UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONOMICAS.

"CONTROL INTERNO PARA UN SISTEMA TRANSACCIONAL DE REMESAS FAMILIARES EN UNA ENTIDAD BANCARIA"

TESIS

PRESENTADA A LA HONORABLE JUNTA DIRECTIVA DE LA FACULTAD DE CIENCIAS ECONÓMICAS

POR

FREDY WILIAN GÓMEZ ESCOBAR

PREVIO A CONFERÍRSELE EL TÍTULO DE

CONTADOR PÚBLICO Y AUDITOR

EN EL GRADO ACADEMICO DE

LICENCIADO

Guatemala, enero de 2007.

MIEMBROS DE LA JUNTA DIRECTIVA DE LA
FACULTAD DE CIENCIAS ECONÓMICAS

DECANO:	Lic. José Rolando Secaida Morales
SECRETARIO:	Lic. Carlos Roberto Cabrera Morales
VOCAL 1ro.	Lic. Canton Lee Villela
VOCAL 2do.	Lic. Mario Leonel Perdomo Salguero
VOCAL 3ro.	Lic. Juan Antonio Gómez Monterroso
VOCAL 4to.	P.C. Efrén Arturo Rosales Álvarez
VOCAL 5to.	P.C. Deiby Boanerges Ramírez Valenzuela

PROFESIONALES QUE REALIZARON
LOS EXAMENES DE ÁREAS PRÁCTICAS BÁSICAS.

MATEMÁTICA ESTADÍSTICA	Licda. Esperanza Roldan de Morales
CONTABILIDAD	Lic. Gaspar Humberto López Jiménez
AUDITORÍA:	Lic. José de Jesús Portillo Hernández

PROFESIONALES QUE REALIZARON

EL EXAMEN PRIVADO DE TESIS

PRESIDENTE:	Lic. Manuel Alberto Selva Rodas.
EXAMINADOR:	Lic Erick Roberto Flores López.
EXAMINADOR:	Lic. Jorge Luis Monzón Rodríguez.

Guatemala, 14 de agosto de 2006.

Licenciado Eduardo Antonio Velásquez Carrera
Decano Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala
Ciudad Universitaria, Ciudad, Zona 12.

Señor Decano:

De conformidad con la designación, que se me hiciera, para asesorar al estudiante **Fredy Wilian Gómez** Escobar en su trabajo de Tesis denominado **"CONTROL INTERNO PARA UN SISTEMA TRANSACCIONAL DE REMESAS FAMILIARES EN UNA ENTIDAD BANCARIA".**

Tengo a bien informar, que en mi opinión el trabajo presentado por el estudiante Gómez Escobar, se ha realizado de conformidad con el plan autorizado y cumple con los requisitos establecidos para una tesis profesional, por lo que me permito recomendarlo para que se proceda al tramite respectivo, y pueda someterse al Examen Privado de Tesis, previo a optar al **Titulo de Contador Público y Auditor**, en el **grado académico de Licenciado.**

Con las muestras más altas de mi consideración, respeto y estima me suscribo del Señor Decano.

Jorge Luis Rivera Ávila
CONTADOR PÚBLICO Y AUDITOR
Colegiado 1206

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE
CIENCIAS ECONOMICAS
Edificio "S-8"
Ciudad Universitaria, Zona 12
Guatemala, Centroamérica

DECANATO DE LA FACULTAD DE CIENCIAS ECONOMICAS. GUATEMALA, VEINTIOCHO DE FEBRERO DE DOS MIL SIETE.

Con base en el Punto NOVENO, inciso 9.1, Subinciso 9.1.1 del Acta 4-2007 de la sesión celebrada por la Junta Directiva de la Facultad el 22 de febrero de 2007, se conoció el Acta AUDITORIA 222-2006 de aprobación del Examen Privado de Tesis, de fecha 15 de noviembre de 2006 y el trabajo de Tesis denominado: "CONTROL INTERNO PARA UN SISTEMA TRANSACCIONAL DE REMESAS FAMILIARES EN UNA ENTIDAD BANCARIA", que para su graduación profesional presentó el estudiante **FREDY WILIAN GOMEZ ESCOBAR**, autorizándose su impresión.

Atentamente,

"ID Y ENSEÑAD A TODOS"

LIC. CARLOS ROBERTO CABRERA MORALES
SECRETARIO

FACULTAD DE CIENCIAS ECONOMICAS
EL SECRETARIO
Guatemala, C. A.

LIC. JOSE ROLANDO SECAIDA MORALES
DECANO

FACULTAD DE CIENCIAS ECONOMICAS
EL DECANO
GUATEMALA, C. A.

Smp.

DEDICATORIA

A DIOS: Fuente de sabiduría y amor, que me permitió hacer realidad tan anhelado sueño.

A MI ESPOSA: Briseida, con todo mi amor por su comprensión y apoyo incondicional.

A MIS HIJOS: Fredy José y Francisco Javier, con todo mi amor.

A MIS PADRES: Teófilo Julián Gómez López y Teresa de Jesús Escobar de Gómez, mi agradecimiento especial, por haberme dado la mejor herencia.

A MIS HERMANOS: Edgar, Amilcar y Maynor, con amor y afecto.

A MIS ABUELOS Rigoberto Escobar, Eduarda Mejía, Gregorio Gómez y Teodora López (Q.E.P.D.), por sus sabios consejos y enseñanzas.

A MIS TIAS Y TIOS: Por su apoyo y en especial a Tía Elvira (Q.E.P.D).

A MI ASESOR DE TESIS: Lic. Jorge Luis Rivera Ávila, por brindarme su apoyo y tiempo necesarios para la realización de esta tesis.

AGRADECIMIENTO: A la Facultad de Ciencias Económicas de la Universidad de San Carlos de Guatemala y a todos los catedráticos que contribuyeron en mi formación profesional.

A MIS AMIGOS: Por su comprensión y amistad sincera.

A USTED ESPECIALMENTE:

INDICE

Página

INTRODUCCION

Durante los últimos años el negocio de remesas familiares provenientes de Estados Unidos de América, ha alcanzado gran auge en Guatemala. A tal punto que los ingresos de divisas por este concepto, según datos publicados por el Banco de Guatemala, se han posicionado en la segunda fuente de ingresos de divisas al país.

Las empresas que prestan el servicio de envío de remesas familiares a través de Transferencias Electrónicas, se encuentran constituidas en el país emisor y por medio de los bancos constituidos en Guatemala realizan los pagos a los beneficiarios de las remesas. De esta manera los bancos nacionales con las transferencias electrónicas han incursionado en el negocio de remesas familiares, ya sea que formen parte del mismo grupo financiero al que pertenece la empresa remesadora o por alianzas o convenios.

Para brindar a los usuarios un servicio eficiente y seguro las empresas remesadoras y los bancos deben implementar sistemas informáticos que además de la eficiencia y rapidez de las transacciones, contengan los controles adecuados.

Los bancos son entidades en donde los sistemas informáticos se utilizan en forma rutinaria, de lo que también deriva la dependencia, a tal punto que sin sistemas informáticos adecuados, cualquier banco se encontraría en una situación de desventaja en relación a la competencia. En consecuencia es necesario para éstos contar con sistemas de información de los mas sofisticados que requiere el medio; pero sin olvidar los controles que aseguren la integridad de los datos procesados.

Los bancos siempre han estado expuestos a riesgos de errores o fraudes. Estos riesgos se han incrementado, a la velocidad de la innovación de la tecnología en informática y la integración de operaciones automáticas.

Con el objeto de formar una concepción general respecto a los servicios que ofrecen los Bancos que operan en Guatemala, en el capítulo I se desarrollan conceptos sobre la banca en Guatemala.

En el capitulo II se expone lo referente a las Remesas Familiares, se abordan conceptos y formas por medio de los cuales los remitentes hacen llegar la ayuda económica a los beneficiarios en Guatemala.

También se identifican de forma general los aspectos legales en materia de lavado de activos y financiación al terrorismo, a que está sujeta la actividad de las empresas remesadoras en Estados Unidos de América, dentro de los que puede mencionarse el Bank Screcy Act – 1970, Money Laundering Control Act – 1986, Anti-Drug Abuse Act – 1988, Crime Control Act – 1990, Anti-Money Laundering Act of 1993, Estatutos y Leyes Federales Aprobadas por el Congreso, The USA Patriot Act (Acta Patriota) y la Prohibition of Unlicensed Money Transmitting Business, (Prohibición de empresas de envío de remesas de dinero, sin contar con la debida licencia).

En el Capítulo III se presenta la definición de control Interno en forma general.

En el Capitulo IV se desarrolla el tema de los sistemas de información y el control interno enfocados a estos. Se exponen conceptos y elementos de control que permiten dar una certeza razonable de la autenticidad, confidencialidad e integridad de la información.

Finalmente en el Capitulo V, se desarrolla una guía del diseño de un sistema integrado de control interno para un sistema transaccional de remesas familiares. Se presenta un caso práctico que proporciona los lineamientos que pueden seguirse para el adecuado diseño de un sistema integrado de control interno para la operación de sistemas, tomándose como ejemplo una empresa remesadora de divisas que se encuentra establecida en el Estado de California de Estados Unidos de América.

En el caso práctico se desarrollan y proponen detalladamente los puntos de control para la protección de la información generada por medio de sistemas.

Con la investigación efectuada se derivan conclusiones y recomendaciones que se presentan al final de la presente tesis.

CAPITULO I

GENERALIDADES SOBRE LOS BANCOS EN GUATEMALA

En Guatemala el sistema bancario está organizado bajo el sistema de Banca Central como lo establece el Artículo No.132 de la Constitución Política de la República de Guatemala

"Las actividades monetarias, bancarias y financieras, estarán organizadas bajo el sistema de banca central, el cual ejerce vigilancia sobre todo lo relativo a la circulación de dinero y a la deuda pública. "

El sistema financiero es dirigido por la Junta Monetaria e inspeccionado por la Superintendencia de Bancos como lo establece el artículo No.133 de la Constitución Política de la República de Guatemala.

"Dirigirá este sistema, la Junta Monetaria, de la que depende el Banco de Guatemala, entidad autónoma con patrimonio propio, que se regirá por su Ley Orgánica y la Ley Monetaria. "

"La Superintendencia de Bancos, organizada conforme a la ley, es el órgano que ejercerá la vigilancia e inspección de bancos, instituciones de crédito, empresas financieras, entidades afianzadoras, de seguros y las demás que la ley disponga."

La Superintendencia de Bancos en la publicación, mensual que corresponde a los datos del mes de Septiembre 2006, detalla que a esa fecha en el país existían 26 bancos en funcionamiento, los que se detallan a continuación:

1. El Crédito Hipotecario Nacional de Guatemala
2. Banco Inmobiliario, S. A.
3. Banco de los Trabajadores
4. Banco Industrial, S. A.
5. Banco de Desarrollo Rural, S. A.
6. Banco Internacional, S. A.
7. Banco del Quetzal, S. A.
8. Banco de Exportación, S. A.
9. Banco Reformador, S. A.
10. Citibank, N. A. Sucursal Guatemala
11. Banco Uno, S. A.
12. Banco Corporativo, S. A.
13. Primer Banco de Ahorro y Préstamo para la Vivienda Familiar, S.A.
14. Banco de la República, S. A.
15. Banco SCI, S. A.
16. Banco Americano, S. A.
17. Banco Privado para el Desarrollo, S. A. (BANCASOL)
18. Banco de Antigua, S. A.
19. Banco de América Central, S. A.
20. Banco Cuscatlán de Guatemala, S. A.
21. Banco Agromercantil de Guatemala, S. A
22. Banco G&T Continental, S. A.
23. Banco de Crédito, S. A.

En Situación Especial:

24. Banco de Comercio, S. A. (a)
25. Banco del Café, S. A. (b)
26. Banco de Occidente, S. A. (c)

a) La Junta Monetaria Mediante resolución No. JM-13-2007, del 12 de enero de 2007, resolvió suspender las operaciones del Banco de Comercio, Sociedad Anónima.

b) La Junta Monetaria Mediante resolución No. JM-120-2006, de fecha 19 de octubre de 2006, resolvió suspender las operaciones del Banco del Café, Sociedad Anónima.

c) La Junta Monetaria, en resolución JM-69-2006, autorizó la fusión por absorción de Banco de Occidente, S.A., por Banco Industrial, S.A.

1.1 Definiciones

La ley de Bancos y Grupos Financieros, Decreto número 19-2002 del Congreso de la República, contiene las definiciones siguientes:

1.1.1. Grupo Financiero

"Los grupos financieros están conformados por dos o más personas jurídicas, en las que existe control común por relaciones de administración, propiedad, imagen corporativa; o sin que se den dichas relaciones acuerdan el control común; pudiendo ser éstas: Bancos, Sociedades Financieras, Casas de Cambio, Almacenes Generales de Depósito, Aseguradoras, Afianzadoras, Casas de Bolsa, Empresas especializadas en emisión y/o administración de tarjetas de crédito, etc." (2:8)

1.1.2. Empresa Controladora

"Su objeto social exclusivo será la dirección, administración, control y representación del grupo financiero." (2:10)

1.1.3. Subsidiaria:

"Compañía poseída o controlada por otra compañía tenedora o matriz, con mayor frecuencia por medio de la propiedad de las acciones con derecho a voto."(3:489)

1.1.4. Banco

"Son aquellas instituciones cuya actividad principal radica en servir como intermediarios entre capitales ajenos en busca de colocación y empleo; así como, de las distintas personas, individuales o jurídicas, que necesitan de financiamiento para la consecución de sus objetivos y por tal razón acuden a la obtención de préstamos."(2:12)

En resumen los bancos son instituciones encargadas de captar recursos de capital excedentes y transferirlos a los sectores de la actividad económica que los necesitan.

1.2 Clasificación de los bancos

De acuerdo a la ley de Bancos y Grupos Financieros, los bancos se clasifican en:

1.2.1 Privados Nacionales

Estos bancos serán constituidos en forma de sociedades anónimas; pudiendo realizar las distintas operaciones y servicios, así como observar y aplicar lo establecidos en la ley relacionada.

1.2.2 Extranjeros

Podrán operar en Guatemala, por medio de sucursales o bien registrar una oficina de representación para la promoción de negocios y el otorgamiento de financiamiento en el territorio nacional; para lo cual debe apegarse a lo que indica la ley de Bancos y Grupos Financieros; y en lo procedente a la demás legislación vigente.

1.3 Operaciones que realizan

La ley de Bancos y Grupos Financieros Decreto 19-2002 del Congreso de la Republica de Guatemala, autoriza a los bancos a realizar las operaciones descritas en los numerales subsiguientes:

Para efectos de ilustrar las transacciones que realizan los bancos nacionales, se incluyen en cada uno de los tipos de operaciones algunos ejemplos tomados del formulario de la encuesta sobre lavado de activos, realizada por la Superintendencia de Bancos por medio de la Intendencia de Verificación Especial en octubre de 2005.

1.3.1 Activas

Por medio de las cuales surge un derecho a ejercer por parte del banco contra terceros, las operaciones indicadas en la ley en referencia se encuentran las siguientes:

a) Otorgar créditos;
b) Realizar descuento de documentos;
c) Otorgar financiamiento en operaciones de cartas de crédito;
d) Conceder anticipos para exportación;
e) Emitir y operar tarjetas de crédito;
f) Realizar arrendamiento financiero;
g) Realizar factoraje;
h) Invertir en títulos valores emitidos y/o garantizados por el Estado, por los bancos autorizados de conformidad con esta ley o por entidades privadas. En el caso de la inversión en títulos valores emitidos por entidades privadas, se requerirá aprobación previa de la Junta Monetaria;
i) Adquirir y conservar la propiedad de bienes inmuebles o muebles, siempre que sean para su uso.
j) Constituir depósitos en otros bancos del país y en bancos extranjeros; y,
k) Realizar operaciones de reporto como reportador

1.3.2 Pasivas

Representan obligaciones para el banco, en las que este se compromete a dar cualquier tipo de garantía o seguridad, sobre el rendimiento, mantenimiento del valor, recuperabilidad y otros medios que representen la restitución o devolución de los fondos. En la Ley en referencia detalla las operaciones siguientes:

a) Recibir depósitos monetarios;
b) Recibir depósitos a plazo;
c) Recibir depósitos de ahorro;
d) Crear y negociar bonos y/o pagarés, previa autorización de la Junta Monetaria;

e) Obtener financiamiento del Banco de Guatemala, conforme la ley orgánica de éste;
f) Obtener créditos de bancos nacionales y extranjeros;
g) Crear y negociar obligaciones convertibles;
h) Crear y negociar obligaciones subordinadas; y,
i) Realizar operaciones de reporto como reportado.

1.3.3 Operaciones de confianza

Son las operaciones que realizan las instituciones bancarias con el objeto de prestar servicios que no representen compromisos financieros para dichas instituciones.

La Ley de Bancos y Grupos Financieros detalla las siguientes:

a) Cobrar y pagar por cuenta ajena;
b) Recibir depósitos con opción de inversiones financieras;
c) Comprar y vender títulos valores por cuenta ajena; y,
d) Servir de agente financiero, encargándose del servicio de la deuda, pago de intereses, comisiones y amortizaciones.

1.3.4 Pasivos contingentes

Dentro de los servicios denominados “pasivos contingentes” se encuentran: emitir o confirmar cartas de crédito, prestar avales, otorgar garantías y fianzas.

1.3.5 Servicios

Dentro de los servicios que prestan los bancos del sistema se pueden mencionar entre otras las siguientes:

a) Actuar como fiduciario
b) Cartas de crédito
c) Arrendamiento de cajillas de seguridad
d) Compra y venta de moneda extranjera
e) Transferencia de fondos
f) Remesas familiares.
g) Venta de cheques de caja
h) Banca electrónica.

En el siguiente capitulo se presenta la definición de Remesas Familiares, las formas de envío mas usuales utilizadas por los inmigrantes Guatemaltecos y los aspectos legales que les aplican a las empresas que se dedican a prestar este servicio en Estados Unidos de América, especialmente lo referente a la normativa de prevención de lavado de activos y financiamiento al terrorismo (AML/FT).

CAPITULO II

REMESAS FAMILIARES

2.1 Definición

Para muchos el concepto de remesas difiere en cuanto a su forma pero en esencia consiste en dinero que remiten personas, que se encuentran fuera de su país, para apoyar a familiares. A continuación se presentan algunas definiciones que se orientan a ese sentido.

> "Remisión que se hace de una cosa de una parte a otra".(7:1766)
> "Expedir, remitir, exportar, mandar, enviar".(6:176)

En el programa de Formación Económica del Banco de Guatemala con relación con el Sistema de Pagos y Remesas Familiares se definió a las remesas familiares como "[…] los envíos de dinero (en efectivo, cheque, giros, trasferencias, etc.) y de mercancías efectuados por guatemaltecos que viven mayoritariamente en Estados Unidos de América (EE UU) a sus familiares residentes en Guatemala."

En este mismo documento señala que las remesas familiares son enviadas por medio de transferencias electrónicas, money orders, giro, remesa por medio de una empresa remesadora, efectivo con un familiar o amigo.

Las remesas familiares son recursos que envían los emigrantes para ayuda familiar, cubrir necesidades de esposa o compañera de vida, hijos, padres y otros parientes cercanos; que complementan los ingresos que perciben otros miembros de esa familia o que constituyen el único ingreso familiar. Aun cuando el emigrante logra llevarse a su familia, la remesa familiar continúa enviándose, para favorecer a otros miembros de la familia, generalmente padre o madre, que se suspende cuado los lazos familiares se extinguen, el envío de dinero es realizado indistintamente de la situación legal de los remitentes.

2.2 Medios utilizados para el envío de remesas familiares.

Existen diferentes modalidades para el envío de las remesas familiares algunas son registradas por el Banco de Guatemala y otras no. Cuando éstas son remitidas por canales formales son registradas en las estadísticas oficiales, como un ingreso de divisas en la cuenta corriente de la balanza de pagos, situación que no ocurre cuando son enviadas por medios informales, en efectivo, por medio de correos, etc.

La información del ingreso de divisas por concepto de remesas familiares la obtiene el Banco de Guatemala, de las operaciones en moneda extranjera que realizan, los bancos, las sociedades financieras, las bolsas de valores y las casas de cambio. En el Decreto 94-2000 del Congreso de la República Ley de Libre Negociación de Divisas, obliga a éstas a reportar las transacciones que realizan en moneda extranjera.

Dentro de los medios formales de los que el Banco de Guatemala obtiene información para el registro estadístico y los más conocidos y utilizados desde hace años son: el Money Orders y las Transferencias Electrónicas por medio de empresas mercantiles en Estados Unidos.

2.2.1 Money orders:

Son documentos comprados en diferentes tipos de instituciones (financieras y no financieras) en los EUA que posteriormente son enviados por correo (ordinario o certificado). El costo del documento no es superior a los 3 dólares.

Generalmente en muchos centros cambiarios y casas de cambio, no cobran ninguna comisión, pero toman el Money Order a un tipo de cambio, que resulta ser más bajo que el vigente en el mercado, ya que incluye el costo de intermediación del centro cambiario o la casa de cambio.

2.2.2 Transferencias Electrónicas:

Son los envíos realizados por medios electrónicos y que han venido ganando participación en el mercado, debido principalmente a la rapidez y a los pocos requisitos necesarios para hacer uso del servicio. El servicio postal de los Estados Unidos ofrece el servicio de transferencias electrónicas en sustitución del Money Orders.

2.2.3 Apertura de cuentas bancarias en bancos de los Estados Unidos.

Siempre se han realizado esfuerzos para controlar los envíos de dinero de Estados Unidos a países como Guatemala por el tema del lavado de dinero.

A principios del 2006 el gobierno de Estados Unidos, permitió la apertura de cuentas a ciudadanos de países de México y países Centroamericanos.

En consecuencia apareció en el mercado el servicio de depositar en cuentas constituidas en los Estados Unidos con traslado directo a una cuenta en el país destino.

El requisito para una persona que reside en Estados Unidos, sin importar su situación migratoria es solicitar en el Consulado de su país la matricula consular. Este documento es admitido en varios estados de Estados Unidos como documento de identificación. Además el beneficiario debe tener una cuenta en el banco del país donde reside.

2.3 Importancia de las remesas familiares

La importancia de las remesas para la economía guatemalteca, radica en que los ingresos de divisas por remesas familiares han alcanzado, según datos publicados por el Banguat, a posicionarse en la segunda fuente de ingresos del país. Situación que puede probarse, en la balanza cambiaria del país, si al total de los ingresos de divisas se resta lo que corresponde a remesas familiares la situación sería negativa como se muestra a continuación:

Resumen de Balanza Cambiaria de los últimos 3 años

En miles de US Dólares.

Año	Ingresos	Egresos	Balanza	Remesas Familiares	Balanza sin Remesas
2004	16,294,216	15,283,861	1,010,355	2,550,623	(1,540,268)
2005	18,467,169	17,970,564	496,605	2,992,823	(2,496,218)
2006	14,221,241	13,421,038	800,203	2,384,420	(1,584,217)
Total	**48,982,626**	**46,675,463**	**2,307,163**	**7,927,865**	**(5,620,703)**

Las cifras del 2006 están actualizadas al 31/08/2006.
Fuente. www.banguat.gob.gt

A continuación se presenta los ingresos de divisas en concepto de remesas familiares publicado por el Banco de Guatemala de la manera siguiente:

Ingresos de Divisas por Remesas Familiares
En miles de US Dólares.

Mes	2002	2003	2004	2005	2006
Enero	83,156	164,757	194,744	209,450	248,904
Febrero	96,659	144,743	183,739	203,787	254,795
Marzo	109,034	160,778	227,896	246,466	288,966
Abril	139,212	181,087	204,013	253,087	284,440
Mayo	89,752	187,376	210,780	274,281	361,391
Junio	127,976	161,495	212,130	261,104	310,097
Julio	136,525	191,954	206,613	245,807	302,885
Agosto	162,308	178,913	212,782	241,924	332,942
Septiembre	157,339	176,551	211,777	241,584	-
Octubre	176,261	189,881	218,027	278,151	-
Noviembre	142,976	173,376	236,708	265,607	-
Diciembre	158,194	195,593	231,415	271,574	-
	1,581,394	**2,106,504**	**2,550,624**	**2,992,822**	**2,384,420**

Fuente www.banguat.gob.gt

Como se puede apreciar en el cuadro anterior el flujo de efectivo es consistente respecto al mes anterior y esto se debe principalmente a que las remesas familiares son cíclicas, semanal, quincenal, mensual. Sin embargo

el flujo de efectivo puede reflejar incrementos en fechas especiales o eventos únicos en el año como: Día del Cariño, Día de la madre, Día del padre Navidad y pago de matricular escolar.

Es importante mencionar la otra perspectiva respecto al efecto negativo del ingreso de divisas por remesas familiares.

Se puede empezar por señalar que las remesas familiares influye en la caída del precio del Dólar frente al Quetzal, lo que obliga al Banco Central a invertir en operaciones de mercado abierto(OMA), para mantener el tipo de cambio, con la consecuencias de la socialización de las pérdidas.

Las desventajas más fuertes de las remesas familiares es la dependencia que estas originan en la economía del país enfocando principalmente a las familiares que las reciben. Por ejemplo que las personas que reciben dinero del extranjero, pierdan el interés de ser productivos, con la consecuencias de incremento de la migración y violencia entre otros.

2.4 Origen y destino demográfico de las remesas familiares provenientes de Estados Unidos de América.

Según el informe presentado en noviembre de 2005, por la Organización Internacional de Migrantes con cede en Guatemala:

Las remesas familiares son remitidas en su orden principalmente desde los Estados siguientes:

a) California
b) Florida
c) New York
d) Texas

En Guatemala los departamentos receptores de remesas familiares, básicamente son:

a) Huehuetenango,
b) San Marcos,
c) Guatemala,
d) Quetzaltenango.

2.5 Leyes aplicables en materia de lavado de activos y financiamiento al terrorismo para empresas remesadoras constituidas en los Estados Unidos de América.

La legislación aplicable para las empresas de envío de Remesas Familiares, es la del país donde están constituidas, en el caso particular se analizan las empresas constituidas en Estados Unidos de América.

2.5.1 Bank Screcy Act – 1970

En 1970, el Congreso de Estados Unidos de América aprobó la **Ley de Privacidad Bancaria (Banking Secrecy Act, BSA, por sus siglas en inglés)**.

Con la aprobación de la ley BSA se introdujo el Informe de Transacción en Efectivo (Currency Transaction Report, CTR, Forma 4789); el Informe de

Transportación Internacional de Efectivo e Instrumentos Monetarios (Report of International Transportation of Currency or Monetary Instruments, CMIR, Form 4790); y el Informe de Cuentas Bancarias y Financieras Extranjeras. (Report of Foreign Bank and Financial Accounts, FBAR, Form TD F90-22.1).

La ley de Informes de Dinero en Efectivo y Transacciones Extranjeras, Ley Pública No. 91-508, Título II, al igual que los requisitos de las instituciones financieras de mantener archivos, se dieron a conocer como la Ley de Privacidad Bancaria (BSA). Ésta última, dicta a que se reporten ciertas transacciones realizadas con una institución financiera (Forma 4789), y estipula el deber de divulgar las cuentas en el extranjero (TD F90-22.1), y el reportar la transportación de dinero en efectivo en exceso de $10,000 a través de las fronteras de los Estados Unidos (Forma 4790).

Antes de esta regulación no había ningún otro rastro de papel en la institución bancaria, excepto records de la cuenta bancaria si el dinero era depositado. Los bancos no tenían la obligación de reportar las transacciones de grandes cantidades de dinero en efectivo

En resumen requiere que sea remitido un reporte por las transacciones que superan los US$.10,000.00 a La División Criminal (IRS-CI).

2.5.2 Money Laundering Control Act – 1986

El 26 de octubre de 1986, con la aprobación de la **Ley Para el Control de Lavado de Dinero**, el Derecho a la Privacidad Financiera dejó de ser un obstáculo.

Como parte de la nueva ley, el Congreso dejó establecido que una institución financiera no puede ser expuesta a sanciones por proveer información de transacciones sospechosas a las agencias de ley y el orden. Como resultado,

la siguiente versión del CTR contenía un encasillado para marcar cuando se reportaban transacciones sospechosas. Este proceso estuvo vigente hasta abril de 1996, cuando se introdujo el **Informe de Transacción Sospechosa** (Suspicious Activity Report, **SAR** por sus siglas en inglés).

Las entidades deben presentar un SAR si conocen, sospechan o tienen razones para sospechar que la transacción puede estar involucrada en un potencial lavado de dinero u otra actividad ilegal.

El reporte SAR debe presentarse al FINCEN, por sus siglas en inglés Financial Crimes Enforcement Network, por medio electrónico y física, dentro de los treinta días calendario a partir de la fecha de su detección como transacción sospechosa.

Los reportes SAR constituyen la piedra angular del sistema de información del Bank Screcy Act (BSA), de tal manera que los examinadores estatales y federales focalizan una parte sustancial de su revisión en la evaluación de las políticas, procedimientos y procesos de las entidades para identificar e investigar transacciones sospechosas.

2.5.3 Anti-Drug Abuse Act – 1988

Requiere llevar un registro de las transacciones en efectivo mayores de US$.3,000.00, además de identificar al cliente plenamente.

2.5.4 Crime Control Act – 1990

Requiere colaboración para las entidades reguladoras, esta acta esta dedicada principalmente a la reducción del suministro de drogas y proporciona los fondos para la lucha contra el narcotráfico, al mismo tiempo fortalece la confiscación de bienes relacionados.

2.5.5 Las Regulaciones de la Oficina para Control de los Activos Extranjeros (OFAC)

La OFAC es una dependencia del Departamento del Tesoro de los Estados Unidos de América, y sus siglas significan , traducido al español se refiere a la Oficina para el Control de Activos Extranjeros. Su función es administrar y hacer cumplir las sanciones económicas y de negocios de acuerdo con la política de seguridad nacional de Estados Unidos de América, en contra de países terroristas, narcotraficantes internacionales y los vinculados en actividades de producción y proliferación de armas de destrucción masiva. Esta oficina mantiene y actualiza una base de datos con nombres de personas vinculadas con tales actividades delictivas.

Las personas, empresas, negocios u organizaciones que están en la jurisdicción de Estados Unidos de América no pueden ni deben otorgar financiamientos ni realizar ningún trato comercial o de negocios con las personas que aparecen en el listado OFAC. Éste listado esta disponible en la página www.treas.gov/ofac.

2.5.6 Estatutos y Leyes Federales Aprobadas por el Congreso

Título 31, Código de Impuestos Internos, Sección 5331 – fue aprobada en el año 2001 como resultado de la Ley Patriota ésta duplica la obligación de reportar al Código de Impuestos Internos según la Sección 6050 I en la forma 8300. El reporte dual de esta información ahora se puede proveer al IRS y al Departamento del Tesoro, Red Para el Cumplimiento de Crímenes Financieros **FINCEN.**

2.5.7 Prohibition of Unlicensed Money Transmitting Business, Prohibición de empresas de envío de remesas de dinero, sin contar con la debida licencia) 18 USC § 1960

2.5.8 The USA Patriot Act (Acta Patriota)

Fue la respuesta del Congreso Norteamericano, a los atentados del 11 de Septiembre del 2001. Se basa fundamentalmente en la resoluciones de la quincuagésima asamblea general y de las resoluciones 1373 y 1390, de las Naciones Unidas en Nueva York, del acta de nacionalidad y de inmigración de los Estados Unidos y la de la ley de Seguridad Nacional Norteamericana. Esta ley, ha sido revisada y actualizada en diferentes ocasiones, aunque ha sido impugnada por grupos de los derechos civiles en los Estados Unidos por vulnerar los derechos de privacidad y confidencialidad de la información.

Es una ley extraterritorial, abarca jurisdicción internacional y se apoya en los tratados internacionales y convenios bilaterales.

Es la más estricta y contundente arma en contra del terrorismo y el crimen internacional organizado.

2.6 Leyes aplicables en materia de lavado de activos y financiamiento al terrorismo para empresas pagadoras constituidas en Guatemala.

2.6.1 Ley Contra el Lavado de Dinero u Otros Activos, Decreto No. 67-2001 del Congreso de La República y su Reglamento Acuerdo Gubernativo No. 118-2002.

El objetivo de esta Ley es prevenir, detectar y sancionar el lavado de dinero u otros activos procedentes de la comisión de un delito y establecer las normas que para este efecto deberán observar las personas obligadas.

2.6.2 Ley para Prevenir y Reprimir el Financiamiento del Terrorismo Decreto No.58-2005 del Congreso de la República y su Reglamento Acuerdo Gubernativo No. 86-2006.

El artículo 17 del Reglamento de la Ley citada, obliga a presentar a los bancos nacionales, a la Intendencia de Verificación Especial de Guatemala, dentro de los primeros cinco días hábiles del mes siguiente a que corresponda, el reporte de las remesas recibidas o enviadas mensualmente mayores a US$.2,000.00 o su equivalente en moneda nacional.

2.6.3 Código Penal, Decreto Número 17-73 del Congreso de la República, Artículo 391. Tipifica el delito de Terrorismo.

En este se sanciona con penas severas (prisión de uno a cincuenta años y penas económicas) actos relacionados con el terrorismo.

2.6.4 Código Procesal Penal, Decreto No. 51-92 del Congreso de la República, Artículo 278, congelamiento de fondos terroristas.

Se refiere al decomiso del producto del delito o de los bienes utilizados para financiar el terrorismo.

2.6.5 Código Procesal Civil y Mercantil, Decreto Ley 107 del Jefe de Gobierno, Artículo 530, embargo de bienes por el delito de terrorismo.

2.6.6 Ley Contra la Narcoactividad, Decreto No. 48-92 del Congreso de la República.

Establece en el Ministerio Público Fiscalías específicas contra la narcoactividad y el lavado de dinero

2.7 Fraudes o errores en remesas familiares

Debido a que para las instituciones financieras es perjudicial para su prestigio, dar a conocer públicamente que han sido sujeto a fraudes o errores. No fue posible establecer si en el periodo que cubre el presente trabajo registraron pérdidas por errores o fraudes.

Sin embargo, el incumplimiento de la normativa de lavado de activos puede ser fatal para las empresas de remesas familiares porque las sanciones son muy altas. Además de la cancelación de las cuentas bancarias por los bancos de Estados Unidos de América ya que ningún éstos querrá verse afectada por el incumplimiento de esta normativa.

2.8 Sanciones y penas

La OFAC es una dependencia del Departamento del Tesoro de los Estados Unidos de América, y sus siglas significan, traducido al español se refiere a la Oficina para el Control de Activos Extranjeros

Entre las sanciones penales se encuentran diversos tipos de multa que oscilan entre US$250.000 y pueden llegar hasta US$10.000.000, para empresas, y desde US$10.000 hasta US$5.000.000 para individuos. También pueden ser impuestas penas de prisión desde 5 hasta 30 años, y en ocasiones ambos tipos de sanción pueden ser aplicados.

Las sanciones administrativas son impuestas directamente por la OFAC y también pueden consistir en multas que van desde US$11.000 hasta US$1.000.000, u otras como bloqueo de activos y fondos, hasta la confiscación de los mismos, de acuerdo con la respectiva regulación.

2.9 Tipologías de lavado de activos.

A manera de ilustración del material presentado, en el Congreso Regional sobre la Prevención el Lavado de Dinero y Financiamiento al Terrorismo, por el Dr., Mauricio Canos Castro profesor de la Universidad Javeriana de Bogota, Colombia, se toman las tipologías de lavado de dinero detectados en Colombia. Se citan como ejemplo las tipologías que han sido descubiertas por las autoridades de ese país derivado de la lucha contra el lavado de activos.

2.9.1 Giros varios

En materia de remesas se ha intensificado el movimiento de capitales en Colombia, por tanto se ha implementado controles como cruces de números telefónicos con los cuales se detecta que llegan giros para varias personas, pero el número telefónico de confirmación es el mismo; adicionalmente, se encuentran los movimientos en las cuentas con consignaciones entre US$6.000 y US$10.000 de la misma ciudad o diferentes ciudades y lo que se ha detectado, es que corresponde al pago de los giros.

2.9.2 Devolución de giros

Otra modalidad es la devolución de estos mismos giros encontrando que a los pocos días era depositado un cheque de una casa de giros o de cambios lo cual permite evidenciar que desafortunadamente los delincuentes encuentran la forma de entrar el dinero por los escasos controles que tienen las casas de giros o cambios.

2.9.3 Cruces de Ordenantes en los que se encuentran múltiples beneficiarios

Aunque aparentemente esta tipología se pudiera descubrir fácilmente, la falta de información actualizada permite el lavado de dinero de una persona en el exterior que envía dinero a múltiples beneficiarios en el país receptor.

2.9.4 Cruces de Beneficiarios que les envían dinero múltiples ordenantes

Este caso se presenta frecuentemente y para no ser detectado se utiliza a diferentes operadores de remesas que al no compartir la información entre operadores y al no estar consolidada la información hace más fácil la operación.

2.9.5 Fraccionamiento de remesas

El envío de remesas por parte de inmigrantes a sus familias en el país de origen, permite la utilización ocasionalmente de mover recursos ilícitos provenientes de organizaciones criminales o para la financiación de actividades terroristas.

Las diferentes organizaciones criminales envían el dinero por esta modalidad, a sus países de origen por giros que generalmente son fraccionados y en la cual se utilizan muchos beneficiarios, llamados "pitufos", que en la mayoría de las veces son amas de casa, estudiantes o desempleados o a veces también utilizan identidades falsas.

Con este fin fraccionan o dividen la suma en montos más pequeños, casi siempre por un valor menor al establecido por las autoridades de control. Otra de las características es que los delincuentes utilizan diferentes operadores tanto en el exterior como en el país de origen para enviar su dinero.

Una vez el supuesto beneficiario, recibe el dinero y se lo entrega al verdadero beneficiario y cobra una comisión por el servicio prestado.

Toda empresa sea cual fuere su actividad principal persigue que sus operaciones se realicen con el máximo de beneficio y al mas bajo costo(eficiente y eficaz), sin transgredir leyes, la moral, la ética al realizar operaciones y lo dispuesto por la administración, esto es precisamente la eficiencia en las operaciones y se puede alcanzar con un control interno bien desarrollado. En el siguiente capítulo se define el control interno y sus elementos desde una perspectiva general.

CAPITULO III

CONTROL INTERNO

3.1 Definición del Control Interno.

Varios autores de libros sobre este tema, coinciden en afirmar que se define como un proceso diseñado para proporcionar información financiera oportuna, proteger los recursos de la empresa, incentivar la eficiencia y efectividad operativa, prevenir errores, fraudes y en fin incentivar al personal al cumplimiento de los objetivos y políticas de la administración.

A continuación se describen algunas definiciones:

"Comprobación, inspección, fiscalización, intervención."(9:561)

"Proceso por medio del cual las actividades de una organización quedan ajustadas a un plan preconcebido de acción y el plan se ajusta a las actividades de la organización."(3:122)

"Abarca el planeamiento y la utilización de todos los medios por los cuales, desde el punto de vista financiero, la dirección consigue del modo más eficaz proteger los bienes de la empresa, administrar sus operaciones corrientes y planear el futuro."(1:19)

"Comprende el plan de organización (1) y la totalidad de los métodos, sistemas y procedimientos, que en forma ordenada, se adoptan en una organización, para asegurar la protección de todos los recursos (2), la obtención de información correcta, segura y oportuna (3), la promoción de la economía, eficiencia y efectividad operacional (4) y la adhesión del personal a los objetivos y políticas debidamente predefinidos por la dirección (5)."(8:1)

"El control interno se define como un proceso, ejecutado por personal de la entidad, diseñado para cumplir los objetivos específicos. La definición amplia, abarca todos los aspectos del control de un negocio, permitiendo así que un directivo se centre en objetivos específicos. El control interno consta de cinco componentes interrelacionados, los cuales son inherentes a la forma como la administración maneja la empresa. Los componentes están ligados, y sirven como criterio para determinar cuándo el sistema es objetivo."(10:4)

"Se entiende por control interno el conjunto de planes, métodos y procedimientos adoptados por una organización, con el fin de asegurar que los activos están debidamente protegidos, que los registros contables son fidedignos y que la actividad de la entidad se desarrolla eficazmente de acuerdo con las políticas trazadas por la gerencia, en atención a las metas y objetivos previstos."(11:233)

3.2 Elementos del Control Interno

El informe COSO(Comite of Sponsoring of the Treadway Comisión), plantea cinco componentes que se detallan a continuación.

3.2.1 Ambiente de control

"El ambiente de control establece el tono de una organización, para influenciar la conciencia de control de su gente. Es el fundamento de todos los demás componentes de control interno, proporcionando disciplina y estructura." (10:25)

Los factores que intervienen en el ambiente del control son:

- Integridad
- Valores éticos
- Competencia de los empleados.
- Filosofía de la administración
- Asignación de responsabilidad y autoridad
- La forma de organización o estructura organizativa de la entidad.
- La atención y dirección que se le presta al Consejo de Administración.
- Métodos de control administrativo para supervisar y dar seguimiento al desempeño incluyendo Auditoria Interna.

El ambiente de control tiene una influencia profunda de cómo se estructuran las actividades del negocio, se establecen los objetivos y se valoran los riesgos. Este elemento refleja el espíritu ético de una entidad respecto al comportamiento de las personas, la responsabilidad con que realizas sus actividades, además sirve de base para el resto de elementos.

3.2.2 Valoración y evaluación de Riesgos.

Cada entidad se expone a diversos riesgos como resultado de la naturaleza de sus operaciones estos, pueden ser internos o externos. Los riesgos deben valorarse en el sentido de saber cuáles serán aceptados y los controles que se serán puestos en práctica con el objetivo de disminuir el riesgo a márgenes aceptables.

Dentro de los factores de riesgo interno se ponen como ejemplo :

- Interrupción del sistema de información que afecte directamente el flujo normal de operaciones de la entidad.
- La calidad del personal, mal entrenamiento y falta de motivación para la identificación de los empleados con la entidad.
- El acceso a los activos a los empleados derivado de la operación de la entidad puede motivar fraudes.

Factores externos:

- Desarrollo tecnológicos
- Cambio de las necesidades o espectativas de los clientes
- Competencia
- Cambios en la legislación.
- Catástrofes naturales.

3.2.3 Información y comunicación

La información sin duda alguna es unos de los activos más importantes que posee una entidad. Esta información debe ayudar a la consecución de los objetivos.

"El sistema de información produce documentos que contienen información operacional, financiera y relacionada con el cumplimiento, la cual hace posible operar y controlar el negocio." (10:71)

A menudo los sistemas de información se enmarcan únicamente en el ciclo de los sistemas de entrada, proceso y salida, relacionando directamente operaciones de contabilidad, ventas facturación, inventarios, etc.

Pero el concepto de sistemas de información contempla aspectos mas amplios como información de cambios en el mercado, la competencia, los gustos de los clientes, cambios en la demanda, información de productos equivalentes de la competencia.

La calidad y oportunidad de la información generada por los sistemas afecta la habilidad de la administración en la toma de decisiones. Los sistemas de información para proporcionar la información apropiada deben tener las características siguientes: La información debe ser apropiada, oportuna, actual, exacta y finalmente accesible al usuario .

3.2.4 Supervisión y monitoreo.

"Los sistemas de control requieren que sean monitoreados, un proceso que valora la calidad del desempeño del sistema en el tiempo. Ello es realizado mediante acciones de monitoreo." (10:83)

Los sistemas de control interno son cambiantes derivado de la nueva forma de operar, cambio de personal. El monitoreo asegura que el control se encuentra operando en optimas condiciones.

El monitoreo se puede realizar sobre la marcha de las operaciones o por evaluaciones separadas. Pero entre mas efectivas son la evaluaciones sobre la marcha las evaluaciones separadas serán mas distantes.

3.2.5 Actividades de Control

La definición según el informe COSO es el siguiente: “Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que se estén llevando a cabo las directivas administrativas”.(10:59)

Las actividades de control se deben ejecutar en todos los niveles de la organización y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgos: conociendo los riesgos, se implementan los controles destinados a evitarlos o minimizarlos.

En el siguiente capítulo se desarrolla lo relacionado al control interno aplicado a los sistemas de información informáticos, partiendo de la teoría general de sistemas de información.

CAPITULO IV

SISTEMAS DE INFORMACION Y EL CONTROL INTERNO

4.1 Definición general de sistema

Varios autores definen estos sistemas de información de manera general como:

"Un conjunto de componentes destinados a lograr un objetivo particular de acuerdo a un plan."(8:14)

"Es un conjunto de componentes que interaccionan entre si para lograr un objetivo" (11:19)

"Es un conjunto de elementos organizados que se encuentran en interacción, que buscan alguna meta o metas comunes, operando para ello sobre datos o información sobre energía o materia u organismos en una referencia temporal para producir como salida información o energía o materia u organismos.(4:33)

"Conjunto de elementos (físicos y lógicos), procedimientos y elemento humano que unificados bajo métodos sistematizados, permiten la captura, registro, ordenamiento, clasificación, transformación y presentación de datos que pueden ser utilizados como información veraz, exacta y necesaria."(12:1)

En definitiva en estas definiciones se detallan los componentes de un sistema que se resume en: Que tiene que haber una entrada, un proceso y una salida. En este proceso participan elementos físicos y lógicos que de forma coordinada participan para el logro de un objetivo.

4.2 Teoría General de los sistemas de Información

De manera popular la palabra sistema es una forma de hacer las cosas o la actuación de varios elementos para alcanzar un objetivo. En la siguiente definición se describe el concepto de sistemas de información de la manera siguiente:

"Es un procedimiento simple de entrada, proceso y salida, en donde un dato de entrada se transforma en una información útil de salida mediante algún proceso anterior."(4:161)

Al incorporar el termino de información estos autores consideran la información como parte elemental de un sistema.

Por consiguiente, un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. Estos elementos son de naturaleza diversa y normalmente incluyen:

El equipo computacional, es decir, el hardware necesario para que el sistema de información pueda operar. Lo constituyen las computadoras y el equipo periférico que puede conectarse a ellas.

El recurso humano que interactúa con el Sistema de Información, el cual esta formado por las personas que utilizan el sistema, alimentándolo con datos o utilizando los resultados que genere.

Los datos fuente que son introducidos en el sistema; son todas las entradas que necesita el sistema para generar como resultado la información que se desea.

Los programas son parte del software del sistema de información que hará que los datos de entrada introducidos sean procesados correctamente y generen los resultados que se esperan.

4.2.1 Ciclo de Vida de los Sistemas de Información.

También llamado ciclo de desarrollo de los sistemas de información, es un enfoque por etapas de análisis y diseño, que postula que el desarrollo de los sistemas mejora cuando existe un ciclo específico de actividades del analista y de los usuarios.

Un sistema de información realiza cuatro actividades básicas: entrada, almacenamiento, procesamiento y salida de información.

4.2.2 Características de los sistemas de información modernos:

- Sistemas sencillos sirviendo a funciones y niveles múltiples dentro de la empresa.

- Acceso inmediato en línea a grandes cantidades de información.
- Fuerte confiabilidad en la tecnología de telecomunicaciones.
- Mayor cantidad de inteligencia y conocimientos implícita en los sistemas.
- La capacidad para combinar datos y gráficas.

4.2.3 Objetivos de los Sistemas de Información:

Las aplicaciones de sistemas de información tienen su origen en casi todas las áreas de una empresa y están relacionadas con todas actividades de la organización.

Para alcanzar los objetivos, las empresas emprenden proyectos de desarrollo de sistemas de Información por una o más de las siguientes razones, por consiguiente estas serán los objetivos que debe cubrir un sistema eficiente:

Las 5 letras "C":

Capacidad

- Mayor velocidad de Procesamiento.
- Incremento en el Volumen.
- Recuperación más rápida de la información.

Control

- Mayor exactitud y mejora en consistencia.

Comunicación:

- Mejora en la comunicación.
- Integración de áreas de la Empresa.

Costos

- Monitoreo de costos.
- Reducción de costos.

Competitividad

- Atraer clientes.
- Dejar fuera a la competencia.
- Mejores acuerdos con los proveedores.
- Desarrollo de nuevos productos.

4.3 Clasificación de los Sistemas de Información

4.3.1 Transaccionales

Estos sistemas logran la automatización de procesos operativos dentro de una organización. Como por ejemplo en las instituciones bancarias las transacciones de pago, cobros, depósitos, etc. En resumen son grandes recolectores de información.

R. Jonson autor del Libro Teoría, administración e integración de sistemas, los define como:

"Los sistemas de procesamiento de transacciones (TPS) tienen como finalidad mejorar las actividades rutinarias de una empresa y las que depende toda la organización." (8:25)

Las principales características de este tipo de sistemas de información se puede agrupar en las siguientes:

- A través de éstos suelen lograrse ahorros significativos de mano de obra.
- Normalmente son el primer tipo de sistemas de información que se implanta en las organizaciones, porque la intención es agilizar e incrementar la operatoria de transacciones de forma eficiente.

- Son intensivos en entrada y salida de información; sus cálculos y procesos suelen ser simples y poco sofisticados.
- Tienen la propiedad de ser recolectores de información.
- Son fáciles de justificar ante la dirección ya que sus beneficios son visibles y palpables.

4.3.2 De Información Gerencial

Se les nombra de varias maneras, como por ejemplo: Sistemas Gerenciales, Sistemas Ejecutivos o Sistemas de Soporte para la Toma de Decisiones en Grupo ó sistema de información para la administración (MIS).

Aunque se llamen de distintas maneras, la esencia de estos, es que no sustituyen la función de los sistemas transaccionales, si no que toman de base los datos almacenados por las transacciones realizadas.

Estos sistemas emiten reportes de tipo gerencial para toma de decisiones.

Proporciona la información que será empleada en los procesos de decisión administrativos. Trata con el soporte de situaciones de decisión bien estructuradas. Es posible anticipar los requerimientos de información más comunes.

Los usuarios de este tipo de sistemas utilizan una base de datos compartida para la administración. Esta base de datos almacena, datos y modelos que ayudan al usuario para el uso e interpretación de la información.

Dentro de las características principales, se pueden mencionar las siguientes:

- Suelen introducirse después de haber implantado los sistemas transaccionales.

- Suelen ser intensivos en cálculos y escasos en entradas y salidas de información.

- La información que generan sirve de apoyo a los mandos intermedios y de alta administración en el proceso de la toma de decisiones.

- No suelen ahorrar mano de obra.

- La justificación económica para el desarrollo de estos sistemas es difícil.

- Suelen ser sistemas de información, interactivos y amigables, con altos estándares de diseño gráfico y visual, ya que están dirigidos al usuario final.

- Apoyan la toma de decisiones que por su naturaleza son repetitivas.

- Pueden ser desarrollados directamente por el usuario final sin la participación operativa de los analistas.

4.3.3 Para el Soporte de Decisiones

Este sistema es similar a los sistemas de información tradicionales para la administración, porque ambos dependen de una misma base de datos. Regularmente ésta es histórica pero está separada de la base de datos que se actualiza constantemente con el flujo de operaciones.

Este tipo de sistemas hacen evaluaciones y presentan opciones dando un soporte más directo en cada etapa de toma de decisiones y esta es la diferencia de los Sistemas de Información Gerencial.

"Los sistemas para el soporte de decisiones (DSS) ayudan a los directivos que deben tomar decisiones no muy estructuradas, también denominadas no estructuradas o decisiones semiestructuradas" (8:29)

Están diseñados para cubrir las necesidades específicas y particulares de la alta administración de la empresa. Esto implica que diferentes ejecutivos pueden requerir información o formatos de presentación distintos para trabajar en una compañía en particular. Lo anterior se debe a que los factores críticos del éxito pueden variar de un ejecutivo a otro.

Extraen, filtran, comprimen y dan seguimiento a información crítica del negocio. El sistema debe contar con capacidad de manejar información que proviene de los Sistemas Transaccionales de la empresa y/o de fuentes externas de información. Esta información externa puede provenir de bases de datos externas, periódicos y cartas electrónicas de la industria, entre otros; todo esto en temas tales como nuevas tecnologías, clientes, mercados y competencia, por mencionar algunos.

Implica que los ejecutivos puedan interactuar en forma directa con el sistema sin el apoyo o auxilio de intermediarios. Esto puede representar un

reto importante, ya que muchos ejecutivos se resisten a utilizar en forma directa los recursos computacionales por el temor a cambiar.

Es un sistema desarrollado con altos estándares en sus interfases hombre-máquina, caracterizado por gráficas de alta calidad, información tabular y en forma de texto. El protocolo de comunicación entre el ejecutivo y el sistema permite interactuar sin un entrenamiento previo.

Pueden acceder a información que se encuentra en línea, extrayéndose en forma directa de las bases de datos de la organización. Esta característica del EIS permite al ejecutivo penetrar en diferentes niveles de información. Por ejemplo, puede conocer las ventas por país, por zona geográfica, por cliente y por línea de producto, penetrando a su gusto en los niveles internos y más detallados de la información en caso necesario.

El sistema esta soportado por elementos especializados de hardware, tales como monitores o videos de alta resolución y sensibles a; tacto, ratón e impresoras con tecnología avanzada.

Es importante señalar que en muchas ocasiones los términos Sistemas de Información para Ejecutivos (EIS) y Sistemas de Soporte para Ejecutivos (ESS: Executive Support Systems) son utilizados como sinónimos. Sin embargo, las siguientes características adicionales deben estar presentes para considerar a un EIS:

- Contempla las facilidades de comunicación electrónica, tales como correo electrónico de voz y datos, teleconferencia y procesadores de texto.

- Capacidades de análisis de datos, tales como hoja electrónica de cálculo, lenguajes especializados de consulta .

- Herramientas para la organización personal del ejecutivo, tales como calendario, agenda y tarjetero electrónico.

- Como podemos observar, los EIS poseen múltiples características, estas han permitido elevar el nivel de confianza en la toma de decisiones, esto gracias a que los EIS permiten obtener una visión desde diferentes ángulos de los datos, reduciendo con ello en gran medida la incertidumbre en el proceso de toma de decisiones.

Un cuestionamiento muy frecuente es: ¿Cómo logran los EIS mejorar la toma de decisiones? Este mejoramiento se logra al optimizar la información de los reportes corporativos o divisionales de la organización, esta optimización se hace a través de:

- La redefinición los métodos de recopilación de la información, esto permite que quien este encargado de tomar decisiones no se involucre en la obtención de los datos de manera directa, sino que se enfoque sus energías al análisis de la información.

- El mejoramiento de la certidumbre de los datos.

- Haciendo más rápido el proceso de obtención de la información.

- Mediante la realización de cambios en la manera de presentar la información, haciendo uso de nuevas técnicas de presentación como: gráficas, histogramas, dibujos y animaciones.

- El rediseño de los sistemas actuales de reportes, mediante los cuales se les da mayor importancia a los factores críticos que permitirán tener un mejor rendimiento de la organización.

- Los EIS contribuyen de manera importante a apoyar la toma de decisiones al permitir redefinir y reorientar algunas de las fases del ciclo administrativo de una organización, principalmente a la planeación y control. Esto permite a la organización optimizar en la asignación de recursos, tanto cuantitativos como cualitativos; además de mejorar sus procesos y por ende aumentar sus utilidades.

4.3.4 Expertos

Este tipo de sistema también se conoce como sistema basado en conocimiento, estos consisten en un conjunto de programas de ordenador que son capaces, mediante la aplicación de conocimientos, de resolver problemas en un área determinada del conocimiento o saber y que ordinariamente requerirá de la inteligencia humana.

Estos sistemas están diseñados para simular el comportamiento humano. Puede considerarse a la inteligencia artificial como el campo principal de los sistemas expertos.

Estos sistemas capturan , utilizan el conocimiento de un experto, para solucionar problemas particular de la organización. A diferencia de los otros sistemas este elige la mejor opción sobre la base de la información proporcionada.

4.4 El control interno informático

Los sistemas están expuestos a una diversidad de peligros y amenazas. Dentro de estos cabe mencionar: desastres naturales, incendios, fraudes, fallas en los sistemas, errores y omisiones, intercepción, deficiencias, sabotajes, etc.

Para hacer frente a los peligros y amenazas es necesario contar con un "Sistema integrado al proceso administrativo, en la planeación, organización dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos computarizados." (10:2)

A continuación se detallan algunos requisitos indispensables que deben cumplir los controles informáticos para que sean operantes.

- Reportar prontamente los errores.
- Futuristas
- Señalar excepciones
- Objetivos
- Flexibles
- Económicos
- Comprensibles
- Conducir a la acción correctiva.

Los controles deben prevenir errores o fraudes, siendo futuristas señalando las alteraciones a los procesos establecidos, estos deben ser moldeables para adaptarse a las necesidades de la empresa por consiguiente esto implica que no deben resultar más caros que lo que se controla.

4.4.1 En la operación de sistemas

La importancia del control interno en la operación de sistemas estriba en que contando con este elemento básico se pueden prevenir errores y deficiencias de operación, así como el uso fraudulento de la información y sistemas, robo de información, piratería. Además se puede prevenir la modificación de información almacenada y los programas.

Estos controles sirven para verificar los datos que serán procesados, considerando la exactitud, la suficiencia y calidad. En resumen vigilan la captura de datos y emisión de resultados.

Los controles de procesamiento se refieren al ciclo que sigue la información desde la entrada hasta la salida de la información. Lo que conlleva a asegurar que todos los datos sean procesados, garantizar su exactitud.

Consisten en todos los registros necesarios para el control de las transacciones (formularios preimpresos, reportes, registros y procedimientos) y que tienen por objetivo evitar errores involuntarios e irregularidades en las transacciones, además se puede enmarcar el evitar los desperdicios de recursos de la institución.

Se pueden categorizar de la manera siguiente:

4.4.1.1 Formularios preimpresos

Estos permiten guiar el registro inicial de las transacciones en un formato uniforme. El diseño de formularios es un eficiente control preventivo en la captura de datos. Un buen diseño de los formularios permite que los datos sean completos y precisos, evitando errores y omisiones.

4.4.1.2 Identificación de transacciones

Toda operación que se registre debe ser identificada de una forma adecuada. Esta identificación puede ser por ejemplo por número de serie, secuencia o código de transacción.

4.4.1.3 Acceso restringido a formularios en blanco.

Todos los formularios fuente en blanco deben estar controlados para evitar el uso fraudulento, en la entrada de datos.

4.4.1.4 Segregación Funcional

El departamento de programación y de usuarios finales, debe estar separado en el sentido que el departamento de programación no realice operaciones que no le competen .

Segregación a nivel de usuarios a nivel de autorizaciones de transacciones, registro y control fisico.

4.4.1.5 Identificación del usuario.

Los usuarios deben identificarse con un código de seguridad, mediante el cual se definen restricciones para el proceso de transacciones y el acceso a los archivos y al sistema en general.

4.4.1.6 En la entrada de datos

Los controles en la entrada deben asegurar que los datos autorizados para el proceso sean suficientemente validados, estén completos y protejan su integridad.

4.4.2 Sobre la seguridad física y lógica de los sistemas.

4.4.2.1 Seguridad física

El objetivo es proteger los sistemas tanto en la parte de hardware, software, documentación y medios magnéticos de los riesgos por pérdidas, extravíos o por daños físicos. Así mismo de los potenciales riesgos que se pueden dar en el acceso de personal no autorizado sin los controles adecuados de seguridad física; en los incendios; en las interrupciones de energía eléctrica; en inundaciones por filtraciones de agua y, en los controles de acceso lógico.

La mayoría de la literatura que trata sobre seguridad hace mayor énfasis, sobre la seguridad en la red, ya que es un tema candente derivado a las constantes innovaciones de tecnología y las incursiones maliciosas de usuarios no autorizados de los últimos tiempos.

José Dagoberto Pinilla en su obra Auditoria Informática Aplicaciones en Producción define a la seguridad física como:

"Todo lo relacionado con la seguridad y salvaguarda de los bienes tangibles de los sistemas computacionales..."(7:164)

A menudo el hardware suelen estar más vulnerable a los ataques físicos que los que pudieran realizarse por medio de la red. Como ejemplo de estos ataques se pueden mencionar los realizados por usuarios locales mal intencionados, delincuentes, ratas, insectos etc.

Los ejemplos anteriores muestran algunas vulnerabilidades, por los cuales la seguridad física debe estar en primer plano.

La seguridad física involucra como mínimo los siguientes aspectos:

- Control de Acceso
- Seguridad contra Incendios
- Suministro de Energía
- Aire Acondicionado
- Detección de Agua
- Guardias de Seguridad
- Telecomunicaciones
- Cambios en equipos (harware)

Además se pueden mencionar:

- Ubicación del Servidor y Acceso físico.
- Topología de la Red.
- Contraseñas de Bios y de Consola.
- Controles biométricos de acceso.
- Hardware de la red.
- Seguridad general del Harware

4.4.2.1.1 Control del acceso

Aunque la inversión en sistemas de control de acceso no debe ser necesariamente onerosa como la implantación de vidrios a pruebas de balas, guardias armados las 24 horas del día o cámaras de video.

Si se deben contemplar controles adecuadamente razonables para evitar el acceso de individuos e incluso de personal “no autorizado” al centro de procesamiento o a las áreas de manejo de datos o información oficial y exclusiva.

Estos sistemas de seguridad deben contemplar el uso de claves de seguridad a ser ingresadas a través de un componente electrónico ubicada en cada área o por medio del uso de una tarjeta plástica codificada.

La asignación de claves debe estar dada por el representante del área de sistemas y deberán ser modificadas periódicamente para evitar cualquier infiltración dentro del archivo maestro de claves o el otorgamiento de las mismas entre usuarios.

Cabe indicar que debe haber para el efecto una interrelación entre cada área que responsabiliza a un individuo a través del uso de una clave, y el área de control que asigna y controla las claves emitidas a los usuarios.

El no conocer sobre el despido, renuncia o ausencia de un personal determinado durante un tiempo específico o permanente provocaría que el proceso de control de acceso no tenga éxito por daños provocados por actos de sabotaje, robos, asaltos, etc.

Los accesos también deben ser otorgados sobre la base de la necesidad mínima y dependiendo de los casos bajo la supervisión del Responsable de Sistemas.

Cuando se reasigne personal a otras funciones en las que no requieran del acceso que tenían previamente autorizado; el permiso debe ser revocado una vez que la persona sea reasignada en sus funciones. Así mismo en el periodo de vacaciones del personal debe aplicarse este mismo concepto.

Las movilizaciones de equipos o medios magnéticos deben ser realizadas sólo por personal autorizado y deben seguir el procedimiento de control de movilizaciones de equipos. El guardia de seguridad debe

asegurarse que las movilizaciones de equipos o medios magnéticos tanto de ingreso como de egreso se efectúen con las autorizaciones del caso.

El personal que corresponda a la categoría de visitantes y que requieran movilizarse por el centro de procesamiento o afines deberán utilizar una tarjeta que indique su calidad de "visitantes" y estar siempre escoltados o supervisados por personal de la institución y su ingreso y salida debe quedar registrado en una bitácora del área.

La limpieza y aseo del centro de procesamiento y afines debe efectuarse en presencia del personal de la institución. Dicho personal de limpieza debe ingresar previo a la identificación ante el guardia de seguridad quien debe constatar su nombre dentro del registro del personal externo a la empresa y el horario autorizado para su acceso.

Debe prohibirse el ingreso de personal con maletas o bolsos u objetos que no fueran los que constituyan o sirvan para su labor de limpieza y aseo.

Las tarjetas de acceso a áreas restringidas así como las tarjetas de visitantes deben ser reportadas inmediatamente en el caso de perdidas, al personal de seguridad y al Responsable de sistemas a fin de revocar el uso de dichas tarjetas.

Para casos de emergencia, el personal de seguridad debe tener las llaves del centro de procesamiento y de las oficinas. Estas deben conservarse en sobre sellado, bajo seguridad y revisado periódicamente por Auditoría.

Los horarios de ingreso y salida del personal así como de equipos y medios magnéticos debe ser revisados por el personal de Auditoría periódicamente y comprobado que los movimientos de equipos se hayan

efectuado de acuerdo a los controles establecidos y que, el ingreso y salida del personal se haya efectuado en el horario establecido y con los permisos respectivos para entradas o salidas fuera de horario.

Es importante que las empresas prevean la obtención de una póliza que resguarde pérdidas o daños de sus activos fijos.

4.4.2.1.2 Seguridad contra Incendios

El centro de procesamiento y afines debe poseer detectores de humo los cuales deben activarse de forma automática al momento de una emanación considerable de humo. Estos dispositivos deben probarse regularmente para corroborar su funcionamiento. En caso de ser detectores de incendios con prolongación automática de agua, deben ubicarse en áreas lejos de los equipos y material no recuperable por contacto con agua.

El centro de procesamiento debe disponer de suficientes extintores de incendios movibles y que deben ser probados periódicamente a fin de que estos puedan funcionar en los casos de emergencias.

Debe hacerse una revisión visual de su presurización procediendo a enviar a cargar o descargar el extintor al centro de mantenimiento respectivo.

Así mismo debe señalizarse el área de tal forma que se especifique las áreas en que se prohíbe fumar o utilizar material combustible.

Los extintores a ser usados varían de acuerdo a la clase de riesgo de incendio que se presenten.

El centro de procesamiento y afines debe ser estructurado con equipos, muebles y material no inflamable. Es preferible la no-utilización de cortinas

en el centro de procesamiento. El equipamiento eléctrico como cables, deberá ser instalado y elaborado por personal altamente calificado.

Los interruptores de energía deben estar separados por secciones y uno que permita el corte completo del suministro de energía para casos de emergencia, los mismos que deben estar protegidos para evitar su manipulación accidental.

Por ningún motivo se debe fumar en el área de procesamiento. Cualquier material de fácil combustión, como hojas, manuales, formularios, deberá estar ubicados lejos de las zonas calientes y del posible contacto con elementos inflamables.

4.4.2.1.3 Suministro de Energía

Toda empresa debe poseer un UPS (Uninterruptable Power Supply/Fuente Interrumpida de Energía) para protegerse de cualquier suspensión o caída del suministro eléctrico.

Adicionalmente al UPS debe existir un Generador de Energía a ser utilizado en casos de emergencia también, el cual debe ser probado periódicamente a fin de asegurar su operación.

Tanto el Generador de energía como el UPS deben proyectarse a ser utilizados hasta el 70% de su carga.

Cabe indicar que el UPS está en constante funcionamiento, no sólo para soportar la ausencia de luz por un periodo determinado sino también en intermitencias o picos eléctricos.

Es importante hacer una correcta evaluación de las especificaciones que debe tener un UPS antes de adquirirlo a fin de que este soporte todos los equipos del centro de procesamiento y afines. Esta evaluación debe estar a cargo del Responsable de Sistemas.

A estos equipos se le debe dar mantenimiento regularmente.

La energía del centro de procesamiento y afines debe ser exclusiva y no compartida con otras áreas.

En casos de emergencias es importante que el personal del centro de procesamiento esté familiarizado con los procesos respectivos a fin de qué, al momento de trabajar sólo con energía brindada por el UPS, los equipos no indispensables sean apagados, a fin de alargar el tiempo de suministro alterno de energía.

Como herramienta de emergencia, se debe contar siempre con luces de emergencia o con linternas de baterías.

4.4.2.1.4 Aire Acondicionado

El centro de procesamiento debe ser mantenido a una temperatura entre 18-19°C, con una humedad entre el 45%-50%.

Para el centro de procesamiento debe existir independiente del sistema central de aire acondicionado, dos equipos de aire acondicionado “especiales” de los cuales uno actúe como respaldo del otro cuando este no pueda operar correctamente.

La característica de estos equipos no es la común de los aires acondicionados normales.

Estos equipos principalmente acondicionan automáticamente la temperatura, la humedad, controlan el fluido de aire y son silenciosos, evitando de esta forma, daños en las computadoras y demás equipos que conforman el centro de procesamiento.

En casos de contingencias en las cuales no se cuente con la operatividad del acondicionador de aire principal y a falta del equipo de respaldo; podrían mantenerse disponibles ventiladores de pedestales a fin de refrescar los equipos principales mientras dure la emergencia.

4.4.2.1.5 Detección de Agua

Es muy raro que una empresa utilice detectores de agua en sus centros de procesamiento no por su ineficacia sino por falta de conocimiento sobre la existencia de estos tipos de equipos. Estos dispositivos son importantísimos para mantener al centro de procesamiento, lejos de filtraciones de agua, principalmente en los puntos débiles, como son los lugares cercanos a los equipos de aire acondicionado.

Estos dispositivos pueden ser detectores de agua por sonido o por sensibilidad. Se pueden usar individualmente de acuerdo a las necesidades de cada empresa o pueden combinarse, es decir; pueden usarse en ciertos sectores claves los censores de agua y humedad (lugares donde se ubiquen equipos acondicionadores de aire) y en otros pueden usarse los detectores audibles (cercanos a griferías o ductos de agua).

Las alarmas deben ser mantenidas y probadas periódicamente para asegurar su operación.

De forma complementaria a los sistemas automáticos, se puede detectar visualmente filtraciones o emanaciones de agua en los pisos falsos y paredes.

4.4.2.1.6 Guardias de Seguridad

Los Guardias de Seguridad deben asegurar la vigilancia permanente de las oficinas y principalmente del centro de procesamiento y afines. Ninguna persona no autorizada podrá ingresar al centro de procesamiento sin el permiso respectivo.

Deberán también verificar que el personal de visita se encuentre en el piso y con la persona visitada. De igual forma el egreso de visitantes debe quedar registrado y deberá ser controlado a través de las tarjetas de visita y del registro de firma y hora de salida por parte del visitante.

Dependiendo de las dimensiones de la empresa y de la sensibilidad de la información que manejen, se suelen establecer cámaras de seguridad por pisos o sectores, las cuales son monitoreadas por grupo de guardias de seguridad en los sitios de control destinados para el efecto.

4.4.2.1.7 Telecomunicaciones

Se define a las comunicaciones como el arte y la ciencia de "Comunicar". Este simple concepto se extiende a las telecomunicaciones, las cuales consisten en "Comunicar" a través de alguna distancia, utilizando medios electrónicos, eléctricos, ópticos, por cable, fibra o electro magnéticamente. Las telecomunicaciones son sencillamente, medios de transmisión, recepción e intercambio de señales.

"Es todo lo relacionado con la seguridad y protección de los niveles de acceso, privilegios, recepción y envío de información por medio del sistema de

computo, protocolos, software, equipos e instalaciones que permitan la comunicación y la transmisión de la información en la empresa, etc."(7:165)

Entre las seguridades que deben observarse en el ámbito de telecomunicaciones están los cables de comunicaciones y eléctricos deben mantenerse de forma protegida para asegurar que funcionen adecuadamente.

Los equipos de comunicación como módems, nodos, controladores, servidores, etc. deben estar protegidos dentro del lugar físico donde se encuentren y en un ambiente acorde a las especificaciones técnicas proporcionadas por el manufacturador y/o proveedor del equipo.

En toda la empresa y principalmente en el centro de procesamiento, los cables eléctricos deben estar dentro de canaletas o tuberías de plástico que es un material no conductor de energía eléctrica. Para el caso de cables de redes (transmisor de voz y datos, generalmente se utilizan tuberías metálicas).

Los cables, sean estos eléctricos o no, deben estar en sitios perfectamente señalados para el efecto y ordenados, utilizando los elementos necesarios que se encuentran en el mercado para su protección contra circuitos o daños producidos por negligencia, agua, roedores, etc.

Actualmente las empresas dedicadas al diseño de ambientes, proporcionan paredes movibles las cuales tienen integrado en los paneles, las canaletas para cables. Es importante recalcar que este tipo de paneles debe ser usados fuera del área de procesamiento, ya que generalmente el material que las recubre es de tela, por tanto de fácil combustión.

Si bien es cierto que el Administrador de empresas encargará al Responsable de Sistemas de su empresa la ejecución o instalación de cableado eléctrico o estructurado (para redes), no es menos cierto que debe conocer sobre cuales serán los puntos que deben cubrirse en este tipo de instalaciones:

Instalación eléctrica: Proyecto y ejecución de obra civil, tendido de ductos (plástico), tendido de cables. Provisión e instalación de: tomacorrientes, tableros, supresores de pico (estabilizadores de tensión-UPS), etc.

Cableado Estructurado: Proyecto y ejecución de obra civil, tendido de ductos (metálico o plástico), tendido de canaletas, tendido de cables de voz y datos. Provisión e instalación de: gabinetes, conectores, patcheras, hubs, ruteadores, etc. provisión e instalación de equipamiento informático y su correspondiente software.

Servicio de mantenimiento de redes: Puede incluir todo el equipamiento informático (Servidores, computadoras personales, impresoras, etc.), como así también el chequeo y corrección de problemas en el tendido de la red y sus componentes activos. En instalaciones preexistentes, se ofrece el Servicio de Certificación de la Red.

4.4.2.1.8 Cambios en equipos (hardware).

Se presenta una secuencia de pasos a seguir para un adecuado cambio de equipo.

a. Recepción del requerimiento por parte del usuario autorizado.
b. Evaluación del impacto a causarse con el cambio

c. Aprobación de usuario de los riesgos e impacto a causarse con el cambio.
d. Definición de pruebas del cambio solicitado
e. Determinación de Instrucciones y criterios por escrito, necesarios para el correcto cambio de hardware.
f. Determinación de lugar, fecha, hora, recursos físicos y humanos requeridos para la implementación del cambio en el ambiente de producción.
g. Ejecución del cambio.
h. Aprobación formal del Usuario en el registro de control de cambios.
i. Entrenamiento al usuario
j. Actualización del inventario de equipos
k. Actualización del inventario de configuración de equipos y de los planos de la sala de computación.
l. Revisión de contratos de mantenimiento y garantías para los equipos, de tal manera que se asegure el soporte necesario para la configuración efectuada

4.4.2.2 Seguridad Lógica

"Es todo lo relacionado con los bienes intangibles de los centros informáticos..." (4:164)

Los Controles de Acceso lógico son de vital importancia ya que permiten proteger los recursos tales como programas, archivos, transacciones, comandos, utilitarios, etc.

A continuación se definen los lineamientos para implementar los mecanismos de control sobre el acceso lógico tanto local como remoto, a los recursos del centro de procesamiento de datos y afines.

En el ámbito general, los permisos de acceso deben estar basados en la necesidad del usuario por conocer la información. Esto implica que los permisos deben ser respaldados y justificados de acuerdo a la función que desempeña el usuario.

En casos de emergencia en que los recursos suelen estar desprotegidos y, en las que se requiere que otra persona diferente a la autorizada efectúe un acceso lógico, deberá hacerlo siempre bajo adecuada supervisión. Posterior a la emergencia deberá darse de baja ese usuario y clave o reemplazada con una nueva clave por seguridad.

Los sistemas de control de acceso lógico deben contemplar las violaciones al mismo. Mantener un registro histórico de todos los accesos inclusive de los intentos fallidos o violaciones de su seguridad debe producirse en forma automática.

Las claves de acceso deben resguardarse en sobres debidamente sellados y guardados en caja fuerte. En casos de emergencia, el responsable de la caja fuerte bajo autorización del Responsable de Sistemas, podrá entregar a quien este último indique, la clave que está resguardada. Deberá mantenerse un registro de los accesos a estas claves respaldadas y las autorizaciones respectivas.

Los usuarios son responsables de las claves que tienen asignadas. Por ningún motivo debe divulgarse o intercambiarse claves con otros usuarios. Cualquier resultado de no-cumplimiento de este punto, quedará exclusivamente bajo responsabilidad del usuario respectivo.

La empresa debe establecer un ente que se encargue de administrar las seguridades, usuarios y claves. Las funciones asignadas será la de controlar y mantener actualizada la lista de usuarios y claves asignadas a los diferentes recursos y de establecer políticas de cambios periódicos a fin de evitar desviaciones en las seguridades de los recursos.

4.4.2.2.1 Identificación de Usuarios

Los usuarios no deberán nunca compartir sus identificaciones como usuarios y sus claves o contraseñas. Cada nuevo usuario debe ser solicitado y justificado al responsable de sistemas y una vez aprobado, deberá ser canalizado a través del Administrador de seguridades para su asignación y control respectivo.

Es importante que el responsable de sistemas, informe tanto al solicitante como al Administrador de Seguridades, cuáles son los tipos de accesos que tendrá el nuevo usuario, así como también los no accesos, los cuales inclusive podría abarcar hasta restricciones a nivel de terminales.

Ningún usuario puede crearse sin su correspondiente clave o contraseña (password) ya que este constituye el único medio de control de seguridades.

Las claves deben consistir como mínimo de 6 caracteres alfanuméricos (números y letras), los cuales serán elegidos por el usuario. En otras ocasiones y dependiendo de los recursos a los que se tendrá acceso, las claves son asignadas directamente por el Administrador de seguridades e informadas al usuario, Ej.: usuarios de red y claves de red.

Es importante que el Administrador de usuarios no tenga dentro de sus registros la misma clave para otros usuarios. De producirse este caso, deberá cambiarse la clave inmediatamente e informado al usuario respectivo de la nueva clave. También debe en este caso tomar en cuenta los siguientes factores:

No deben existir claves de diferentes usuarios con caracteres iguales en las mismas posiciones, Ej.: 123SRRG y 123LRRG.

Debe estipularse la cantidad de caracteres numéricos a usarse en la clave.

Debe estipularse la cantidad máxima de caracteres.

Las claves deberán ser cambiadas mínimo cada 30 días. Para los casos de claves de usuarios altamente sensitivos deberá evaluarse un tiempo mayor de cambio.

Los intentos fallidos deberían ser máximo en un total de tres con clave incorrecta. Cumplidos los tres intentos fallidos, el usuario debe quedar bloqueado. Estos intentos deben quedar registrados en el sistema para su posterior control.

Las claves no deben visualizarse. Su almacenamiento debe ser en forma encriptada (codificada).

Cada acceso a cada recurso debe contener una clave específica y no repetirse.

Si el usuario considera el cambio de su clave por perdida de su confidencialidad, debe solicitar al Administrador de seguridad, la asignación de una nueva clave inmediatamente.

Hay programas que contienen usuario y clave por default (defecto) para facilitar su instalación. Esta debe cambiarse una vez que el programa haya sido instalado.

Las claves deben respaldarse en sobres de seguridad y deberán realizarse pruebas aleatorias para verificar su autenticidad y actualidad.

4.4.2.2.2 Suspensión de claves de acceso a los sistemas.

Las claves de acceso a los sistemas deben ser suspendidos por las siguientes causas:

Cuando los empleados se ausenten por vacaciones.

Cuando su usuario y clave no haya sido utilizado por un lapso de 30 días.

A evaluación del Administrador de seguridades y responsable de sistemas por accesos en fines de semana y feriados.

Cuando supere los intentos máximos de accesos fallidos a recursos asignados o no.

En cualquiera de estos casos se debe analizar e investigar los motivos y para rehabilitar el usuario, deberán solicitarse las autorizaciones nuevamente, dependiendo del tipo de suspensión aplicada. Para el caso de suspensiones por inactividad del sistema, este debe solicitar la re-entrada de la clave nuevamente.

4.4.2.2.3 Acceso a Datos

Los datos serán almacenados en medios magnéticos tales como disquetes, cartuchos, cintas o CDS. A estos datos, solo podrá accesar el personal autorizado.

La información impresa debe clasificarse de acuerdo a su seguridad.

En caso de accesos fallidos a datos, el sistema debe mantener dicha información en detalle con el nombre del usuario, fecha, aplicación, archivos, etc. A los que se pretendía accesar, así como también el número de intentos.

De igual forma el sistema debe llevar un control sobre los intentos exitosos posteriores a varios intentos fallidos. Estos pueden manejarse a través de logs (archivos de actividades cronológicas) de seguridad que deben ser revisados periódicamente por el administrador de seguridad.

Las empresas deben diseñar el procedimiento que les permita asegurar con éxito el control de la seguridad de los accesos a datos.

4.4.2.2.4 Acceso a Programas y Utilitarios

Los accesos a programas y utilitarios deben estar segmentado de acuerdo al perfil del usuario. La clasificación general es:

Los usuarios del sistema, los programadores del sistema y, personal de producción.

Los usuarios del sistema son los que podrán generar transacciones reales, o usar las funciones del sistema en producción. Podrán también

ingresar a los archivos generados por el sistema producto de las transacciones.

Los programadores solo deben tener acceso al ambiente de pruebas o desarrollo. No deben tener acceso a transacciones reales o a ingresar a funciones del sistema en producción.

El personal de producción, debe asegurarse que acceda solo a la información definida para cada usuario. Podrá efectuar las tareas definidas para el área de producción pero previniendo el acceso a datos mediante cualquier tipo de herramienta de programación o a través de programas de aplicación.

Las bibliotecas de los programas y utilitarios deben estar separadas tanto para desarrollo como para producción.

Es importante que los programas en desarrollo también sean mantenidos a nivel de versión y con los datos de fecha, hora y usuario que lo desarrolló. Es vital mantener al menos la última y penúltima actualización, de esta forma en caso de reversión se podrá ir a cualquiera de las dos últimas versiones.

En caso de ser necesario, sí se puede permitir el acceso de bibliotecas del ambiente de desarrollo tanto al usuario del sistema como al personal de producción.

Antes de que un sistema sea pasado a producción debe efectuarse una evaluación del nivel de seguridades que brinda ese programa o utilitario. Es importante que un Auditor de Sistemas y el responsable de Control Interno

verifique para determinar si el sistema cumple con las especificaciones técnicas y contiene las seguridades y controles adecuados.

Los cambios que se efectúen posteriores a programas en producción deben efectuarse de acuerdo al Control de Cambios.

4.4.2.2.5 Controles de Aplicación

Los controles de Aplicación se constituyen en aquellos enfocados a controles por los usuarios y controles por los sistemas. Los controles por los usuarios están dados sobre los datos de entrada, datos fijos, ítems rechazados o en espera, datos de salida. Los controles por los sistemas se enfocan en los datos de entrada, ítems en espera, y sobre el procesamiento.

Los controles por los usuarios se refieren a la responsabilidad que el mismo debe tener en la preparación y aprobación de las transacciones (datos de entrada); en la modificación de datos fijos en los archivos maestros y de tablas del sistema responsabilizándose por la integridad y exactitud de los mismos (datos fijos); en el control de las transacciones rechazadas o en suspenso, las cuales deben ser corregidas inmediatamente de acuerdo a su fecha contable (ítems rechazados y en suspenso) y finalmente es el responsable de los errores o desviaciones presentadas y detectadas en los datos de salidas.

Los Controles por los sistemas son aquellos que proveen y garantizan que los datos ingresados son digitados íntegramente (datos de entrada); que los ítems rechazados y en suspenso se identifiquen correctamente y se mantengan pendientes de una solución (ítems rechazados y en espera); y finalmente que el sistema posea mecanismos de control del procesamiento para asegurar que la información fue procesada con los archivos de datos correctos y además brindando a través de las diferentes etapas del

procesamiento, un seguimiento de la transacción que permita mantener una adecuada evidencia de auditoría (sobre el procesamiento).

Entre los diferentes controles para los sistemas se pueden citar los de entrada de datos, los cuales están dados mediante la generación de controles por transacciones, controles por totales, controles por secuencia, controles por tamaño de registro, verificación de clave, etc. Estos controles no deben ser seleccionados sino mas bien aplicados todos, ya que tienen una función específica durante todo el trayecto de la operación de entrada.

Con los Controles por transacciones se establece una aprobación de la misma antes de su procesamiento, esto en aprobaciones automatizadas.

Para aprobaciones manuales es preferible que esta sea dada al final del procesamiento o cuando la transacción ya está completa, Ej.: Cuando se efectúa un ingreso de una compra en el sistema de compras y la aprobación del pago de la misma se realiza antes de dicho ingreso al sistema, mediante firma en un documento; no se estará seguro de que el ingreso se haya efectuado de forma correcta con las cantidades, proveedor y demás datos de la transacción original. Para evitar fraudes, es importante en este caso aprobar o firmar una vez que la transacción haya sido completada, es decir al final.

Existe otro tipo de controles que van dirigidos al mantenimiento de la información, respecto de cambios de ítems, precios, cantidades, etc.

Con los Controles por Totales se establece un registro que asegure que todas las transacciones ingresadas sean totalizadas.

Los Controles por Secuencia son aquellos que automáticamente o manualmente va generando una secuencia del registro ya sea a nivel de formularios pre-numerados o a través de una secuencia generada automáticamente por documento que se ingresa.

Los Controles de tamaño de Registro confirman que la longitud del mensaje quede registrada de acuerdo a los parámetros técnicos establecidos y se evite la transmisión de información no contemplada en la transacción. En algunos casos también puede evaluarse la necesidad de transmisión de la información de forma codificada la cual hará más difícil el descifrar la información. Esto último es muy usado cuando la información es altamente sensitiva.

Los Controles de Aplicación deben en todo caso asegurar que los usuarios ingresen o afecten sólo lo autorizado y definido para cada uno de ellos.

4.4.2.2.6 Controles de Actividades del Programador de Sistemas.

Las actividades del programador de sistemas deben asegurar que el programa diseñado cumpla con los requerimientos solicitados, seguridades e inviolabilidad del caso. El responsable de sistemas se encargará de verificar antes de que el programa sea puesto en producción, de que el programador haya documentado debidamente el programa o cambio, que se hayan efectuado las rutinas de validación y verificación y de que se hayan completado las pruebas del sistema.

Es importante que se realicen verificaciones de las entradas y salidas de datos para todos los registros y que sea imposible la manipulación de algún registro en particular, por Ej.: Los programadores de aplicaciones bancarias (cuentas corrientes o ahorros) podrían programar débitos o

créditos a cuentas sin que estas sean detectadas a simple vista. Es vital que se implante un mecanismo de control y verificación que certifique que el programa en mención cumple con los requerimientos solicitados y las seguridades del caso.

4.4.2.2.7 Control de cambios a la programación.

Es importantísimo el determinar mecanismos para dar cumplimiento a un Control de cambios efectuados en cualquier elemento del ambiente de producción como pueden ser programas, equipos, utilitarios, etc.

Con esto se da una estructura de formalidad a la administración de los cambios a fin de que estos sean evaluados técnicamente y a nivel de empresa o negocio y, para que los cambios sean incorporados de forma consistente con la respectiva autorización del responsable de sistemas.

Así mismo el control de cambios se completa con el análisis de impacto en el usuario final el cual debe estar en pleno conocimiento de los mismos. Estos riesgos deben ser evaluados y analizados con antelación.

El control de cambios es una herramienta fundamental para mantener registro cronológico de lo que está sucediendo en nuestro sistema computacional o sus dispositivos.

No solo es un medio de información que permite actualizar la documentación técnica sino también permite la toma de decisiones respecto a la solución de fallas o inconsistencias presentadas posterior a las implementaciones de dichos cambios.

A continuación se presenta una secuencia de aspectos que se deben considerar para realizar cambios a los programas o utilitarios:

a. Recepción del requerimiento por parte del usuario autorizado.

b. Evaluación del impacto a causarse con el cambio.

c. Aprobación de usuario de los riesgos e impacto a causarse con el cambio.

d. Ejecución del cambio en ambiente de desarrollo.

e. Definición de pruebas del cambio solicitado.

f. Pruebas del cambio por personal de desarrollo en ambiente de desarrollo.

g. Auditoría de sistemas al cambio a realizarse.

h. Control Interno del cambio a realizarse.

i. Depuración del cambio luego de auditoría y control interno.

j. Pruebas del cambio por parte de los usuarios, en ambiente de desarrollo.

k. Aprobación formal del usuario en el registro de control de cambios.

l. Aprobación formal del responsable de sistemas en el registro de control de cambios.

m. Determinación de instrucciones y criterios por escrito, necesarios para la correcta transferencia al ambiente de producción y su reversión en caso de que sea necesario ejecutarlo.

n. Determinación de lugar, fecha, hora, recursos físicos y humanos requeridos para la implementación del cambio en el ambiente de producción.

Formato sugerido para el control de cambios en los programas.

<table>
<tr><td colspan="4">FORMULARIO DE CONTROL DE CAMBIOS</td></tr>
<tr><td colspan="4">Nombre de la aplicación afectada:</td></tr>
<tr><td colspan="4">Nombre del proceso(s) afectados(s):</td></tr>
<tr><td>Descripción</td><td>Condición actual</td><td>Fecha</td><td>Observaciones</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>Descripción</td><td>Condición después del cambio</td><td>Fecha</td><td>Observaciones</td></tr>
<tr><td>Beneficios</td><td>Motivos del cambio</td><td colspan="2">Propuesto por</td></tr>
<tr><td colspan="4">Aprobado usuario
(nombre, fecha, firma y comentarios)</td></tr>
<tr><td colspan="4">Aprobado por Jefe Inmediato</td></tr>
<tr><td>Aprobado Jefe de Desarrollo</td><td colspan="3">Autorizado por Gerencia de Sistemas</td></tr>
<tr><td colspan="4">Lugar y fecha de implementación</td></tr>
<tr><td colspan="4">Recursos requeridos</td></tr>
</table>

4.4.2.2.8 Firewall o muro de fuego:

Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada e Internet. El firewall determina cual de los servicios de red pueden poseer accesos dentro de ésta por los que están fuera, o viceversa, es decir, quien puede entrar para utilizar los recursos de red pertenecientes a la organización o que usuarios o programas tienen derechos a salir a Internet. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través de él mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración, desafortunadamente, este sistema no pude ofrecer protección alguna una vez que el agresor lo traspasa. Un firewall es vulnerable: él no protege de la gente que esta dentro de la red interna, éste trabaja mejor si se complementa con una defensa interna.

4.4.2.2.9 Antivirus

Según el glosario publicado en el sitio Web de Panda Software, los antivirus se definen como:

"todos aquellos programas que permiten analizar la memoria, las unidades de disco y otros elementos de un ordenador, en busca de virus".

CAPITULO V

CONTROL INTERNO PARA UN SISTEMA TRANSACCIONAL DE REMESAS FAMILIARES EN UNA ENTIDAD BANCARIA

En los capítulos anteriores se expusieron conceptos sobre remesas familiares, control interno, regulación que deben cumplir las empresas remesadoras de divisas, además se proporciona la teoría de sistemas de información así como los controles para el resguardo de la información.

En el presente capítulo, con el objeto de proponer el control interno para un sistema transaccional de remesas familiares en una entidad bancaria, se estudia un caso práctico.

Antes de iniciar a describir cada paso para la incorporación de controles internos a los sistemas de información, se deben conocer las generalidades de la empresa, la cual se presenta a continuación.

5.1 Antecedentes

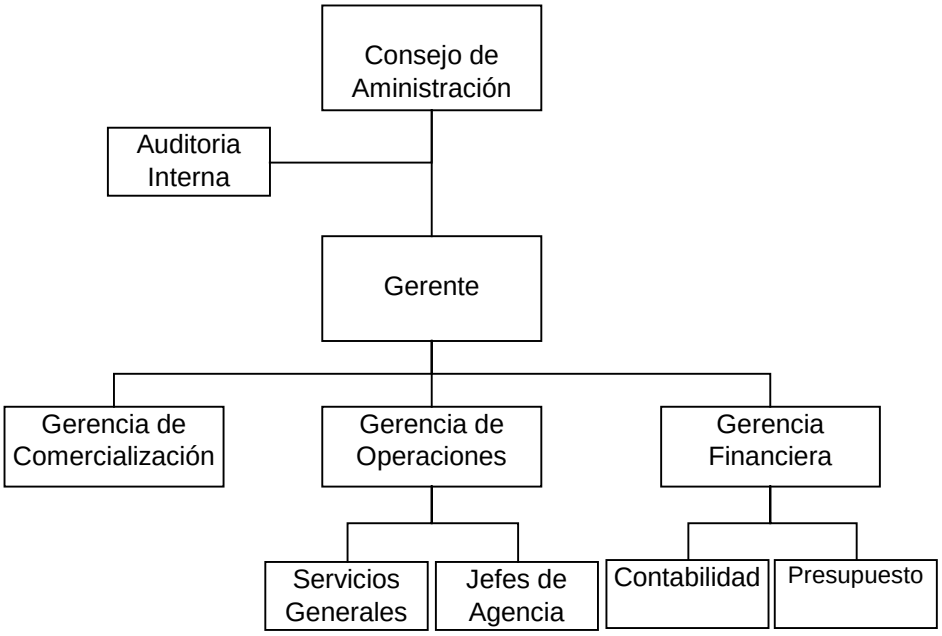
En los numerales siguientes se presenta la información de la empresa remesadora y del banco pagador, por discrecionalidad de la información de éstas se cambio el nombre real.

5.1.1 Antecedentes de la Empresa Remesadora

La empresa Moneyusa.Corp fue fundada en el año de 2001, bajo las regulaciones del Estado de California, con el objetivo principal de brindar el servicio de transferencias electrónicas de remesas familiares de forma eficiente.

5.1.1.1 Estructura Organizativa.

La estructura organizativa de la empresa es la siguiente:

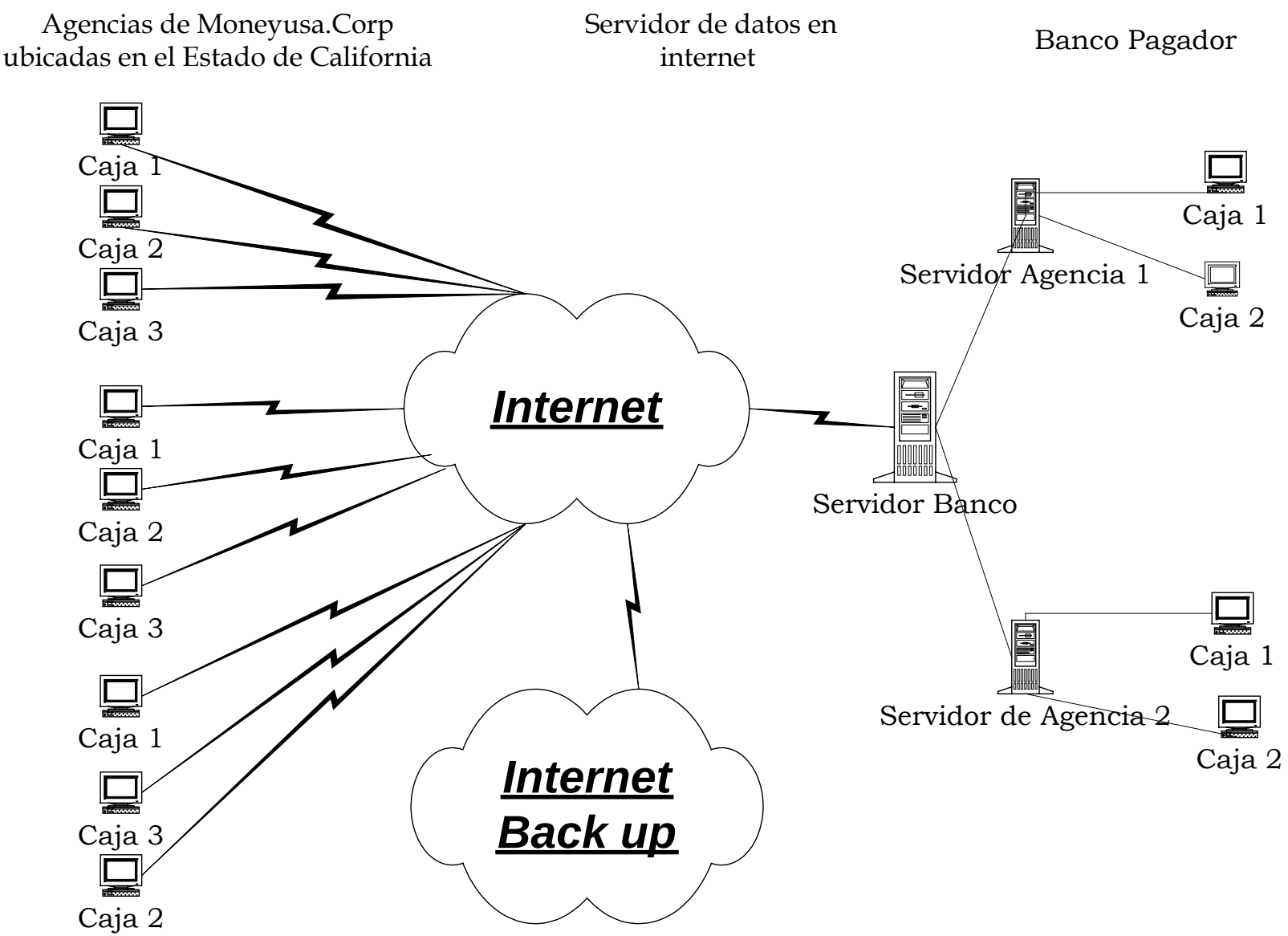


5.1.1.2 Diagrama de sistemas de computación.

Derivado a que la captación de las remesas es realizada en Estados Unidos de América, y además de ofrecer el servicio de pago inmediato (cuestión de minutos) en el país destino, fue necesario para la compañía diseñar un sistema que preste el servicio de forma eficiente.

El sistema que permite interactuar entre los puntos de recepción y los puntos de pago a los beneficiarios se encuentra alojado en un servidor de Internet.

A continuación se presenta el diagrama del sistema:


Agencias de Moneyusa.Corp
ubicadas en el Estado de California
Servidor de datos en
internet
Banco Pagador
Caja 1
Caja 2
Caja 3
Caja 1
Caja 2
Caja 3
Caja 1
Caja 3
Caja 2
Internet
Internet
Back up
Servidor Banco
Servidor Agencia 1
Caja 1
Caja 2
Servidor de Agencia 2
Caja 1
Caja 2

5.1.2 Del Banco Pagador

El “Banco Chapín” es el banco relacionado en Guatemala, éste banco firmó un contrato de servicio con la Empresa “Moneyusa.Corp” para el pago de remesas familiares provenientes de Estados Unidos de América.

El Banco Chapín tiene una infraestructura de 139 agencias distribuidas en los departamentos de Guatemala.

5.2 Proceso contable.

A continuación se detallan las principales partidas derivadas de la actividad de remesas familiares que registra Moneyusa.Corp (Empresa Remesadora) y el Banco Chapín (Banco Pagador),

a. Registro de la recepción de dinero de los remitentes.

El dinero es recibido por medio de la caja del receptor de las agencias de la empresa Moneyusa.Corp, el sistema transaccional de remesas al final del día cuando se realiza el cierre de operaciones envía una partida contable de la manera siguiente:

Registros contables de Moneyusa.Corp (Empresa Remesadora)

		Debe	Haber
Registro de remesas recibidas del remitente			
Como ejemplo se toma el total de las remesas recibas durante el 2005, ver el cuadro resumen de movimiento de remesas durante 2005			
		Debe	**Haber**
101101	Caja General	116,246,496	
305101	Remesas por pagar		112,836,375
601102	Comisiones		3,410,121
	Total	**US$.116,246,496**	**US$.116,246,496**

Registros contables del Banco del Chapín (Banco Pagador en Guatemala)

El Banco Chapín (Banco Pagador), no registra operación contable.

b. Depósito del dinero recibido en las Agencias de Moneyusa.Corp.(Remesadora).

Registros contables de Moneyusa.Corp (Empresa Remesadora)

Registro de los depósitos realizados al " Banco California " por las Agencias.

		Debe	Haber
101103	Disponibilidades Cta Remesas	112,836,375	
101103	Disponibilidades Cta Gastos de Operación	3,410,121	
101101	Caja		116,246,496
	Total	**US$.116,246,496**	**US$.116,246,496**

Registros contables del Banco del Chapín (Banco Pagador en Guatemala)

El Banco Chapín (Banco Pagador), no registra operación contable.

c. Registro del pago de las remesas a beneficiarios por banco pagador.

Las remesas familiares son pagadas a los beneficiarios en Guatemala por el "Banco el Chapín" por cuenta de la remesadora, cuando éste paga las remesas su sistema actualiza en línea el sistema transaccional de la empresa Moneyusa.Corp. En consecuencia al final del día La empresa Moneyusa.Corp(Remesadora) y el Banco Chapín(Banco Pagador) realizan los registros siguientes:

Registros contables de Moneyusa.Corp (Empresa Remesadora)

Registro de remesas pagadas por el "Banco del Chapín " al beneficiario

		Debe	Haber
305101	Remesas por pagar	112,738,802	
305101	Liquidaciones por pagar Bancos		112,738,802
	Total	**US$.112,738,802**	**US$.112,738,802**

Registros contables del Banco del Chapín (Banco Pagador en Guatemala)

Registro de remesas pagadas por el "Banco del Chapín " al beneficiario

		Debe	Haber
104601	Pagos por cuenta ajena	112,738,802	
101101	Caja General		112,738,802
	Total	**US$.112,738,802**	**US$.112,738,802**

d. Pago de liquidaciones a bancos:

Los pagos se realizan emitiendo cheques de la cuenta de depósitos de la remesadora donde fueron depositados los fondos provenientes de remesas.

Realizarlo de esta manera facilita la labor de control, ya que en definitiva la sumatoria de las cuentas de pasivo Remesas por pagar y Liquidaciones por pagar bancos deben corresponder al saldo de la cuenta de disponibilidades. Las partidas contables son las siguientes:

Registros contables de Moneyusa.Corp (Empresa Remesadora)

Registro de liquidaciones pagadas al "Banco del Chapín"

		Debe	**Haber**
305101	Liquidaciones por pagar Bancos	112,738,802	
101103	Disponibilidades /Cta. Remesas		112,738,802
	Total	**US$.112,738,802**	**US$.112,738,802**

Registros contables del Banco del Chapín (Banco Pagador en Guatemala)

Registro de liquidaciones pagadas al "Banco del Chapín"

		Debe	**Haber**
101605	Cheques por compensar	112,738,802	
104601	Pagos por cuenta ajena		112,738,802
	Total	**US$.112,738,802**	**US$.112,738,802**

e. Registro de comisiones convenidas con el banco pagador.

Derivado a que los pagos realizados por los bancos son registrados en línea al sistema transaccional de la remesadora, al final del día este sistema genera el registro contable siguiente:

Registro de las comisiones por pagar al "Banco del Chapín" por los pagos por cuenta ajena

701102	Comisiones	655,380	
305101	Comisiones por pagar		655,380
		US$.655,380	**US$.655,380**

Registro de las comisiones por pagar al "Banco del Chapín" por los pagos por cuenta ajena

104601	Comisiones por cobrar	655,380	
601102	Comisiones		655,380
		US$.655,380	**US$.655,380**

Moneyusa.Corp
Resumen de Movimiento de Remesas durante 2005
Valores en US$.

	Recibidas		Pagadas		Saldo	
Mes	Unidades	Valores	Unidades	Valores	Unidades	Valores
	Saldo anterior				368	147,000.00
Ene-05	18,699	7,486,285.07	17,945	7,184,457.02	1,122	448,828.05
Feb-05	19,061	8,199,644.96	18,341	7,889,985.08	1,842	758,487.93
Mar-05	21,084	8,756,851.07	22,101	9,179,166.66	825	336,172.34
Abr-05	21,470	9,941,657.30	20,946	9,699,175.20	1,349	578,654.43
May-05	23,615	10,239,546.84	23,829	10,332,609.12	1,134	485,592.15
Jun-05	21,684	9,883,108.68	21,851	9,958,958.73	968	409,742.10
Jul-05	22,772	10,199,891.52	21,014	9,412,379.55	2,726	1,197,254.07
Ago-05	22,298	9,612,358.68	24,440	10,535,443.59	584	274,169.16
Sep-05	21,618	9,235,793.93	21,621	9,237,101.25	581	272,861.83
Oct-05	24,825	10,336,641.12	24,479	10,192,090.47	927	417,412.48
Nov-05	20,259	8,815,043.01	20,681	8,998,653.36	506	233,802.13
Dic-05	24,935	10,129,552.46	24,908	10,118,782.02	533	244,572.57
	262,317	**112,836,375**	**262,152**	**112,738,802**		
		(a)		**(b)**		

Moneyusa.Corp
Resumen de comisiones
Valores en US$.

Cobradas a los remitentes			Pagadas a los Bancos		
Mes	Unidades	Comisión US$. 13.00	Mes	Unidades	Comisión US$. 2.5
Ene-05	18,699	243,087	Ene-05	17,945	44,861
Feb-05	19,061	247,787	Feb-05	18,341	45,851
Mar-05	21,084	274,092	Mar-05	22,101	55,253
Abr-05	21,470	279,104	Abr-05	20,946	52,365
May-05	23,615	306,989	May-05	23,829	59,573
Jun-05	21,684	281,892	Jun-05	21,851	54,626
Jul-05	22,772	296,030	Jul-05	21,014	52,534
Ago-05	22,298	289,868	Ago-05	24,440	61,099
Sep-05	21,618	281,034	Sep-05	21,621	54,053
Oct-05	24,825	322,725	Oct-05	24,479	61,196
Nov-05	20,259	263,367	Nov-05	20,681	51,701
Dic-05	24,935	324,149	Dic-05	24,908	62,269
Total	**262,317**	**3,410,121**	**Total**	**262,152**	**655,380**
		(a)			**(e)**

(a) Las comisiones cobradas a los remitentes de las remesas es una cuota fija de US$13.00.

(e) Las comisiones que cobra el banco pagador es de US$.2.5 por cada remesa pagada.

Para el costo de ambas comisiones no existe un patrón a seguir de cobro estas van en función de la Competencia.

5.3 Control interno en sistemas de remesas familiares utilizado por el banco pagador y la empresa remesadora.

En los numerales siguientes se proponen aspectos de control para la protección de los sistemas de remesas familiares.

5.3.1 Controles que se deben implementar en un sistema de remesas familiares, para la protección de la seguridad operativa del sistema

Para el control operativo de cualquier empresa es necesario implementar primordialmente políticas y procedimientos que regulen la operación y que fomenten una cultura organizacional de control. A continuación se presenta un despliegue de puntos de control esenciales para el buen funcionamiento del sistema de remesas familiares.

5.3.1.1 Formularios preimpresos

Un diseño adecuado de formularios permite guiar el registro de las operaciones por consiguiente constituye un buen control preventivo.

Para evitar el uso anómalo de los formularios, se deben resguardar y mantenerse controlados.

5.3.1.2 Restricción de acceso a usuarios

Se debe diseñar el sistema a medida que los usuarios se puedan identificar. A estos se les deben asignar los privilegios en el sistema conforme al papel que desempeñan en la empresa. Si es cajero no debe tener acceso para hacer modificaciones a los registros contables.

Los permisos de acceso deben estar basados en la necesidad de los usuarios y el papel que desempeñan en la empresa, esto implica que todo acceso debe ser autorizado por funcionario. Es esencial diseñar un formulario que contenga la descripción de los accesos solicitados y su justificación, este formulario debe estar firmado por el jefe de área.

El sistema debe mantener control de todos los accesos inclusive los intentos fallidos.

Lo importante es promover una cultura de control que minimice el riesgo de fraudes internos.

Derivado a que el sistema se encuentra alojado en Internet, por la cobertura que esto significa, se deben tomar en consideración los criterios de control como restringir el uso a un horario de trabajo, o un control cruzado con el control de ingreso a las instalaciones, mantener un listado de IP (Protocolo de Internet. El conjunto de estándares tecnológicos y especificaciones técnicas que permiten que la información sea transmitida de una red a otra a través de todo Internet.) de tal manera que únicamente se permitan operaciones por medio de computadoras autorizadas, esto aplica para las cajas receptoras de la empresa remesadora así como del servidor del banco pagador.

Cuando un empleado se retira temporal o totalmente de la empresa se deberá suspender los permisos del sistema, como medida de control se debe establecer un lapso de tiempo prudencial de no acceso para inhabilitar este permiso.

5.3.1.3 Puntos de control que deben aplicarse a las operaciones del receptor.

Al inicio del día se debe asignar un fondo a cada cajero.

Se debe diseñar el sistema a efecto de que se pueda personalizar los montos máximos que debe tener un cajero, en consecuencia el sistema debe desplegar mensajes de alerta cuando la caja supera la cantidad estipulada. Pero en ningún momento debe desplegar el monto que el cajero debe tener en su caja.

Al final de la jornada el cajero debe contar el efectivo de su caja y este debe ser cotejado con el efectivo según el sistema. Para realizar esta prueba de efectivo el sistema debe tener la opción de ingresar el monto del dinero contado por el cajero y debe remitir un mensaje al sub jefe de la agencia si no existieran diferencias este deberá autorizar el cierre, de lo contrario deberá apersonarse al lugar de trabajo del cajero y realizar el arqueo correspondiente y se procederá a hacer el cargo del faltante o el registro de sobrante si existiese.

Otro aspecto importante de observar, es que las cajas de recepción de efectivo únicamente deben contener instalado el sistema de remesas y ningún otro programa, la razón de este control es derivado a que estos programas podrían utilizarse para simular una certificación que el efectivo recibido ha sido operada en el sistema.

Los cajeros no deben realizar operaciones personales de envío desde su caja, para lograr este objetivo se debe diseñar un sistema de alerta amarrado a una base de datos que deberá requerírsele a cada empleado para iniciar la relación laboral. Como por ejemplo, nombre completo de la madre, padre, hermanos y cónyuge.

5.3.1.4 Sistema de Contabilidad

La contabilidad debe estar diseñada para poder proporcionar información por agencias.

La contabilidad debe ser un módulo del sistema general, que permita actualizar los movimientos en línea.

5.3.1.5 Controles para el manejo de efectivo en la empresa remesadora.

Las empresas remesadoras manejan volúmenes de efectivo bastante significativos, dependiendo de su tamaño por consiguiente es necesario para estas contar con controles que ayuden a mitigar el riesgo de errores o irregularidades que afecten su situación financiera.

Dentro de los controles indispensables para el manejo del efectivo se proponen principalmente los siguientes:

a) Realizar arqueos de efectivo periódicamente.
b) Depositar íntegramente el efectivo recibido.
c) Asignar montos límite a las cajas de los receptores.

d) Realizar conciliación diaria de los depósitos enviados por las agencias.

5.3.2 Controles que se deben implementar en un sistema de remesas familiares, para la protección de la seguridad lógica.

- Prohibir uso de cuentas anónimas y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. En cualquier caso debe registrarse en la bitácora todos los cambios de ID.

- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

- Cuando un empleado es despedido o renuncia a la Compañía, debe desactivarse su cuenta antes de que deje el cargo. contraseñas y el control de acceso.

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

- Prohibir que los usuarios se compartan contraseñas o revelarlas a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

- Prohibir el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

- Para el acceso remoto a los recursos informáticos de la Compañía, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

- Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione su contraseña.

- Si el sistema de control de acceso no está funcionando de forma apropiada, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Compañía, pudiendo ser causal de despido.

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

- La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.

- No debe concederse una cuenta a personas que no sean empleados de la compañía a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

- Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Gerente de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens).

- Obtener una certificación del sitio de internet del sistema de remesas familiares.

5.3.3 Controles que se deben implementar en un sistema de remesas familiares, para la protección de la seguridad de la base de datos.

- Los archivos de bitácora (logs) y los registros de auditoría que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses.

- Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

- Los servidores de red y los equipos de comunicación, routers, etc. deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

5.3.4 Controles para la seguridad en la telecomunicación de datos.

- Todos los cambios en la central telefónica y en los servidores y equipos de red de la Compañía, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

5.3.5 Casos de la implementación de controles a un sistema transaccional de remesas familiares.

Por la naturaleza del negocio de remesas familiares, todas los esfuerzos deben estar encaminados para detectar errores o fraudes internos y externos, además de contar con instrumentos para prevención de lavado de activos y financiamiento al terrorismo.

a) Perfiles para los distintos usuarios del sistema.

b) Las claves de acceso deben ser de ocho dígitos mínimo, el sistema verifica que éstos contengan la cantidad de dígitos, que no sean repetidos por lo menos dentro de las 10 claves utilizadas.

c) Suspensión de accesos cuando un empleado se retira, el sistema suspende los accesos por períodos de inactividad.

d) Como cultura se ha indicado a los cajeros de no dejar habilitados sus claves cuando se retiran de las cajas, el sistema automáticamente suspende las sesiones en el sistema por inactividad y envía un reporte para sancionar al cajero.

e) Se creó un código dígito verificador que es calculado cuando el beneficiario se presenta a la ventanilla.

f) Toda la información que viaja en la red, tanto claves de acceso, como información de remesas, es cifrada. Para garantizar la información que viaja en la red se contrató los servicios de una empresas cifrado de información.

g) Se colocó un sistema de alertas para transacciones sospechosas, por ejemplo si un cajero envía dinero a un destinatario con un homónimo de su nombre o familiares es detectado por el sistema.

h) Debido a que el sistema se encuentra en Internet, el sistema para habilitar una caja solicita la clave de supervisor. Además el sistema identifica la dirección IP de la computadora que se esta comunicando y si no es la correcta la rechaza.

i) El sistema requiere un monto mínimo de efectivo en las cajas de los cajeros, si estos se exceden el sistema automáticamente le da una alerta para que haga entregas parciales de efectivo. Con esta acción el sistema disminuye el riesgo de que un cajero pueda ingresar al sistema remesas que efectivamente no recibe y que estas sean cobradas de inmediato en el país destino.

j) El sistema al momento del pago valida si las remesas no han sido pagadas con anterioridad, que el estatus no haya cambiado.

k) Para todos los cambios el sistema guarda bitácora del usuario, fecha y hora en que se realizó el cambio.

l) La identificación del IP del banco pagador es controlada de la misma manera en que se controlan las computadoras del los cajeros de recepción.

m) Utilización de Antivirus para la protección del servidor central y de cajas de recepción.

n) En las cajas de recepción de efectivo únicamente se tiene instalado la aplicación de comunicación con el servido de Web, para reducir el riesgo de falsificación de certificaciones.

o) La información alojada en el servidor transaccional es trasladada en línea a otro servidor que sirve como soporte al no estar en línea el servidor principal.

p) El servidor transaccional cuenta con firewall(muro de fuego) que filtra toda la comunicación de acceso.

5.3.6 Controles de sistema para la prevención del lavado de activos y financiamiento al Terrorismo (AML/FT Antimoney Laudering / Fiancial Terrorist),

5.3.6.1 Remesadora de Divisas:

El sistema debe tener la opción de cargar listas negras como por ejemplo OFAC y generadas por la propia compañía, para que valide antes de hacer un envío de remesas familiares reduciendo así el riesgo de sanciones de las entidades reguladoras.

El sistema debe mantener un registro de los remitentes que contenga, número de identificación, dirección, teléfono, familiares, origen de los fondos, frecuencia de las remesas.

El sistema debe generar un perfil del cliente sobre la base de la información recopilada del cliente, en el sentido que permita enviar señales de alerta si las operaciones que realiza el cliente no concuerdan con el perfil establecido.

El sistema debe estar diseñado a manera que pueda generar reportes de beneficiarios y remitentes. Por ejemplo generar un detalle de remesas recibidas por beneficiario provenientes de varios remitentes y a la inversa generar reporte de un solo remitente para varios beneficiarios.

El sistema debe generar reportes de remesas por número de teléfono de los beneficiarios.

5.3.6.2 Banco pagador:

De la misma manera el Banco pagador debe mantener controles que le permitan monitorear las remesas por beneficiario y remitente.

El sistema debe generar reportes que le permitan establecer si varios remitentes envían remesas a un solo beneficiario o viceversa varios beneficiarios reciben remesas de un solo remitente.

El sistema debe permitir asignar un parámetro de medición de la razonabilidad de recepción de remesas en cuanto al tiempo.

CONCLUSIONES

1. En la actualidad, las remesas familiares ocupan un lugar importante en la economía del país, ya que genera ingresos de divisas significativos que se reflejan en la balanza cambiaria del país, adicionalmente crea una diversidad de fuentes de empleo directos e indirectos.

2. Un sistema de control interno bien fortalecido en los sistemas transaccionales influye directamente en la confidencialidad, integridad y disponibilidad de la información, en el presente trabajo se exponen elementos esenciales para una adecuada incorporación de estos controles.

3. Para las instituciones financieras la intermediación entre las empresas remesadoras con el beneficiario además de la comisión que cobra a ésta, le favorece, porque se abre un nuevo mercado ya que a éstos se le puede ofrecer otro tipo de servicios financieros, como cuentas de ahorro, cuentas de cheques, créditos, entre otros.

4. Las empresas de remesas familiares están expuestas a multas y sanciones en función de la actividad que desempeñan, si su infraestructura es utilizada para el lavado de activos o financiamiento al terrorismo, el monto de las multas es elevado y las sanciones son fuertes inclusive el cierre de la empresa.

RECOMENDACIONES

1. La instituciones de gobierno deberán incentivar el incremento de la actividad productiva aprovechando estos flujos de efectivo a fin de evitar la dependencia a estas debido a que esto podría fomentar el ocio y en consecuencia el incremento de la delincuencia.

2. Que las empresas que se dedican a la actividad de remesas familiares, tomen en consideración los elementos que se definen en el presente trabajo, para implementar un sistema integrado de control interno en su sistema transaccional, que les permita mantener la confidencialidad, integridad y disponibilidad de la información.

3. Que las instituciones bancarias pagadoras de remesas familiares visualicen mas allá del cobro de la comisión y busquen el aprovechamiento del transito de usuarios en sus agencias convirtiendo a éstos en clientes al incentivar el ahorro o la prestación de servicios.

4. El Contador Público y Auditor que asesore o participe en la implementación de un sistema de control interno para un sistema transaccional de empresas remesadoras de divisas debe observar la normativa legal vigente a la que ésta se encuentre sujeta y principalmente lo referente a la normativa de lavado de activos y financiamiento al terrorismo.

BIBILIOGRAFIA

1 Bradford Cadmus –Control Interno Control el Fraude y el Derroche– Primera Edición –México: Editorial Prometeo, 1956. – 220p.

2 Congreso de la Republica de Guatemala – Ley de Bancos y Grupos Financieros – Decreto 19-2002. –38p.

3 Eric L. Kohler. –Diccionario para Contadores– Décima Edición– México: Editorial Limusa, S.A. de CV., 2001–717p.

4 Muñoz Razo, Carlos –Auditoria en sistemas Computacionales– Primera Edición– México: Pretice Hall Hispanoamericana, S.A., 2002 –796p.

5 Murdick, Robert G. y Rooss, Joel E. –Sistemas de Información Administrativa– Segunda Edición– México: Pretice Hall Hispanoamericana, S.A., 1988– 550p.

6 Océano Multimedia –Enciclopedia del Consultor 2000– Océano Grupo Editorial, S.A.

7 Pinilla F. José Dagoberto –Auditoria informática aplicaciones en producción– Primera Edición– Colombia: Editorial Computextos Laser, 1997 –238p.

8 R. Jonson, F.E. Kast, J.E. Rosenzneig. –Teoría, Integración y administración de sistemas. Primera Edición– México: Editorial Limusa,1977 –215p.

9 Real Academia Española –Diccionario de la Lengua Española– Vigésima Primera Edición– España: Editorial Espasa Calpe, S.A.,2001 –2133p.

10 Comité of Sponsoring of the Treadway Comisión – Control Interno Estructura Conceptual Integrada / Traductor Samuel Alberto Mantilla B.-1era. Edición – Colombia: Ecoediciones, 1998 – 140 p.

11 Cepeda, Gustavo – Auditoria y Control Interno—Colombia: McGraw-Hill, 1999. –233p.

12 KPMG América Latina. – Guías sobre Auditoria de PED, y evolución del Control Interno en sistemas de PED.— México.1991.-197p.