esta decisión la realiza la administración, y corresponde únicamente a Auditoría Interna emitir su opinión acerca de que es lo más aconsejable para la empresa.

5.1.2.2 ANALISIS

Es el proceso de averiguar qué es lo que se requiere de un sistema (análisis de requisitos) y de definir estos requisitos en forma clara y concisa (especificación de requisitos). Esta etapa se iniciará por medio de una solicitud por escrito de los usuarios, en donde requerirán la implantación del sistema en red. Estas solicitudes por escrito, por lo regular, están realizadas en un diseño estándar, las cuales se pueden denominar: Formularios para Solicitud de Sistemas.

La especificación del sistema contendrá una declaración de las funciones del sistema así como las restricciones con las cuales tendrá que trabajar el productor del mismo. También contendrá gran cantidad de información adicional; por ejemplo, los detalles del hardware que se usará y la capacitación que tendrá que proporcionar el productor, así como una especificación de las herramientas de software especiales que se usarán en el proyecto.

Un principio fundamental en el desarrollo de un sistema computarizado es que, cuanto más rápido se detecte un error, menor será el efecto de éste en el costo del proyecto que se desarrolla y el tiempo necesario para concluirlo. Los errores que se cometen durante la planificación del sistema, análisis y requisitos, y que no se detectan sino hasta las pruebas del sistema y de aceptación, pueden ocasionar grandes excesos en el costo de un proyecto; es más, en algunos casos han provocado la cancelación de proyectos millonarios. Por ello, existe la necesidad de detectar los errores lo más pronto posible, sobre todo al realizar el análisis de requisitos y la especificación del sistema.

Las pruebas constituyen la actividad principal que se desarrolla para revisar un sistema, pero no se les puede emplear durante la especificación del sistema ni inmediatamente después, ya que no se dispone del código del programa. Por tanto, se emplean otras técnicas, de las cuales una de las más poderosas es *la revisión de especificación del sistema*.

En el proyecto de implantar una red que comunique a un banco con sus agencias, afin de ofrecer un mejor servicio, esta revisión se puede realizar a través de un grupo que esté representado por las personas interesadas en el proyecto, con el objeto de examinar la especificación del sistema.

El personal que participa en la revisión de especificación del sistema, puede estar representado por: los analistas responsables del desarrollo de la especificación del sistema, otro miembro, quizás el diseñador del sistema, y un usuario con conocimientos del tema (receptor-agador, visa de cheques, etc.).

En la revisión de especificación del sistema, es común emplear una lista de verificación con preguntas que deben formularse en esta etapa del proyecto. A continuación se presentan algunas de las preguntas más importantes:

1. ¿Están claramente definidos los requisitos que se quieren de la red?
2. ¿Se presentan los requisitos en términos del usuario?
3. ¿Se puede rastrear requisitos funcionales desde la declaración de requisitos hasta la especificación del sistema?
4. ¿Son técnicamente factible los requisitos?
5. ¿Pueden verificarse los requisitos?
6. ¿Qué tipo de prueba se requiere para cada requisito?
7. ¿Existen directrices de diseño o de implantación?

En esta etapa, Auditoría Interna se encargará de evaluar las políticas, procedimientos y normas que se llevaron a cabo para realizar el análisis. Dentro de esta evaluación, se determinará la obtención de datos sobre la operación, flujo, nivel, jerarquía de la información que se tendrá a través del sistema, así como sus límites o interfases con otros sistemas. Se han de comparar los objetivos del sistema a desarrollar con las operaciones actuales, para ver si el estudio de la ejecución deseada es compatible con la actual. Asimismo, verificará los procedimientos sobre la asignación y supervisión del estado de la solicitud del nuevo sistema, para verificar si este se está realizando conforme lo planificado.

Por aparte, velará que el formulario de solicitud se incorpore a la documentación de soporte del nuevo sistema. Este funcionará como una fuente de documentación de su autorización, proceso de prueba y traslado a la categoría de producción.

5.1.2.3 DISEÑO DEL SISTEMA

Para el diseño del sistema sólo hay un insumo real: la especificación del sistema. Su objetivo es desarrollar la arquitectura general de un sistema, la cual satisfaga las funciones de la especificación del mismo, siguiendo los lineamientos del documento aprobado para llevar a cabo su ejecución. El diseño de un sistema normalmente lo desempeña un analista de sistemas de un alto nivel, un individuo muy técnico, quien tiene un amplio conocimiento del equipo actual de hardware, el sistema operativo y los otros programas del sistema, además de los objetivos (definidos por los usuarios) del nuevo sistema propuesto. En particular, se refiere a esta persona como a un analista/diseñador de sistemas. El objetivo del diseñador es producir una arquitectura de sistema expresada en función de unidades de programa (módulos, procedimientos, subrutinas), cada una de las cuales pueda entregarse individualmente a las personas encargadas para su programación.

Por aparte, el trabajo de auditoría interna se centralizará en diseñar los controles internos y la determinación de los procedimientos de operación y decisión, para la red que se desea implantar. Al respecto, se hace referencia al tema identificado con el numeral 4.5 del Capítulo IV, el cual se desarrolló en torno a "*Elementos Necesarios a Considerar para el Establecimiento de un Sistema de Control Interno, en un Sistema de Redes Electrónicas*".

5.1.2.4 DESARROLLO DEL SISTEMA

Durante la fase de desarrollo, es donde el sistema de redes electrónicas se crea, es decir, los programas del sistema se realizan, se prueban y se documentan. Una vez que se ha definido con un lenguaje de diseño de programa, el siguiente paso del ciclo del sistema es la programación. Este proceso es el menos difícil, pues sólo comprende la traducción de las unidades de programa, expresadas en lenguaje de diseño, a código de programa. Es decir, que implica una traducción

directa de los enunciados del lenguaje de diseño del programa a enunciados en lenguaje de programación.

Esta actividad será responsabilidad directa del programador. Sin embargo, el Auditor Interno podrá efectuar pruebas de lo programado en el sistema de redes, principalmente en lo que se refiere a los programas fuente, a fin de garantizar que se cumplan los requisitos de las especificaciones funcionales, verificando datos, transacciones, reportes, archivos, anotando las fallas que pudieran ocurrir e indicar que se realicen los ajustes necesarios. Los niveles de prueba deben ser selectivos y pueden ser agrupados en módulos. Esta función tiene una gran importancia en el ciclo de la evaluación del sistema, ya que busca comprobar que el sistema cumple las especificaciones del usuario, que se haya desarrollado de acuerdo a lo planeado, que tenga controles necesarios y que efectivamente cumpla con los objetivos y beneficios esperados. Para ello, el auditor interno podrá auxiliarse de los paquetes o software de auditoría vigentes en el mercado.

Al evaluar el desarrollo del sistema de redes electrónicas se tendrá presente que todo sistema debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, para reducir la duplicidad de datos y reportes, y obtener una mayor seguridad en la forma más económica posible. De ese modo se contará con los mejores elementos para una adecuada toma de decisiones.

5.1.2.5 IMPLANTACION DEL SISTEMA

Después de haber desarrollado el sistema, se entra a la fase de implantación. El objetivo principal de esta etapa es entregar el sistema terminado al usuario. Una vez que el usuario acepta el sistema y el personal de operaciones lo revisa, el sistema se traslada al ambiente en el cual se realizará la comunicación en línea a través de la red física y es en ese momento cuando el personal de operaciones lo administra. Para realizar tal objetivo, es necesario realizar los siguientes pasos:

- a) **Preparación de la Implantación**



Antes de implantar un sistema de red, será necesario revisar entre otros asuntos los siguientes: a) Planes de emergencia, por si hay una caída de línea (no hay comunicación) en la red, a fin de aplicar procedimientos alternos, tales como: transmitir vía radio con otras agencias o central, los depósitos y consulta de fondos de cheques que se presenten para su cobro; b) Los manuales de procedimientos, en relación a las funciones que se modificarán por motivo de la implantación de la red; c) Capacitación al personal, en función a la red; d) Las políticas de control interno, tendientes a proporcionar una seguridad efectiva y eficiente, de las operaciones realizadas en la red; e) Otras que se consideren necesarias.

En esta etapa es importante que el Auditor Interno se involucre, derivado de los cambios en cuanto a procedimientos que tendrá que aplicar en sus revisiones al nuevo sistema.

b) Métodos para realizar la Implantación

Previo a implantar y dejar funcionando a la red, es necesario que se realicen las pruebas de aceptación del nuevo sistema en red. Las pruebas de aceptación representan el método mediante el cual se verifica que, el sistema nuevo en red funciona según lo planificado. Los tres métodos de pruebas de aceptación son: los sistemas en paralelo, los sistemas por fases y el sistema directo.

Sin embargo, para realizar cualquiera de estos métodos, se deben de tener políticas y procedimientos para la documentación de las pruebas de aceptación, las que deben incluir: Las normas para el proceso de prueba, los requisitos de involucramiento por parte del grupo usuario, los requisitos de documentación para las pruebas de aceptación así como las de resultados y, los requisitos con respecto a la revisión de las pruebas de aceptación por individuos independientes del equipo de desarrollo.

- 1) **Método del Sistema Paralelo.** *Ventajas:* Los sistemas nuevos y viejos se ejecutan a la vez; los resultados del procedimiento del sistema o programa nuevo se comparan con los del sistema o programa viejo. Se identifican y corrigen los problemas potenciales antes de colocar el sistema nuevo en la biblioteca de producción. El enfoque de sistemas paralelos provee la certeza de que si el sistema nuevo no funciona adecuadamente, las operaciones continúan sin interrupción. *Desventajas:* Existe la tendencia de comparar los resultados sin tener un entendimiento completo de las diferencias funcionales entre los dos sistemas. Para ser efectivas, las pruebas paralelas deben incluir todos los tipos de transacciones posibles y también evaluar la habilidad del sistema de administrar los volúmenes de transacciones.

- 2) **Método del Sistema por Fases.** *Ventajas:* El método de sistema por fases elimina progresivamente el sistema viejo e implanta el sistema nuevo. Este enfoque evita comparaciones e interacciones entre el sistema viejo y el nuevo. El sistema nuevo no procesa el trabajo del sistema viejo, el cual puede contener errores. Como resultado, la evaluación del sistema nuevo se basa directamente en su desarrollo. *Desventajas:* Aunque los resultados de procesamiento de diferentes fases pueden ser exactos y completos en cada componente, las funciones generales de los sistemas quizás no estén adecuadamente integradas, especialmente si diferentes equipos trabajan en diferentes fases.

- 3) **Método del Sistema Directo.** *Ventajas:* El método directo requiere que se realice una conversión directa, de una sola vez, del sistema viejo al sistema nuevo. El método directo es un método de un costo relativamente bajo para instalar un nuevo sistema. *Desventajas:* Cuando se implanta el método directo significa que inmediatamente se comienza a confiar en el sistema nuevo y no existe un período de prueba para identificar los posibles problemas u omisiones. Los usuarios no pueden comparar los resultados de procesamiento del sistema nuevo con los del sistema viejo.

Una institución bancaria guatemalteca, utilizó el método del sistema paralelo, a fin de realizar el cambio de su sistema mecánico (a través de máquinas NCR) al sistema de redes electrónicas. Este cambio lo realizó de la siguiente manera: el registro de las operaciones en las cuentas de depósito se realizaban por medio de máquinas NCR, la actualización de los saldos se llevaba a cabo a través de la comunicación vía radio. Con el objeto de no interrumpir el servicio a los clientes, en caso fallara el sistema en red, el cambio se hizo en paralelo. Se comenzó por instalar el sistema en red en todas las agencias, es decir colocando el hardware y software necesario para la comunicación electrónica. Posteriormente, se hizo un back-up de los archivos del computador central que se relacionaban con las cuentas de depósitos monetarios y se trasladaron a un servidor auxiliar. Luego, se estableció un período de tres meses, para llevar el método paralelo. En ese período se actualizó simultáneamente los saldos en las cuentas de depósitos monetarios a través de los dos sistemas, y se compararon diariamente sus resultados para establecer sus diferencias. Al concluir el período de prueba, ya se habían realizado los ajustes necesarios al nuevo sistema, por lo que se obtuvieron resultados satisfactorios.

c) Revisión Post-Implantación y Seguimiento

Por último se harán revisiones, en un principio más frecuentes, a fin de verificar el desarrollo del nuevo sistema en red implantado en una institución bancaria. En relación al trabajo del Auditor Interno, esta revisión se orientará a establecer debilidades que resulten en el control interno, derivadas del cambio realizado.

En resumen, el auditor es responsable de confirmar tanto antes como después de la implementación, la confiabilidad del nuevo sistema en red y, específicamente, la fiabilidad de los programas en ejecución. Las confirmaciones realizadas en la etapa de pre-implantación, son confirmaciones establecidas en el momento, mientras que las de la etapa de post-implantación deben ser dinámicas y continuas.

5.2 PREPARACION Y CAPACITACION DEL AUDITOR INTERNO EN REDES ELECTRONICAS

La mayoría de auditores no cuentan con suficiente experiencia en lo relativo al funcionamiento de sistemas de redes electrónicas, lo que obliga a un conocimiento más profundo sobre tal aspecto.

La auditoría en operaciones realizadas a través de redes electrónicas depende en gran parte, al conocimiento que el auditor tenga de la tecnología de los computadores, así como de los diferentes componentes que conforman parte de un sistema de red. Por consiguiente, el Auditor Interno debe participar en programas y cursos de auditoría que le permitan desarrollarse en este campo, con el fin de obtener un conocimiento más profundo con el que pueda realizar una mejor actividad profesional.

Para una adecuada capacitación es conveniente que el Auditor Interno conozca aspectos como los siguientes:

- a) Conocimientos generales de un Sistema de Redes Electrónicas. Esto será necesario para que pueda ser efectivo en su labor de prevención de fraudes.
- b) Habilidades para el análisis de riesgos.
- c) Metodologías que estén orientadas a operaciones realizadas a través de redes.
- d) Técnicas para hacer más eficiente y efectivo su trabajo.
- e) Análisis y diseño de sistemas.
- f) Programación.

Por consiguiente, el mayor o menor grado de capacitación dependerá como en cualquier otra situación, de los objetivos del trabajo que debe desarrollar.

5.3 TECNICAS Y PROCEDIMIENTOS DE AUDITORIA

Normalmente, el entendimiento y la información descriptiva acerca de la instalación de un sistema de redes electrónicas y de los controles generales, se obtiene por medio de una



combinación de indagación, observación e inspección de los documentos y procesos del sistema. Dichos procedimientos también pueden proveer evidencia de auditoría sobre la efectividad del diseño, la operación de los procedimientos pertinentes y servir como pruebas de control.

Las pruebas que realizará el auditor interno, una vez se haya instalado el sistema de redes, serán de cumplimiento y sustantivas. Las pruebas de cumplimiento están dirigidas al diseño u operación de un procedimiento o política de la estructura de control interno, para evaluar su efectividad, para evitar o detectar declaraciones incorrectas importantes en una aseveración del sistema de redes que se aplique. Las pruebas sustantivas se desarrollarán como aquellos procedimientos analíticos y las pruebas de detalle, efectuadas para detectar las declaraciones incorrectas importantes incluidas en los componentes de saldo de cuenta, clase de transacción y revelación realizada por el sistema de redes electrónicas.

A continuación se describen algunos procedimientos que pueden realizar el Departamento de Auditoría Interna, con respecto al desarrollo de un sistema de redes electrónicas:

5.3.1 PRUEBA DEL PROCESO Y RESULTADOS DE UNA OPERACION EN UNA CUENTA DE DEPOSITOS MONETARIOS, A TRAVES DE LA RED ELECTRONICA, CON DATOS DEL AUDITOR

Este método provee al sistema implantado (en este caso un sistema de red) una serie de transacciones de prueba para que sean procesadas. Las transacciones contienen información válida y ficticia, con el objeto de establecer que la información ficticia no es procesada.

Para utilizar este método eficazmente, el auditor primero debe estudiar cuidadosamente la documentación del sistema de redes, haciendo énfasis en la disposición del registro de entrada, los tipos de transacciones válidas y ficticias y la lógica del procesamiento. Después el auditor genera un conjunto de transacciones ficticias que serán utilizadas para comprobar si la lógica opera tal como lo indica la documentación. En forma anticipada el auditor debe calcular el resultado de cada transacción para después compararlo con el programa de procesamiento. Un ejemplo sería realizar varios depósitos y retiros en una cuenta de depósitos monetarios, elegidas

para el efecto, a través de la red, y en forma anticipada haber calculado el saldo de la cuenta, después de haber realizado las operaciones ficticias.

5.3.2 UTILIZACION DE SISTEMAS DE SOFTWARE PARA REALIZAR PRUEBAS DE AUDITORIA EN UN SISTEMA DE REDES ELECTRONICAS

Un sistema de software para auditoría consiste en un conjunto de rutinas de ordenador, realizadas en lenguajes de programación, las cuales puede emplear el auditor para verificar los registros en un sistema de procesamiento electrónico de datos (PED) de una organización. Estos paquetes vienen con una serie de aplicaciones que indican, de manera sencilla, qué tipo de información se desea procesar. Para ello, el software de los programas de auditoría traducen los datos del programa a examinar a una base de datos, utilizando para ello, lenguajes de programación (Cobol, Basic, C, Pascal, otros). A través de la base datos, la información se organiza para dar un servicio eficiente a las aplicaciones, centralizando los datos y minimizando aquellos que son redundantes. En vez de separar los datos en archivos separados para cada aplicación, los datos son almacenados físicamente para aparecer a los usuarios en una sola ubicación, por lo que una base de datos, sirve a muchas aplicaciones.

Un objetivo operativo fundamental de la mayoría de los sistemas de software para auditoría es facilitar, al auditor que disponga de una escasa preparación informática, la verificación de registros y archivos realizados a través de un sistema PED. Sin embargo, las dificultades aparecen a la hora de enfrentarse a situaciones no comunes, en tales casos, el auditor deberá tener algunos conocimientos generales de informática y además contar con el apoyo de personal especializado en la materia.

Uno de los problemas principales, es el de obtener tiempo para la utilización de la computadora central de la institución para llevar a cabo las aplicaciones del software de auditoría. En ese sentido, se podrá copiar los archivos que se desean auditar, y llevar a cabo los trabajos en un centro de proceso de datos ajeno.

Dentro de las aplicaciones que suelen desempeñar los sistemas de software para auditoría, se encuentran las siguientes:

- a) Interpretar la especificación de auditoría para el proceso del archivo, examinar los errores, e imprimir las instrucciones y mensajes de error.
- b) Escoger e imprimir los registros que cumplen los criterios especificados por el auditor. Por ejemplo: Las cuentas de depósitos monetarios con un saldo mayor a Q.100,000.00, cuentas que reflejen un saldo negativo, registros en blanco en el campo destinado a especificar el nombre, etc.
- c) Resumir los datos del archivo obteniendo los totales mediante campos numéricos. Por ejemplo: Establecer rangos por montos de cuentas.
- d) Calcular valores adicionales a partir de los datos del archivo. Ejemplo: calcular el interés devengado por una cuenta durante un mes y compararlo con el calculado por el software operativo de la red.
- e) Ordenar el archivo en un orden específico.
- f) Imprimir confirmaciones de auditoría y preparar toda la información sobre confirmaciones necesarias para su análisis y seguimiento.

5.3.3 METODO DE RASTREO DE UNA OPERACION REALIZADA EN LA RED

La técnica de rastreo es una opción que usualmente viene en la mayoría de los lenguajes de programación. Este método produce informes que indican la secuencia de instrucciones ejecutadas en las transacciones de procesamiento. Este procedimiento puede considerarse como una auditoría de los caminos de control en lugar de una verificación del programa. Para utilizar eficazmente esta técnica, el auditor rastrea manualmente una transacción y compara el rastreo manual con el realizado por el computador. Una comparación cuidadosa indica que las transacciones fueron procesadas por cada instrucción apropiada para esa operación, pero no asegura la exactitud de las transacciones individuales.

5.3.4 OTRAS TECNICAS

Existen otras técnicas de auditoría en relación a la evaluación del funcionamiento de un sistema de redes electrónicas y su aplicación en las operaciones de los depósitos monetarios. Dichas pruebas dependerán de qué es lo que quiere evaluar y en que momento. En ese sentido, el Auditor Interno podrá hacer uso de su ingenio, a fin de verificar un proceso o la aplicación de una política de control.

5.4 CARACTERISTICAS DE UN SISTEMA DE REDES ELECTRONICAS QUE INFLUYEN EN UNA AUDITORIA

Como se definió en el Capítulo III, una red se define como un grupo de ordenadores (servidores y terminales en general) interconectados a través de uno o varios caminos o medios de transmisión, con el fin de transferir e intercambiar información. En ese sentido, el objetivo primordial de una red es la comunicación, y es precisamente ese aspecto en donde se deben enfocar los esfuerzos de auditoría, es decir, buscar una seguridad razonable de que esa comunicación es confiable, eficiente y oportuna.

Al tener la idea de implantar un sistema de redes, es importante evaluar la seguridad del movimiento de la información entre computadores. El proceso de planeación de sistemas debe promover que en la red sea óptima la comunicación y, describir entre otras cosas: la ubicación planeada de las terminales, los tipos de mensajes requeridos, el tráfico esperado en las líneas de comunicación y otros factores que afectan el diseño.

Asimismo, al llevar una auditoría en un sistema de comunicación en red, es necesario considerar entre otras cosas las siguientes:

- a) Si es una red local, o sea una LAN, se deberá considerar su topología, a fin de determinar sus debilidades y las opciones que brindan los fabricantes para superar las deficiencias.

- b) Si es necesario utilizar una red privada o pública para la comunicación remota, se deberá tener en cuenta el uso de un adecuado protocolo que proporcione seguridad de que la información no pueda ser leída por un tercero ajeno a la entidad bancaria.
- c) Otra situación que debe tomarse en cuenta es lo relacionado a los virus, ya que éstos pueden infiltrarse fácilmente a través de la red. Para ello se debe verificar de que existan políticas adecuadas de prevención, herramientas útiles en caso de que se detecte alguno y el grado de exposición del sistema operativo en que opera la red.
- d) El establecimiento y control de password será necesario para identificar a los usuarios de la red, así como medir los privilegios que éstos tienen en la misma.

Estos son algunos aspectos de inicio que se deberán tomar en cuenta al realizar un trabajo de auditoría en un sistema de redes. Sin embargo, a medida de que se vaya desarrollando el trabajo de auditoría, podrían encontrarse diversas situaciones que provoquen una debilidad dentro de la comunicación de la información, por lo que éstas se deberán tomar en cuenta para revisiones posteriores, a fin de verificar si tales debilidades ya fueron resueltas.

5.5 EL USO DE ESPECIALISTAS EN REDES ELECTRONICAS

Dentro de las Normas de Auditoría, emitidas por el Instituto Guatemalteco de Contadores Públicos y Auditores –IGCPA-, se define a un especialista así: “Es la persona que posee habilidades o conocimientos especiales en un campo específico que no sea contable o de auditoría, por ejemplo: actuarios, valuadores, abogados, ingenieros, geólogos, etc”.²¹

En ese sentido el Auditor Interno podrá hacer uso de un especialista, a fin de que este le proporcione un asesoramiento acerca del adecuado funcionamiento de una red electrónica. Este

²¹ Instituto Guatemalteco de Contadores Públicos y Auditores, Norma de Auditoría No. 4, recopilación 1992, Pág. 15

ndrá que tener conocimiento en las áreas de diseño de sistemas, programación, configuración de redes, protocolos y otros que tengan relación con un sistema en red.

Entre los aspectos que hay que considerar al utilizar el trabajo de un especialista, el ICPA propone, en la Norma de Auditoría No. 4, que se investigue del mismo lo siguiente:

- 1) Capacidad que tiene el especialista en la materia que examinará.
- 2) Reputación o posición del especialista en un gremio.
- 3) Parentesco que puede tener con el cliente (en este caso se referiría a la persona o entidad que lleve a cabo la implementación del sistema de red) y el efecto que esta situación pudiera tener en el trabajo que desarrollará.

Por aparte, el auditor deberá indicar cuales son los objetivos y alcance del trabajo del especialista, aclarar la metodología que se seguirá para ejecutar el trabajo encomendado y determinar si dichos objetivos son suficientes para obtener la evidencia que necesita el auditor. El especialista debe conocer perfectamente el uso que se le dará a los resultados de su trabajo y ponerse de acuerdo con el auditor sobre la forma y contenido del informe final.

El auditor deberá documentar adecuadamente la utilización del especialista. En la planificación del trabajo de auditoría, deberá explicar los motivos que lo llevaron a decidir que era necesaria la utilización de un especialista. De la misma manera, debe definir los objetivos del trabajo, principales procedimientos que aplicará y los resultados que se espera obtener. Además, deberá dejar dentro de sus papeles de trabajo, las fechas en que se llevarán a cabo las reuniones con el especialista.

Por último, se deberá tener en cuenta que es importante solicitar al especialista una declaración por escrito, sobre la relación que pudiera tener con las personas o entidad que tengan a cargo el establecimiento de la red y obtener un informe detallado sobre los resultados de su trabajo.

5.6 EJEMPLOS DE PAPELES DE TRABAJO

En este apartado se desarrolla un caso práctico que ejemplifica la participación de Auditoría Interna de una institución bancaria, en la evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósitos monetarios. Para ello se proporciona la siguiente información:

- a) El Banco Buena Suerte, S. A., ha venido registrando sus operaciones en la ventanilla, por medio de máquinas registradoras NCR. Para el pago de cheques en sus agencias utiliza la radio, con lo que consigue cerciorarse que la cuenta de que se trate tenga los fondos necesarios. Luego verifica manualmente las firmas, las cuales están archivadas en ficheros. Cuando las firmas no aparecen en los ficheros, puede ser que las mismas no han sido remitidas por la agencia que corresponda, debido a que la cuenta se abrió recientemente o hubo un cambio en el registro de firmas. En ese sentido, se consultan las firmas por radio y se hace una descripción verbal, a fin de conciliar la firma del cheque, *lo cual se considera de alto riesgo*. Los depósitos monetarios de cuentas de otras agencias se reciben y posteriormente se dictan a la agencia por la radio para que sea actualizado su saldo. Tanto los cheques como los depósitos de la propia agencia son operados en ese momento mediante tarjetas, en donde se lleva el saldo de la cuenta. Las personas que se necesitan para las operaciones anteriormente descritas son: un receptor-pagador, quien es el encargado de manejar el dinero; y un visa, quien se encarga de revisar la redacción, consultar los fondos de los cheques y transmitir por la radio los depósitos recibidos de cuentas de otras agencias.
- b) La empresa que se contrató para llevar a cabo el proyecto es Sistemas Empresariales, S. A.
- c) El sistema estará dividido en dos tipos de red, LAN Y WAN, para uso interno y externo, respectivamente. La topología de la red LAN será Jerárquica. En la red WAN se utilizará el servicio de la empresa Mayapac, la cual se encargará de arrendar líneas dedicadas para la comunicación de los datos desde las terminales remotas.

- d) Algunas de las características de la red, son las siguientes: El computador central será un IBM-9221, arquitectura 390, modelo 120, con una memoria real de 30 MB, y una memoria virtual de 122 MB. Su capacidad de almacenamiento es de: a) Dos discos modelos 9336 de 5.5 GB; b) Dos cintas modelos 9347 de 6250 BPI/1600 BPI; y c) Un cartucho modelo 9390E de 8 GB. Productos a instalar: a) Medio ambiente: VSE/ESA release 1.3.0; b) Sistema operativo VSE/ESA System Package 5.1.1; c) Manejador de Comunicaciones ASF/VTAM, versión 3.3.0; d) Sistema de Monitoreo CICS/VSE, versión 2.2.0; e) Protocolo de comunicación SDLC, BSC (sincrónicos); f) Manejador de Archivos VSE/VSAM, versión 2.1.1. En las terminales se contará con el siguiente equipo: a) Las quince agencias, con las que cuenta la institución bancaria, contarán con tres estaciones de trabajo, más una máquina centralizadora que se encargará de transmitir y administrar la información, por lo que en total sumarán 60 terminales remotas. En la agencia central habrán 10 terminales más; b) El Lenguaje utilizado en las terminales será SAFE; y c) Software utilizado en terminales será FBSS;
- e) El personal del Departamento de Organización y Métodos de la institución bancaria, juntamente con empleados de Sistemas Empresariales, S. A., elaboraron flujogramas para definir los pasos que se deben llevar a cabo en la ejecución de una actividad específica, relacionada con depósitos monetarios. Dentro de las actividades que fueron flujogramadas se tiene conocimiento que se encuentran las siguientes:
- Apertura de una cuenta de depósitos monetarios
 - Captura de Firmas
 - Entrega de chequeras
 - Pago de cheques

La Gerencia General de la entidad bancaria ha solicitado al Auditor Interno del banco que, con base en la información anteriormente descrita, evalúe los flujogramas elaborados (conjuntamente con un análisis de los controles incluidos en los mismos), relacionados con actividades específicas que se realizarán en el nuevo sistema de redes electrónicas que se desea implantar, y pida la opinión a un especialista acerca del mismo.

BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

CENTR

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Programa general de trabajo.

No.	DESCRIPCION	REFER.
1	Examen del proceso de apertura de una cuenta de depósitos a la vista girables con cheque	A
2	Examen del proceso de captura de firmas	B
3	Examen del proceso de entrega de chequeras	C
4	Examen del proceso de pago de cheques	D
5	Verificación del diseño de la red	E

CONCLUSION:

Excepto por las deficiencias en los procesos para la apertura de una cuenta y para el pago de un cheque, Cédulas A y D, respectivamente, en opinión del suscrito, el sistema de red para el manejo de los depósitos monetarios del banco, provee seguridad razonable para el proceso y la transferencia de datos.

RECOMENDACION:

Para efectos de eliminar las deficiencias señaladas, se sugiere tomar en cuenta las recomendaciones descritas en los respectivos papeles de trabajo.

Hecho Por: EADA
Fecha: 02/01/98
Revisado Por: BS
Fecha: 04/01/98

BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

A

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Examen del proceso de apertura de una cuenta de depósitos a la vista girables con cheque.

DIVULGACION:

De acuerdo a instrucciones de Gerencia General, se procedió a evaluar los flujogramas presentados por Sistemas Empresariales, S.A., conjuntamente con el Departamento de Organización y Métodos de esta institución bancaria, relacionado con "El Proceso de Apertura de una Cuenta de Depósitos a la Vista Girables con Cheque". Los procedimientos descritos en dichos flujogramas, obedecen al cambio que se realizará en las operaciones de depósito monetarios, en virtud del plan que se tiene para instalar un sistema de red electrónica que realice operaciones en línea.

Nó.	DESCRIPCION	REFER.
1	Evaluación del proceso de apertura de una cuenta de depósitos a la vista girables con cheque	A-1
2	Evaluación del proceso de investigación de una cuenta nueva	A-2
3	Evaluación del proceso de denegación de apertura de una cuenta nueva	A-3

CONCLUSION:

Excepto por la deficiencia encontrada en el proceso de apertura de una cuenta de depósitos a la vista girables con cheque (Ver cédula A-1), el resultado de la verificación es razonable.

RECOMENDACION:

Se recomienda que, dentro del flujograma "Proceso de Apertura de una Cuenta de Depósitos a la Vista Girables con Cheque", el cuenta-habiente verifique sus datos antes de que los mismos se ingresen al computador. Además, que en los procedimientos del mismo flujograma, se incluya la posibilidad de que el "Encargado de Apertura de Cuentas", accese de forma incorrecta los datos del cuenta-habiente al computador, haciéndose participe la actuación de la Jefatura, en el sentido de proporcionar el password necesario para corregir el error efectuado.

Hecho Por: EADA
Fecha: 02/01/98
Revisado Por: BS
Fecha: 04/01/98

BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

A-1

1/2

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Evaluación del proceso de apertura de una cuenta de depósitos a la vista girables con cheque.

TRABAJO REALIZADO:

La verificación consistió en hacer un análisis de los diferentes procesos que se tienen que realizar para la apertura de una cuenta de depósitos a la vista girables con cheque. En ese sentido, el examen principió con el proceso propio de la apertura; es decir, cuando el cliente se presenta al banco por primera vez para abrir su cuenta. Asimismo, se hicieron entrevistas con las personas involucradas en este proceso, con el objeto de conocer su opinión acerca de los nuevos procedimientos propuestos, derivado de la implantación del nuevo sistema.

TIPOS DE CONTROLES INCLUIDOS EN EL PROCESO:**Controles de Entrada:**

- Verificación de los documentos de identificación del cuenta-habiente que desea abrir su cuenta.
- Asignación del número de cuenta, el cual contiene dentro de sí, un dígito verificador.

Controles de Procesamiento:

- Verificación de los datos de la papelería de apertura, por parte del cliente.
- Verificación dentro de los límites y grados de razonabilidad por el programa, antes de transmitirlos a través de la red.

Controles de Almacenamiento de Datos

- Copia magnética registrada por la apertura de la cuenta.

Controles de la Información de Salida

- Verificación por parte del encargado de apertura de cuentas, de la papelería de apertura, además de la firma del cliente, así como de la información accesada al computador.
- Reporte de cuentas aperturadas, realizado al final del día.

RESULTADO DE LA VERIFICACION:

En relación a los procedimientos que se tienen que realizar en este proceso, se determinó que después del paso identificado con el número 9, en donde se llena a máquina la solicitud de chequera del cliente, se procede a acceder al computador, tanto la información de la cuenta nueva, como la solicitud de chequera personalizada (pasos 10 y 11). Posteriormente, se llena a máquina el depósito monetario y se entregan los documentos de apertura al cliente, quien previo a firmar, verifica sus datos escritos por el encargado de apertura de cuentas. Seguidamente el encargado revisa si los documentos están bien firmados (pasos del 12 al 18).

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Evaluación del proceso de apertura de una cuenta de depósitos a la vista girables con cheque.

Cabe destacar que, dentro de los pasos descritos anteriormente se observaron las siguientes deficiencias: La primera consiste en acceder al computador la información de la cuenta nueva y la solicitud de la chequera personalizada, sin que antes haya revisado el cliente los documentos de apertura. El riesgo que figura en este procedimiento es que se ingresen al computador datos equivocados del cuenta-habiente y que los mismos no se corrijan posteriormente, lo cual puede dar problemas, tanto al cliente como a la misma institución. La segunda deficiencia observada tiene relación con la primera, y es que se observa que dentro del flujograma no se contempla la posibilidad de acceder datos incorrectos del cliente al computador. Esto traería el involucramiento del jefe inmediato superior del encargado de apertura de cuentas, ya que es éste el responsable de tener el password para modificar cualquier error ingresado al sistema de computación.

CONCLUSION:

De conformidad con los procedimientos de auditoría efectuados se concluye que, los pasos para la apertura de una cuenta de depósitos a la vista girables con cheque, presenta dos deficiencias relacionadas con el proyecto de implantación del sistema de red, las cuales consisten en:

- 1 Se accesa la información de apertura de cuenta al computador, sin que el cuenta-habiente previamente haya revisado sus datos, a fin de verificar si éstos están correctos o no.
- 2 En el flujograma no se contempla la posibilidad de que se accesen de forma incorrecta los datos del cuenta-habiente al computador.

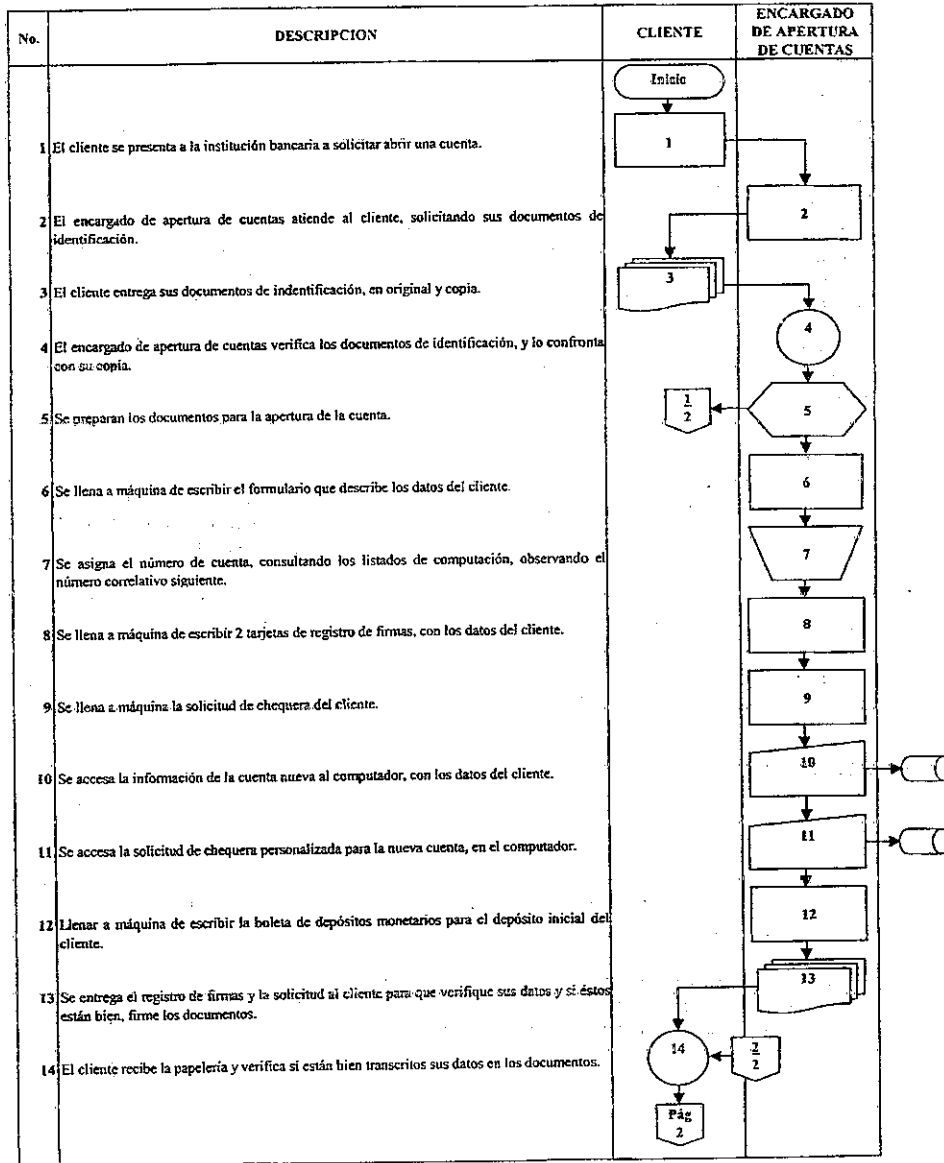
RECOMENDACIONES:

De acuerdo a las deficiencias observadas, se estima necesario considerar las siguientes recomendaciones:

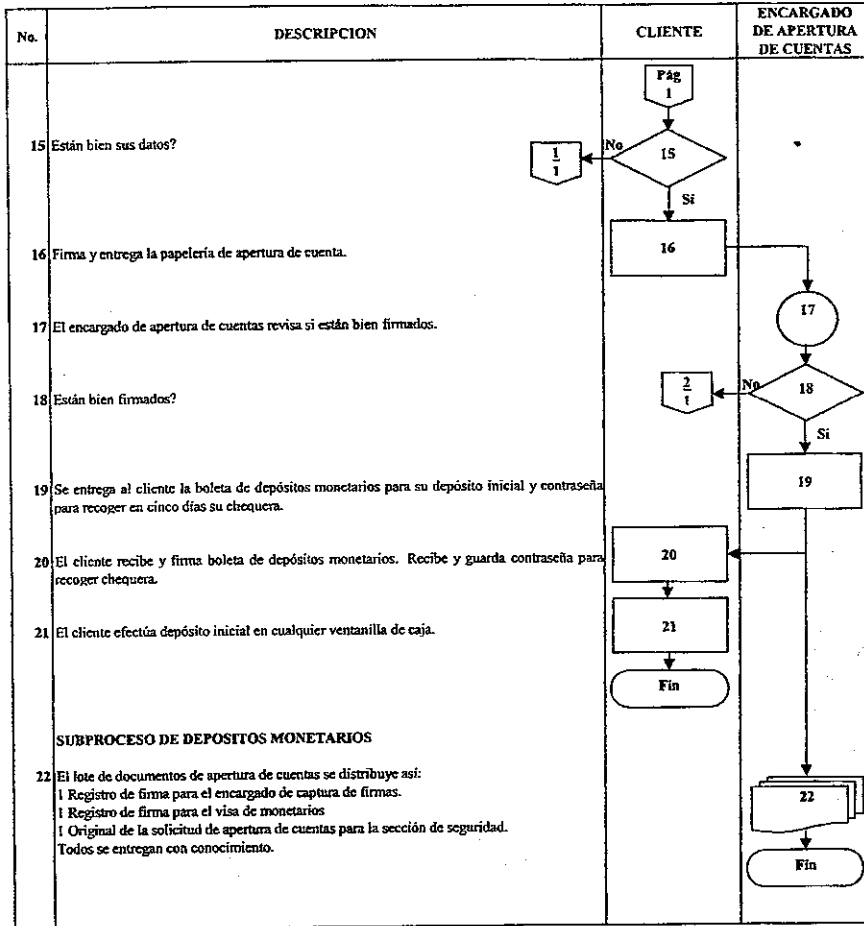
- 1 Que después del paso No. 9 descrito en el flujograma, se realicen los pasos correlativos contemplados del numeral 12 al 18. Inmediatamente después de estos pasos, se realicen los procedimientos contemplados en los numerales 10 y 11. (Ver cédula A-1.1)
- 2 Se incluya en el flujograma el procedimiento a realizar cuando se accesen de forma incorrecta los datos del cliente al computador, haciéndose participe la actuación del jefe del Encargado de Apertura de Cuentas, para que éste proporcione el password necesario para corregir el error efectuado.

Hecho Por: EADA
Fecha: 02/01/98
Revisado Por: BS
Fecha: 04/01/98

**PROCESO DE APERTURA DE UNA CUENTA DE DEPOSITOS A LA VISTA
GIRABLES CON CHEQUE
DEPARTAMENTO OPERATIVO**



**PROCESO DE APERTURA DE UNA CUENTA DE DEPOSITOS A LA VISTA
GIRABLES CON CHEQUE
DEPARTAMENTO OPERATIVO**



BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

A-2

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Evaluación del proceso de investigación de una cuenta nueva.

TRABAJO REALIZADO:

Con el fin de continuar con la verificación de los diferentes procesos que se tienen que realizar para la apertura de una cuenta de depósitos a la vista girables con cheque, derivado del nuevo sistema en red que se desea implantar, se procedió a evaluar el flujograma que detalla el Proceso de Investigación de una Cuenta Nueva. Asimismo, se hicieron entrevistas con las personas involucradas en este proceso, con el objeto de conocer su opinión acerca de los nuevos procedimientos propuestos, derivado de la implantación del nuevo sistema. Cabe destacar que este proceso no tiene una relación directa con el manejo de computadores que conecten a la red; sin embargo, es un complemento del método que se lleva para abrir una cuenta de depósitos monetarios.

TIPOS DE CONTROLES INCLUIDOS EN EL PROCESO:

Controles Manuales:

- Firma de conocimiento tanto del encargado de apertura de cuentas, como de la secretaria de seguridad.

Controles Preventivos:

- Investigación realizada para indagar sobre las referencias personales del cliente, dirección reportada, récord bancario y datos generales.
- Segregación de funciones que existe en el proceso de investigación de una cuenta nueva, en la cual participan varias personas.

RESULTADO DE LA VERIFICACION:

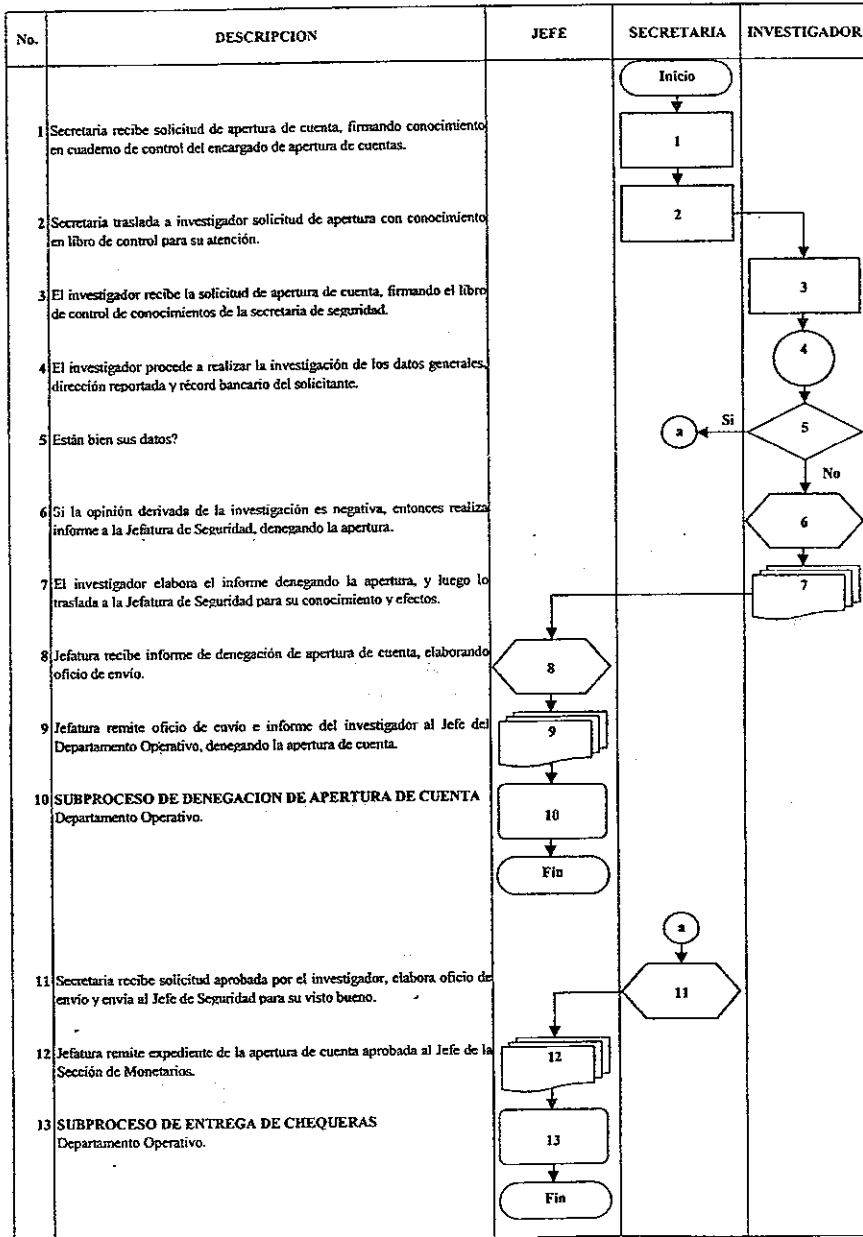
De acuerdo al análisis que se realizó en el flujograma, no se detectó ninguna deficiencia en el proceso que se describe para la investigación de una cuenta nueva. Asimismo, al hacerse las entrevistas con las personas involucradas en este proceso, manifestaron su buena aceptación acerca de la implantación del nuevo sistema de red electrónica para el manejo de las operaciones de depósito monetarios.

CONCLUSION:

De conformidad con los procedimientos de auditoría efectuados se concluye que, el proceso que se describe en el flujograma para llevar a cabo la investigación de una cuenta nueva, es razonable.

Hecho Por: EADA
Fecha: 02/01/98
Revisado Por: BS
Fecha: 04/01/98

**PROCESO DE INVESTIGACION DE UNA CUENTA NUEVA
SECCION DE SEGURIDAD**



BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

A-3

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Evaluación del proceso que se realizará para la denegación de apertura de una cuenta nueva.

TRABAJO REALIZADO:

Revisado ya el proceso de Investigación de una Cuenta Nueva, el siguiente flujograma que se examinó fue el de Denegación de Apertura de una Cuenta. El análisis consistió en observar el proceso que se detalla en dicho flujograma para determinar su congruencia, secuencia lógica y fiabilidad de cada paso realizado. Asimismo, se hicieron entrevistas con las personas involucradas en este proceso, con el objeto de conocer su opinión acerca de los nuevos procedimientos propuestos, derivado de la implantación del nuevo sistema.

TIPOS DE CONTROLES INCLUIDOS EN EL PROCESO:**Controles Preventivos:**

- Investigación realizada para indagar sobre las referencias personales del cliente, dirección reportada, récord bancario y datos generales.
- Segregación de funciones que existe en el proceso de la apertura de una cuenta, participando en él varias personas.
- La autorización realizada por dos funcionarios distintos, en las órdenes de pago por concepto de denegación de la apertura de una cuenta, por un monto mayor a Q. 500.00.

RESULTADO DE LA VERIFICACION:

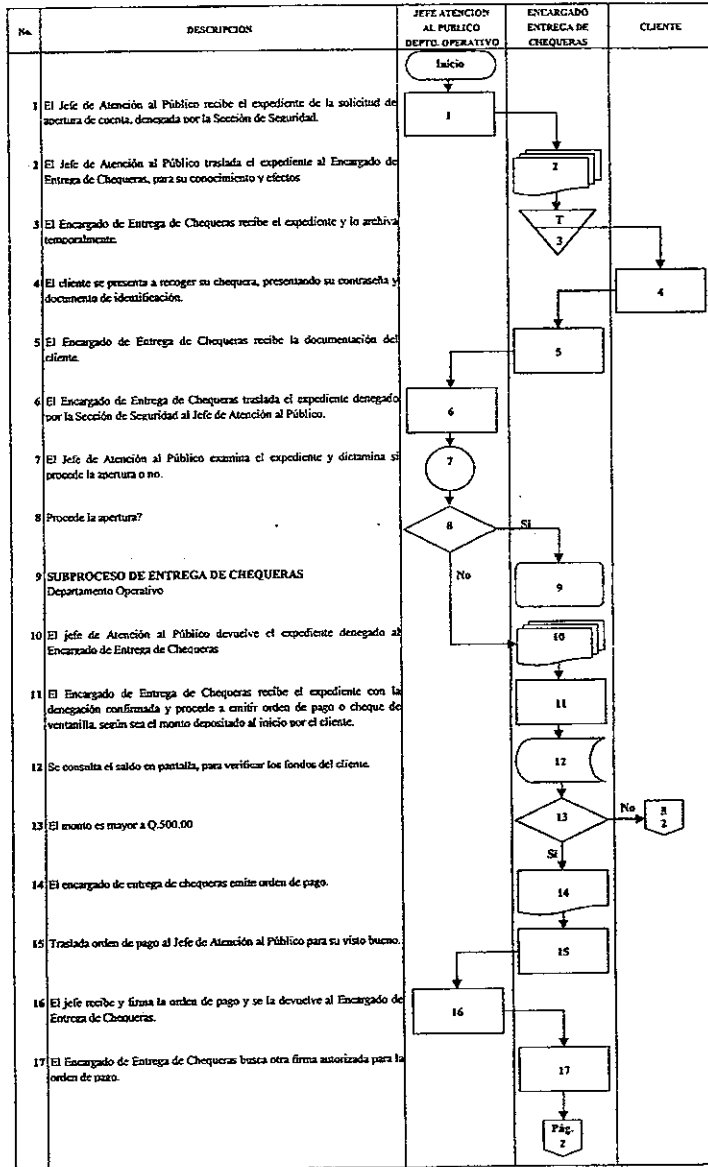
De acuerdo al análisis que se realizó en el flujograma, no se detectó ninguna deficiencia en el proceso que describe la denegación de apertura de una cuenta.

CONCLUSION:

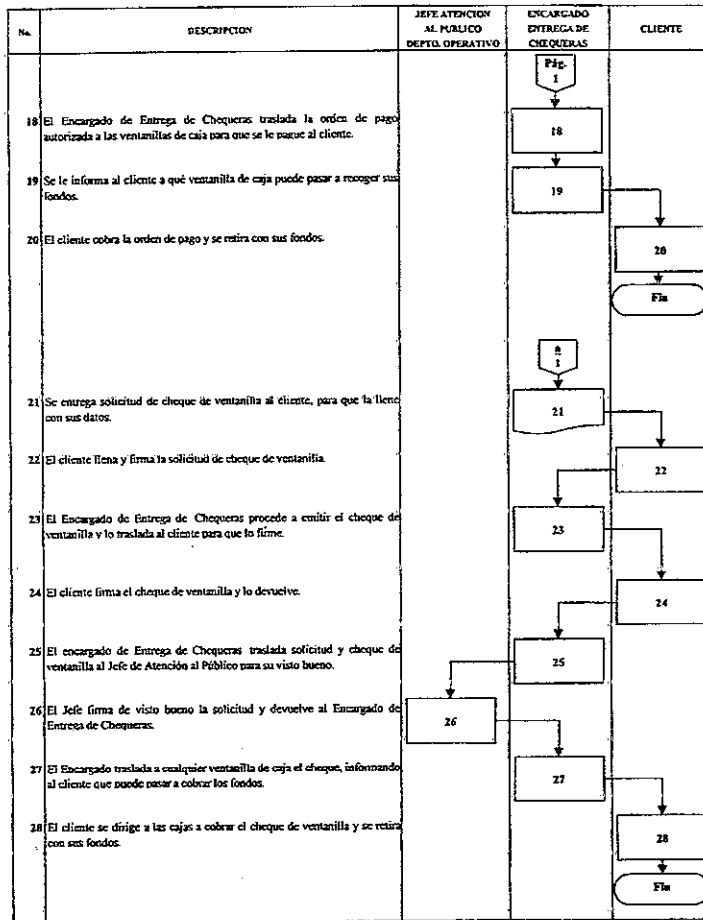
De conformidad con los procedimientos de auditoría efectuados se concluye que, el proceso que se describe en el flujograma para llevar a cabo la denegación de apertura de una cuenta, es razonable.

Hecho Por: EADA
Fecha: 02/01/98
Revisado Por: BS
Fecha: 04/01/98

PROCESO QUE SE REALIZA PARA LA DENEGACION
DE APERTURA DE UNA CUENTA NUEVA
DEPARTAMENTO OPERATIVO



PROCESO QUE SE REALIZA PARA LA DENEGACION
DE APERTURA DE UNA CUENTA NUEVA
DEPARTAMENTO OPERATIVO



TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Examen del proceso de captura de firmas.

TRABAJO REALIZADO:

La verificación consistió en hacer un análisis de los diferentes procedimientos que se tienen que realizar en el proceso de captura de firmas. En ese sentido, el examen consistió en evaluar la congruencia, secuencia lógica y fiabilidad de cada paso descrito en el flujograma obtenido para el efecto. Asimismo, se hicieron entrevistas con las personas involucradas en este proceso, con el objeto de conocer su opinión acerca de los nuevos procedimientos propuestos, derivado de la implantación del nuevo sistema.

TIPOS DE CONTROLES INCLUIDOS EN EL PROCESO:**Controles Manuales:**

- El conocimiento firmado por el encargado de captura de firmas, por concepto de la recepción de los registros de firma.
- El envío de los registros de firma a microfilm, a través de conocimiento.

Controles en los Datos de Entrada:

- Identificación de una sola terminal para escanear los registros de firma.
- Identificación de usuario, ya que el encargado de captura de firmas es la única persona autorizada para realizar esta labor.

Controles de Procesamiento:

- Verificación de las firmas en pantalla, después de haberse escaneado las mismas.
- Verificación de los datos capturados en la computadora, provenientes de la tarjeta de firmas.
- Cotejo del total de las tarjetas físicas de firmas contra el total de los registros procesados en la computadora.

Controles de Almacenamiento de Datos:

- El back-up realizado al final del día de las firmas capturadas en el disco duro.
- El diskette de contingencias que contiene las firmas grabadas de un día anterior, el cual se utilizará en caso de que alguna agencia no haya recibido adecuadamente la transmisión de firmas.
- El archivo permanente de los registros microfilmados.

BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

B

2/2

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Examen del proceso de captura de firmas.

Controles de la Información de Salida:

- El listado impreso por el Departamento de Procesamiento Electrónico de Datos, de los registros capturados el día anterior.

RESULTADO DE LA VERIFICACION:

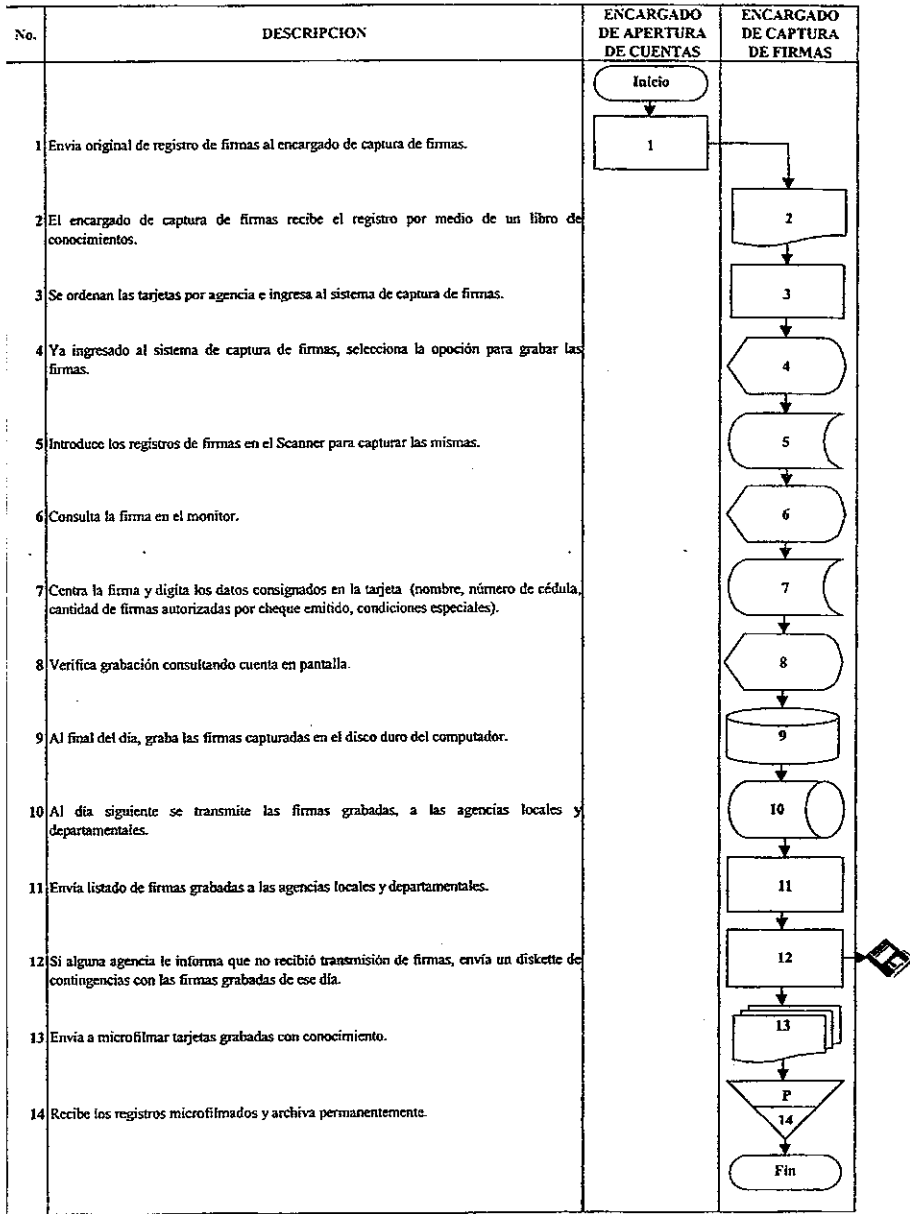
De acuerdo al análisis que se realizó en el flujograma, no se detectó ninguna deficiencia en el proceso que describe la captura de firmas.

CONCLUSION:

De conformidad con los procedimientos de auditoría efectuados se concluye que, el proceso que se describe en el flujograma para llevar a cabo la captura de firmas, es razonable.

Hecho Por: EADA
Fecha: 02/01/98
Revisado Por: BS
Fecha: 04/01/98

**PROCESO DE CAPTURA DE FIRMAS
DEPARTAMENTO OPERATIVO**



BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

C

1/2

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Examen del proceso que se realizará para entrega de chequeras.

TRABAJO REALIZADO:

La verificación consistió en hacer un análisis de los diferentes procedimientos detallados en el flujograma obtenido para el efecto. En ese sentido, el examen consistió en evaluar la congruencia, secuencia lógica y fiabilidad de cada paso descrito en el proceso propuesto para entregar chequeras. Asimismo, se hicieron entrevistas con las personas involucradas en este proceso, con el objeto de conocer su opinión acerca de los nuevos procedimientos propuestos, derivado de la implantación del nuevo sistema.

TIPOS DE CONTROLES INCLUIDOS EN EL PROCESO:

Controles Manuales:

- El conocimiento firmado por el encargado de entrega de chequeras, por concepto de la recepción del listado de emisión de chequeras entregado por el encargado del control y verificación de chequeras.
- El archivo cronológico, por fecha y número de cuenta, de las chequeras personalizadas que se encuentran por entregar, el cual es realizado por el encargado de entrega de chequeras.
- La anotación realizada en el libro de control de entrega de chequeras, para llevar un historial de las chequeras entregadas y establecer qué empleado realizó la entrega.

Controles Preventivos:

- Segregación de funciones que existe en el proceso de entrega de chequeras, en el cual participan dos personas.
- Verificación del documento de identificación del cliente que solicita que se le entregue la chequera.
- Verificación en la computadora del saldo, firma y número de cédula, antes de entregar la chequera al cliente.

Controles de la Información de Salida:

- Cotejo realizado entre las chequeras físicas personalizadas y el reporte emitido por el Departamento de Procesamiento Electrónico de Datos.

BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

C
2/2

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Examen del proceso que se realizará para entrega de chequeras.

RESULTADO DE LA VERIFICACION:

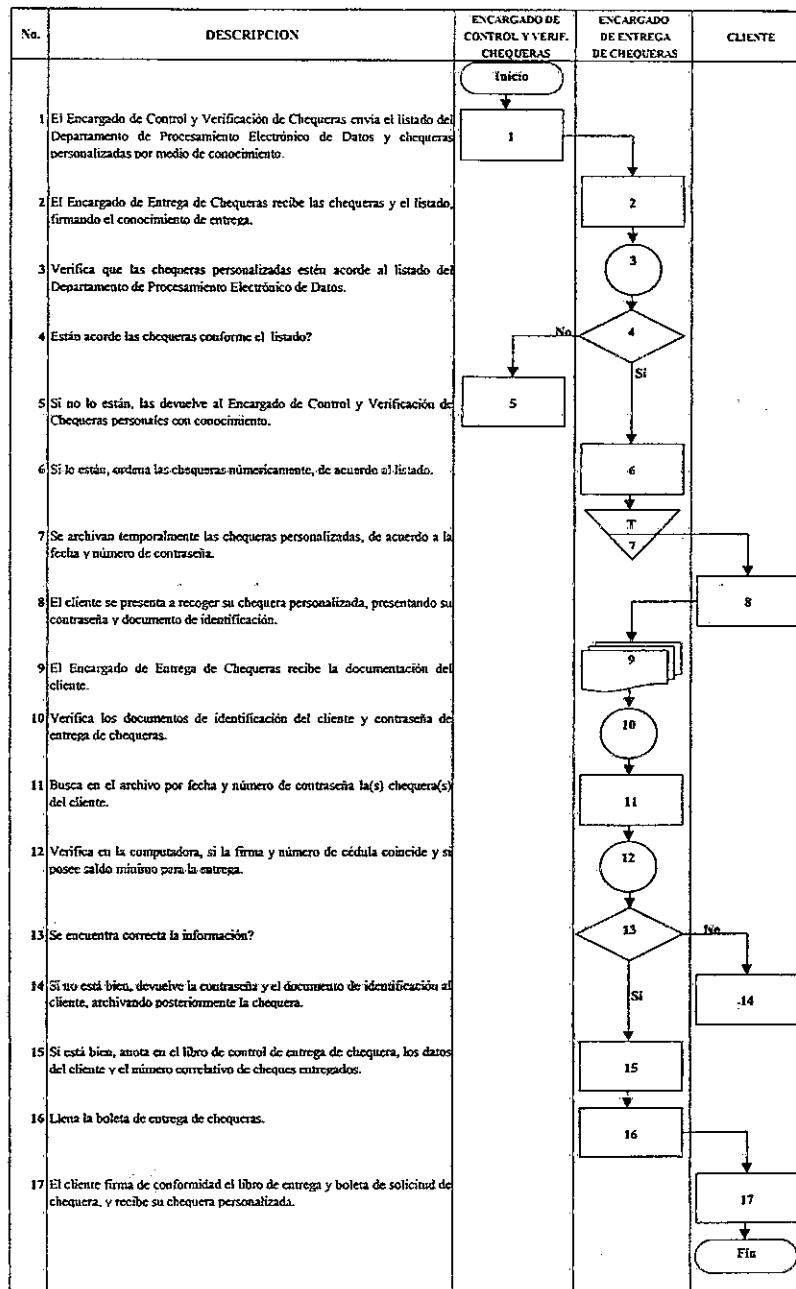
De acuerdo al análisis que se realizó en el flujograma, no se detectó ninguna deficiencia en el proceso que describe los pasos para entrega de chequeras.

CONCLUSION:

De conformidad con los procedimientos de auditoría efectuados se concluye que, el proceso que se describe en el flujograma para llevar a cabo la entrega de chequeras, es razonable.

Hecho Por: EADA
Fecha: 02/01/98
Revisado Por: BS
Fecha: 04/01/98

PROCESO QUE SE REALIZA PARA ENTREGA DE CHEQUERAS
DEPARTAMENTO OPERATIVO



BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

D

1/2

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Examen del proceso de pago de cheques.

TRABAJO REALIZADO:

La verificación consistió en hacer un análisis de los diferentes procedimientos detallados en el flujograma obtenido para el efecto. En ese sentido, el examen consistió en evaluar la congruencia, secuencia lógica y fiabilidad de cada paso descrito en el proceso propuesto para el pago de un cheque. Asimismo, se hicieron entrevistas con las personas involucradas en este proceso, con el objeto de conocer su opinión acerca de los nuevos procedimientos propuestos, derivado de la implantación del nuevo sistema.

TIPOS DE CONTROLES INCLUIDOS EN EL PROCESO:**Controles Manuales:**

- La boleta de rechazo realizada por el receptor-pagador, en la cual consta el motivo por el cual se rechazó un cheque.

Controles Preventivos:

- Segregación de funciones que existe en el proceso de pago de un cheque, en el cual pueden participar dos personas.

Controles en los Datos de Entrada:

- Verificación del documento de identificación del cliente que solicita que se le pague un cheque.
- Verificación del texto (fecha, valor en letras y en números), firma, endoso, monto y fondos, antes de proceder a pagar el cheque.
- Autorización del Jefe de Caja, cuando el monto del cheque es mayor a Q. 50,000.00.

Controles de Transmisión:

- Identificación de las terminales autorizadas para realizar el pago de los cheques.
- Identificación del receptor-pagador que realiza las operaciones, a través de su password.
- Encriptación de los datos entre la terminal y el computador central.

Controles de Procesamiento:

- Número de autorización que certifica la máquina, cuando el valor del cheque es rebajado al saldo de la cuenta contra la cual se giró.
- Verificación realizada por el sistema, del monto autorizado para ser pagado por el receptor-pagador, sin la autorización del Jefe de Caja (en este caso hasta Q. 50,000.00).

BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

D

2/2

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Examen del proceso de pago de cheques.

Controles de Almacenamiento de Datos:

- El archivo que genera la operación en el computador central.
- El archivo de los documentos fuente que dieron origen a la operación.

Controles de la Información de Salida:

- El cuadro que se emite al final del día, en donde se detalla un resumen de las operaciones realizadas por cada receptor-pagador.
- El cuadro que se realiza un día posterior, de las operaciones de caja.
- Los reportes emitidos de los cheques pagados por cada receptor-pagador.

RESULTADO DE LA VERIFICACION:

En relación a los procedimientos que se tienen que realizar en este proceso, se determinó que en el paso identificado con el número 11 del flujograma, en donde el Jefe de Caja verifica, para los cheques arriba de Q. 50,000.00, texto, firma, endoso y fondos; no se confirma por teléfono con el cuenta-habiente la autenticidad del cheque antes de proceder a su autorización para el pago.

CONCLUSION:

De conformidad con los procedimientos de auditoría efectuados se concluye que, dentro del flujograma que describe el pago de un cheque, existe una deficiencia en cuanto al pago de los mismos, por un monto arriba de Q. 50,000.00.

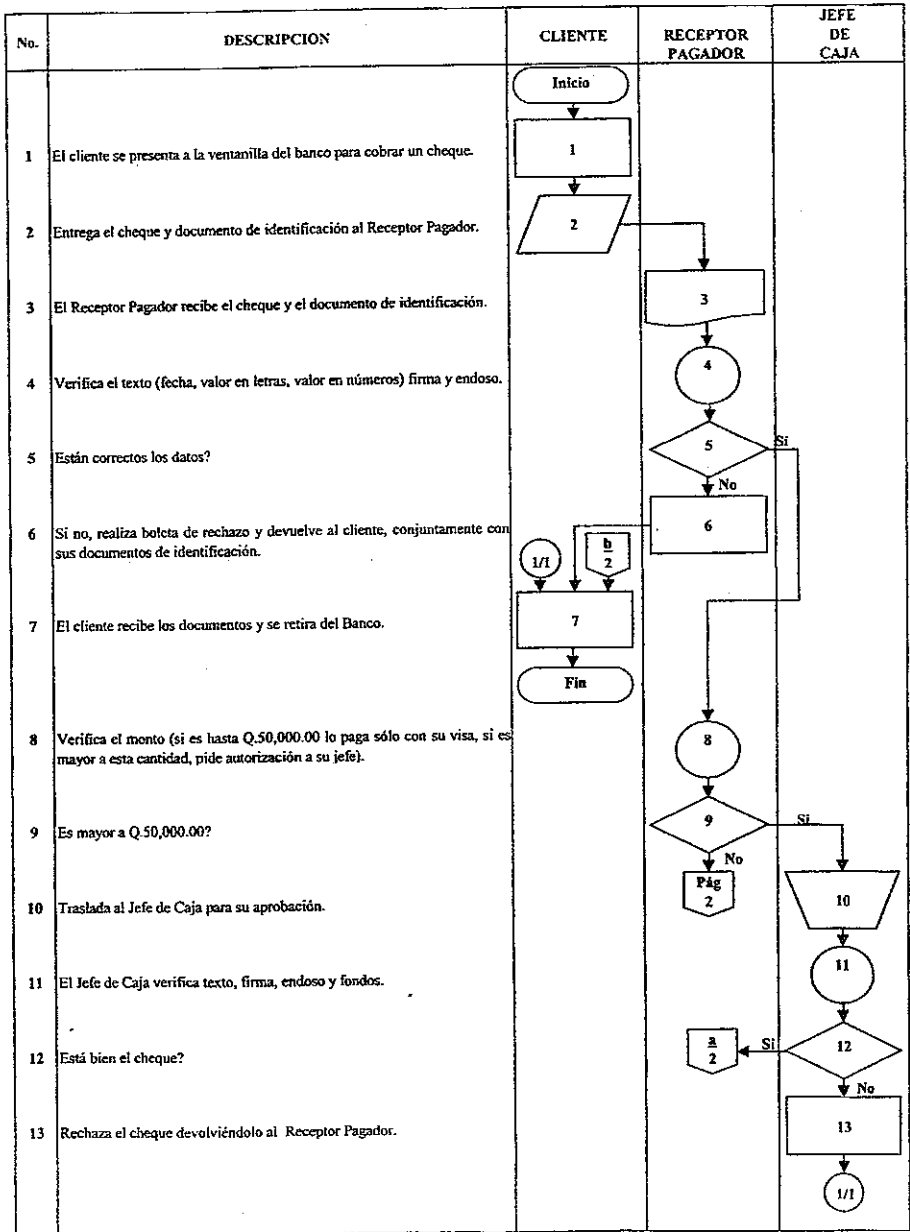
RECOMENDACION:

De acuerdo a la deficiencia observada, se estima necesario incorporar lo siguiente:

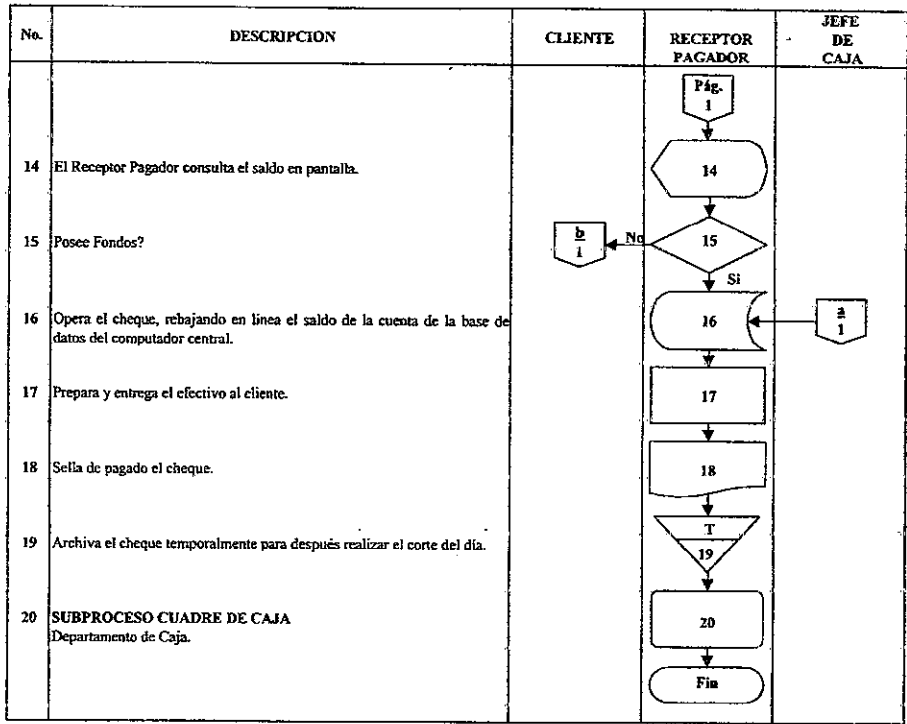
En el procedimiento No. 11, como una responsabilidad del Jefe de Caja, confirmar con el cliente, vía telefónica, aquellos cheques que se presenten para su cobro arriba de Q. 50,000.00.

Hecho Por: EADA
Fecha: 02/01/98
Revisado Por: BS
Fecha: 04/01/98

**PROCESO DE PAGOS DE CHEQUES
DEPARTAMENTO DE CAJA**



**PROCESO DE PAGOS DE CHEQUES
DEPARTAMENTO DE CAJA**



BANCO BUENA SUERTE, S. A.
Departamento de Auditoría Interna

E

TRABAJO GENERAL:

Evaluación del diseño de un sistema de redes electrónicas que se usará para manejar operaciones de depósito monetarios.

TRABAJO ESPECIFICO:

Verificación del diseño de la red.

TRABAJO REALIZADO:

- 1 Mediante oficio de fecha 30 de diciembre de 1997, el Ingeniero Juan Pérez manifestó que de conformidad con la evaluación que había llevado a cabo respecto a la configuración de la red, la que servirá para realizar operaciones de depósito monetarios, provee una certeza razonable de transmisión, diseño y programación.
- 2 Se verificó que el trabajo del especialista fue llevado a cabo de conformidad con la planificación general del proyecto, en aspectos tales como: el alcance del estudio, la presentación técnica y la fecha en que se presentó el informe. De lo anterior se obtuvieron resultados satisfactorios.
- 3 Se procedió a desarrollar procedimientos de operación y decisión para la red que se desea implantar, tales como: políticas de autorización de usuario, niveles de acceso, políticas de sitio, y otras, las cuales fueron trasladadas a Sistemas Empresariales, S. A., mediante oficio No. 197-97 de fecha 30 de diciembre de 1997.

CONCLUSION

El resultado de la verificación es razonable.

Hecho Por: EADA
Fecha: 02/01/98
Revisado Por: BS
Fecha: 04/01/98

CONCLUSIONES

1. De acuerdo con la hipótesis formulada en el plan de investigación, se determinó que los riesgos genéricos puros, percibidos desde el punto de vista financiero, derivados de no tener instalado un adecuado sistema de control interno en las operaciones de las cuentas de depósitos monetarios realizadas a través de un sistema de redes electrónicas, y que pueden afectar a una institución bancaria, son:
 - a. Los delitos que se pudieran cometer en contra de su patrimonio y/o cuenta-habientes.
 - b. Ser sujetos de multas y/o sanciones.
 - c. Errores, omisiones y/o irregularidades que ocasionen deficiencia en el servicio bancario.
 - d. Ocurrencia de incendios, explosiones, pérdidas y/o extravíos.

2. La participación de Auditoría Interna en la implantación de un sistema de redes electrónicas, para el manejo de las operaciones en las cuentas de depósitos monetarios, se debe realizar desde un inicio, derivado de la importancia de incluir desde ese momento los controles necesarios que aseguren la calidad, confiabilidad y oportunidad del sistema que se desea desarrollar.

3. El Auditor Interno deberá considerar que al implantar los diversos controles en un sistema de redes electrónicas, éstos no disminuyan la capacidad productiva de la institución bancaria en el manejo de sus operaciones.

4. Es importante que el Auditor Interno, antes de implantar una política de seguridad de red en un sitio, establezca que la misma no afecta a otros sitios que puedan tener sus propias políticas de seguridad de red.

5. El objetivo primordial de un sistema de redes electrónicas es transferir e intercambiar información entre servidores y terminales, a través de uno o varios caminos o medios de transmisión, por lo que el Contador Público y Auditor deberá enfocar su evaluación en torno a la confiabilidad, eficiencia y oportunidad de esa comunicación.

RECOMENDACIONES

Cuando el Auditor haya identificado y evaluado los riesgos financieros a que están expuestas las operaciones de depósitos monetarios realizadas a través de redes electrónicas, deberá establecer un *“Programa Integral de Protección en Red”*, el cual se podrá llevar a cabo de acuerdo con el siguiente orden:

- a. Establecer una cultura organizacional que genere un alto grado de conciencia a todos los niveles involucrados en el sistema.
- b. Desarrollar una educación permanente que refuerce la cultura organizacional.
- c. Implantar políticas y estándares de seguridad en la red que sean efectivos para proteger la inversión y recursos de la información del banco.
- d. Establecer normas y procedimientos que conformen el sistema propio de control interno el cual proporcione una efectiva y eficaz seguridad a la institución bancaria en las operaciones de las cuentas de depósitos monetarios realizadas en el sistema de redes electrónicas.

La actuación de Auditoría Interna en la implantación de un sistema de redes electrónicas, para el manejo de las operaciones en las cuentas de depósitos monetarios, debe realizarse de acuerdo con las fases o etapas que se llevan a cabo para la construcción de un nuevo sistema:

- a. **Inicio:** Evaluar la forma en que se abordará el problema, la posibilidad de cumplir los objetivos planteados (recopilándolos para verificar posteriormente si éstos se cumplieron), así como el costo-beneficio que se obtendrá de la realización del proyecto.
- b. **Análisis:** Examinar las políticas, procedimientos y normas que se llevaron a cabo para realizar el análisis de la especificación del sistema.

- c. **Diseño:** Establecer controles internos y determinar los procedimientos de operación y decisión, para la red que se desea implantar.
 - d. **Desarrollo:** Verificar que el sistema garantice el cumplimiento de los requisitos de las especificaciones funcionales y que se haya desarrollado de acuerdo a lo planeado.
 - e. **Implantación:** Realizar pruebas selectivas en el sistema para establecer que el mismo tenga los controles necesarios, que haya confiabilidad en la comunicación de datos y que efectivamente cumpla con los objetivos y beneficios esperados.
3. Para que un control en un sistema de redes electrónicas no disminuya la capacidad productiva de la institución bancaria en el manejo de sus operaciones, el Auditor Interno deberá tomar en cuenta lo siguiente:
- a. Un control no evitará que los usuarios cumplan con sus tareas en forma efectiva.
 - b. El costo de proteger una amenaza debe ser menor que el costo de recuperación, si es que se ve afectado por la amenaza de seguridad.
 - c. Involucrar al tipo adecuado de personas para el diseño de un sistema de control interno en una red electrónica.
 - d. Un control efectivo es algo que todos los usuarios de la red y administradores pueden aceptar, y estar dispuestos a reforzar.
4. Para que una política de seguridad de red en particular, no afecte a otras políticas de seguridad de red de otros sitios, es importante que el Auditor Interno agrupe las metas, las necesidades y requerimientos de seguridad de todas las redes interconectadas. Esto es un punto importante, porque es posible lograr una política de seguridad de red que salvaguarde los intereses de unos, pero que pueda ser perjudicial para otros.

5. El Contador Público y Auditor al llevar a cabo una evaluación en un sistema de redes electrónicas debe utilizar, entre otras, las siguientes técnicas y procedimientos de auditoría:
- a. Utilización de sistemas de software o paquetes de auditoría.
 - b. Prueba del proceso y resultados de una operación, a través de la red electrónica, con datos del auditor.
 - c. Método de rastreo en una operación realizada en la red.
 - d. Otras técnicas de auditoría, las cuales dependerán del tipo de evaluación que se realizará en la red.

BIBLIOGRAFIA

A. Goxen / M.A. Goxens. "Enciclopedia de Contabilidad 1. Contabilidad General". Volumen 1. Barcelona, España. 1990.

Aragón Aldana, César Aníbal. "Planeación y Desarrollo de un Sistema de Información Computarizado". Guatemala. 1996.

Arévalo Alburez, José Alejandro. "Auditoría de Sistemas de Información Basados en Computadoras Electrónicas". Centro de Formación Profesional Tayasal. Guatemala. 1990.

Azzollini, Vicente. "El Auditor Interno y los Cajeros Automáticos". Pistas de Auditoría, Boletín del Instituto de Auditores Internos. Noviembre / Diciembre 1988.

Black, Uyles. "Redes de Computadoras, Protocolos, Normas e Interfaces". Macrobit Editores, S.A. México. 1990.

Carreño, Manuel. "Prevención del Fraude Informático en Entidades Financieras". Desarrollo Profesional Avanzado. El Salvador. 1998.

Cashin, James A. y otros. "Enciclopedia de la Auditoría". Editorial Océano. Barcelona, España. 1993.

De Casso, Ignacio y Francisco Cervera. "Diccionario de Derecho Privado". Editorial Labor, S.A. España. 1954.

De Paz Suyen, Miriam Carolina. "Importancia de la Supervisión de Auditoría Interna en el Departamento de Caja y Depósitos de un Banco Privado". Facultad de Ciencias Económicas, Universidad de San Carlos de Guatemala. 1993.

- Delgado, Xiomar. **"Auditoría en Informática"**. Centro Latinoamericano de Capacitación y Consultoría, S.A. Guatemala. 1997.
- Echenique, José Antonio. **"Auditoría en Informática"**. Editorial McGraw-Hill. México. 1994.
- Fernández Díaz, Aurelio. **"Estudio y Evaluación de un Sistema de Control Interno Contable"**. Primera edición. Guatemala. 1985.
- González Arévalo, Carlos. **"Sistema Bancario Moderno"**. Departamento de Publicaciones, Facultad de Ciencias Económicas, Universidad de San Carlos de Guatemala. 1990.
- Ince, D.C. **"Ingeniería de Software"**. Addison Wesley Iberoamericana. Estados Unidos. 1993.
- Instituto Guatemalteco de Contadores Públicos y Auditores. **"Normas de Auditoría"**. Recopilación 1992. Guatemala. 1992.
- Juárez Leal, Raúl Stuardo. **"Red de Datos en la Sección Financiera de una Entidad Descentralizada del Sector Público de Guatemala"**. Guatemala. 1994.
- Juárez Ortiz, Claudia Patricia y Miriam Irene Silva Sical. **"Controles Internos Utilizados en Auditoría de Sistemas de Computación"**. Guatemala. 1992.
- Kell, Walter G. y otros. **"Auditoría Moderna"**. Compañía Editorial Continental, S.A. de C.V. México. 1987.
- León, Deeynar Estuardo. **"Interconexión de Redes Remotas"**. Guatemala. 1994.

- Lizano, Eduardo. **"La Reforma Financiera en América Latina"**. Editorial Centro de Estudios Monetarios Latinoamericanos. Primera edición. México. 1993.
- Meigs, Walter B. y otros. **"Principios de Auditoría"**. Editorial Diana. Segunda Edición. México. 1985.
- Mock, Theodore y Jerry L. Turner. **"Evaluación y Juicio del Auditor en Relación con el Control Interno Contable"**. Instituto Mexicano de Contadores Públicos, A.C. Segunda edición. México. 1993.
- Molina M., Ernesto R. **"Contabilidad Bancaria"**. Colección "Textos Modernos". Editorial Piedra Santa. Undécima edición. Guatemala. 1988.
- Porter W., Thomas Jr. **"Auditoría de Sistemas Electrónicos"**. Editorial Herrero Hnos., Sucs., S.A. México. 1988.
- Real Academia Española. **"Diccionario de la Real Academia Española"**. Editorial Espasa Calpe, S.A. Décimo octava edición. Madrid. 1956.
- Reyes Calderón, José Adolfo. **"Seguridad Bancaria"**. Banco de Guatemala. Primera edición. Guatemala. 1990.
- Schwartz, Mischa. **"Redes de Telecomunicaciones, Protocolos, Modelado y Análisis"**. Editorial Addison-Wesley Iberoamericana. Estados Unidos. 1994.
- Siyan, Karanjit y Chris Hare. **"Internet y Seguridad en Redes"**. Editorial Prentice Hall Hispanoamericana, S.A. México. 1995.
- Superintendencia de Bancos. **"La Auditoría y el Procesamiento Electrónico de Datos"**. Guatemala. 1976.



- Velásquez Vásquez, Efraín de Jesús. **"Los Riesgos en la Auditoría en la Información Procesada por P.E.D."**. Facultad de Ciencias Económicas, Universidad de San Carlos de Guatemala. 1993.
- Villacís V., Juan. **"Guía Práctica de Auditoría Interna para Bancos"**. Banco de Guatemala. 1993.
- Zacarías, Roberto Vinicio. **"Estudio, Evaluación y Diseño de un Sistema de Control Interno Contable y Administrativo de una Cooperativa Agrícola"**. Guatemala. 1988.
- ----- **"Estrategias Financieras Frente a la Integración Económica"**. Instituto Guatemalteco de Contadores Públicos y Auditores. Revista No. 87. Noviembre 1993.
- ----- **"Perspectivas del Sistema Financiero Guatemalteco en el Contexto de la Globalización de la Economía"**. Instituto Guatemalteco de Contadores Públicos y Auditores. Revista No. 84. Diciembre 1992.
- ----- **"Programa de Modernización del Sistema Financiero Nacional"**. Banco de Guatemala. Septiembre 1993.
- ----- **"Recomendaciones para Apertura de Cuentas y Principales Operaciones con el Público"**. Asociación de Banqueros de Guatemala. Circular No. 16-95. 1995.