UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS

"EL CONTROL DEL RIESGO OPERACIONAL EN EL ÁREA DE TARJETAS DE CRÉDITO DE UNA INSTITUCIÓN BANCARIA"

TESIS

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

POR

JORGE ISAAC GONZÁLEZ VÁSQUEZ

PREVIO A CONFERÍRSELE EL TÍTULO DE

CONTADOR PÚBLICO Y AUDITOR

EN EL GRADO ACADÉMICO DE

LICENCIADO

Guatemala, Abril 2007

JUNTA DIRECTIVA DE LA FACULTAD DE CIENCIAS ECONÓMICAS

Decano	Lic. José Rolando Secaida Morales.
Secretario	Lic. Carlos Roberto Cabrera Morales.
Vocal I	Lic. Canton Lee Villela.
Vocal II	Lic. Mario Leonel Perdomo Salguero.
Vocal III	Lic. Juan Antonio Gómez Monterroso.
Vocal IV	P.C. Efrén Arturo Rosales Alvarez.
Vocal V	P.C. Deiby Boanerges Ramírez Valenzuela.

PROFESIONALES QUE REALIZARON LOS EXÁMENES DE ÁREAS PRÁCTICAS

Auditoría	Lic. Moisés Mardoqueo Sapón Ulin.
Contabilidad	Lic. Carlos Echeverría Guzmán.
Matemática-Estadística	Lic. Carlos H. Hernández.

PROFESIONALES QUE REALIZARON EL EXAMEN PRIVADO DE TESIS

Presidente	Lic. Manuel Fernando Morales García
Examinador	Lic. Guillermo Javier Cuyun González
Examinador	Lic. Carlos Roberto Mauricio García

ORIGINAL DEL DICTAMEN DEL ASESOR

CUARTA HOJA: EN BLANCO PARA ORDEN DE IMPRESIÓN

DEDICATORIA

A DIOS	Ser Todopoderoso que nos guía, guarda e ilumina con su gran amor en todos los caminos y por regalarnos la sabiduría necesaria para desenvolvernos en la vida.
A JESUCRISTO	Hijo de Dios, por el regalo de la vida eterna y su gran amor para con nosotros.
A MI PADRE	Jorge E. González Fuentes. Por su ejemplo de responsabilidad y lucha en la vida que me inspiran a avanzar en el campo profesional y personal. Mil gracias por todo Padre; que Dios recompense los esfuerzos realizados en beneficio nuestro.
A MI MADRE	Rosa F. Vásquez de González Q.E.D. Por su amor, valores y comprensión brindados cuando estuvo con nosotros. Dios la tenga descansando en sus brazos.
A MI ESPOSA	Magda Anzueto. Amada esposa, amiga y consejera, quien con su don de inculcar la consecución de la metas, me apoyó grandemente para alcanzar este logro. Gracias por toda la paciencia y cariño brindado durante el transcurso de mi carrera.
A MI HIJO	Jorge Antonio, mi gran tesoro y motivo de inspiración para continuar luchando en todos los campos de la vida en búsqueda de un futuro promisorio. Sirva este logro de ejemplo de perseverancia y dedicación para él.
A MIS HERMANOS	Con gran cariño para todos por el apoyo brindado en cada etapa de mi vida.
A MIS SUEGROS	Por la disposición incondicional de aprecio recibido en todo momento.
A MIS AMIGOS	Gracias por su amistad y soporte en cada etapa de la carrera. Especial agradecimiento a Jaime López y Maco Oliva.
A MI ASESOR	M.A. Edwin Martínez, por los conocimientos compartidos y por ser un ejemplo en el campo profesional.
A LA USAC	Por brindarme la oportunidad de formarme en sus salones. Espero poder devolver parte de lo recibido a la sociedad y la misma Universidad.

CONTENIDO

CAPITULO III
ADMINISTRACIÓN DE RIESGO OPERATIVO, SEGÚN EL COMITÉ DE BASILEA

CAPITULO IV
ADMINISTRACIÓN DE RIESGO OPERATIVO EN EL ÁREA DE TARJETAS DE CRÉDITO

CAPÍTULO V
CASO PRÁCTICO

"CONTROL DE RIESGO OPERATIVO EN EL ÁREA DE TARJETAS DE CRÉDITO SEGMENTO ORO, DEL BANCO PRIVADO GOLDBANK, SOCIEDAD ANÓNIMA"

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

INTRODUCCIÓN

En la actualidad el empleo del efectivo, el cheque, la letra de cambio y el pagaré, siguen siendo una práctica regular en el comercio para satisfacer necesidades de pago y crédito respectivamente, sin embargo; existe desde hace algunas décadas, una forma de pago y crédito diferente: **La tarjeta de crédito**, cuya utilización resulta cada vez más frecuente en el mundo moderno por las bondades que ofrece. Derivado de lo anterior y del auge de aceptación en casi todo tipo de comercio y su promoción de forma masiva por los bancos del sistema, éste modo de pago ha provocado una serie de riesgos operativos inherentes y potenciales que requieren un análisis particular para controlarlos y mitigarlos.

Por otra parte, las instituciones financieras son por mucho, pioneras y modelos en el tema de administración de riesgos, derivado de la necesidad de mantener en lumbrales apropiados las posibles pérdidas a las que pueden estar expuestas por no contar con medidas de control y prevención oportunos, confiables y eficientes. Tal calificación, aunada con la proximidad de entrada en vigencia en los países de primer mundo del acuerdo de Basilea II, el cual establece requerimientos de capital por riesgo operativo, incrementan la importancia de conocer y administrar apropiadamente dicho riesgo en los bancos y en especial en aquellos que realizan la actividad de emisión de tarjetas de crédito. Para el efecto, el presente trabajo comprende cinco capítulos que de manera somera, abordan el tema de "Control del riesgo operativo en el área de tarjeta de crédito de una institución bancaria".

El primer capítulo se refiere a las generalidades de la tarjeta de crédito, haciendo una reseña de su historia, sus características y funcionamiento. Además, la relación del sistema financiero guatemalteco -en especial de los bancos privados- con la emisión del producto tarjeta de crédito conociendo su entorno, cuota de mercado y principales procesos que efectúan de manera común; así como las Leyes que les enmarcan el actuar como emisores de tarjetas de crédito.

En el segundo capítulo son analizados los diversos riesgos a los que están expuestas las entidades bancarias, haciendo énfasis en el riesgo operativo y sus aspectos siguientes: Conceptualización,

antecedentes, tipología, métodos para el cálculo de requerimiento de capital –incluidos requisitos para cada método- y descripción de los potenciales riesgos operativos en el área de tarjetas de un emisor bancario. Además, se efectúa el cálculo de requerimiento de capital para riesgo operativo, conforme el Método del Indicador Básico, mismo que comprende la identificación de los diversos ingresos del banco sin subdividir en líneas de negocio y que deben multiplicarse por un factor constante denominado Alfa.

El tercer capítulo se refiere a las recomendaciones para la apropiada administración del riesgo operativo según publicaciones del Comité de Basilea; así como, un análisis del entorno internacional sobre el tema en mención.

En el cuarto capítulo, denominado "Administración del riesgo operativo en el área de tarjetas de crédito" se presenta de forma ejemplificada la aplicación de las principales recomendaciones emitidas por el Comité de Basilea sobre la administración del riesgo (en éste caso del área de tarjetas de un emisor bancario), los controles internos que debieran existir y el papel de la Auditoría Interna sobre el particular. Finalmente, se presentan los resultados de una encuesta realizada a algunos bancos privados guatemaltecos emisores de tarjetas, sobre varios aspectos relacionados con la gestión de riesgos operativos y su comprensión del Acuerdo de Basilea II.

El quinto y último capítulo, comprende la materialización de los cuatro capítulos previos, pues de manera práctica se efectúa un trabajo de identificación, evaluación, control y mitigación de riesgos operativos en el área de tarjeta de crédito del banco –ficticio- GOLDBANK,S.A., actividad llevada a cabo por un grupo designado por el Comité de Riesgo Operativo de esa entidad, quienes utilizando las herramientas necesarias, presentan como producto final: el informe de hallazgos y recomendaciones para la administración del riesgo sujeto de estudio.

Finalmente, se presentan las conclusiones a las cuales se llegó como resultado del trabajo efectuado y se sugieren recomendaciones que a criterio del autor debieran considerarse en el tema.

METODOLOGÍA

Congruente con los objetivos definidos en la planificación del trabajo, la presente investigación comprendió una serie de actividades que permitieran establecer las causas que incrementan la exposición al riesgo operativo en los bancos privados emisores de tarjetas de crédito, analizar la diversidad de riesgos comprendidos en esta clasificación y conocer las mejores prácticas para administrarlo.

a) Método utilizado: Deductivo.

En el desarrollo de la investigación se analizaron aspectos relacionados de manera general con la utilización, condiciones, procesos, etc. de las tarjetas de crédito. De igual forma se analizó el riesgo operacional, para que una vez tratados ambos temas se pudiera avanzar en sus aspectos específicos como las medidas de control necesarias, definición de modelos de gestión de riesgo, etc.

b) Técnicas.

Fue necesaria la aplicación de diversas técnicas para el desarrollo de la presente investigación, tales como: la recopilación de datos bibliográficos, observación, entrevistas y encuestas a funcionarios responsables de la administración de riesgo operativo de algunos bancos del sistema, así como el análisis e interpretación de tales resultados.

c) Comprobación de Hipótesis.

Una de las razones fundamentales de este trabajo es la comprobación de la hipótesis planteada al inicio de la investigación, la cual afirma que como consecuencia de la inapropiada administración del riesgo operativo en las entidades bancarias emisoras de tarjetas de crédito, se potencian las pérdidas económicas a causa de fraudes internos o externos, deficiencias en los procesos y el deterioro de la imagen del banco. Tal afirmación es verdadera pues según los resultados de la investigación los bancos privados nacionales reconocen que las pérdidas por concepto de riesgo operativo son considerables.

CAPITULO I

LA TARJETA DE CRÉDITO EN INSTITUCIONES BANCARIAS

1.1 Origen y Evolución de la Tarjeta de Crédito (29: 01).

La tarjeta de crédito es considerada como un eslabón más de la cadena que inició desde el trueque de metales preciosos, dinero (billetes), cheques, letras de cambio, transferencias, órdenes bancarias, etc. En los países desarrollados, actualmente la tarjeta de crédito representa el principal medio de pago a nivel nacional e internacional.

Sobre los orígenes o circunstancias que generaron la necesidad de la creación de este medio de pago, se relaciona principalmente al desarrollo de las actividades mercantiles, al auge de la sociedad de consumo y de la contratación en masa. En cuanto a las necesidades que generalizaron su utilidad se encuentran, entre algunas las siguientes: Evitar la movilización de dinero en efectivo y simplificar la actividad comercial de los consumidores, aplazar obligaciones de pago en las transacciones, favoreciendo al portador el diferimiento del reembolso, además de disminuir riesgos de transporte de dinero.

El surgimiento de marcas especializadas en la emisión de tarjetas data de 1950 cuando *Dinners Club* fue constituida, esta empresa había colocado veinte mil tarjetas para 1952 y superaba el millón de tarjetahabientes para 1959. Muy pronto fue extendiéndose a un amplio espectro de compras, cubriendo consumos como diversiones, viajes y turismos; hasta que llegó a admitirse para pagar todo tipo de bienes y servicios, no sólo en el ámbito de EEUU sino también internacionalmente. El rendimiento que obtenía Dinners Club, producto de la comisión que cobraba por la actividad de emisor y la importancia que iba tomando dentro de la economía estadounidense, desató el surgimiento de la competencia, tal es el caso de American Express Company (1958), entidad que se especializaba como agencia de viajes y emisión de cheques de viajero, la cual encontró en la frecuencia de viajes de

sus clientes la fortaleza del crecimiento al extremo que para la década de los 80´s había desplazado a Dinners Club. Otro emisor fue Carte Blanche (1959) creada por la cadena hotelera Hilton, que no trascendió al mismo nivel que los demás.

1.1.1 Origen de los Emisores Bancarios (29:05).

A partir de 1951 los bancos norteamericanos se abrieron al creciente mercado de las tarjetas de crédito. La primera tarjeta emitida por una institución bancaria fue la del Flatbush National Bank de New York, en 1947, pero un paso importante en este tema lo dio el Franklin National Bank of New York (1951) quien fue el primero en emitir una tarjeta utilizable por clientes de otras instituciones financieras -26 bancos que ofrecían su tarjeta, con 750 mil titulares y 11 mil establecimientos afiliados-.

En 1959 el *Bank of America* de California emitía la tarjeta de mayor aceptación: *BankAmericancard* que para 1961 había colocado más de un millón de tarjetas con volúmenes de negocio de US$75MM. Esta marca fue cedida en 1966 a una sociedad especializada denominada *BankAmericard Service Corporation,* creada por el propio banco, la cual posteriormente fue renombrada *National BankAmericard Incorporated (NBI) y e*n 1969 tenía 3,000 bancos asociados. El desarrollo internacional de esta importante marca tuvo su origen en 1974, creándose la organización internacional IBANCO, que en 1977 adoptó el nombre de **Visa Internacional**. La NBI se convirtió en Visa USA e IBANCO en Visa Internacional, adoptando tal nombre porque era internacionalmente comprensible y aceptable.

Por otra parte en 1966 los principales bancos de California siguieron la misma fórmula iniciada por el Bank of América, entre ellos se encontraban: Wells Fargo Bank, United California Bank, Bank of California y el Crocker National Bank, formaron también una asociación sin ánimo de lucro para emitir una marca de tarjeta en común, la llamaron California Bank Card Association, responsable del diseño de la tarjeta MasterCharge. La MasterCharge, a partir de 1979, pasó a denominarse **MasterCard**.

La BankAmericard (VISA) y la MasterCard, así como otras tarjetas de ámbito más reducido, introdujeron el sistema de adhesión de emisores a una marca, con el compromiso de admisión de las tarjetas de esa marca en cualquiera de los bancos que disfrutan de la licencia, sistema que se generaliza finalmente como medio de expansión mundial de las grandes marcas de tarjetas. Fuera de los Estados Unidos, se fue otorgando licencias a los bancos para emitir tarjetas de crédito y para 1972 existían 15 países con la concesión de marca correspondiente.

1.2 Características de las tarjetas de crédito.

"La tarjeta de crédito es una tarjeta de plástico con el logotipo y nombre del banco emisor, un número de identificación, el nombre del titular, las fechas de expedición y vencimiento de la misma. También señala si puede utilizarse en el país o en el extranjero; en el reverso tiene una banda magnética y otra donde se encuentra la firma del propietario" (24:22)

Este medio de pago electrónico posee ciertas características que la distinguen como instrumento financiero, los cuales van desde la mera forma o detalles en su personalización, información grabada en la misma y estructura o forma de control de la cuenta por parte del emisor. Para el efecto, a continuación se detallan sus principales características.

1.2.1 Características Físicas: (29:3-8).

1.2.1.1. **Número de cuenta.** Representa la identificación de la tarjeta emitida, este número debe constar de 16 posiciones de los cuales los primeros seis identifican el BIN (Bank Identification Number), el cual representa la identidad del emisor, el país y categoría de tarjeta.

1.2.1.2. **Fecha de emisión y vencimiento de la tarjeta (cuenta):** La primera identifica la fecha en que la cuenta o tarjeta fue emitida, mientras que la fecha de vencimiento define la validez que tiene para ser utilizada, el estándar establecido es de tres años y se presenta con la combinación del mes y año de su vencimiento. Ejemplo: 09/07 que significaría válida hasta septiembre del año dos mil siete.

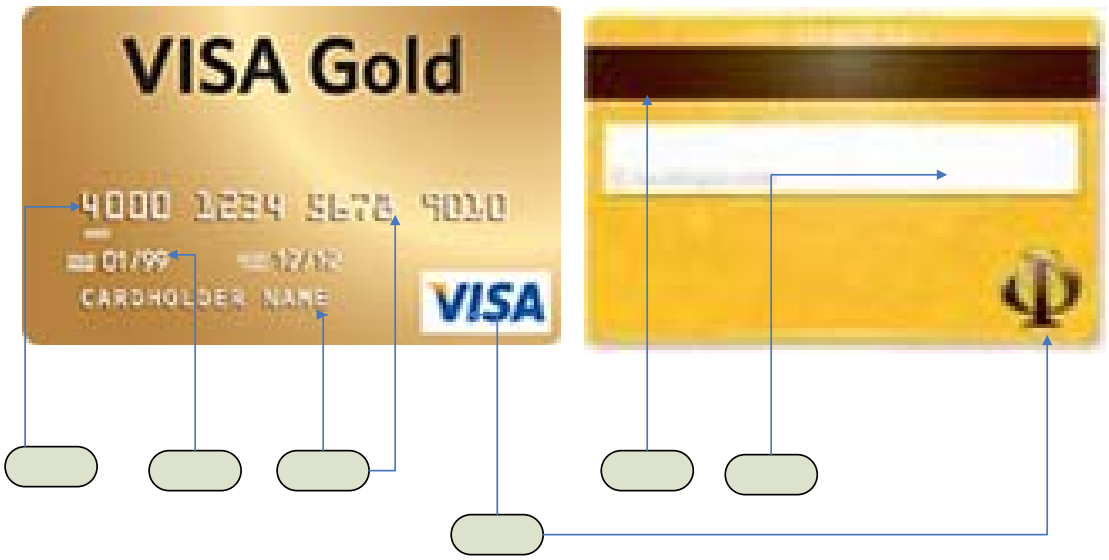
1.2.1.3. **Personalización:** Denominada "Grabada" y conocida también como "Troquelada", cuyos datos son definidos en relieve en el plástico. Para el efecto se utilizan equipos sofisticados denominados "Máquinas Realzadotas".

1.2.1.4. **Banda Magnética:** Es una banda fabricada de materiales especiales con la capacidad de almacenar información, tal como: El detalle de la cuenta, vencimiento y PIN. La misma facilita la transacción con la tarjeta de crédito en cajeros y puntos de venta. Está ubicada en el reverso de la tarjeta.

1.2.1.5. **Panel de Firma:** Es el espacio reservado para que el tarjetahabiente estampe su rúbrica, como una medida de prevención de utilización por terceros. Está ubicada en el reverso de la tarjeta.

1.2.1.6. **Otras características físicas:** Existen otras características no menos importantes, tales como: Los colores, hologramas y medidas de seguridad en la generación de cada tarjeta, los cuales son diseñados por las entidades fabricantes de los plásticos y no por los emisores.

FIGURA No. 1
CARACTERÍSTICAS FÍSICAS DE UNA TARJETA DE CRÉDITO



1.2.2 Características de administración y control de la tarjeta (cuenta).

A continuación se describen algunos elementos de la administración y el control de las tarjetas de crédito, sin los cuales las empresas emisoras tendrían grandes contratiempos**.**

1.2.2.1 **Límite de Crédito:** Es el importe por el que fue autorizado utilizar la línea de crédito.

1.2.2.2 **Comprobante de pago**. Denominado "voucher" es el pagaré que extienden los establecimientos comerciales o de servicio a los tarjetahabientes al realizar los pagos.

1.2.2.3 **Estado de Cuenta:** Es un informe oficial que extiende el emisor de forma periódica, el cual contiene el número de cuenta, fecha de corte, fecha de pago, monto utilizado y disponible de crédito; pago mínimo, cargos del período (si fuese utilizado el financiamiento), pago de contado, detalle de cada cargo efectuado y pagos realizados.

FIGURA No 2

MODELO DE ESTADO DE CUENTA MENSUAL,

EMITIDO POR UNA ENTIDAD BANCARIA

BANCO EJEMPLO, S.A
(SU LOGO)

Cuotas Vencidas	Saldo en mora	Cargo Mensual	Pago en Cuotas	Pago Mínimo
2	Q 500.00	Q 3,585.17	Q 1400.00	Q 1,460.00

Juan Ejemplo TH

Número de Cuenta	Fecha Corte	Saldo Anterior
4200XX1111111111	12/09/2005	Q 15, 857.87

Fecha	Descripción de operaciones	Fecha de Transacción	Débitos	Créditos
16/08	Retiro ATM Banamex, Durango México.	16/08	Q 1,112.04	
18/08	PAGO EFECTUADO EN AGENCIA XXX1	18/08		Q 3,275.00
30/08	Consumo POS El Corte Inglés Barcelona España	22/08	Q 2,473.13	
			Q 3,585.17	Q 3, 275.00
	Saldo Total		**Q 3,585.17**	**Q 3,275.00**
		Nuevo saldo deudor		Q 16,168.04
		Intereses y cargos		Q 200.00
		Total del adeudo		Q 16,368.04

BONIFICACIÓN EN PUNTOS	
Puntos Ganados	1000
Puntos Disponibles	5,536
	Fecha de Pago sin intereses
	14/09/2005

Fuente: Modelo de estado de cuenta presentado en el sitio WEB: www.tarjetascuscatlan.com

1.2.2.4 **Contrato:** Es un documento que contiene la información general del cliente y las cláusulas que regirán la relación con este. Es decir, contiene los derechos y obligaciones, tanto del emisor como del tarjetahabiente y representa la aceptación de las condiciones pactadas.

1.2.2.5 **Período de financiamiento:** El financiamiento que ofrece cada entidad, varía de conformidad con sus políticas crediticias. En Guatemala se ofrecen financiamiento de 24 meses, o de 36 meses.

1.2.2.6 **Intereses Financieros:** Monto que debe pagar el tarjetahabiente a la institución emisora por el uso del financiamiento, el cual se determina al aplicar una tasa de interés compuesto sobre el adeudo a la fecha de corte.

1.2.2.7 **Cargos por servicios:** Retribución o pago que debe efectuar a la institución bancaria el tarjetahabiente, por concepto de servicios o condiciones preestablecidas por el uso de la tarjeta de crédito.

1.2.3 Tipos de tarjetas.

Categorías de tarjetas de crédito: Cada Miembro emisor de tarjetas, puede solicitar a la entidad que respalda la emisión (Ejemplo VISA) la autorización para generar diversos tipos de tarjetas de las cuales las más comunes son: Local, Internacional, Dorada y Platinum; distinguiéndose una de la otra por ciertas características, tales como: Aceptación restringida o internacional, beneficios, características físicas, pero principalmente límites de crédito.

1.3 Funcionamiento de las tarjetas de crédito.

Para explicar el funcionamiento, es necesario comentar sobre los elementos o fases que intervienen en el proceso, siendo los siguientes:

1.3.1. Cliente ó tarjetahabiente.

El cliente o tarjetahabiente es quien con la autorización y calificación como sujeto de crédito por parte del Emisor, utiliza la tarjeta de crédito para pagar bienes o servicios. Dicha situación conlleva para el cliente el derecho de obtener satisfactores mediante el uso de la línea de crédito otorgada, con la correspondiente obligación de efectuar el pago de los fondos utilizados de manera inmediata (de acuerdo a las políticas de cada emisor para el pago de contado) o bien utilizando el financiamiento.

1.3.2. Comercio afiliado o punto de venta.

Es la entidad comercial dedicada a la venta de bienes o la prestación de servicios que acepta como medio de pago la tarjeta de crédito. Para operar es necesario afiliarse y aceptar las condiciones o reglas del Adquiriente.

1.3.3. Adquirente.

Entidad dedicada a proveer los elementos necesarios a los comercios que se afilien para poder operar y realizar los cobros mediante el uso de tarjetas. Para lograr tal objetivo, estas entidades ofrecen la capacitación a los comercios sobre la forma de operar y liquidar los cobros realizados, además de la infraestructura de comunicación, los instrumentos de cobro denominados POS (Point of sale), y también la logística de liquidación que puede ser mediante la extensión de cheques o el acreditamiento en cuenta del comercio (de mayor uso).

Estas entidades están autorizadas por las empresas que respaldan la emisión de tarjetas (VISA, Mastercard, Dinners), pues es con ellas que efectúan la liquidación de las operaciones diarias y estas últimas realizan los cargos a cada banco emisor, según les corresponda. En Guatemala existen dos empresas dedicadas a esta actividad: Credomatic y Visanet.

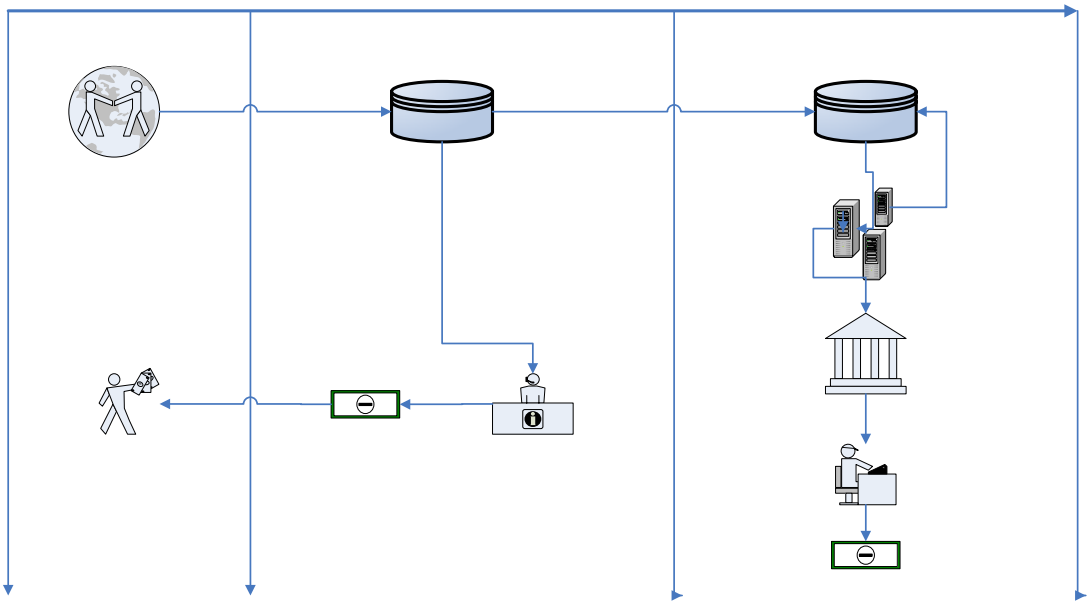
1.3.4. Procesador o Autorizador.

Es la entidad que posee los medios tecnológicos y la información de cada cuenta (disponibilidad, vencimiento, claves, bases de datos, etc.) para poder autorizar las transacciones que el tarjetahabiente desee efectuar. Para el efecto se establecen estándares de calidad de respuesta y disponibilidad de servicio para no perjudicar la reputación de la marca que respalda las tarjetas, estos estándares validan aspectos como: Tiempo de respuesta por transacción, cantidad de operaciones autorizadas o fallidas y cualquier inconveniente que represente riesgo en la eficiencia del pago electrónico.

Una vez conceptualizados cada uno de los elementos que intervienen en el proceso de funcionamiento de una tarjeta de crédito, es factible identificar el inicio del ciclo de una transacción con tarjeta de crédito, desde que el cliente adquiere un bien o contrata un servicio y presenta la tarjeta como medio

de pago en sustitución del dinero, el comercio afiliado procede al cobro de dicha operación utilizando las herramientas (POS y medios de comunicación) proporcionadas por el Adquirente realiza la solicitud de autorización que es otorgada por el procesador (sea el mismo emisor o la entidad contratada por éste), concluyendo el ciclo con la generación del comprobante de autorización que representa la facultad de otorgar los bienes o servicios por parte del comerciante y la obligación del tarjetahabiente. El siguiente esquema muestra gráficamente dicho procedimiento:

FIGURA No. 3
PROCESO DE AUTORIZACIÓN DE OPERACIONES CON TARJETA DE CRÉDITO



Fuente: Infografía realizada por Jorge González Vásquez 09092006.

En los párrafos previos han sido tratados los conceptos más generales de la historia, características y esquema de funcionalidad de la tarjeta de crédito, con el afán de entender el entorno que a su alrededor conlleva realizar la actividad de emisión de ese medio de pago.

En ese orden de ideas, el sistema financiero guatemalteco y especialmente las entidades bancarias, desarrollan la actividad de concesión de préstamos bajo la modalidad de tarjeta de crédito, como una forma de diversificar su portafolio de servicios financieros, considerando los márgenes de utilidad que les representa. Por ello y tomando en cuenta, la relación que existe entre las entidades bancarias

y la actividad de emisión de tarjetas de crédito en Guatemala, se hace necesario conocer acerca de la estructura del sistema financiero, para facilitar la comprensión del tema principal. A continuación se presenta un esbozo de lo comentado.

1.4. El Sistema Financiero Guatemalteco (22:02)

"El sistema financiero es el conjunto de instituciones y organizaciones públicas y privadas que tienen como función principal otorgar los recursos financieros de ciertas personas que disponen de excedente de dicho recurso, hacia aquellas personas individuales o jurídicas que necesitan del mismo" (20:25)

El Sistema financiero guatemalteco se encuentra organizado bajo la estructura de Banca Central, lo cual significa que corresponde a un órgano superior (La Junta Monetaria) la definición de las políticas en materia económica para todas las entidades que lo conforman. A continuación se definen las entidades que conforman el órgano central y el sistema financiero.

1.4.1 La Junta Monetaria.

Tiene a su cargo la determinación de la política monetaria, cambiaria y crediticia del país y vela por la liquidez y solvencia del Sistema Bancario Nacional, asegurando la estabilidad y el fortalecimiento del ahorro nacional.

1.4.2 Banco de Guatemala (BANGUAT).

Tiene como objetivo contribuir a la creación y el mantenimiento de las condiciones más favorables al desarrollo ordenado de la economía del país, para lo cual propicia las condiciones monetarias, cambiarias y crediticias que promuevan la estabilidad en el nivel general de precios.

1.4.3 Superintendencia de Bancos (SIB).

Es un órgano de banca central, eminentemente técnico, actualmente organizado conforme a la Ley de Supervisión Financiera (Decreto 18-2002);. Ejerce la vigilancia e inspección de los Bancos,

Instituciones de Crédito, Empresas Financieras, Entidades Afianzadoras, de Seguros y las demás que la ley disponga.

1.4.4. Sistema financiero regulado.

A esta clasificación del sistema financiero, pertenecen las instituciones supervisadas por la Superintendencia de Bancos, de conformidad con lo que establece el Decreto 18-2002 del Congreso de la República "Ley de Supervisión Financiera" y el artículo 133 de la Constitución de la República de Guatemala. Entre dichas entidades se encuentran las siguientes:

1.4.4.1 Bancos.

"Instituciones que pueden realizar intermediación financiera, consistente en la realización habitual, en forma pública o privada, de actividades que consistan en la captación de dinero, o cualquier instrumento representativo del mismo, del público, tales como la recepción de depósitos, colocación de bonos, títulos y otras obligaciones, destinándolo al financiamiento de cualquier naturaleza, sin importar la forma jurídica que adopten dichas captaciones y financiamientos" (10:04).

A la fecha de esta investigación el sistema bancario guatemalteco estaba conformado por: 24 entidades que en conjunto poseían activos por Q 88,672 Millones, Q 7,427 Millones de Capital y utilidades equivalentes a un rendimiento de capital de 15% en su conjunto (Q1,126 MM).

1.4.4.2 Emisores de tarjetas de crédito.

Son entidades financieras y en su mayoría instituciones bancarias (Pero existen emisores en el sistema no regulado, bajo la figura de emisores privados), dedicadas a ofrecer una fuente alterna de financiamiento a personas físicas o jurídicas, además de proveer servicios de pago a comerciantes y consumidores utilizando como medio un dispositivo plástico denominado Tarjeta de Crédito.

1.4.4.3 Otras entidades financieras reguladas.

Por su poca participación en el mercado financiero, a continuación se listan las entidades que conjuntamente con los bancos y las empresas emisoras de tarjetas conforman el sistema regulado:

- Sociedades financieras privadas.
- Almacenes generales de depósito.
- Compañías de seguros y fianzas.
- Casas de cambio.
- Instituto de Hipotecas Aseguradas.

1.4.5 Sistema financiero no regulado.

En contraposición a las entidades del sector regulado, este grupo no es supervisado por la Superintendencia de Bancos, pero no dejan de representar un importante papel dentro de la economía nacional. A esta clasificación corresponden entre otras, las siguientes entidades:

- Organizaciones no gubernamentales (ONG´s).
- Bolsa de valores.
- Casas de bolsa.

1.5 Emisores bancarios de tarjetas de crédito.

La tarjeta de crédito emitida por una entidad bancaria difiere de una que haya sido comercializada por una privada principalmente, en el origen de los fondos que utiliza, los que toma del público a través de la actividad de intermediación financiera, mientras que los emisores privados utilizan capitales particulares para la concesión de créditos.

También puede definirse a la tarjeta de crédito de un banco como: "Un instrumento financiero a través del cuál una institución bancaria, como emisor de la tarjeta, concede a sus clientes mediante la

suscripción de un contrato de adhesión, una línea de crédito revolvente hasta por un importe determinado. En el clausulado del contrato de adhesión, el banco establece las condiciones bajo las cuales otorga el crédito al usuario, así como también la forma en que éste deberá retribuir o pagar al banco sus adeudos, compras inmediatas, pagos diferidos, etc.".(29:52).

Aunque la emisión de tarjetas en Guatemala data desde 1975, en la actualidad ha tenido un crecimiento importante debido a la modernización del sistema bancario el cual ha visto en esta modalidad de crédito de consumo una oportunidad de crecimiento en la colocación de los recursos tomados del público, pues ofrece la segregación del riesgo crediticio en una gran cantidad de unidades.

1.5.1 Situación Actual de los Emisores Bancarios guatemaltecos.

Según información publicada por la Superintendencia de Bancos (a la fecha de esta investigación), doce entidades registraban activos por concepto de financiamientos otorgados bajo la modalidad de tarjeta de crédito. Esta situación refleja la importancia que posee la actividad de emisor de tarjetas en el sistema bancario, al representar el 50% del total de bancos.

1.5.1.1 Participación en el mercado de tarjetas de crédito.

Cada emisor bancario, adopta las medidas comerciales que mejor considere a sus planes de expansión y colocación, apoyándose en la publicidad principalmente y/o con equipos de ventas especializados en la colocación de estos productos.

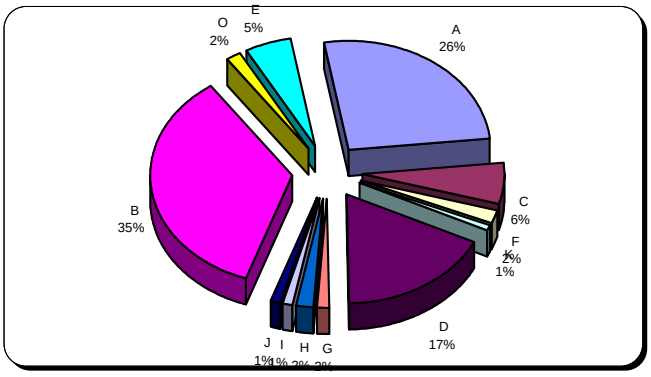
Un reciente estudio privado, realizado sobre el mercado de tarjetas de crédito, reveló que existen varias entidades bancarias y no bancarias, que se dedican a esta actividad, de donde sobresalen tres en particular con casi el setenta y cinco por ciento del mercado guatemalteco.

CUADRO No. 1

PARTICIPACIÓN DEL MERCADO DE TARJETAS DE CRÉDITO

EMISORES BANCARIOS DE GUATEMALA

CODIGO EMISOR 1/	TARJETAS EMITIDAS *
A	150,000
C	35,000
F	10,000
K	5,000
D	100,000
G	9,000
H	10,000
I	7,000
J	6,000
B	200,000
O	10,000
E	30,000
TOTAL	**572,000**



1/ Código asignado sin revelar identidad del Emisor, para proteger la fuente de información.

* = Datos Estimados, según investigación de mercado.

Fuente: Investigación de mercado efectuada por una entidad financiera.

Análisis: El mercado de tarjetas de crédito en Guatemala, ha ido creciendo como resultado del acceso al financiamiento que principalmente las entidades bancarias ofrecen en la actualidad, mismo que responde a la baja exposición a riesgo crediticio por dispersión en varias unidades deudoras, así como de la liquidez que en los últimos años goza el sistema financiero.

1.5.1.2 Información financiera de los emisores bancarios.

A continuación se hace el análisis únicamente de los montos colocados bajo la figura de tarjeta de crédito versus la totalidad de la cartera de los doce bancos emisores en Guatemala.

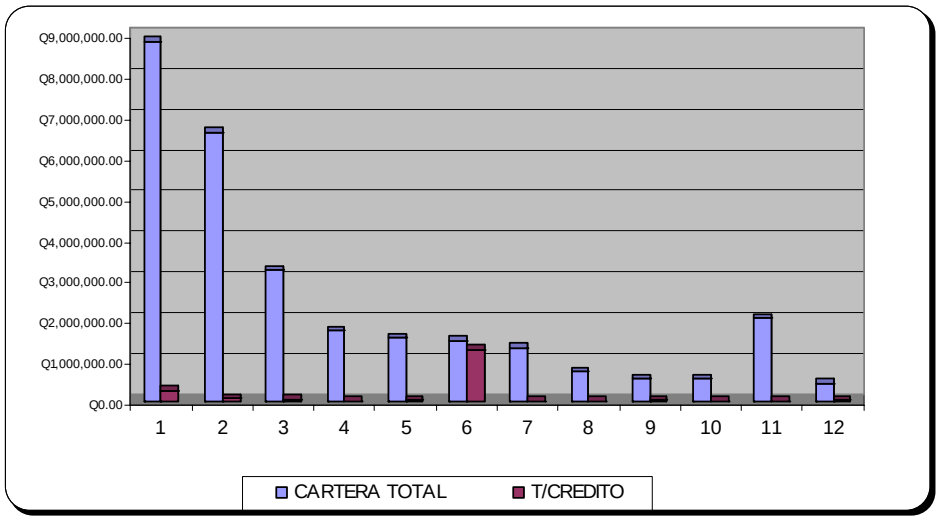
CUADRO No. 2
CARTERA DEL SISTEMA BANCARIO,
Y PARTICIPACIÓN DE LA TARJETA DE CRÉDITO.

Cifras en Miles de Quetzales
Al 30 de septiembre de 2006

		CARTERA POR ENTIDAD		
Ref	BANCOS EMISORES	CARTERA TOTAL	T/CREDITO	%
1	Banco Industrial, S.A.	Q8,864,806.00	Q266,978.00	3%
2	Banrural, S.A.	Q6,618,482.00	Q75,721.00	1%
3	Banco Agromercantil, S.A.	Q3,223,706.00	Q52,427.00	2%
4	Banco de los Trabajadores	Q1,742,069.00	Q14,971.00	1%
5	Banco Internacional, S.A.	Q1,567,311.00	Q38,820.00	2%
6	Banco Uno, S.A. 1/	Q1,512,584.00	Q1,287,249.00	85%
7	Banco de Exportación,S.A	Q1,317,226.00	Q19,095.00	1%
8	Crédito Hipotecario Nacional	Q738,397.00	Q7,356.00	1%
9	Banco de la República, S.A.	Q556,196.00	Q37,390.00	7%
10	Banco de Comercio, S.A.	Q556,146.00	Q12,993.00	2%
11	Cuscatlán de Guatemala	Q2,046,237.00	Q14,059.00	1%
12	Banco de Antigua, S.A.	Q458,925.00	Q27,610.00	6%
	Totales	Q29,202,085.00	Q1,854,669.00	6%

1/ Esta Entidad registra las operaciones de tarjeta, bajo la figura de factoraje.
Fuente: Informe "Cartera de Créditos por Garantía" página www.sib.gob.gt de la Superintendencia de Bancos de Guatemala.

GRAFICA ESTADÍSTICA DEL CUADRO No. 2



Fuente: Informe "Cartera de Crédito por garantía" sitio WEB: www.sib.gob.gt

Análisis: De acuerdo a las publicaciones de la SIB, el rubro de tarjeta de crédito a la fecha de la investigación presentaba el 6 % del total de la cartera de los bancos.

1.6 Principales operaciones en el área de tarjeta de crédito de un emisor bancario.

Los bancos que desarrollan la actividad de comercialización de tarjetas de crédito, llevan a cabo actividades particulares, las cuales son:

1.6.1 Comercialización.

Consistente en la labor comercial de identificar clientes que se adapten a las políticas crediticias de la entidad, ésta representa el inicio del proceso en la colocación del producto. Para realizar la labor de venta o comercialización, el banco posee o contrata personal especializado, que utilizando la información disponible en diversas fuentes, como por ejemplo: la base de clientes de la propia entidad, de empresas comerciales afines al banco o de personas recomendadas; identifican y contactan a potenciales clientes que pueden obtener una tarjeta de crédito.

Los factores críticos del proceso de comercialización, los integran la calidad de las bases de datos seleccionadas, porque pueden encontrarse incompletas, desactualizadas o la integridad de la información puede ser dudosa.

1.6.2 Análisis y autorización de las tarjetas de crédito.

En esta fase se analiza cada uno de los casos o solicitudes crediticias presentadas por la parte comercial; en ella se preparan expedientes con la información que deben completar los candidatos a obtener una tarjeta de crédito, regidos por los aspectos estipulados en la normativa externa (reglamento de riesgo crediticio emitido por la Superintendencia de Bancos) e interna (políticas crediticias de la institución bancaria) sobre las cuales se basan los juicios de aprobación o negación de las solicitudes.

En lo referente al proceso, se realizan análisis de carácter cuantitativo y cualitativo, refiriéndose el primero a los aspectos monetarios tangibles, mientras que los segundos conllevan otras condiciones no monetarias. Los procedimientos generales en esta fase, son:

- Revisión del récord crediticio del solicitante. Mediante consultas en sistemas internos o externos se obtienen las referencias de compromisos y récord de pagos del solicitante en el mismo banco o cualquier entidad financiera.

- Evaluación de la capacidad de pago. Considerando que la tarjeta de crédito es una modalidad de crédito de consumo, el analista basa su juicio de recuperación en la capacidad de pago que posea el solicitante.
- Confirmación de la información presentada. No obstante, el potencial cliente está obligado a presentar información fehaciente dentro de la solicitud, la entidad bancaria valida que contenga datos verídicos para salvaguardar sus intereses y para evitar sanciones legales.
- Evaluación crediticia. Consiste en reunir y analizar todas las variables que se conozcan y a través de un software especializado o utilizando herramientas electrónicas de cálculo, se conjugan para determinar el resultado final de evaluación, sea ésta autorización, negación o reconsideración de la tarjeta de crédito.
- Comité o responsable de autorización de créditos. Una vez emitida la opinión del analista crediticio, el expediente se traslada a un funcionario responsable o al Comité de autorizaciones para que emitan el visto bueno final o requieran un nuevo análisis de considerarse necesario.

1.6.3 Emisión y entrega de la tarjeta.

La emisión de la tarjeta inicia con la personalización, dicho proceso se realiza en equipos de alta tecnología, propiedad del banco o a través de los servicios de empresas particulares, especializadas en realizar esa labor (outsourcing). Posteriormente es preparada para su posterior entrega al cliente, para lo cual se adjunta las indicaciones de uso y procedimiento de activación, publicidad, etc., dentro de un sobre especial para su entrega final. La entrega se realiza de diversas maneras de conformidad con los procedimientos de cada banco, siendo las siguientes: Por correo particular, correo externo, en la red de agencias.

1.6.4 Autorización electrónica de transacciones con tarjetas de crédito.

Para lograr la conclusión de la transacción, existen programas tecnológicos especializados en el manejo de este tipo de información, dentro del cual se parametrizan las condiciones de funcionalidad de cada tarjeta. Dichos parámetros deben estar apegados a la normativa de la entidad que respalda la emisión y las políticas del banco. En estos sistemas se almacenan las bases de datos necesarias, para

que las operaciones sean aprobadas o denegadas, siguiendo los protocolos de comunicación utilizados para este tipo de transacciones electrónicas.

La complejidad de este proceso consiste en poseer sistemas capaces de atender las demandas de respuesta requeridas según los estándares internacionales, así como de las medidas de seguridad para evitar ser utilizadas de manera fraudulenta. Es importante citar que este proceso representa el núcleo del funcionamiento de la tarjeta de crédito, por cuanto de él depende la creciente aceptación como medio de pago de dicho instrumento.

1.6.5 Gestiones.

Una vez en circulación la tarjeta de crédito, pueden surgir varias circunstancias que generen gestiones, entendiéndose éstas a las solicitudes, reclamos o requerimientos por parte de los clientes ante el banco. Tales gestiones pueden ser resultado de diversas situaciones, por ejemplo: Inconformidad con el servicio a consecuencia de la no recepción de estados de cuenta, datos del cliente incorrectos; cambios en las condiciones del crédito (aumento o disminución); cancelaciones y cualquier tipo de solicitud.

Para realizar esta labor, las entidades poseen personal operativo que a través de sistemas informáticos de administración de tarjetas de crédito, operan cada una de las solicitudes, con sus usuarios asignados, en opciones específicas y con los niveles de autorización correspondientes para evitar duplicidad, errores y posibles fraudes.

Corresponde a esta actividad la atención de reclamos de clientes por rechazo a cargos inexistentes, lo que genera el seguimiento o disputa de transacciones con adquirientes nacionales e internacionales sean por situaciones imputables a los clientes, comercios o provocados por fraude con tarjetas, actividad que suele denominarse “Intercambio”. Cada gestión atendida es adjuntada al expediente de la tarjeta que la genera, para efectos de llevar control individualizado por cuenta y con ello poseer información del historial del cliente, además de prever reclamos posteriores sobre gestiones solucionadas previamente.

1.6.6 Cobranza.

Existe la posibilidad de incumplimiento de pago de las cuotas pactadas entre el banco y el tarjetahabiente, al ocurrir tal evento, la entidad emisora posee un procedimiento de cobranza, el cual consiste en la localización del cliente de manera personal o telefónica para requerirle el cumplimiento de su obligación de pago. Esta actividad es muy delicada y es realizada por personal capacitado tanto en relaciones interpersonales como en mecanismos de persuasión; por cuanto puede ser un factor de desvinculación de clientes, si los mecanismos no son apropiados.

1.6.7 Registro Contable.

Las transacciones que ocurran a causa del uso y administración de la tarjeta de crédito deben registrarse contablemente, siendo las principales:

- Registro de operaciones aprobadas: Registra los consumos o retiros realizados durante determinado periodo de tiempo (usualmente diario), aplicando directamente al saldo de la cartera el monto de dichas operaciones, y registrando una cuenta por pagar correspondiente a la obligación ante los adquirentes. En el mismo registro también se aplican las comisiones relacionadas directamente con la transacción, tales como los cargos por consumo de combustible, comisiones por uso de cajeros y cualquier otra relacionada con la transacción.
- Pago a los adquirentes. El pago de la obligación por parte del banco a los adquirentes se efectúa cargando la cuenta por pagar registrada durante la ocurrencia de las transacciones y las comisiones gasto a favor de los adquirentes, en contraparte se registra el pago con la forma que corresponda (emisión de cheque de caja o crédito a cuenta constituida en el mismo banco u otro diferente), y las comisiones devengadas por el uso de la tarjetas en los comercios afiliados.
- Cálculo de intereses y comisiones. Corresponde al registro de los intereses por financiamiento de los saldos en las tarjetas a la fecha de corte o el cobro de comisiones pactadas con los clientes. El registro contable se efectúa incrementando el saldo de la cartera, con abono a las cuentas de resultado por concepto intereses y comisiones.

- Registro de Gestiones. Entre las más frecuentes se encuentran el reembolso de intereses y comisiones, para lo cual la partida contable se realiza en forma inversa al registro original.
- Control de plásticos. El registro contable de los plásticos conllevan el momento de su adquisición, mismo que consiste en registrar un activo con abono a la cuenta por pagar. Posteriormente, conforme se van utilizado, se registran con cargo a una cuenta de gasto y abonando el activo original. Además por el riesgo que representa su uso, se lleva un control en cuentas de registro del cual se abonan las salidas por los plásticos utilizados en el día, semana o mes, según las políticas del banco.

1.7 Marco legal aplicable a las entidades bancarias emisoras de tarjetas de crédito.

En los extractos que a continuación se citan de cada una de las leyes, se hace referencia únicamente a los temas relacionados con la actividad de emisión de tarjetas, así como de los riesgos que deben administrar los bancos en el giro de dicha actividad financiera.

1.7.1 Ley de Bancos y Grupos Financieros -Decreto 19-2002- (10:02)

Sobresalen de esta Ley entre otros temas, los siguientes:

- Régimen legal (Arto. 05) En este se establecen las normas que rigen el quehacer de las entidades bancarias y hace referencia a la aplicabilidad de la normativa no financiera que le corresponda en los casos no contemplados en la misma.
- Régimen de empresas especializadas en servicios financieros y empresas de apoyo al giro bancario (Capítulo III artículos 36, 37 y 39). Se hace referencia al tema de emisión y administración de tarjetas de crédito, el financiamiento por parte del banco a las actividades de emisión.
- Operaciones y Servicios (Arto. 41) "*Los bancos autorizados podrán efectuar las operaciones en moneda nacional o extranjera y prestar los siguientes servicios… b.1) Otorgar créditos… b.5) Emitir y operar tarjeta de crédito*."
- Tasas de interés, comisiones y recargos (Arto. 42)

- Administración de Riesgos (Título IV, artículos del 50 al 58).

  Riesgos (Arto.55) "*Los bancos y las empresas que integran grupos financieros deberán contar con procesos integrales que incluyan, según el caso, la administración de riesgos de crédito, de mercado, de tasa de interés, de liquidez, cambiario, de transferencia, operacional y otros a que estén expuestos, que contengan sistemas de información y un comité de gestión de riesgos*…"

  Sistema de información de riesgos (Arto.58) "*La Superintendencia de Bancos implementará un sistema de información de riesgos, para lo cual los entes a que se refiere la presente Ley están obligados a proporcionar la información que para el efecto determine dicha Superintendencia".*

- Adecuación de Capital (Arto 64). "*Los Bancos deberán mantener permanentemente un monto mínimo de patrimonio en relación con la exposición a los riesgos de crédito, de mercado y otros riesgos, de acuerdo con las regulaciones de carácter general que para el efecto emita la Junta Monetaria…*"

1.7.2 Ley de Supervisión Financiera –Decreto 18-2002- (13:03)

Esta Ley contempla los fines y estructura organizacional de la Superintendencia de Bancos, además la autoridad sobre las entidades sujetas a supervisión (Banco de Guatemala, bancos, sociedades financieras, instituciones de crédito, afianzadoras, aseguradoras, almacenes de depósito, casas de cambio, grupos financieros y empresas controladoras de grupos financieros).

Por otra parte establece cada una de las funciones que tiene la Superintendencia, entre las que sobresalen: La evaluación de políticas y procedimientos que aseguren que las entidades financieras cuenten con procesos integrales de administración de riesgo y efectuar recomendaciones de naturaleza prudencial para administrar riesgos (Artículo 03. Funciones).

1.7.3 Código de Comercio (11:110)

Con respecto al tema de tarjetas de crédito, el Código de Comercio hace referencia en sus artículos 757 y 757 Bis respectivamente, los aspectos siguientes: Los requisitos mínimos que deben solicitarse a

los clientes para la autorización de una tarjeta de crédito y la tasa de financiamiento aplicable por las entidades emisoras de tarjetas.

1.7.4 Ley Contra el Lavado de Dinero u Otros Activos. (16:02)

La tarjeta de crédito puede ser utilizada como instrumento para el blanqueo de activos, mediante el consumo de fuertes montos y su pronto pago a la entidad, acto que materializaría el blanqueo si los fondos fueran de dudosa procedencia. Por tal situación esta ley contempla los siguientes aspectos relacionados con el tema:

- Las personas obligadas (Arto.18). "*Se consideran personas obligadas las siguientes: 1) Las entidades sujetas a la vigilancia de la Superintendencia de Bancos… 3) Las entidades emisoras y operadoras de tarjeta de crédito*".
- Registros (Arto. 21). Este artículo hace referencia a que las entidades obligadas deben llevar un registro de sus clientes y sus operaciones. En el caso de los emisores de tarjetas, la Superintendencia requiere el formulario TC-01 en el que se registra la información de los tarjetahabientes.
- Actualización y conservación de registros (Arto.23).
- Procedimiento y Sanciones (Arto. 31). El Estado fija para las personas obligadas por el incumplimiento de esta Ley, sanciones que oscilan entre los USD$10mil hasta USD$25mil.
- Para el desarrollo de los preceptos contenidos en la Ley, fue emitido bajo el Acuerdo Gubernativo número 118-2002 el "Reglamento de la ley contra el lavado de dinero u otros activos"-

1.7.5 Ley para Prevenir y Reprimir el Financiamiento del Terrorismo –Decreto 58.2005-. (15:02) y su reglamento –Acuerdo Gubernativo 86-2006-.

Esta Ley se relaciona estrechamente con la de prevención de lavado de dinero, pero se diferencia de ésta última, en que su fin es: prevenir utilizar los fondos constituidos en las entidades financieras para la adquisición de bienes o servicios en favor de grupos terroristas; mientras que la de lavado, establece

el marco para evitar que las fuentes de dinero ilícitas ingresen a las instituciones con el objetivo de legitimizarlas.

1.7.6 Reglamento para la administración del riesgo de crédito (25:03)

La Junta Monetaria por su parte, emitió el reglamento para la administración de riesgo de crédito, el en cual se definen las directrices para las instituciones bancarias sobre el apropiado manejo de los activos crediticios. En éste se hace referencia al tema de la tarjeta de crédito en los artículos siguientes:

- Créditos de consumo (Arto 03). "*…También se considera dentro de esta categoría las operaciones realizadas a través del sistema de tarjetas de crédito de personas individuales*".
- Aprobación y formalización de créditos (Artos. 09 y 10). En estos artículos se menciona que la autorización de cualquier tipo de crédito debe tener la aprobación jerárquica apropiada y que la formalización debe hacerse mediante un contrato que responda a las condiciones y estructura de la operación.
- Información a requerir de los solicitantes y deudores (Artos. 13 y 14). Estos artículos detallan cada uno de los requisitos a considerar para la evaluación, autorización y formalización de un crédito.
- Información financiera de solicitantes y deudores de créditos de consumo (Arto. 20).
- Valuación de Activos Crediticios (Título IV, Capítulo I). La SIB requiere un informe trimestral (cierre de los meses de marzo, junio, septiembre y diciembre) sobre la valuación de sus activos crediticios, agrupados bajo criterios preestablecidos y clasificados por categoría de exposición a riesgo crediticio, siguientes: a) riesgo normal; b) riesgo superior al normal; c) pérdidas esperadas; d) pérdidas significativas esperadas y e) alto riesgo de irrecuperabilidad. El espíritu de esta valuación es la creación de reservas por contingencias provenientes del incumplimiento de las obligaciones del deudor.

CAPITULO II

LOS RIESGOS EN LAS INSTITUCIONES BANCARIAS

Las operaciones propias de las instituciones bancarias conllevan implícitamente la toma de riesgos, situación que no les es ajena pues en la adecuada administración del mismo se encuentra su éxito o fracaso. Los riesgos son parte de la actividad bancaria, puesto que en su giro normal de administrar fondos de terceras personas para trasladárselas a otras (intermediación financiera) conlleva implícitamente riesgo. Fuera de la intermediación, los bancos realizan otras actividades como el cobro por cuenta de terceros, la prestación de servicios electrónicos, etc., que igualmente representan una probabilidad de sufrir pérdidas de no administrarse los factores involucrados de manera apropiada.

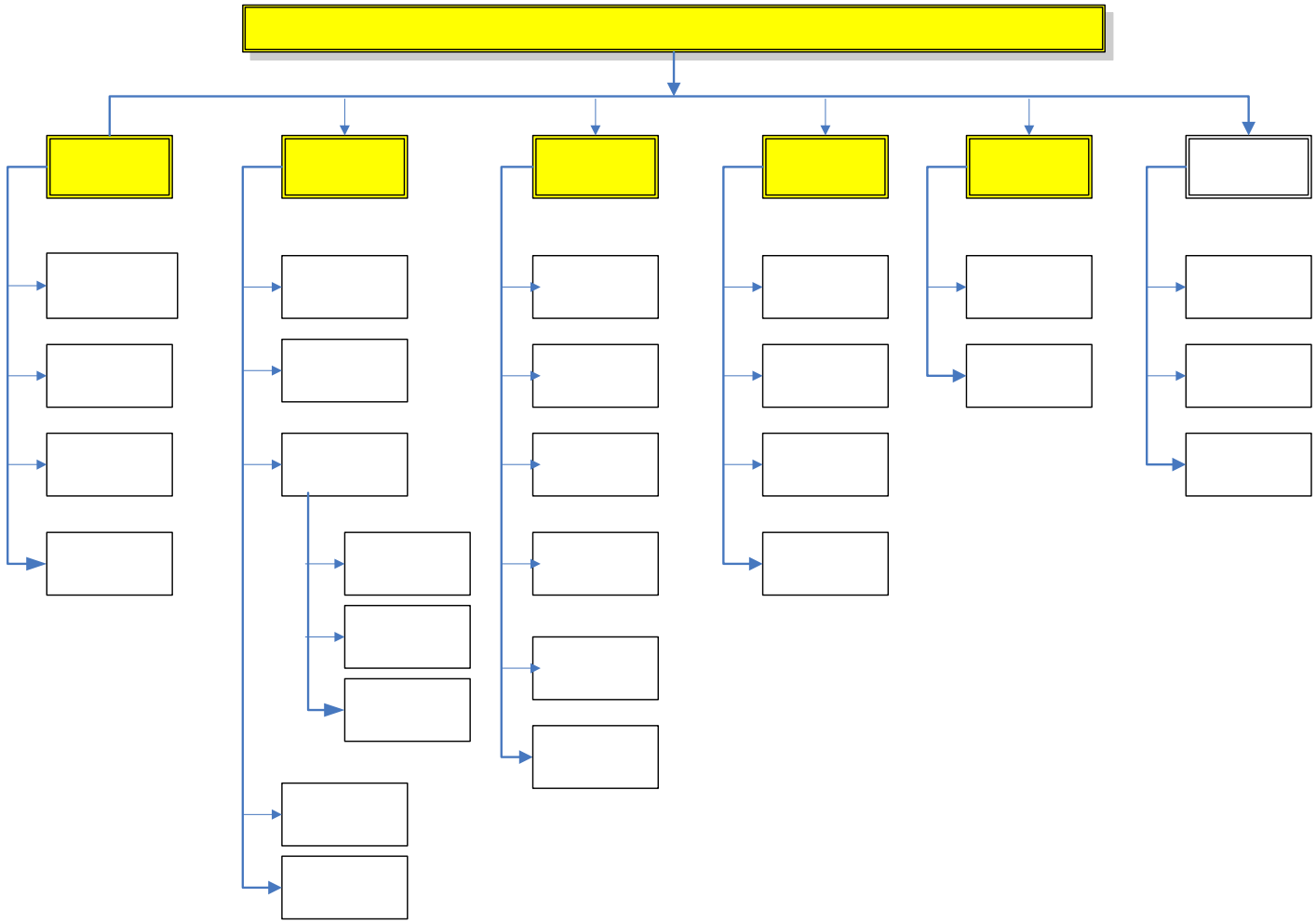
"La palabra riesgo proviene del latín *Risicare*, ´ que significa atreverse o transitar por un sendero peligroso" En realidad tiene un significado negativo, relacionado con peligro, daño siniestro o pérdida. Sin embargo el riesgo es parte inevitable de los procesos de toma de decisiones en general y de los procesos de inversión en particular. El beneficio que se pueda obtener por cualquier decisión o acción que se adopte, debe asociarse necesariamente con el riesgo inherente a dicha decisión o acción" (27:13)

2.1 Clasificación de riesgos bancarios.

Categorizar los riesgos a los cuales se encuentran expuestos los bancos, es una tarea que requiere de la experiencia y comprensión de las diversas actividades que desarrollan estas entidades, por tal motivo existen diversas publicaciones que tratan dicha clasificación, enfocados en función del conocimiento de cada autor, citando los aspectos que a su criterio son los de mayor impacto.

FIGURA No. 4

RIESGOS DE UNA INSTITUCIÓN BANCARIA



2.1.1 Riesgo Financiero.

2.1.1.1 Riesgo de Mercado: Posibilidad de que el valor presente de un portafolios se mueva adversamente ante los cambios en la variables macroeconómicas que determinan el precio de los instrumentos que componen una cartera de valores" (27:16).

2.1.1.2 Riesgo de tasa de interés: "Es la exposición a sufrir pérdidas por parte de los intermediarios, como consecuencia de los cambios experimentados en las tasas de interés, producto del descalce o desequilibrios que se genera entre los plazos de recuperación o retorno de los activos y de los vencimientos de los depósitos u obligaciones" (23:9).

2.1.1.3 Riesgo Cambiario: "Es el riesgo que enfrentan las ganancias de capital que se origina por movimientos en las tasas de cambio que afectan el valor de los activos y pasivos del banco" (23:9)

2.1.2 Riesgo de Imagen.

Es el riesgo que resisten las ganancias o el capital debido a una opinión pública negativa. El riesgo de reputación es particularmente dañino para los bancos considerando que la naturaleza de su negocio requiere mantener la confianza de sus depositantes, acreedores y el mercado en general.

2.1.3 Riesgo de Competencia.

"Incluye lo que se llama inteligencia de mercado, esto es el conocimiento de la competencia en forma sistemática, cómo la competencia afecta y qué riesgos provoca a la entidad".(23:9)

2.1.4 Riesgo de Liquidez.

"Se refiere a las pérdidas que puede sufrir una institución al requerir mayor cantidad de recursos para financiar sus activos a un costo posiblemente inaceptable. También a la imposibilidad de transformar

en efectivo un activo o portafolio. Este riesgo se presenta en situaciones de crisis, cuando en los mercados hay únicamente vendedores" (27:16)

2.1.5 Riesgo de País o Transferencia.

"En adición al riesgo inherente de crédito de la contraparte, los préstamos internacionales también incluyen el riesgo país, que se refiere al riesgo asociado con el ambiente económico, social y político donde el prestatario tiene su domicilio" (23:8)

2.1.6 Riesgo de Información.

"Es el riesgo resultante de las fallas en el cumplimiento con requerimientos transaccionales, de documentación o analíticos para obtener el tratamiento contable deseable, el cual contempla los siguientes riesgos: Riesgo de tecnología, de privacidad, de disponibilidad, de integridad y sistemas de información". (23:10)

2.1.7 Riesgo Crediticio.

"Se define como la pérdida potencial producto del incumplimiento de la contraparte en una operación que incluye el compromiso de pago". (27:16) "Posibilidad de sufrir una pérdida por el incumplimiento de las obligaciones contractuales de pago, tal incumplimiento suele estar motivado por un retroceso en la solvencia de los agentes prestatarios, relacionado con problemas de liquidez, pérdidas continuadas e incluso quiebra en el caso de las empresas" (33:27)

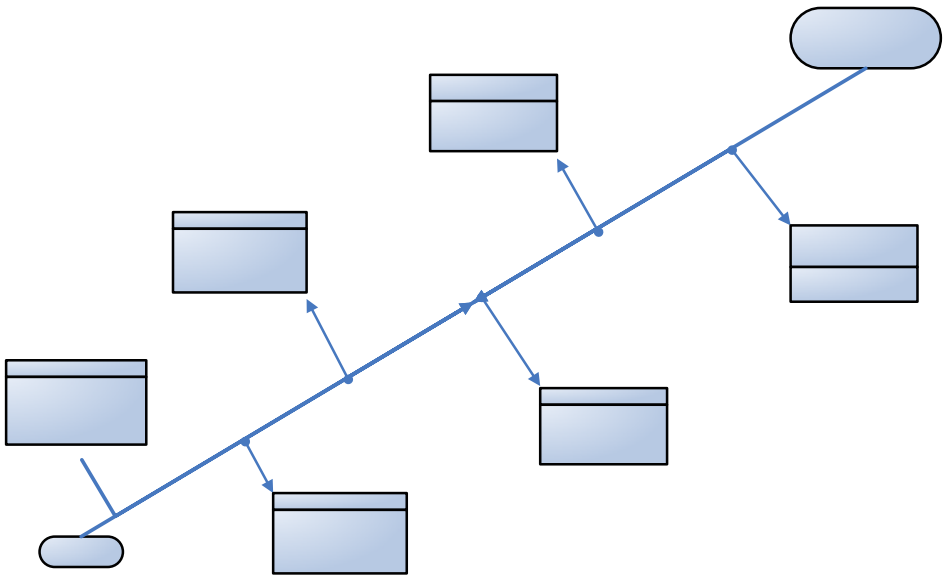
2.2 El Riesgo Operativo.

En el mes de septiembre de 2001, el grupo de trabajo del Comité de Basilea ubicado en el Banco Internacional de pagos (BIS) de la ciudad de Basilea Suiza, revisó la definición de riesgo operativo que se había propuesto desde 1999 para quedar como sigue: **"El riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos"** (7:128). Es importante aclarar que el grupo del Comité de Basilea, incluyó el riesgo legal en el riesgo operativo, puesto que la inapropiada observancia de un proceso

podría desembocar en una querella por parte de un tercero con quien habría el banco incumplido parcial o totalmente la prestación de un servicio, por ejemplo. Por otro lado excluyó los riesgos estratégico y de reputación.

En la siguiente figura se puede observar el desarrollo de la conceptualización del riesgo operativo por parte del Comité de Basilea.

FIGURA No 5
ENTORNO REGULATORIO DEL RIESGO OPERACIONAL



FUENTE:
"El Riesgo Operativo"
VII Congreso Latinoamericano de AI y Administración de Riesgos
Comité Latinoamericano de Auditoría Interna

2.2.1 Tipología del Riesgo Operacional según el Comité de Basilea.

La clasificación o tipología del riesgo operacional, se refiere a la separación de aquellos factores que integran o pueden llegar a considerarse como potenciales pérdidas para las instituciones a causa del citado riesgo.

2.2.1.1 Fraude Interno. Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas

empresariales (excluidos los eventos de diversidad y discriminación) en las que se encuentra implicada, al menos, una parte interna de la empresa.

2.2.1.2 Fraude Externo. Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o a soslayar la legislación por parte de un tercero.

2.2.1.3 Relaciones laborales y seguridad en el puesto de trabajo. Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o de eventos de diversidad / discriminación.

2.2.1.4 Clientes, productos y prácticas empresariales. Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos o de la naturaleza o diseño de un producto.

2.2.1.5 Daños a activos materiales. Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

2.2.1.6 Incidencias en el negocio o fallos en los sistemas. Pérdidas derivadas de incidencias en el negocio provenientes de fallos en los sistemas de información.

2.2.1.7 Ejecución, entrega y gestión de procesos. Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

CUADRO No. 3

CLASIFICACIÓN PORMENORIZADA DE TIPOS DE EVENTOS DE PÉRDIDA POR RIESGO OPERATIVO (7: Anexo 7)

CATEGORÍAS DE EVENTO (Nivel 1)	CATEGORÍAS DE EVENTO (Nivel 2)	EJEMPLOS DE ACTIVIDADES (Nivel 3)
Fraude Interno	• Actividades no autorizadas • Hurto y Fraude	• Txs no reveladas • Txs no autorizadas • Fraude • Hurto • Extorsión • Falsificación • Robo
Fraude Externo	• Hurto y Fraude • Seguridad de los Sistemas	• Hurto • Robo • Falsificación de documentos • Daños por ataques informáticos • Robo de información
Relaciones laborales y de seguridad en el trabajo	• Relaciones Laborales • Higiene y seguridad en el trabajo • Diversidad y discriminación	• Remuneración • Prestaciones sociales • Indemnización de trabajadores • Seguridad del área de trabajo • Todo tipo de discriminación
Clientes, productos y prácticas empresariales	• Divulgación de información • Productos defectuosos • Actividades de asesoramiento	• Abusos de confianza • Incumplimiento de contratos • Productos mal diseñados • Abuso de información confidencial
Daños a activos materiales	• Desastres y otros acontecimientos	• Pérdidas por desastres • Terrorismo • Delincuencia
Fallas en los sistemas	• Sistemas	• Hardware / Software • Telecomunicaciones • Fallas en los suministros
Ejecución, entrega y gestión de procesos	• Ejecución y mantenimiento de operaciones • Seguimiento y presentación de informes • Aceptación de clientes y documentación • Gestión de cuentas de clientes. • Distribución y proveedores	• Errores de introducción de datos • Errores contables • Fallos en las entregas • Incumplimiento de informar • Inexistencia de autorizaciones • Documentos jurídicos incompletos • Accesos no autorizados • Subcontratación

Fuente: Anexo 7 del documento Convergencia internacional de medidas y normas de capital, Comité de Basilea, junio 2004.

2.3 Requerimientos de capital para riesgo operativo, según Basilea II (7:128)

La importancia que reviste el estudio, administración y control de riesgo operativo en las instituciones bancarias, la constituyen en primera instancia la necesidad intrínseca de los órganos superiores o directivos de manejar apropiadamente los riesgos existentes en este tipo de empresas, y por otro lado a raíz de las propuestas realizadas por Basilea II, las entidades financieras deben considerar al riesgo operativo como parte de un nuevo marco regulatorio de requerimiento de capital, para lo cual deberán considerar la adopción de uno de los tres métodos siguientes: a) El Método del indicador básico, b) El método estándar y c) Método de medición avanzada.

Tales métodos para calcular el requerimiento de capital, están definidos en orden creciente de sofisticación y sensibilidad al riesgo, por lo que la propuesta del Comité es que las entidades vayan progresando a lo largo de la gama de métodos disponibles a medida que desarrollen sistemas y prácticas de medición más apropiados.

2.3.1 Método del indicador básico (7:128).

Representa el método más general y está enfocado para su utilización en entidades que se encuentran en el inicio de la administración del riesgo operativo o donde no puedan establecerse con claridad las líneas de negocio necesarias para la aplicación de los siguientes métodos. Bajo éste, se deberá cubrir el riesgo operativo con un capital equivalente al promedio de los tres últimos años de un porcentaje fijo de sus ingresos brutos anuales positivos. Al calcular ese promedio, se deben excluir los datos de cualquier año en el que el ingreso bruto anual haya sido negativo o igual a cero. Expresado en fórmula, se describe así:

$$\mathbf{KBIA = [\Sigma(GI_{1...n}*\alpha)] / n}$$

Donde:

KBIA = La exigencia de capital en el método del Indicador Básico.

GI = Ingresos brutos anuales medios, cuando sean positivos, de los últimos tres años.

n = Número de años (entres los tres últimos) en lo que los ingresos brutos fueros positivos.

α (Alfa) = 15%, parámetro establecido por el Comité, que relaciona el capital exigido al conjunto del sector con el nivel del indicador en ese sector.

Se definen como ingresos brutos, los ingresos netos en concepto de intereses más otros ingresos netos ajenos a intereses. Para el efecto se deben excluir los siguientes rubros: a) Provisiones por incumplimientos de pagos de intereses, b) beneficios o pérdidas realizados por la venta de valores de la cartera de inversión, y c) partidas extraordinarias.

CUADRO No. 4

EJEMPLO DE CÁLCULO DEL REQUERIMIENTO DE CAPITAL PARA RIESGO OPERATIVO SEGÚN EL MÉTODO DE INDICADOR BÁSICO

BANCO EJEMPLO,S.A.
CALCULO DE REQUERIMIENTO DE CAPITAL PARA R.O. SEGÚN BASILEA II
METODO: INDICADOR BÁSICO
Cifras en Miles de Quetzales

Ingresos Brutos	2003	2004	2005
Productos Financieros	Q645.503	Q703.852	Q605.222
Comisiones MN y ME	Q19.702	Q22.101	Q25.502
Otros Ingresos por Servicios	Q28.705	Q15.804	Q21.536
Resultado Neto operaciones internac.	Q26.015	Q45.000	Q50.003
Resultados Extraordinarios	Q500	Q1.500	Q0
TOTALES	**Q720.425**	**Q788.257**	**Q702.263**

Fuente: Informes de Gestión del Banco Ejemplo, S.A.

FÓRMULA:

$$K_{BIA} = [\ \sum(GI_{1...n} * \alpha)]/n$$

Donde:

KBIA La Exigencia de capital Método del Indicador Básico.
GI Ingresos brutos anuales medios. (720425, 788257, 702263)
n Número de años en los que los ingresos brutos fueron positivos. (3 años)
α 15 %, parámetro establecido por el Comité de Basilea. (0.15)

Desarrollo del cálculo.

KBIA = [∑(720425 + 788257 + 702263) * 0.15)]/3
KBIA = [2,210,945 * 0.15)]/3
KBIA = [2,210,945 * 0.15)]/3
KBIA = [331641.75 / 3]
KBIA = 110,547.25

CAPITAL REQUERIDO (Miles de Q)	AÑOS (n)
110,547	**3**

2.3.2 Método estándar (7:130)

Bajo este método, las actividades de los bancos se dividen en ocho líneas de negocio: Finanzas corporativas, negociación y venta, banca minorista, banca comercial, pagos y liquidación, servicios de agencia, administración de activos e intermediación minorista. El ingreso bruto de cada línea de

negocio es un indicador amplio que permite aproximar el volumen de operaciones del banco y, con ello, el nivel de riesgo operativo que es probable que asuma el banco en estas líneas de negocio. El requerimiento de capital de cada línea de negocio se calcula multiplicando el ingreso bruto por un factor denominado beta que se asigna a cada una de tales líneas. El factor beta es una aproximación que definió el Comité, basado en el historial de pérdidas debido al riesgo operativo en el sector bancario en su conjunto.

La exigencia de capital se calcula como la media de tres años de la suma simple de las exigencias de capital regulador en cada una de las líneas de negocio. Expresado en fórmula, se describe así:

$$\mathbf{KTSA = \{ \Sigma \text{ años } 1\text{-}3 \max [\Sigma (GI1\text{-}8 * \beta 1\text{-}8), 0] \} / 3}$$

Donde:

KTSA = La exigencia de capital en el Método Estándar.

GI1-8 = Los ingresos brutos anuales de un año dado, como se define en el método del indicador básico, para cada una de las ocho líneas de negocio.

β1-8 = Un porcentaje fijo, establecido por el Comité, que relaciona la cantidad de capital requerido con el ingreso bruto de cada una de las ocho líneas de negocio. Los valores de los factores **beta (β)** se enumeran a continuación:

Finanzas Corporativas	18%	Negocios y Ventas	18%
Banca Minorista	12%	Banca Comercial	15%
Pagos y liquidación	18%	Servicios de agencia	15%
Administración de activos	12%	Intermediación minorista	12%

Por aparte, existe un método alternativo –ASA- el cual es igual al estándar, salvo en dos líneas de negocio: banca minorista y banca comercial. En el caso de estas líneas de negocio, los préstamos y los anticipos, multiplicados por un factor fijo “m”, sustituyen a los ingresos brutos como indicador de riesgo; los factores beta de la banca en ambas líneas son los mismos que en el Estándar.

2.3.2.1 Criterios de Admisión para utilizar el método Estándar.

- El Consejo de administración y su alta gerencia, deben participar activamente en la vigilancia del marco de gestión de riesgo operativo.
- Debe poseer un sistema de gestión del riesgo operativo conceptualmente sólido que aplique en su totalidad.
- Debe contar con recursos suficientes para utilizar la metodología en las principales líneas de negocio, así como en los ámbitos de control y auditoría.
- Desarrollar políticas específicas y documentar criterios para insertar en el marco estándar los ingresos brutos de las líneas de negocio y actividades existentes.

2.3.3 Método de Medición Avanzada –AMA- (7:131)

En este método, el requerimiento de capital será igual a la medida de riesgo generada por el sistema interno del banco para el cálculo del riesgo operativo, el cual deberá permitir estimar de forma razonable las pérdidas inesperadas, combinando datos relevantes de pérdidas internas como externas, análisis de escenarios, así como el entorno del negocio y los factores de control interno que son específicos al banco; utilizando los siguientes criterios de admisión: a) Generales, b) Cualitativos, c) Cuantitativos y d) Cobertura del riesgo. El sistema de medición del banco también deberá poder llevar a cabo la asignación de capital económico por riesgo operativo entre las ocho distintas líneas de negocio.

2.3.3.1 Criterios de admisión general.

- Su Consejo de administración y su alta dirección, según corresponda, participan activamente en la vigilancia del marco del riesgo operativo.
- Posee un sistema de gestión del riesgo operativo conceptualmente sólido que aplica en su totalidad.
- Cuenta con recursos suficientes para utilizar la metodología en las principales líneas de negocio, así como en los ámbitos de control y auditoría.

2.3.3.2 Criterios cualitativos.

- Contar con una unidad de gestión del riesgo operativo que se encargue del diseño y aplicación del marco de gestión de dicho riesgo.

- Contar con técnicas que distribuyan el capital por riesgo operativo entre las principales líneas de negocio.
- Mantener informado oportunamente a las unidades de negocio, alta dirección y Consejo sobre la exposición al riesgo operativo y del historial de pérdidas debidas a éste.
- Documentar debidamente el sistema de gestión de riesgo operativo. En este sentido la entidad debe poseer políticas, controles y procedimientos internos relativos a la gestión del riesgo operativo.
- Contar con la **validación** de parte de los auditores externos y/o del supervisor sobre el funcionamiento del sistema de gestión de riesgo, así como la transparencia y accesibilidad del flujo de datos asociados a dicho sistema.

2.3.3.3 Criterios cuantitativos.

i) Criterio de solidez del método avanzado.

El banco deberá ser capaz de demostrar que el método seleccionado, identifica eventos generadores de pérdidas graves.

ii) Criterios Detallados.

Estos criterios se refieren a medidas o efectos del cálculo de los requerimientos mínimos de capital regulador, siendo los siguientes:

- Todo sistema interno para el cálculo del riesgo operativo deberá ser acorde a la definición oficial establecida por el Comité.
- Presentar como requerimiento mínimo, la suma de las pérdidas esperadas (EL) y de las inesperadas (UL).

- Los sistemas de cálculo deberán incluir la utilización de datos internos, externos relevantes, análisis de escenarios y factores que reflejen el entorno del negocio y los sistemas de control interno.
- Contar con un proceso creíble, transparente, bien documentado y comprobable para ponderar los valores dentro de un sistema general de medición del riesgo operativo.

iii) Datos internos.

En este aspecto se establece que los bancos deberán realizar un seguimiento de sus registros sobre pérdidas con arreglo a los criterios establecidos. El seguimiento de los datos internos de eventos de pérdidas es un requisito esencial para el desarrollo y funcionamiento de un sistema creíble de medición del riesgo operativo. Esta información es básica para ligar las estimaciones de riesgo del banco a su historial de pérdidas efectivas.

iv) Datos externos.

El sistema de estimación del riesgo operativo deberá utilizar datos externos relevantes, sean datos públicos o agregados al sector bancario, especialmente cuando existan motivos para creer que el banco está expuesto a pérdidas de carácter infrecuente, pero potencialmente graves.

v) Análisis de escenarios.

Este proceso se sirve del conocimiento de directivos experimentados y de expertos en gestión de riesgos para obtener evaluaciones razonadas de las pérdidas graves que podría sufrir la entidad. Para el efecto el banco podrá utilizar escenarios basados en opiniones periciales junto con datos externos.

vi) Factores relacionados con el entorno de negocio y con el control interno.

Además de utilizar los datos de pérdida, ya sean reales o basados en escenarios, la metodología de evaluación del riesgo aplicada al conjunto de la entidad bancaria deberá

identificar aquellos factores básicos de su entorno de negocio y de su control interno que pueden modificar su perfil de riesgo operativo.

2.3.3.4 Cobertura del riesgo.

Si el banco utiliza el método AMA, estará autorizado a reconocer el efecto reductor que generan los seguros en las medidas de riesgo operativo utilizadas en el cálculo de los requerimientos mínimos de capital regulador. El reconocimiento de la cobertura de los seguros se limitará al 20% del requerimiento total de capital por riesgo operativo calculado con el AMA.

2.4 El riesgo operativo en el área de tarjetas de crédito.

La actividad bancaria como emisor de tarjetas de crédito presenta la exposición a una serie de riesgos operacionales provocados en gran parte por la complejidad de las operaciones electrónicas necesarias para su funcionamiento, el otorgamiento de créditos y el grado de conocimiento o confianza necesarios en el personal que realiza el back office.

La estructura bajo la que opera esta área dentro de las instituciones bancarias –Departamento o Gerencia-, cuenta con las siguientes divisiones: Ventas y centro de atención al cliente, personalización y distribución de tarjetas, intercambio, atención de gestiones y reclamos. Además de las citadas, pueden formar parte las áreas de análisis crediticio, contabilidad y cobranza; o estas pueden ser realizadas por los departamentos específicos que el banco posea para tal efecto.

En concordancia con los principales procesos que en el área de tarjeta de crédito se realizan citados en el punto 1.6 del Capítulo I, el análisis del riesgo operativo al que está expuesta la actividad de emisión de tarjetas se presenta en función a la tipología establecida por el Comité de Basilea en el acuerdo de Basilea II, el cual reconoce siete tipos de eventos que generan exposición al riesgo operativo.

2.4.1 Fraude Interno en el área de tarjetas de crédito.

Entendiendo al fraude interno como el involucramiento de personal interno de la empresa en la comisión de alguna actividad ilícita con el objeto de apropiarse de bienes o lograr ventajas por la información que administra, este evento puede presentarse en el área de tarjeta en las siguientes situaciones, por ejemplo:

- Suplantación del tarjetahabiente en el proceso de entrega**.** En este caso el delincuente se da cuenta de que a cierto cliente le fue autorizada una tarjeta con cupo alto; entonces, en unión con un empleado del banco, presenta una cédula falsa y reclama la tarjeta, pero el cliente real nunca la recibe (3:07)
- Aumentos fraudulentos de cupos. Este tipo de fraude consiste en que contando con los accesos al sistema de administración de las tarjetas, el empleado realiza la modificación del límite de crédito de un tarjetahabiente, quien en componenda realiza el consumo o retiro de la nueva disponibilidad, posterior a la utilización proceden a devolver el límite de crédito al valor inicial con la intención de que se presente como un sobregiro imputable a la entidad.(3:07)
- Robo de información o venta de bases de datos. Este tipo de ilícito consiste cuando un empleado extrae la información de la base de datos de clientes (especialmente con calificación importante) con el objeto de venderla a otra entidad dedicada a la emisión de tarjetas. Este fraude es de los más difíciles de monitorear o prevenir, debido a que la consulta de bases es necesaria en varios procesos, lo que dificulta la identificación del origen de la extracción ilícita.
- Eliminación de cargos y comisiones. Este ilícito es cometido por empleados que contando con los accesos correspondientes al sistema, exoneran de cargos por servicios o comisiones por el uso de la tarjeta a clientes con quienes existe relación de cualquier tipo.
- Tarjeta gemela. Durante el proceso de personalización de las tarjetas, puede efectuarse una copia con datos de una cuenta existente, tal situación provoca que circulen dos tarjetas con la aplicación de cargos a una sola. Este fraude puede ser cometido por el personal que tiene acceso al equipo de personalización de tarjetas.

- Fraude en la devolución de tarjetas por el cliente. La devolución de la tarjeta de crédito por parte de un usuario, requiere de controles eficientes para minimizar fraudes, pues pueden presentarse casos en los cuales no se anulan los plásticos, ni se presenta la evidencia de devolución y posteriormente aparecen cargos fraudulentos ejecutados por funcionarios internos, generalmente.(3:08)
- Colusión y funcionarios infieles. Se identifican diferentes ilícitos por parte de los empleados, quienes vulneran los controles para activar tarjetas y usarlas antes de entregarlas al verdadero usuario. (3:08)
- Autorización de tarjetas que no cumplen los requisitos establecidos por el banco. Este fraude ocurre cuando no obstante las evaluaciones y confirmaciones realizadas por los analistas de créditos son negativas, la resolución favorable la establecen funcionarios de mayor jerarquía dentro de la institución.
- Generación de bonificaciones inexistentes. La mayoría de emisores de tarjetas otorgan a sus clientes bonificaciones por el uso de las mismas, ya sea bajo la modalidad de puntos, reembolsos u otro medio de compensación. Dichos valores pueden acreditarse por parte de un empleado a favor de un determinado cliente si las operaciones no son automatizadas o los controles en el sistema no garantizan la integridad de información.
- Sabotaje. Son muchos los factores que pueden generar sabotaje por parte de un empleado, por ejemplo el descontento con las políticas laborales de la entidad. Este evento puede acarrear grandes pérdidas dependiendo de la experiencia que posea la persona que lo cometa, pues existen procesos y activos más sensibles a este fraude, citándose como ejemplos: El software para el procesamiento de las transacciones con tarjeta, el equipo utilizado para la personalización de tarjetas, la bóveda de almacenamiento de tarjetas vírgenes, etc.

En síntesis, el fraude interno es un problema cada día más creciente a consecuencia del deterioro de valores o como resultado de situaciones de inseguridad al que pueda estar sometido el empleado de la entidad emisora. En cualquier caso, las medidas de control que puedan establecerse deben ser lo suficientemente efectivas para evitar cualquier pérdida a consecuencia de este tipo de evento.

2.4.2 Fraude externo con tarjetas de crédito.

Derivado que la utilización de la tarjeta de crédito se realiza de manera masiva y fuera del control del emisor, la exposición al fraude externo es el de mayor impacto para los bancos que se dedican a esta actividad financiera. Tal es el grado de pérdidas que registran los emisores anualmente por este concepto que representan la necesidad de la creación de provisiones significativas y al mejoramiento de los controles para contrarrestarlo.

A continuación se presentan los tipos de fraudes externos más frecuentes en este tema.

- Duplicación de la banda magnética –Skimming-. Este fraude consiste en copiar la información contenida en la banda magnética de la tarjeta, para lo cual utilizan un aparato llamado "Datófono" el cual almacena los datos de hasta 400 tarjetas. La estrategia utilizada por grupos delictivos especializados en este tipo de fraude, consiste en contratar los servicios de personal de establecimientos de cualquier categoría, quienes al tener en su poder la tarjeta para efectuar los cargos por consumos del verdadero cliente, realizan la copia mediante el deslizamiento en el datófono, logrando con esa acción poseer la información general de la cuenta. Posteriormente, utilizando equipo de cómputo y software apropiado, realizan la personalización de tarjetas con la información contenida en el aparato citado, obteniendo una copia de la tarjeta defraudada.

  La materialización del fraude, consiste en utilizar la tarjeta copiada para la adquisición de bienes o pago de servicios, los cuales son cargados a la cuenta del verdadero tarjetahabiente. La incidencia de este fraude en las entidades bancarias emisoras, lo representa la responsabilidad de parte de la entidad para hacer efectivo los pagos a los establecimientos, sin importar que provengan de una copia de tarjeta (caso particular de emisores de tarjetas VISA).
- Suplantación de identidad o uso de documentos falsos. Ocurre cuando los defraudadores buscan lograr la autorización de una tarjeta de crédito, presentado para el efecto información de otras personas y falsificando los documentos que respalden la solicitud de crédito. Esta manera de realizar fraude, aunque no muy frecuente en el país, representa una amenaza a los esquemas de análisis y autorización de tarjetas en cualquier entidad.

- Tarjeta caliente. Es aquella que utilizan los delincuentes antes que el tarjetahabiente llame a la entidad para pedir que la bloqueen por pérdida o robo. Este tipo de fraude es muy común, especialmente en supermercados y estaciones de servicio de combustible por las facilidades que ofrecen para realizar operaciones sin control alguno. (3:06)
- Tarjeta alterada. Se cometen con tarjetas cuya información se ha modificado total o parcialmente. Los delincuentes toman la tarjeta y le cambian el número, puesto que conocen y calculan el dígito de chequeo y consiguen números válidos de personas con cupos considerables. (3:06)
- Plástico falsificado. "Falsificaciones de mala calidad: hologramas desprendidos, logotipos incompletos, microtextos que no aparecen. Sin embargo muchas de estas tarjetas son aceptadas en el comercio". (3:06).
- Comprobantes previamente elaborados**.** Otro nombre que se le da a esta modalidad de fraude es el de comprobantes falsos o lavado de comprobantes. En ella se imprimen los comprobantes con elementos diferentes de la misma tarjeta, se distribuyen en comercios debidamente autorizados y pasan como auténticos (3:06).
- Fraudes con telemercadeo**.** Este es un fraude donde el delincuente llama a una de las muchas empresas de telemercadeo y hace el pedido de un artículo con cargo a la tarjeta de crédito. Toda la información que solicitan es verdadera, incluso los sitios de recepción de la mercancía (3:07)
- Uso indebido de la tarjeta. Este fraude consiste en cargos que el tarjetahabiente no reconoce, pero que por no tener indicios de duplicación (falta de puntos de compromiso por ejemplo), se le atribuyen a personas cercanas al cliente que sin su autorización efectúan transacciones fraudulentas. Existen casos en que los responsables son los esposos (as), empleados de confianza, novios (as), etc.
- Autoría del tarjetahabiente**.** Ocurre cuando el tarjetahabiente, personalmente o a través de terceros, utiliza o facilita su tarjeta en transacciones que posteriormente rechazará (3:07).

- Doble facturación. La persona paga la cuenta en un restaurante o un bar con tarjeta de crédito, pero el mesero solicita la autorización de la tarjeta dos o tres veces en el POS, y luego trata de imitar la firma del cliente en los otros recibos (3:08).
- Acceso a los sistemas. Este fraude consiste en violentar las medidas de seguridad de los sistemas mediante técnicas de computación avanzadas, con la intención de robar información que facilite la utilización de tarjetas creadas con bases reales del emisor.
- Fraude en cajeros automáticos. Se efectúa mediante la instalación de mecanismos que atrapan la tarjeta en la ranura donde se ingresan en el cajero, posteriormente el usuario en su intento por bloquear la tarjeta acepta ayuda del defraudador quien en esa acción logra obtener el número de identificación personal del tarjetahabiente y finalmente realiza las transacciones fraudulentas.
- Fraude por Internet. Se realiza por personas que con un alto grado de conocimiento técnico en el ámbito informático, realizan la intercepción de los datos de tarjetas reales que son utilizadas en sitios Web que las acepte como medio de pago, y con dicha información realizan compras en el mismo medio con cargo a las tarjetas reales.
- Número de cuenta inexistente. Consiste en generar números de tarjetas de manera aleatoria mediante programas de computación y con ellos intentar autorizaciones telefónicas o en las páginas Web. Al igual que en el caso del fraude por Internet, se requiere de un nivel de conocimiento informático alto, así como sobre tarjetas de crédito, para cometerlo.
- Lavado de dinero o financiamiento al terrorismo. Aunque la intención no es defraudar al banco con las operaciones realizadas con tarjetas de crédito, esta modalidad es utilizada para la adquisición de bienes cuantiosos que posteriormente pagan con dinero proveniente de fuentes ilícitas, situación que consumaría el delito de lavado de activos. Por otra parte, las tarjetas pueden utilizarse para adquirir materiales o bienes en favor de terroristas.

En ambas situaciones la consecuencia de pérdida, la genera la obligación que tiene el banco como persona obligada de velar porque no ocurran tales eventos, según lo establecen las Leyes emitidas sobre dichos temas.

2.4.3 Relaciones laborales y de seguridad en el trabajo, en el área de tarjeta de crédito.

Este riesgo operativo, se refiere a aquellas situaciones de tipo laboral que afecte a las personas que se desempeñen en el área de tarjeta de crédito. En tal sentido, se consideran las pérdidas que puedan ser imputables al banco por reclamaciones del personal derivadas de demandas interpuestas por incumplimiento de contratos laborales, accidentes dentro del área de trabajo, medidas de seguridad e higiene inapropiadas para desarrollar las labores, despidos no justificados, discriminación racial o sexual, etc.

2.4.4 Clientes, productos y prácticas empresariales, en el área de tarjeta de crédito.

Debido a las prácticas comerciales que existen en el mercado de tarjetas de crédito, este riesgo representa la posibilidad de registrar pérdidas a consecuencia de situaciones como por ejemplo:

- Productos mal diseñados o defectuosos. Esta clasificación concentra la posibilidad de pérdidas al banco, como resultado del inapropiado análisis, bajos controles de calidad o defectos no detectados antes de entregar la tarjeta de crédito al cliente. Puede citarse como ejemplo, la emisión de tarjetas con problemas de grabación de la información en la banda magnética, situación que acarrea molestias para el cliente ante los rechazos de la misma y consecuentemente conlleva el deterioro de imagen ante el cliente y el establecimiento afiliado. Otro ejemplo puede ser la emisión de un nuevo tipo de tarjeta, donde en la definición de los parámetros de funcionalidad, no se consideran los establecidos por la marca que respalda a nivel internacional y puede acarrear sanciones por parte de esta o hasta el extremo de cancelar la relación comercial con el banco.
- Inapropiado asesoramiento de la funcionalidad del producto. La posibilidad de registrar pérdidas por no contar con equipos de venta o postventa que asesoren apropiadamente a los clientes sobre la funcionalidad de la tarjeta entregada, son los que se concentran en esta categoría de riesgo. Puede considerarse en esta las pérdidas para el banco en el seguimiento

de cobro del pago mínimo, donde parte del problema radica en la inapropiada indicación al cliente sobre sus responsabilidades adquiridas al aceptar la tarjeta de crédito, situación que muchas veces es obviada por la intención de colocar el producto, primordialmente.

2.4.5 Daños a activos materiales.

Tal como su nombre indica, este riesgo se refiere a las posibles pérdidas que pueda sufrir el emisor de tarjetas por daños inesperados en sus activos. Dichas pérdidas pueden ser a consecuencia de desastres naturales, actos vandálicos, terrorismo, etc. Los principales equipos expuestos a pérdidas por este riesgo son: Hardware para el procesamiento de las transacciones, del personal del área y para la personalización de tarjetas.

2.4.6 Fallas en los sistemas.

Esta categoría de riesgo operativo, concentra las pérdidas como consecuencia de la interrupción de un programa o de los sistemas de comunicación necesarios para la operatoria de las tarjetas de crédito. Reviste especial importancia por cuanto la funcionalidad de las tarjetas depende de buena parte, de la correcta operatoria de los equipos y sistemas. Entre las eventualidades existentes, se encuentran:

- Fallas en el hardware y software. La ocurrencia de alguna falla en el equipo de computación y los programas que se utilizan en el área de tarjeta de crédito como tal, así como de las funciones de autorizador si fuese el caso, conllevan la exposición a pérdidas económicas, al dejar de percibir comisiones por concepto de consumos, cobro de intereses por financiamientos no utilizados, comisiones por consumos en gasolineras, comisiones por utilización de redes de cajeros automáticos, etc; de imagen, ante los establecimientos afiliados y los clientes por la credibilidad del uso de tarjetas del emisor; sanciones y multas, por parte de la marca que respalda la emisión de las tarjetas, si el problema es recurrente.
- Fallas de comunicación. El riesgo existe ante la posibilidad de que se pierda la comunicación entre las partes que intervienen en la transacción realizada con la tarjeta de crédito a consecuencias de fallas en las redes, protocolos de comunicación, etc.

2.4.7 Ejecución, entrega y gestión de procesos.

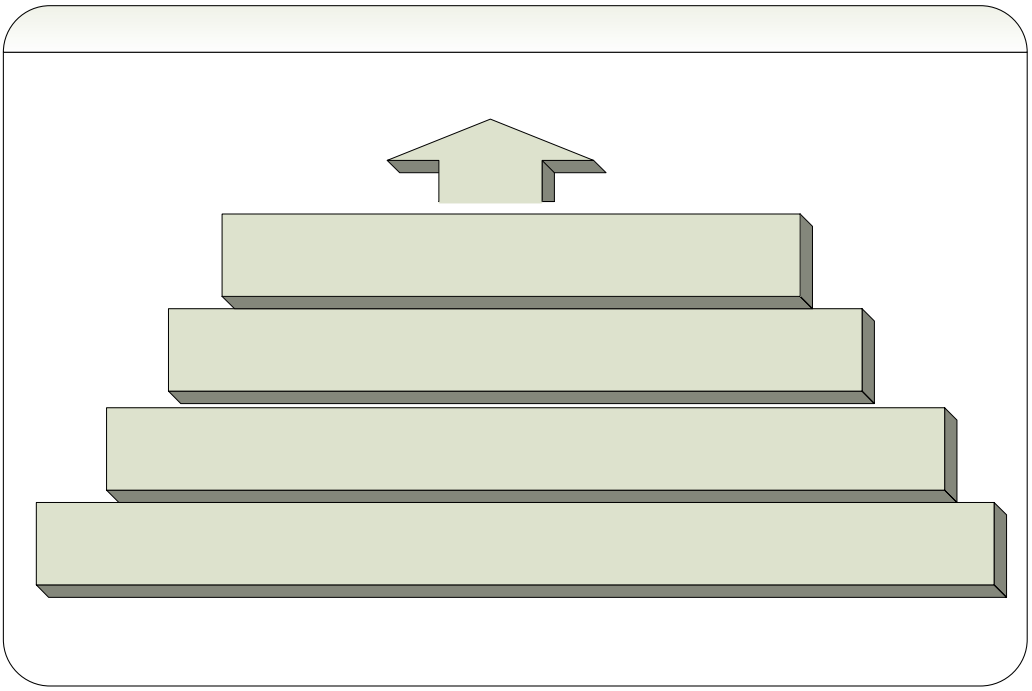
Constituye uno de los riesgos operativos más frecuentes en el área de tarjeta de crédito, situación que se debe a que esta categoría encierra aquellas posibles pérdidas a causa de los siguientes eventos:

- Errores de todo tipo. Corresponde a esta categoría, por ejemplo: Los errores en la introducción de datos, contables, humanos, etc. Algunas de los inconvenientes o inconsistencias que pueden ejemplificarse son las multas o sanciones por falta de información contable, información financiera no fiable, bases de datos mal registradas y sus consecuencias en las consultas que se realicen, pérdida o destrucción de documentos relevantes, mala atención de gestiones, reembolsos incorrectos, cargos inexistentes, etc.
- Inexistencia de autorizaciones. La posibilidad de efectuar operaciones por concepto de gestiones que requieran autorización de funcionario competente pero que no sean cumplidas, es una de las pérdidas que pueden registrarse por este concepto.
- Documentos jurídicos incompletos. Los expedientes de tarjeta de crédito incluyen como parte medular, la información de conocimiento de cliente y el contrato con el banco, mismo que por diversas circunstancias pueden dejarse de completar apropiadamente provocando la probabilidad de ser sujetos a multas por parte de la Superintendencia o afectar el proceso de cobro en caso de incumplimiento de pago por parte del tarjetahabiente.
- Fallos en la entrega. En este tipo de riesgo se encuentran los problemas que puedan existir en el envío y entrega de tarjetas donde puede ocurrir la suplantación de identidad, pérdida de la tarjeta, entrega incorrecta, etc. Por otra parte, también se catalogan las consecuencias en la entrega de estados de cuenta, aspecto que puede provocar pérdidas de información confidencial y mala atención a clientes, entre otras.
- Accesos no autorizados a sistemas o lugares de máxima seguridad.
- Subcontratación de servicios. Actualmente con el objeto de minimizar costos, la tendencia del outsourcing es creciente, para el caso de los emisores de tarjetas, uno de los servicios que contratan es el referente al de autorizador de transacciones, el cual contrae una serie de riesgos operacionales conexos. Otro servicio usualmente contratado es el de personalización de tarjetas, el cual representa mayor riesgo por efectuarse fuera del control de la institución.

CAPITULO III
ADMINISTRACIÓN DE RIESGO OPERATIVO, SEGÚN EL COMITÉ DE BASILEA

El Comité de Basilea describe en el documento "Prácticas sanas para la administración y supervisión del riesgo operativo" publicado en agosto de 2003, un conjunto de principios que proveen un marco para la efectiva administración y supervisión del riesgo operativo, haciendo énfasis en que los bancos y las autoridades de supervisión pueden utilizarlo para tal fin.

FIGURA No. 6
PASOS ELEMENTALES PARA ADMINISTRAR EL RIESGO OPERATIVO



Fuente: Documento "Prácticas sanas para la administración y supervisión del riesgo operativo" febrero 2003.

3.1 Desarrollo de un entorno adecuado de administración de riesgos (9:11)

Corresponde al directorio y la alta gerencia la creación de una cultura organizacional que dé máxima prioridad a una efectiva administración del riesgo y el cumplimiento de controles sanos. Dichas acciones serán más efectivas, si se destacan altos estándares de conducta ética en todos los niveles del banco, que puedan determinar la expectativa de integridad para los empleados al efectuar las actividades que les competen.

3.1.1 Principio 1: Responsabilidad del directorio.

"El directorio deberá estar consciente de los principales aspectos de los riesgos operativos del banco, como una categoría diferente de riesgo a ser administrado, y deberá aprobar y revisar periódicamente el marco de administración, mismo que debe especificar los principios para la identificación, evaluación, monitoreo y control / mitigación del riesgo operativo".

Este principio se refiere a que el directorio debe aprobar la implementación de un marco para la administración explícita del riesgo operativo, como un riesgo diferente que pone en peligro la seguridad y solvencia del banco. El marco de riesgo operativo debe basarse en una definición adecuada, además, debe establecer los niveles de tolerancia que se consideren aceptables, las políticas que definan el enfoque del banco para identificar, evaluar, monitorear y controlar / mitigar el riesgo.

3.1.1.1 Comité de administración de riesgo operativo.

El directorio es responsable de la creación de una estructura gerencial capaz de implementar el marco de administración del riesgo operativo en la empresa, así como la definición de líneas claras de responsabilidad gerencial y para la presentación de informes en todo lo relacionado con el establecimiento de controles internos. Este órgano independiente y técnico, debe estar estructurado de manera que garantice el cumplimiento de los objetivos de la organización en materia de administración de riesgo operativo. Se sugiere su integración y funciones, de la siguiente manera:

- Integración del Comité: Miembros pertenecientes a las diferentes unidades de negocio, planificación estratégica, tesorería, recursos humanos, departamento legal, auditoría y tecnología de información. (19:01)
- Principales funciones: (4: 08)
    - Medir, vigilar y controlar los riesgos que afectan al banco.
    - Proponer metodologías, modelos y parámetros.
    - Vigilar la observancia de los límites de tolerancia aceptables por tipo de riesgo.

- Proporcionar informes a los órganos correspondientes, que permitan analizar el impacto de exposición a riesgos por unidad de negocio o factor.
- Investigar y documentar las causas que se consideran como foco de incremento de riesgos.

3.1.2 Principio 2: Función de Auditoría Interna.

"El directorio deberá asegurar que el marco de administración del riesgo operativo del banco, sea sujeto a una auditoría interna efectiva e integral, por personal competente, independiente desde el punto de vista operativo y con una adecuada capacitación. La función de auditoría interna no deberá tener la responsabilidad directa por la administración del riesgo operativo".

El principio establece que todos los bancos deben poseer estructuras adecuadas de auditoría interna para verificar si las políticas y procedimientos se han implementado y si el marco de administración se está desarrollando efectivamente. Para el efecto, el directorio debe asegurar que el alcance y la frecuencia del programa de auditoría sean adecuados, considerando la exposición a riesgos.

La función de auditoría, es suministrar aportaciones sin incurrir directamente en el desarrollo de las funciones, para las cuales, se recomienda que los bancos cuenten con un órgano específico (Comité de administración de riesgo o una Sección dentro de la organización dedicada exclusivamente a tal efecto).

3.1.3 Principio 3: Responsabilidad de la alta gerencia.

"La alta gerencia debe ser responsable por la implementación del marco de administración del riesgo operativo aprobado por el directorio, además del desarrollo de políticas, procesos y procedimientos para administrarlo en todos los productos, actividades, procesos y sistemas más importantes del banco. El marco se deberá implementar de forma coherente a lo largo de toda la organización, y todos lo niveles del personal deberán entender sus responsabilidades respecto de la administración del riesgo".

El principio indica que la gerencia debe traducir el marco de administración del riego fijado por el directorio, en: políticas, procesos y procedimientos específicos que se puedan implementar y verificar en las diferentes unidades del banco, así como delegar en los puestos clave, la responsabilidad de velar por la efectividad de dichas medidas dentro del ámbito de trabajo y proveyendo los recursos necesarios. En otras palabras, recae en la alta gerencia en coordinación con el órgano específico responsable de la administración del riesgo operativo, la implantación de lineamientos que puedan delimitar las funciones, responsabilidades y mecanismos de control o prevención de ocurrencia de riesgos operacionales.

3.2 Administración de riesgos: Identificación, evaluación, monitoreo, mitigación / control (9:13).

La base para la administración del riesgo operativo la constituye la responsabilidad del directorio, la alta gerencia y la auditoría interna; empero, para poder materializar los lineamientos establecidos en la primera fase, deben realizarse cuatro actividades, las cuales son:

3.2.1 Principio 4: Identificación y evaluación.

"Los bancos deberán identificar y evaluar el riesgo operativo inherente en todos los productos, actividades, procesos y sistemas importantes. También, deberán asegurar que antes de introducir o emprender productos, actividades, procesos y sistemas nuevos, el riesgo operativo inherente en los mismos sea sujeto a procedimientos adecuados de evaluación".

Esta etapa es esencial para el desarrollo posterior de un sistema viable de monitoreo y control del riesgo operativo. Comprende tomar en cuenta los factores internos de la estructura del banco, tales como: actividades, calidad del recurso humano, cambios organizativos y rotación del personal; y por otra parte, los factores externos siguientes: cambios en el sector, avances tecnológicos y marco legal. El objetivo es identificar los eventos que puedan generan mayor impacto negativo para la institución, establecer el perfil de riesgo y asignar los recursos necesarios para su control.

Para una adecuada identificación de riesgos operativos, el Comité (Basilea) recomienda el uso de las herramientas siguientes:

- Auto-evaluación o evaluación del riesgo.
- Mapeo de riesgos.
- Indicadores de riesgo.
- Medición.

3.2.2 Principio 5: Monitoreo y comunicación a los órganos competentes.

"Los bancos deberán implementar un proceso para monitorear regularmente los perfiles del riesgo operativo y las exposiciones importantes a pérdidas. La información pertinente, se deberá presentar regularmente a la alta gerencia y el directorio que apoya la administración proactiva del riesgo".

Como monitoreo se entiende a la función de mantener control sobre las actividades y asignar responsables de observar el cumplimiento de las normas establecidas. El monitoreo es indispensable en la administración del riesgo operativo y representa la ventaja de la oportuna detección y corrección de deficiencias en las políticas, procesos y procedimientos; pudiendo reducir en gran medida la potencial frecuencia o seriedad de un evento de pérdida. Esta actividad no debe comprender únicamente los eventos de pérdidas operativas, sino prever potenciales fuentes de riesgo como: el crecimiento rápido del banco, la implantación de productos nuevos, la rotación del personal, transacciones truncadas, tiempo de inactividad del sistema, etc.

3.2.3 Principio 6: Control y/o mitigación.

"Los bancos deberán tener políticas, procesos y procedimientos para controlar y/o mitigar riesgos operativos importantes. Para el efecto, deberán hacer una revisión periódica de sus estrategias de limitación o control de riesgos y deberán ajustar su perfil –de riesgo operativo- de acuerdo con dichas estrategias".

Un componente indiscutible en el control / mitigación del riesgo operativo es el control interno, el que establece que exista una adecuada segregación de funciones y que el personal no sea asignado a responsabilidades que puedan dar lugar a un conflicto de intereses, por lo cual las áreas que podrían generar tal fenómeno deben ser identificadas, minimizadas y sujetas a un proceso independiente de monitoreo y revisión.

Además de la segregación de obligaciones, el banco debe asegurar que haya otras prácticas internas para controlar riesgos operativos, como por ejemplo:

- Monitoreo de umbrales o límites de riesgo asignados.
- Medidas para el acceso a, y uso de, registros y activos.
- Velar porque el personal cuente con experiencia y capacitación adecuada en sus funciones asignadas.
- Identificar líneas o productos en los que el retorno parece ser incoherente con expectativas razonables (ejemplo: actividades de bajo riesgo con alto retorno).
- Verificación y reconciliación regulares de transacciones y cuentas.
- Medidas preventivas en el desarrollo de nuevos productos.
- Medidas preventivas en caso de ocurrencia de desastres naturales o siniestros internos.

3.2.4 Principio 7: Planes de contingencia.

"Los bancos deberán tener planes de contingencia y de continuidad de las actividades, para asegurar su capacidad de operar de forma constante y limitar sus pérdidas en caso de una seria interrupción de sus actividades".

Existe la posibilidad de ocurrencia de eventos desfavorables fuera del control del banco, que pueden resultar en la incapacidad de cumplir con alguna o todas sus obligaciones, especialmente si está dañada o inaccesible la infraestructura física, de telecomunicaciones, o de tecnología de información. Las acciones recomendadas incluyen: identificar los principales procesos críticos comerciales,

operativos e informáticos; a los que se deben establecer procedimientos alternos para reanudar su continuidad. Dichos planes de recuperación deben revisarse y certificarse periódicamente para determinar la coherencia entre las operaciones y planes comerciales, así como para garantizar que se puedan ejecutar en algún evento poco probable.

3.3 Papel de los Supervisores (9:19)

3.3.1 Principio 8: Marco de administración de riesgos.

"Los Supervisores bancarios deberán exigir que todos los bancos, independientemente de su tamaño, tengan un marco efectivo para identificar, evaluar. monitorear y controlar / mitigar riesgos operativos importantes, como parte de un enfoque general para la administración de riesgos".

Este principio define el rol de los Supervisores para exigir que los bancos desarrollen marcos de administración de riesgo operativo, que sean coherentes con los principios definidos por el Comité de Basilea, sin importar el tamaño, complejidad y perfiles de riesgo de cada institución. En la medida que los riesgos operativos amenazan la seguridad y solvencia de los bancos, los supervisores tienen la responsabilidad de requerir, utilizar y desarrollar mejores técnicas para administrar esos riesgos.

3.3.2 Principio 9: Evaluación del marco de administración.

"Los Supervisores deberán llevar a cabo, directa o indirectamente, evaluaciones independientes de las políticas, procedimientos, y prácticas de un banco, respecto de los riesgos operativos. Además, deberán asegurar que existan mecanismos adecuados que les permitan estar al tanto de las evoluciones en este aspecto".

Este principio hace referencia a las actividades que debe realizar el Supervisor en el proceso de evaluación del riesgo operativo dentro de una institución bancaria.

3.4 Papel de la divulgación (9:21)

3.4.1 Principio 10: Divulgación del enfoque de administración de riesgo operativo.

"Los bancos deberán divulgar suficiente información al público, para que los participantes en el mercado puedan evaluar su enfoque para la administración del riesgo operativo".

El Comité de Basilea hace énfasis en la trascendencia, que representa una divulgación pública oportuna y frecuente para la disciplina de mercado y por ende una administración de riesgo más efectiva. En éste sentido, recomienda que el banco debiera publicar su marco de administración de riesgo operativo de forma que permita a los inversionistas y contrapartes determinar si identifica, evalúa, monitorea y controla / mitiga, efectivamente el riesgo operativo.

De acuerdo a los planes del Comité, el acuerdo de Basilea II (el cual establece requerimientos de capital por la exposición a riesgo operativo) cobrará vigencia a partir del año 2007 en los países que conforman el Comité, situación que ha motivado que las entidades bancarias de Latinoamérica hayan emprendido acciones entorno al tema y sobre el que se han obtenido indicadores, normativas y tendencias del sector; las cuales se describen a continuación:

3.5 Administración del Riesgo Operativo en Latinoamérica.

3.5.1 Indicadores a nivel de la Región Latinoamericana (18: 37-81)

Una de las principales preguntas en torno al tema del riesgo operacional es poder determinar donde se producen las pérdidas por ese concepto, para lo cual es prioritario determinar el tipo de entidad, la complejidad del tipo de negocio, tipo de clientes a los que se orienta, etc. Con ese objetivo, una firma consultora realizó recientemente un estudio a nivel latinoamericano sobre la percepción de los bancos respecto a la identificación de áreas vulnerables, tipo de riesgo con mayor presencia en la región y herramientas utilizadas para su control. Del citado estudio, se extraen los indicadores siguientes:

- A nivel regional los bancos presentan mayor exposición al riesgo, en las líneas de negocio siguientes: Banca Minorista, de empresas y corporativa, así como en negociación y ventas.

- Tipología de riesgo con mayor grado de exposición. Gestión de procesos para las bancas de empresas y corporativa; Fraude externo para la línea de negocio banca minorista, segmento que incluye operaciones con tarjetas de crédito.
- México considera con mayor grado de exposición en el siguiente orden a las líneas de negocio: banca de empresas, corporativa y minorista, representando la primera línea de negocio un 17% del volumen de operaciones de ese vecino país. En el segmento de banca minorista los principales riesgos a los cuales consideran mayor exposición son: Fraude externo, gestión de procesos, fallas en los sistemas.
- Banca minorista –línea de negocio que incluye operaciones con tarjeta de crédito- representa 43% del volumen de negocio a nivel regional y los principales riesgos que le afectan dentro de cualquier segmento, son: el fraude externo y la gestión de procesos.
- Fraude externo. Provocado por las causas siguientes: Uso fraudulento de tarjetas de crédito 38%, Robos y atracos 31% y violación de la seguridad informática 31%.
- En cuanto a los mecanismos utilizados por las entidades de Latinoamérica para salvaguardar y mitigar las pérdidas por concepto de riesgos operativos, son comunes la contratación de seguros, dotación de provisiones, planes de contingencia y outsourcing. También son empleadas la medidas siguientes:
    - Políticas de control de auditoría, redundancia de la infraestructura, revisión y actualización de hardware y software, políticas de prevención de riesgos laborales, planes de incentivos, mejoras en el servicio de atención al cliente, reducción de intervención manual.

3.5.2 Administración del riesgo operativo, adoptado en México.

Por la cercanía existente entre Guatemala y México, además de los antecedentes en cuanto a la adopción de medidas previamente implantadas en aquel país y posteriormente en el nuestro, es necesario el estudio del entorno o la situación en la que se encuentra el análisis del riesgo operativo en el vecino país. Al respecto, ya se han tratado los resultados del estudio efectuado a un grupo de entidades del mercado mexicano, en donde sobresalió que el principal riesgo considerado es el fraude

externo y a su vez lo genera el fraude con tarjetas de crédito. No obstante; el estudio presentó el enfoque desde el punto de vista de las propias entidades, pero cabe resaltar también el papel de la Comisión Nacional Bancaria y de Valores (CNBV), órgano estatal que en junio del año 2004 emitió el documento "Disposiciones de carácter prudencial en materia de administración integral de riesgos aplicables a las instituciones de crédito", en el que se describen los lineamientos en materia de administración de riesgos, incluido el operativo.

3.5.3 Administración del riesgo operativo en Guatemala.

Para el caso de Guatemala, el tema de administración del riesgo operativo es de reciente incursión en el medio bancario, no obstante; La Superintendencia de Bancos ha iniciado una serie de acciones tendientes a la identificación y administración de este tercer riesgo que integra el nuevo acuerdo de Basilea II, entre los que figura el envío de circular (Enero 2006) en la que requieren a los bancos un informe acerca de la situación en que se encuentra el tema de administración integral de riesgos, incluido el operativo. Asimismo, han sido disertadas diversas charlas que abordan el tema, como por ejemplo: Riesgo operativo, Dr. Ángel Vilariño y Riesgo operativo y gobierno de TI, Dr. Iván Laguado.

Uno de los riesgos a los que la Superintendencia de Bancos confiere principal interés, es el Tecnológico (probabilidad de ocurrencia de pérdidas a consecuencia de fallas en los sistemas y comunicación) el cual es parte del riesgo operativo. La causa por la que este riesgo es considerado crítico, la constituye la dependencia de los sistemas informáticos en casi la totalidad de funciones del sector bancario nacional.

CAPITULO IV
ADMINISTRACIÓN DE RIESGO OPERATIVO EN EL ÁREA DE TARJETAS DE CRÉDITO

Siendo parte de una entidad bancaria el departamento o área de tarjeta de crédito está sujeta a las consideraciones que sobre dicho tipo de entidad, aplica en el tema de administración de riesgo operativo. En consecuencia, debería existir un responsable o grupo de responsables que realicen las diversas fases que conlleva la administración de riesgo dentro de dicha área, las cuales son:

4.1 Identificación y evaluación de riesgos.

En esta fase, el objetivo es lograr identificar los sucesos que dentro del área o al producto de tarjeta de crédito puedan generar mayores pérdidas. Por tal razón, es necesario contar con la información que proporcione los elementos de juicio para la evaluación de riesgos, tales como: Manuales de procedimientos, registro de capacitación al personal, informes de auditoría interna o externa, reglamentos externos aplicables, contratos adquiridos en el área, registros históricos de contingencias, bitácoras de caídas de sistema, control de gestiones, reclamos de clientes, etc.

Por otro lado, debe estimarse la frecuencia con que pueden presentarse los riesgos identificados, así como cuantificar la probable pérdida que puedan ocasionar. Posteriormente deben catalogarse la importancia de cada riesgo identificado, utilizando medidas como por ejemplo: bajo, alto, medio, la cual puede ser establecida por el impacto que generen de acuerdo al conocimiento técnico del evaluador, o puede expresarse por la llamada ecuación de la exposición: $PE = F * X$; donde:

PE = Pérdida Esperada o Exposición, expresada en valores monetarios y en forma anual.

F = Frecuencia, veces probables en que el riesgo se concrete en el año.

X = Pérdida estimada para cada caso en que el riesgo se concrete, expresada en valores.

Mediante una auto-evaluación o utilización de matrices de medición de riesgo, pueden identificarse los principales riesgos a los cuales estarían expuestas las operaciones realizadas con tarjetas de crédito, los cuales pueden ser:

4.1.1 Por proceso:

CUADRO No. 5

IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS POR PROCESO

Comercialización de tarjetas

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Inapropiado asesoramiento del producto.	Poca capacitación al personal de ventas sobre las características de la tarjeta a ofrecer, situación que desemboca en cancelaciones prematuras o mala reputación para el banco. **Recomendación:** Mantener altos estándares de capacitación a los equipos de venta, evaluaciones y seguimiento por parte de la jefatura encargada.	**ALTO** Por la rotación, típica del personal.
Suplantación de identidad o uso de documentos falsos.	Presentación de documentos falsos, alterados o de otras personas, a los empleados que comercializan el producto. **Recomendación:** Revisión de los documentos (establecidos como política del banco) en presencia del cliente y verificación de confiabilidad de las bases de datos utilizadas para comercializar.	MEDIO Por el volumen de solicitudes
Deficiencias en el formulario IVE.	Errores en la complementación de la información requerida en el formulario IVE establecido para la relación comercial con el cliente; situación que puede provocar multas o sanciones por parte del ente supervisor. **Recomendación:** Capacitación a la fuerza de ventas sobre la mejor manera de complementar el formulario, delegar responsables de revisiones en un área operativa.	MEDIO Por el volumen de solicitudes

Análisis y autorización de las tarjetas de crédito

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Autorización de tarjetas que no cumplen los requisitos crediticios.	Negligencia en el desempeño de las funciones o colusión por parte de los analistas de créditos con terceras personas, para la aprobación de solicitudes que no cumplen los requisitos. **Recomendación:** Niveles de autorización superiores de acuerdo a montos autorizados, revisión y supervisión de solicitudes que comprometan la independencia de los analistas (familiares, recomendados), segregación de funciones de confirmación.	MEDIO Por el volumen de solicitudes analizadas

Suplantación de identidad o uso de documentos falsos.	Fraude externo -con niveles altos de ocurrencia-, el cual desemboca en autorización de tarjetas a personas inexistentes o a quienes les hayan robado su identidad (obtención de documentos e información necesarios para solicitar créditos). **Recomendación:** Revisión de características de seguridad de los documentos presentados, abstinencia de aceptación de documentos enviados vía fax o referencias telefónicas móviles, confirmación con el cliente de teléfonos registrados en los burós de información pública.	**ALTO** Por el volumen de solicitudes analizadas

Emisión y entrega de la tarjeta

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Suplantación del tarjetahabiente en el proceso de entrega.	Fraude interno que provoca pérdidas por el uso de la tarjeta por un tercero sin el reconocimiento del solicitante original. Este riesgo se incrementa si se trata de preautorización de tarjetas porque el cliente real, nunca estuvo enterado de la existencia de la misma. **Recomendación:** Mayor control sobre el procedimiento y del personal que realiza ésta actividad. Inventario actualizado de contraseñas de entrega, de preferencia cotejando la firma de recibido con la de solicitud o del documento de identificación. Priorizar la revisión para tarjetas doradas o platinum.	BAJO Por la ocurrencia poco probable.
Tarjeta gemela	Generación de dos tarjetas relacionadas a una misma cuenta, por el empleado que realiza la personalización de plásticos. La consecuencia son cargos no reconocidos por el verdadero tarjetahabiente. **Recomendación:** Control pormenorizado de los plásticos utilizados para la personalización, velar por la apropiada segregación de funciones y supervisión en cada lote de tarjetas emitidas.	BAJO Por la ocurrencia poco probable.
Fallos en la entrega	Deficiencias en el envío y entrega de las tarjetas a los propietarios reales, pérdida de estados de cuenta y publicidad del emisor. **Recomendación:** Contratación de empresas especializadas en la entrega de documentos de valor, control de tarjetas entregadas.	**ALTO** Por el volumen de operaciones
Activación incorrecta de tarjetas	Fallas en los procedimientos de activación de tarjetas, provocando el uso fraudulento de tarjetas por terceras personas. **Recomendación:** Activación a los propietarios personalmente en oficinas de atención. Telefónicamente: Rotar preguntas de confirmación (cédula – dirección, cédula-teléfonos, etc.).	**ALTO** Por el volumen de operaciones

Autorización electrónica de transacciones.

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Fallas en el hardware y software.	Fallas en los servidores o del sistema que administra las autorizaciones electrónicas de operaciones con tarjeta de crédito, generando mal servicio a los clientes y dejar de obtener beneficios económicos directos a consecuencia de las mismas. **Recomendación:** Revisión constante de la funcionalidad de los equipos, pruebas de estrés a los sistemas, monitoreo de disponibilidad de los servicios, planes de contingencia.	MEDIO Por los equipos y sistemas disponibles actualmente.
Fallas de comunicación.	Irregularidad en los servicios de telecomunicación utilizados para enviar y recibir los mensajes electrónicos de autorización de las operaciones con las tarjetas de crédito; generando mal servicio a los clientes y dejar de obtener beneficios económicos directos a consecuencia de las mismas. **Recomendación:** Monitoreo de disponibilidad de los servicios, planes de contingencia.	MEDIO Por los equipos y sistemas disponibles actualmente.
Duplicación de la banda magnética –Skimming-	Generación de una tarjeta duplicada, mediante la copia fraudulenta de la información contenida en la banda magnética. Como resultado se registran cargos no efectuados por el tarjetahabiente real, resultando en pérdidas directas para la entidad emisora. **Recomendación:** Altos niveles de monitoreo electrónico de autorizaciones, confirmación de operaciones con el tarjetahabiente, recomendaciones de seguridad a los clientes. A nivel país deberían considerarse las recomendaciones siguientes: Legislación específica sobre el fraude, mejorar la coordinación entre emisores de tarjetas, adopción de tarjetas con chip complementa la autorización de las operaciones.	**ALTO** Por la frecuente ocurrencia y modo de realizarlo.
Tarjeta alterada o número de tarjeta inexistente.	Fraude externo que realizan combinando números aleatoriamente, hasta lograr la identificación de un BIN válido para el emisor. **Recomendación**: Parametrización en el sistema autorizador de transacciones y actualización inmediata en los sistemas de seguridad a nivel internacional para el bloqueo de esas cuentas.	BAJO Por la ocurrencia poco frecuente
Acceso al sistema informático.	Violación de los mecanismos de seguridad del sistema informático por parte de un delincuente experto. A consecuencia puede perderse información de tarjetahabientes, ocurrir sabotaje o infectar con virus informáticos. **Recomendación:** Adquisición de equipos especializados en la identificación y bloqueo a intrusos.	BAJO Por la ocurrencia poco probable.
	Se diferencia del de tarjeta alterada, en que la intercepción de datos de tarjetas reales en la Internet, les favorece contar	BAJO

Fraude por Internet	con la información necesaria para replicar otros cargos a la tarjeta. **Recomendación:** Altos niveles de monitoreo electrónico de autorizaciones, confirmación de operaciones con el tarjetahabiente, recomendaciones de seguridad a los clientes	Por el volumen de compras en este medio.

Gestiones.

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Aumento fraudulento de límite de crédito.	Abuso de confianza del personal con accesos para realizar esa gestión. Las repercusiones son pérdidas por operaciones realizadas sin garantía de reembolso. **Recomendación:** Niveles apropiados de autorización de modificaciones de límites, generación y revisión de reportes diarios de cambios efectuados, monitoreo de cambios en el sistema con parámetros considerados de mayor riesgo.	MEDIO Por volumen de gestiones
Eliminación de cargos y comisiones.	Abuso de confianza del personal con accesos para realizar esa gestión, lo cual representa rebaja en la recepción de comisiones. **Recomendación:** Niveles apropiados de autorización de exoneraciones, generación y revisión de reportes de cambios realizados.	BAJO Por los montos y tipo de txs
Fraude en la devolución de tarjetas por el cliente.	Devolución de tarjetas a la institución por diversas causas (cancelación, revisión, cambio, etc.) que pueden ser utilizadas por empleados deshonestos. **Recomendación:** Inutilización de tarjetas en los casos que ameriten, emisión de contraseñas a los clientes, mismas que requieran registrarse contablemente para mejor control.	MEDIO Por la frecuente ocurrencia
Generación de bonificaciones inexistentes	Créditos o débitos inexistentes de puntos o bonificaciones por parte del personal del área. Uso indebido de los valores defraudados o canje de productos en nombre de terceros. **Recomendación:** Niveles de autorización en los sistemas que administren las bonificaciones, cotejo de firmas en las solicitudes procesadas, integración contable detallada del fondo de puntos o bonificaciones.	**ALTO** Por la frecuente ocurrencia
Extravío de expedientes y/o gestiones.	Pérdida voluntaria o involuntaria de información del cliente por mala custodia de los archivos o dolo. Las repercusiones pueden ser de tipo económico en caso de incumplimiento de pago del tarjetahabiente o legal en el caso de revisión por parte del ente supervisor. **Recomendación:** Establecimiento de responsables directos de la custodia de expedientes, reporte de gestiones operadas para cotejar el traslado de información a sus carpetas.	BAJO Por la ocurrencia poco probable.

Cobranza

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Inapropiada gestión de cobranza.	Metodología de cobro inapropiada o de mala calidad, derivando poca recuperación de la cartera en dificultades o mala imagen de la institución (si los métodos no son indicados). **Recomendación.** Capacitación constante del personal que realiza esta actividad y control de calidad sobre la metodología de cobro empleada.	BAJO Por la ocurrencia poco probable.

Registro Contable.

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Errores y/o fraudes contables.	Negligencia, incompetencia o dolo por parte del personal que realiza el registro contable de las operaciones ocurridas en el área o departamento. Este evento puede generar reparos por parte del ente supervisor o fiscalizador, así como información no fiable. **Recomendación:** Niveles de autorización de los registros contables, integración de saldos contables, análisis de impacto de los errores o análisis de situaciones fraudulentas.	MEDIO Por el impacto que pueden generar.
Informes incorrectos o alterados.	Negligencia, incompetencia o dolo por parte del personal que presenta informes de gestión, comerciales o de resultados del área. **Recomendación:** Revisión o comprobación de cifras en reportes informáticos.	BAJO Por la ocurrencia poco probable.
Error en estimaciones contables.	Representa la posibilidad de ejecución presupuestaria incorrecta, situación que afectaría los resultados esperados por la entidad. Representa mayor importancia si no se consideran pagos como el derecho de uso de la marca que respalda la tarjeta, gastos por concepto de puntos o bonificación a los clientes.	MEDIO Por el impacto que pueden generar.

4.1.2 **Por categoría de riesgo:**

Existen otros riesgos que no pueden delimitarse a un procedimiento en especial o que no corresponden directamente al área de tarjeta de crédito, pero no son menos importantes que los descritos en el apartado anterior, o bien, tienen estrecha relación con el tema; estos son:

CUADRO 6

IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS POR CATEGORÍA DE RIESGO

Fraude Interno

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Robo de información o venta de bases de datos.	Fraude interno conocido también como piratería industrial, sus consecuencias son la pérdida de clientes importantes o prácticas de competencia desleales. **Recomendación:** Control de seguridad en los sistemas que detecten la extracción de información, apropiada selección del personal que administra información.	MEDIO Por la ocurrencia poco probable.
Colusión y funcionarios infieles.	Puede presentarse en todas las actividades del área, provocando pérdidas por beneficios otorgados a clientes de manera indebida. **Recomendación:** Apropiada selección del personal, monitoreo de operaciones inusuales, generación de reportes informáticos.	MEDIO Por el impacto que pueden generar
Sabotaje.	El impacto puede ocurrir en los equipos y sistemas informáticos necesarios para la autorización y administración de las operaciones con tarjetas de crédito. **Recomendación**: Restricción a personal exclusivo al área de equipos computarizados o áreas de seguridad.	ALTO Por el impacto que pueden generar

Fraude externo

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Comprobantes falsos o duplicación de cargos por el comercio.	Riesgo fuera del alcance de control por parte del emisor, pero que puede generar pérdidas a los clientes o al mismo banco por transacciones inexistentes. **Recomendación:** Apoyarse en los adquirientes para sancionar a los comercios fraudulentos.	BAJO Por la ocurrencia poco probable.
Fraude en cajeros automáticos.	Apropiación de las tarjetas en los cajeros automáticos de manera indebida o por medio de engaños, provocando pérdidas a los tarjetahabientes por uso de la tarjeta por terceros. **Recomendación:** Altos niveles de monitoreo electrónico de autorizaciones, confirmación de operaciones con el tarjetahabiente, recomendaciones de seguridad a los clientes.	**ALTO** Por la frecuente ocurrencia
Lavado de dinero o financiamiento al terrorismo.	Utilización de las tarjetas para ocultar el origen de los fondos o para financiar actividades terroristas. Las consecuencias son de tipo de perdida de reputación o implicaciones legales, en caso se compruebe negligencia o dolo por parte del emisor. **Recomendación:** Monitoreo de transacciones inusuales, reporte de operaciones sospechosas, análisis de comportamiento de uso de la tarjeta por el cliente.	MEDIO Por el tipo de producto financiero.

Relaciones laborales y de seguridad en el trabajo.

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Accidentes laborales	Caídas, contagio de enfermedades virales. Las consecuencias son la indisponibilidad del recurso, los reembolsos que deban realizar el banco o demandas en caso de accidentes. **Recomendaciones:** Revisión del medio en donde se desarrollan las actividades para prevenir accidentes, políticas de seguridad física, prestaciones laborales.	BAJO Por la ocurrencia poco probable.
Demandas laborales	Ocurre por el incumplimiento de las leyes laborales en perjuicio de los empleados. Las pérdidas que puede ocasionar son las compensaciones económicas, indemnizaciones, etc. **Recomendación:** Velar por el estricto cumplimiento de la normativa laboral, mantenimiento de provisiones o fondos para compensaciones e indemnizaciones laborales.	MEDIO Por el impacto que pueden generar

Clientes, productos y prácticas empresariales

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Productos mal diseñados o defectuosos	Requerimiento de tarjetas al proveedor con errores en el arte (direcciones, teléfonos de emergencia), fallas en el programa de personalización de tarjetas. **Recomendación:** Control de calidad en la producción de nuevos productos.	BAJO Por la ocurrencia poco probable.

Daños a activos materiales.

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Catástrofes o siniestros.	Ocurrencia de fenómenos naturales o sociales, ejemplo: inundaciones, terremotos, incendios manifestaciones, huelgas, bloqueo de carreteras, etc. Los cuales afectan la prestación de servicios o continuidad del negocio. **Recomendación:** Planes de contingencia para garantizar la continuidad del servicio.	MEDIO Por el impacto que pueden generar

Ejecución, entrega y gestión de procesos.

Riesgo	Descripción del origen, consecuencia y recomendación	Impacto
Errores de cualquier índole.	Por la posibilidad de ocurrencia en las diversas actividades del área o departamento de tarjeta, representan una fuente de riesgo operacional que puede ocasionar pérdidas económicas o de imagen por el servicio prestado. **Recomendación:** Revisión de las actividades que se desarrollen en el área, generación de reporte de operaciones efectuadas, análisis selectivo de operaciones realizadas.	MEDIO Por la frecuente ocurrencia.

Accesos no autorizados a sistemas o lugares de máxima seguridad.	Usurpación de claves o de personas no autorizadas a lugares considerados de máxima seguridad, como la bóveda donde se guardan los plásticos sin utilizar, elevando la posibilidad de ocurrencia de fraudes por autorizaciones no existentes o robo de tarjetas. **Recomendación:** Establecer controles de acceso a los sistemas informáticos, bloqueo de usuarios con cierto número de intentos fallidos, código de acceso rotativos en la bóveda de tarjetas.	MEDIO Por el impacto que pueden generar
Tercerización (Outsourcing)	Siendo responsabilidad del banco emisor los riesgos operativos provenientes de actividades transferidas a un ente externo, existe la posibilidad de ocurrencia de eventos desfavorables, en el caso de los contratos externos para realizar: Procesamiento de transacciones, personalización de tarjetas, cobranza, entrega de tarjetas y estados de cuenta **Recomendación:** Revisar manuales de procedimientos de la empresa subcontratada, establecer planes de contingencia para garantizar el servicio, incluir cláusulas de resarcimiento para el banco en caso de incumplimiento.	**ALTO** Por el impacto que pueden generar

4.2 Monitoreo y comunicación.

Esta fase de administración del riesgo operativo, comprende la función de mantener control sobre las actividades desarrolladas en el área y designar responsables de observar el cumplimiento de las normas establecidas interna o externamente, así como de informar a los órganos correspondientes sobre los hallazgos y reportes de gestión, para que sean éstos los que definan las directrices de control o mitigación. Para el efecto, los responsables del monitoreo deberían considerar lo siguiente:

- Definición de parámetros de control sobre las principales operaciones realizadas por los tarjetahabientes, enfocando la atención hacia las tendencias de fraude que imperen en el sector. De igual forma, sobre las transacciones internas que representen mayor exposición a cometer fraudes internos, tales como: reembolsos, modificaciones de límites, extornos, etc.

- Participar conjuntamente con los responsables de modelar y lanzar nuevas tarjetas al mercado, velando porque existan los mecanismos de control necesarios, pruebas de funcionalidad, cumplimiento de normas externas aplicables, etc.
- Revisar los planes periódicos de capacitación del personal del área, así como analizar la rotación del mismo, velando porque no exista desconocimiento de las funciones y responsabilidades que conlleva el cambio.
- Analizar fuentes externas de riesgo que puedan afectar a la entidad.
- Actualizar la normativa interna aplicable al área de tarjetas, con la finalidad de mantener informado al personal de los cambios que se vayan presentando.

4.2.1 Sistemas informáticos para realizar el monitoreo.

Existe una variedad de sistemas informáticos (software) que ofrecen la funcionalidad de controlar o detectar operaciones que a criterio de cada entidad puedan considerarse de riesgo o inusuales. Por razones de derecho de propiedad intelectual no se mencionan los nombres de los proveedores y de los programas utilizados, pero puede resumirse que ofrecen en mayor o menor escala, las generalidades siguientes:

- Parámetros modificables de control sobre la autorización de operaciones con tarjetas de crédito y sobre las operaciones realizadas por los usuarios internos del sistema.
- Registros de comportamiento por tarjeta, situación que reduce el análisis de riesgo.
- Información a los responsables de monitoreo en tiempo real.
- Compatibilidad con los diversos sistemas utilizados en la entidad.
- Registros históricos de las transacciones analizadas.

4.2.2 Comité de seguridad de emisores de tarjetas.

En nuestro país existe la Gremial de Emisores de tarjetas de crédito, órgano integrado por los responsables de tarjetas de cada entidad emisora (bancaria y no bancaria). Dicho ente, define las políticas comerciales del sector. Así mismo, pertenece a este órgano el comité de seguridad de

emisores, el cual está integrado por los responsables de administración de riesgos con tarjetas de cada entidad y tiene por finalidad velar por el control de fraudes externos cometidos con este medio de pago. Corresponde entre otras, a dicho comité las funciones de monitoreo siguientes:

- Establecer políticas de seguridad comunes en cada entidad.
- Compartir información sobre los principales riesgos que afectan el sector.
- Establecer mecanismos de identificación de comercios fraudulentos y aplicar medidas correctivas al respecto.
- Actualizar a sus miembros en materia de reporte de fraudes.
- Coordinación con los adquirientes nacionales en prevención de fraudes y reclamo de consumos fraudulentos.
- Coordinar las investigaciones para determinar la participación de empleados o comercios involucrados en fraudes.

4.3 Control y mitigación.

Esta tercera etapa comprende el establecimiento de medidas que coadyuven a la reducción o minimización de ocurrencia de los riesgos identificados y evaluados en la primera fase; apoyándose en el monitoreo realizado. Deben establecerse los mecanismos de mitigación que de acuerdo a las políticas de la entidad o conforme el método seleccionado para el cálculo de requerimientos de capital, sea el más apropiado en el área de tarjetas.

En esta etapa, el control interno del área sujeta de estudio, debe revisarse y adecuarse a los objetivos de la entidad en los tres ámbitos siguientes: efectividad y eficiencia operacional, confiabilidad de la información financiera y cumplimiento de políticas, leyes y normas.

4.3.1 Control Interno en el área de tarjetas de crédito. (26:1-8 y 8:5-7)

Siendo el control interno la base a considerar en el administración del riesgo operativo en el área de tarjetas y conscientes del enfoque actual que ofrece seguir los lineamientos del informe COSO y el marco para la evaluación de sistemas de control interno emitido por Comité de Basilea, a

continuación se definen cada uno de esos elementos, para establecer los mecanismos necesarios de control:

4.3.1.1 Ambiente de control.

Se refiere al conjunto de circunstancias que enmarcan el accionar de la entidad y son el reflejo de la actitud asumida por la alta dirección y gerencia con relación a la importancia de los controles para lograr los objetivos del área de tarjetas. Los factores del ambiente de control, son los siguientes:

- La filosofía de alta dirección y gerencia. Lineamientos generales en materia comercial y operativa de la alta gerencia respecto a la comercialización y funcionamiento del producto tarjeta de crédito.
- La estructura, el plan organizacional, los reglamentos y manuales de procedimientos. Comprende la planeación estratégica comercial, las metas de ventas, el reglamento de ética y los manuales de procedimientos aplicables al área, mismos que delimitan las acciones en cada uno de los procesos a desarrollar, definen responsables directos y norman los niveles de autorización necesarios para la salvaguarda.
- La integridad, los valores éticos, la competencia profesional, y el compromiso de todos los empleados del área, así como su adhesión a las políticas y normas establecidas por la alta dirección y gerencia.
- La asignación de responsabilidad al personal. Delimitar actividades o roles al personal de acuerdo al grado de integridad observado.

4.3.1.2 Actividades de control.

Las constituyen los procedimientos establecidos como un reaseguro para el cumplimiento de los objetivos, orientados primordialmente a la prevención de riesgos. Se deben ejecutar en todos los procesos desarrollados en el área, partiendo de la elaboración de un mapa de riesgos, pues al conocerlos se disponen los controles destinados a evitarlos o minimizarlos. El establecimiento de actividades de control no garantiza la eliminación de riesgos, pero si los reduce considerablemente. A continuación se describen las principales actividades de control que pueden establecerse en el área:

- Análisis efectuados por la dirección, en los cuales se definan las prioridades del área, revisión de los informes de gestión, cobranza, etc.
- Seguimiento y revisión por parte de los responsables de las diversas funciones o actividades. Por ejemplo: informe de operaciones diarias en el área, pago a los adquirentes por las operaciones autorizadas, ejecución de procesos automatizado de cobro y cálculo de intereses financieros, etc.
- Comprobación de las transacciones en cuanto a su exactitud, totalidad, y autorización pertinente: aprobaciones, revisiones, cotejos, recálculos, análisis de consistencia, prenumeraciones. Por ejemplo: Autorización de cambios en las bases de datos, extorno de intereses y cargos a los tarjetahabientes, registro contable del área, envío oportuno de estados de cuenta, canje de puntos o beneficios.
- Controles físicos patrimoniales: arqueos, conciliaciones, recuentos. Por ejemplo: revisión de formas en blanco, tarjetas sin utilizar, integración de saldos a favor de los clientes, integración de puntos o beneficios otorgados.
- Dispositivos de seguridad para restringir el acceso a los activos y registros. Corresponde a esta actividad de control y revisión de las bóvedas utilizadas para la custodia de los expedientes de los clientes, las formas en blanco, las tarjetas a utilizar para la personalización y las claves de acceso a los sistemas de administración de tarjetas.
- Segregación de funciones. Al evitar que los aspectos fundamentales de una transacción u operación queden concentrados en una misma persona, se reduce notoriamente el riesgo de errores, despilfarros o actos ilícitos, y aumenta la probabilidad que, de producirse, sean detectados.
- Aplicación de indicadores del desempeño. La importancia de contar con indicadores del desempeño en el área de tarjetas, radica en que la información obtenida podrá utilizarse para la corrección del curso de acción y el mejoramiento del rendimiento a futuro.

Para la aplicación de las actividades de control, deben considerase las normas que les corresponden, siendo estas: Separación de tareas y responsabilidades, coordinación entre tareas, documentación competente, niveles definidos de autorización, registro oportuno y adecuado de las transacciones, acceso restringido a los recursos y activos, rotación del personal en tareas clave, control del sistema de información, control de la tecnología de información.

4.3.1.3 Supervisión.

El objetivo es asegurar que el control interno funcione adecuadamente en el área, a través de dos modalidades: actividades continuas o evaluaciones puntuales. Las primeras conviven directamente con las actividades normales y se ejecutan en el mismo momento de ocurrencia (ejemplo: alertas de operaciones con tarjetas en tiempo real); mientras que las segundas que definen considerando los riesgos que conllevan las actividades y son ejecutados por el personal responsable de supervisión como auditoría interna (ejemplo: revisión del cumplimiento normativo para los expedientes de los tarjetahabientes).

4.3.1.4 Información y comunicación.

Para que el control interno en el área de tarjetas sea funcional, es imprescindible que exista información sobre los indicadores de riesgo, resultados de las actividades de control, indicadores de desempeño del personal, logro de metas y objetivos, etc. Esta información debe trasladarse a cada uno de los integrantes del área para que puedan comprender la importancia del control y que no sea visto como una carga operativa o burocracia en las operaciones, sino como un elemento que apoya el logro de los objetivos.

4.4 Mecanismos de mitigación de riesgo operativo.

Definidas las acciones tendientes a controlar el riesgo, se deben establecer los mecanismos que mitiguen o reduzcan la ocurrencia de aquellos con mayor frecuencia o de alto impacto. Entre las actividades que pueden realizarse para cumplir este fin, se encuentran:

4.4.1 Planes de recuperación o contingencia.

Es recomendable identificar los principales procesos críticos a los cuales se deben establecer planes de recuperación acordes al tamaño y complejidad de las operaciones del área, siendo estas:

- Autorización electrónica de transacciones. Contar con los planes que garanticen su continuidad en caso existan contingencias con los servidores, fallas de comunicación o caídas del sistema. Para el efecto pueden considerarse la contratación de empresas proveedoras de servicios de comunicación alternas a las usualmente empleadas, replicación de los sistemas en otro centro de cómputo, backup de las bases de datos, etc.
- Personalización de tarjetas. En caso ocurran fallas de los equipos utilizados para la personalización, no puede detenerse el proceso por la implicaciones comerciales que representa. Para el efecto debe existir técnicos especializados en la solución de problemas con el equipo (internos o externos) o subcontratar los servicios de empresas que realizan esta actividad, como segunda alternativa.
- Desastres naturales o siniestros. La ocurrencia de fenómenos fuera de los controles humanos o siniestros provocados, pueden ocasionar pérdidas del equipo, información, expedientes, interrupción de servicios, etc. Por ello los planes de contingencia deben considerar medidas de seguridad física como extinguidores, salidas de emergencia para el personal, simulacros de desastres, backup periódico de la información vulnerable; que garantice la continuidad del servicio.
- Huelga o incumplimiento de funciones del personal de ventas. Debido a la importancia de la actividad de comercialización, la potencial ocurrencia de huelgas u otras causas no deben impedir continuar con esta función. Para el efecto, puede contratarse el servicio de equipos externos especializados en ventas, efectuar reuniones periódicas con el personal para determinar si existen inconformidades, entre otros.

4.4.2 Pólizas de seguro.

La opción de contratar pólizas de seguro para la mitigación del riesgo operacional es viable, bajo determinadas circunstancias. En el caso de las operaciones con tarjetas que pueden salvaguardarse mediante la contratación de seguros, están:

- Fraudes externos por operaciones no efectuadas por los tarjetahabientes. Esta cobertura es la más utilizada por los emisores, debido a la alta ocurrencia de siniestros. Para el reclamo de siniestros por parte del emisor ante la aseguradora se establecen una serie de condiciones para hacer efectivo el reembolso, tales como: denuncia a las autoridades de seguridad del país, pruebas de ocurrencia y de la inocencia del tarjetahabiente.
- Equipo y sistemas informáticos (hardware y software). A causa de la importancia que representan y el valor de reemplazo, es usual el aseguramiento de los mismos para garantizar su sustitución en caso ocurra un siniestro.
- Personal del área. El recurso humano por su parte, también puede estar protegido por seguros que disminuyan la responsabilidad para el banco emisor en caso ocurran eventos que puedan afectarlo. Las pólizas más comunes son las de vida y gastos médicos.

4.4.3 Provisiones.

Otra manera interna de mitigar la ocurrencia de riesgos es la creación de fondos o provisiones que respalden a la entidad en caso ocurran eventos desfavorables como los citados en el caso de los seguros. Esta medida ofrece la ventaja de ser financieramente más económica que la contratación de seguros, pero su debilidad radica en la ocurrencia de riesgos de alta magnitud que no puedan ser cubiertos con los montos acumulados.

4.4.4 Tercerización / subcontratación de servicios (Outsourcing).

Considerada también un riesgo operativo, esta opción ofrece a las entidades emisoras de tarjetas, una forma de mitigar los riesgos por las razones siguientes: especialización de tareas encomendadas, logística interna fuerte y contratos que delimitan las responsabilidades de ambas partes en caso

ocurran riesgos operacionales. En caso se opte por esta modalidad de mitigación, el banco emisor debe considerar la responsabilidad que le compete ante el ente supervisor en caso no se consideren todos los factores que puedan generar riesgos operativos.

4.5 Función de Auditoría Interna, para el control del riesgo operativo.

En concordancia con el principio dos de las mejores prácticas para la administración de riesgos operativos emitida por el Comité de Basilea, compete a la Auditoría Interna velar porque dicha administración se lleve a cabo de la manera que mejor logre el apego a las medidas de control interno existente (salvaguardar los activos y apego a las normas establecidas en la entidad por la alta dirección), considerando que tal responsabilidad recae en un comité específico o a su propio cargo si fuese el caso; para el efecto se deberán considerar los aspectos siguientes:

- Seguimiento de las medidas adoptadas por el comité de riesgo operativo –si existiera- para la identificación y evaluación de riesgos operativos por áreas.
- Evaluación y certificación de las herramientas utilizadas para la identificación y evaluación de riesgos operativos.
- Cumplimiento de responsabilidades y roles a cargo de los responsables del análisis de riesgos en la entidad.
- Monitoreo de avances y logros obtenidos por el ente responsable de administración de riesgos operativos.
- Brindar continuidad a los casos en donde han sido detectado debilidades en los procesos para salvaguardar los intereses de la entidad.
- Efectuar pruebas a los análisis presentados por los responsables de administrar el riesgo operativo para validar la integridad y calidad del trabajo desarrollado.
- Emitir informes al Consejo de Administración en los casos que requieran notificar sobre avances, deficiencias y obtención de objetivos a cargo del grupo responsable de administrar el riesgo en la entidad.

Además, este principio reconoce la función que desarrolla la auditoría interna para el control integral de riesgo en caso no se cuente con la estructura organizativa para desarrollar esta actividad en la entidad, lo cual provocaría que tal función recaiga en la auditoría interna (aplica en la mayoría de los casos en entidades pequeñas o de reciente incursión en la medición de riesgos), para el efecto ésta debe ser desarrollada por personal competente y con la preparación técnica apropiada, siguiendo los aspectos que se describen a continuación:

4.5.1 Objetivos y funciones de Auditoría Interna, relacionadas con el riesgo operativo.(6: 2-3)

Acerca de la función de Autoría Interna, existe una normativa emitida por el Comité de Basilea (Rol de la auditoría interna y externa en la medición de riesgos) que establece las directrices sobre las cuales debe realizar su labor, siendo éstas:

- Velar porque el sistema de control interno emitido por el directorio y la alta gerencia, contengan variables de medición y valorización de riesgo operativo en cada una de las tareas que se desarrollen; que existan métodos de monitoreo apropiados al tamaño y complejidad de las operaciones del área, evaluando que las actividades de control definidas por el directorio, sean entendibles, efectivas y funcionales, así como, existan mecanismos de control sobre las operaciones más vulnerables a riesgos.
- Apoyar a la alta gerencia para que, en los informes que ésta presente al directorio, puedan apreciarse los avances del funcionamiento del control interno vigente, así como los riesgos identificados, los mecanismos de control y mitigación establecidos.
- Ser parte del monitoreo de riesgo operativo y coadyuvar en la responsabilidad del directorio y la alta gerencia en la responsabilidad de administración de riesgos. Para llevar a cabo esta función debe analizar y revisar los siguientes aspectos: sistemas de control interno establecidos, metodología de administración de riesgos, sistemas de información electrónica, salvaguarda de activos, medición del capital y su relación con el riesgo operativo, eficiencia de las operaciones, cumplimiento de leyes y regulaciones, códigos de conducta de los empleados e investigaciones especiales.

4.5.2 Normas de auditoría interna, para la administración de riesgos. (32:14)

Por su parte, El Instituto de Auditores Internos (IIA por sus siglas en inglés) contempla una serie de normas aplicables para la administración de riesgos, incluido el operativo. Al respecto, pueden citarse las siguientes:

- Planificación de la auditoría (Norma 2010). Esta norma define la responsabilidad del director ejecutivo o jefe de auditoría para establecer planes de trabajo basados en la identificación de riesgos, con el objetivo de priorizar las actividades a desarrollar, considerando las recomendaciones del directorio y la alta gerencia.
- Gestión y control de riesgos (Normas 2110 y 2120). Estas normas establecen la forma en que debe apoyar el mantenimiento de la efectividad de los controles del área auditada, sin perder congruencia con los objetivos de la entidad; debiendo para el efecto evaluar lo siguiente:
    - Eficiencia de las operaciones. Sugerir o mejorar los procesos del área evaluada.
    - Protección de los activos.
    - Cumplimiento de leyes, regulaciones y contratos.

4.5.3 Planeación y trabajo de auditoría interna, en el área de tarjetas. (32:15)

Compete a la Auditoría Interna la revisión y supervisión del cumplimiento de las medidas de control y mitigación implantadas en cada área de la entidad, incluida tarjeta de crédito. Para el efecto, se describen las actividades que de acuerdo a las normas internacionales de Auditoría Interna, debieran considerarse.

4.5.3.1. Planificación del trabajo.

Comprende la planeación de las funciones, recursos necesarios y responsables de llevar a cabo el trabajo. Para el efecto, el encargo de la auditoría debe considerar los aspectos siguientes:

- Los objetivos del proceso a revisar y los medios con los que se desarrolla. Debe considerarse el cumplimiento de las políticas y normas comerciales, operativas, contables y de cobranza de la tarjeta. Revisión de la funcionalidad de los equipos y programas informáticos utilizados

para el desarrollo de las actividades, reportes utilizados, capacidad del personal que realiza actividades clave, etc.

- Identificar y analizar los riesgos significativos de cada actividad y los medios con los que se mantienen en un nivel de aceptación.
- Oportunidad de introducir mejoras en los sistemas de gestión de riesgos y control de las actividades del área.

4.5.3.2 Objetivos del trabajo.

El objetivo principal del trabajo de auditoría interna es enfocarse a los procesos que presenten mayor exposición a riesgos y controles deficientes. Para el efecto, en la fase de planificación se identifican tales procesos críticos.

4.5.3.3 Alcance del trabajo.

Comprende el campo de acción hasta donde debe extenderse el trabajo de auditoría, por lo cual debe ser suficiente para satisfacer los objetivos planeados, tener en cuenta los sistemas, registros, personal y propiedades físicas relevantes, incluso bajo el control de terceros. Pueden considerarse las actividades siguientes:

- Revisión de la funcionalidad e integridad de los sistemas informáticos utilizados para la autorización de transacciones y para la administración de la base de cuentas.
- Revisión de los procedimientos, controles y actualizaciones sobre: los expedientes de los clientes, registros contables y relación con proveedores de servicios.
- Entrevistas con el personal clave en el área de tarjetas, para comprobar los controles implementados según procedimientos y los efectivamente empleados.
- Revisión de funcionalidad y capacidad de los equipos utilizados para la personalización de tarjetas, equipo de cómputo del personal y servidores.
- Visita a las empresas subcontratadas por el banco para la prestación de algún servicio relacionado con el área sujeta de revisión (mensajería, personalización de tarjetas, cobranza,

comercialización), para comprobar la competencia, calidad del servicio y planes de contingencia; que garanticen baja exposición a riesgo operativo.

4.5.3.4 Programa de trabajo.

Es el documento en que se plasman con el grado de detalle necesario, las actividades que debe efectuar el personal de auditoría para el cumplimiento de los objetivos. Deben establecer los procedimientos para identificar, analizar, evaluar y registrar información durante el desarrollo de las tareas.

4.5.3.5 Desarrollo del trabajo.

Esta fase comprende el trabajo de campo, siguiendo los lineamientos establecidos en el programa y en el que se debe analizar, evaluar y registrar toda la información que coadyuve a lograr los objetivos planeados en materia de control de riesgo operativo. Los procesos que deberían realizarse, son:

- Identificación de la información. Los auditores deben identificar información suficiente, confiable, relevante y útil de manera que les permita evaluar apropiadamente los riesgos operativos del área.
- Análisis y evaluación. Contando con la información suficiente y competente, deben analizar y evaluar de acuerdo al mecanismo que mejor se adapte (ejemplo: autoevaluaciones) la exposición a riesgos operativos en el área.

4.6 **Reglamentación internacional sobre manejo de riesgo con tarjetas de crédito VISA** (11:2-5)

La administración de riesgos es una preocupación que comparten las entidades que respaldan la emisión de tarjetas. En ese contexto, se ofrecen varias herramientas de apoyo a la seguridad y para la prevención de riesgos, tales como: Servicio de boletín de tarjetas canceladas, archivo de excepción, verificación de PIN y el servicio de identificación de riesgos.

Por otra parte, el manual “Account Information Security Standards” establece la responsabilidad del emisor para efectuar una investigación de casos de fraude de cualquier índole, pudiéndose apoyar en

el trabajo realizado por otros emisores, además de estar facultado para entrevistar comercios y tarjetahabientes sospechosos; testigos y representantes de la ley, recuperar tarjetas robadas, perdidas o falsificadas; proveer información a las autoridades para el posible arresto de sospechosos, etc.

De ocurrir deficiencias de control y cumplimiento de la regulación establecida el banco emisor puede ser sujeto de multas que van desde USD$500 hasta USD$25,000 dependiendo de la magnitud de la falta.

En cuanto a la prevención de lavado de activos y el financiamiento al terrorismo se establece que de manera congruente con los requisitos legales y reglamentarios aplicables a cada miembro, se deben implementar y mantener un programa que esté diseñado razonablemente para evitar que sean utilizados para facilitar el lavado o financiamiento de actividades terroristas. El incumplimiento de normas que garanticen la calidad del control contra ese delito, puede provocar desde multas, hasta la cancelación de la licencia al banco emisor. Por su parte la legislación guatemalteca establece en la Ley Contra el Lavado de Dinero u Otros Activos sanciones monetarias que oscilan entre los USD$10mil hasta USD$25mil por el incumplimiento de prevención del delito de lavado de activos.

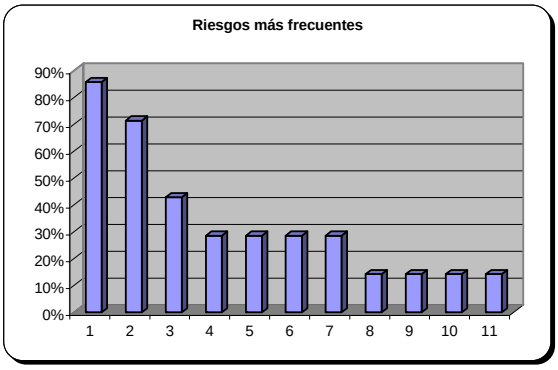
4.7 Administración de riesgo operativo en bancos emisores de tarjetas de crédito en Guatemala.

Como parte del desarrollo del presente trabajo, se realizó una encuesta a los emisores de tarjetas de crédito del medio bancario guatemalteco, para conocer entre otros temas los siguientes: Los riesgos a los cuales presentan mayor exposición, medidas de control y mitigación del riesgo por fraude, responsabilidad de control, conocimiento sobre riesgo operativo en la entidad y existencia de un área especializada en la identificación y evaluación del riesgo. Los resultados se presentan a continuación:

CUADRO No. 7

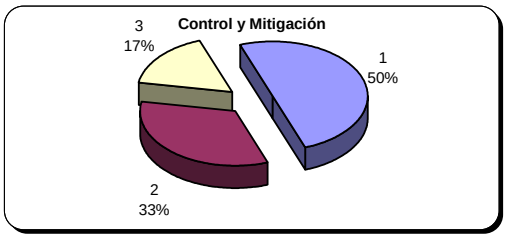
RESULTADO DE LA ENCUESTA A EMISORES BANCARIOS SOBRE EL TEMA DE RIESGO OPERATIVO

No 1	Riesgos más frecuentes	% Bancos
1	Tarjetas robadas	86%
2	Skimming	71%
3	Interrupción de sistemas	43%
4	Fraude en ATMs	29%
5	Fraude en solicitudes	29%
6	Incumplimiento de normas	29%
7	Mal ingreso de datos al sistema	29%
8	Aumentos no autorizados	14%
9	Expedientes incompletos	14%
10	Tarjetas mal diseñadas	14%
11	Desastres naturales	14%
12	Duplicaciòn de cobro en comercios	0%
13	Robo de plásticos por el personal	0%
14	Robo de base de datos	0%
15	Errores contables	0%



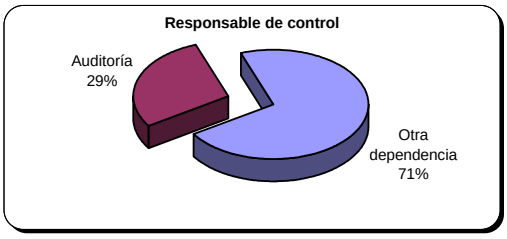
Fuente: Encuesta realizada a 6 entidades bancarias nacionales. Sep-06.

No 2	Opciones de control y mitigación de pérdidas	% Bancos
1	Monitoreo de transacciones	86%
2	Provisiones internas	57%
3	Contratación de seguros	29%



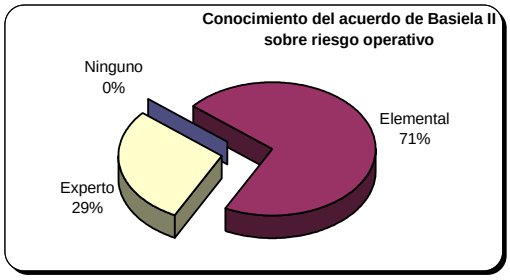
Fuente: Encuesta realizada a 6 entidades bancarias nacionales. Sep-06.

No 3	Recae en la auditoria el control de fraudes con tarjetas en su entidad	% Bancos
	Otra dependencia	71%
	Auditoría	29%
	Dependencia de Riesgo operativo (44, 15, 19 y 31)	57%
	Depto de Tarjeta de crédito	43%



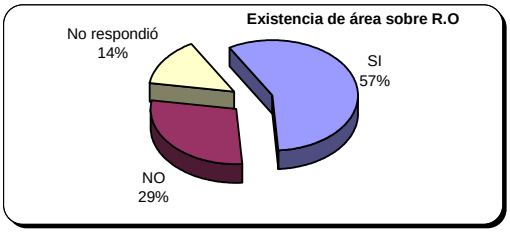
Fuente: Encuesta realizada a 6 entidades bancarias nacionales. Sep-06.

No 4	Conocimiento sobre implicaciones de entrada en vigencia del Acuerdo de Basilea II, respecto a R.O	% Bancos
	Ninguno	0%
	Elemental	71%
	Experto	29%



Fuente: Encuesta realizada a 6 entidades bancarias nacionales. Sep-06.

No 5	Existe área responsable de riesgo operativo.	% Bancos
	SI	57%
	NO	29%
	No respondió	14%



Fuente: Encuesta realizada a 6 entidades bancarias nacionales. Sep-06.

Análisis: Ante los resultados obtenidos producto de la encuesta realizada a un grupo de emisores bancarios, se concluyó que existen varias actividades que esas entidades deben monitorear, evaluar, revisar o en su defecto crear, entre las que destacan las siguientes:

- Reforzar o crear un ente especializado en la administración de riesgo operativo.
- Incrementar los conocimientos respecto al riesgo operativo conforme lo establecido por el Comité de Basilea II.
- Establecer planes de contingencia y medidas de mitigación como el caso de la contratación de pólizas de seguro contra fraudes y eventos externos.
- Definir parámetros de monitoreo acordes al nivel transaccional de la entidad y priorizar los que mitiguen riesgos de mayor frecuencia como por ejemplo: el robo y clonación de tarjetas.

ÍNDICE CASO PRÁCTICO:

"CONTROL DE RIESGO OPERATIVO EN EL ÁREA DE TARJETAS DE CRÉDITO SEGMENTO ORO, DEL BANCO PRIVADO GOLDBANK, SOCIEDAD ANÓNIMA"

CAPÍTULO V
CASO PRÁCTICO

"CONTROL DE RIESGO OPERATIVO EN EL ÁREA DE TARJETAS DE CRÉDITO SEGMENTO ORO, DEL BANCO PRIVADO GOLDBANK, SOCIEDAD ANÓNIMA"

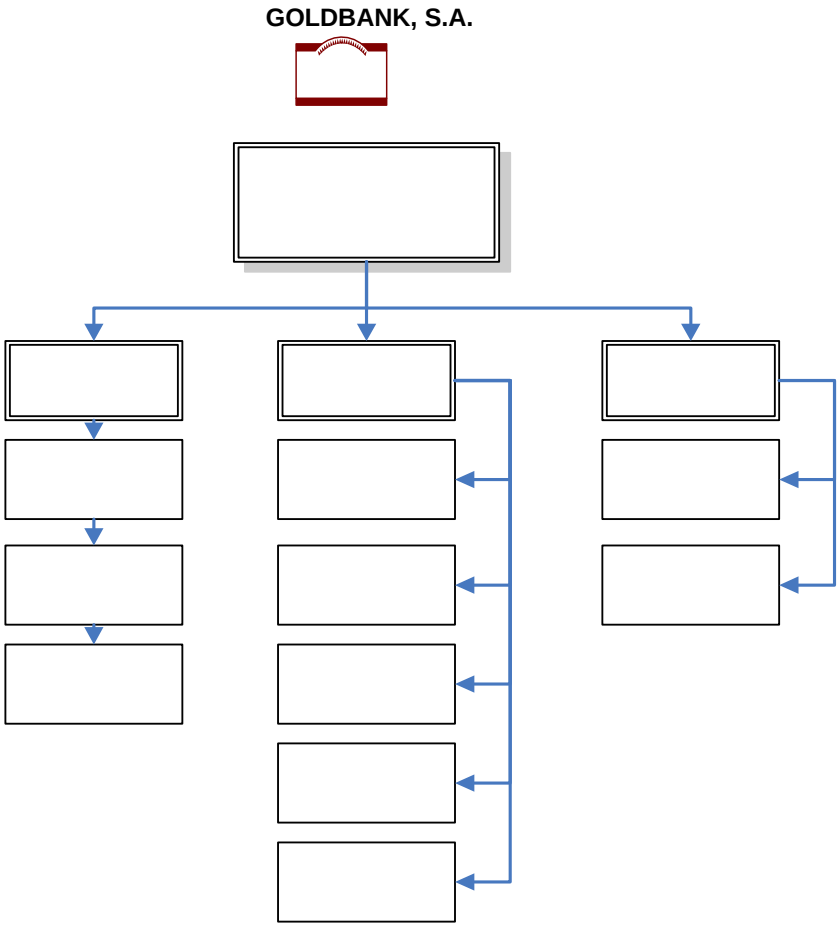
Como un aporte al trabajo de investigación, el presente capítulo aborda de manera práctica la identificación, cuantificación, controles internos a implementar y medidas de mitigación que pueden considerarse para la administración del riesgo operativo en las transacciones con tarjetas de crédito tipo: ORO en una entidad bancaria privada nacional –ficticia- denominada Goldbank S.A.

5.1 Análisis del área de tarjetas del Banco "GOLDBANK, S.A."

Conscientes de la importancia de administrar el riesgo operativo en el área de tarjeta de crédito en especial para el segmento de tarjetas ORO, el Banco GoldBank, S.A. integró un equipo de trabajo para velar por el cumplimiento del control de riesgos en la citada dependencia. Para el efecto, presenta la estructura organizativa que posee la gerencia de tarjeta de crédito, políticas y procedimientos establecidos para el cumplimiento comercial y operativo del área sobre los cuales el grupo responsable deberá efectuar un diagnóstico respecto de los potenciales riesgos existentes y sugerir medidas para prevenirlos y mitigarlos.

5.1.1 Organigrama de la gerencia de tarjeta de crédito.

GOLDBANK, S.A				
ORGANIGRAMA DEL AREA DE TARJETAS		**PT**	RO-01	
AREA DE TARJETA DE CREDITO	**Hecho por**		J.I.G.V	05-11-200X
PERIODO REVISADO: Enero a Diciembre 200X	**Revisado por**		E.L.M.R	15-11-200X



Nota: La estructura sugerida en este ejemplo sólo corresponde a una propuesta del esquema organizativo de una Gerencia de Tarjeta de Crédito de un banco privado, sin embargo; ésta puede integrarse a conveniencia de cada Entidad. Es importante hacer hincapié en el papel de la Auditoría Interna como departamento Staff, necesario para el logro de objetivos de control.

5.1.2 Políticas y requisitos para el otorgamiento de tarjetas de crédito Oro.

Para el otorgamiento de tarjetas de crédito, la entidad ha definido una serie de políticas, algunas de carácter interno que han sido analizadas de acuerdo a las condiciones de mercado o conveniencia de la institución y otras establecidas en la normativa vigente que rige los lineamientos sobre riesgo crediticio.

GOLDBANK, S.A
POLITICAS PARA EL OTORGAMIENTO DE TARJETAS **PT** RO-02
AREA DE TARJETA DE CREDITO **Hecho por** J.I.G.V 05-11-200X
PERIODO REVISADO: Enero a Diciembre 200X **Revisado por** E.L.M.R 15-11-200X

GOLDBANK, S.A. **POLÍTICAS CREDITICIAS PARA LA APROBACIÓN DE TARJETAS ORO**
❖ Personas comprendidas entre las edades de 30 a 65 años.
❖ Nivel socioeconómico C1 ó AB
❖ Ingresos personales superiores a Q10mil mensuales.
❖ Propietario de residencia
❖ Nivel de endeudamiento no mayor al 30% del ingreso mensual.
❖ Reciprocidad con el banco a través de otros productos.
❖ Categoría de calificación interna de cliente A o B.
❖ Actividades no considerables: Políticos, policías, pilotos de transporte y militares.
❖ Zonas no considerables: 18 y 03.

GOLDBANK, S.A. **REQUISITOS, PREVIO A OTORGAR TARJETAS ORO**
❖ Completar el formulario IVE – TC – 01 (Véase modelo de este formulario en el anexo No. III)
❖ Presentar copia de cédula de vecindad o pasaporte.
❖ Estado patrimonial o cuadro que muestre los ingresos y egresos del solicitante, con antigüedad no mayor a dos meses.
❖ Copia de recibo de servicios públicos (Teléfono, agua, energía eléctrica).
❖ Estados de cuentas bancarias ó copia de libreta de ahorros con tres meses de antigüedad.
❖ Constancia de trabajo y copia de boletas de pago para solicitantes con relación de dependencia.
❖ Copia de la patente de comercio, en caso de comerciantes individuales.

5.1.3 Descripción de procesos del área de tarjetas de crédito.

GOLDBANK, S.A				
CEDULA NARRATIVA DE PROCESOS		**PT**	RO-03	
AREA DE TARJETA DE CREDITO	**Hecho por**		J.I.G.V	05-11-200X
PERIODO REVISADO: Enero a Diciembre 200X	**Revisado por**		E.L.M.R	15-11-200X

A continuación se describen los principales procesos que se desarrollan desde la comercialización, análisis crediticio, emisión y logística de distribución de tarjetas, hasta la entrega y uso por parte de los tarjetahabientes de las tarjetas Oro emitidas por el Banco Goldbank, S.A.

- Comercialización. Comprende las actividades que desarrolla el personal de ventas de tarjetas de crédito, siendo las principales:
    - Revisión de bases de datos: Análisis de las bases de datos de potenciales clientes que pueden ser sujetos de crédito para una tarjeta de crédito Oro.
    - Telemercadeo: Venta telefónica del producto financiero a los potenciales clientes.
    - Visita a potenciales clientes: Ofrecimiento del producto financiero directamente al potencial cliente, en esta fase se requieren los documentos necesarios para la formalización del crédito.
    - Traslado al área de análisis crediticio.

- Análisis crediticio y emisión de tarjetas.
    - Recepción y verificación de documentos. Verificación del listado de requisitos para el tipo de tarjeta que solicitan, acuse de recibo para el vendedor que corresponda.
    - Confirmación de cumplimiento de políticas. Validación de cumplimiento de las políticas por parte del solicitante.
    - Confirmación de referencias internas y externas. Este proceso conlleva la verificación de referencias personales o comerciales del solicitante, además en éste se realizan las llamadas telefónicas de confirmación de referencias personales consignadas en la solicitud de crédito.

- Análisis crediticio. El proceso comprende el ingreso de los indicadores financieros del solicitante en el programa de scoring empleado por la entidad.
- Aprobación o rechazo de solicitudes. Esta actividad comprende la revisión de los casos por un comité de autorizaciones, quienes se basan en los resultados del programa que pondera los indicadores financieros y la información que complementa la solicitud. De ser autorizada la tarjeta procede la emisión respectiva, caso contrario se devuelve la papelería con las causas del rechazo.
- Emisión de tarjetas. Este proceso consiste en la generación de la nueva tarjeta en el sistema del banco, para el efecto se alimenta la base de datos con la información personal del nuevo cliente y el sistema asigna el número correlativo de tarjeta.
- Archivo de expedientes. Los casos que son aprobados se documentan con las respectivas actas de autorización y se archivan de manera correlativa en función al número de tarjeta que le corresponda.

- Personalización de tarjetas.
  - Recepción y revisión del lote de tarjetas por generar. Consiste en cotejar la orden de generación de plásticos contra el listado de autorizaciones provenientes del área de análisis de créditos.
  - Solicitud de plásticos a utilizar. Para la personalización de las nuevas tarjetas, son requeridos los plásticos de la bóveda de custodia de tarjetas. El control de tal inventario se encuentra a cargo de una persona específica para esa función.
  - Personalización de tarjetas. Este proceso se realiza empleando el equipo de troquelación, mismo que imprime la información del tarjetahabiente (datos personales, número de cuenta, etc.) en la nueva tarjeta de crédito.
  - Distribución de tarjetas personalizadas. El canal de distribución de las tarjetas de crédito se realiza a través de la red de agencias del banco.

- Distribución de tarjetas.
    - Recepción y control de tarjetas. El proceso consiste en contabilizar en una cuenta de registro las nuevas tarjetas que se reciben en cada agencia y acusar de recibido.
    - Entrega y activación de tarjeta. La entrega se realiza validando la identidad del cliente a través de la presentación de un documento de identificación y la activación se efectúa en línea o a través de un centro de atención al cliente.

- Atención de gestiones. La atención de gestiones comprende varios procesos que son necesarios evaluar dentro de las actividades propias de área de tarjetas, siendo estas:
    - Recepción de gestiones. Consiste en la recepción de las diversas gestiones provenientes de las áreas de atención al cliente del banco, velando por el manejo ordenado y acusando de recibido las mismas.
    - Revisión de documentos necesarios. Cada tipo de gestión requiere ciertos documentos de soporte, por ejemplo: copia de cédula o pasaporte, copia de voucher, la misma tarjeta de crédito, etc., para ello el encargado de las gestiones revisa que cada expediente contenga todos los requisitos mínimos.
    - Operación de las gestiones en el sistema.
    - Información de resultados al solicitante. La notificación del resultado de la gestión se realiza vía telefónica a cada cliente de acuerdo a los estándares de servicio definidos en el área.
    - Archivo de gestiones. Concluido el proceso de operación de la gestión, la misma se archiva en el expediente del cliente.

- Registro contable
    - Generación de reporte de transacciones del día, cuentas por pagar y plásticos utilizados. Diariamente son generados varios reportes que detallan las transacciones del área de tarjeta de las cuales los más importantes son: el detalle de operaciones realizadas con las tarjetas del día anterior tanto en comercios como cajeros

automáticos, el detalle de cuentas por pagar por el uso de las tarjetas y el registro de las tarjetas utilizadas para nuevas emisiones.

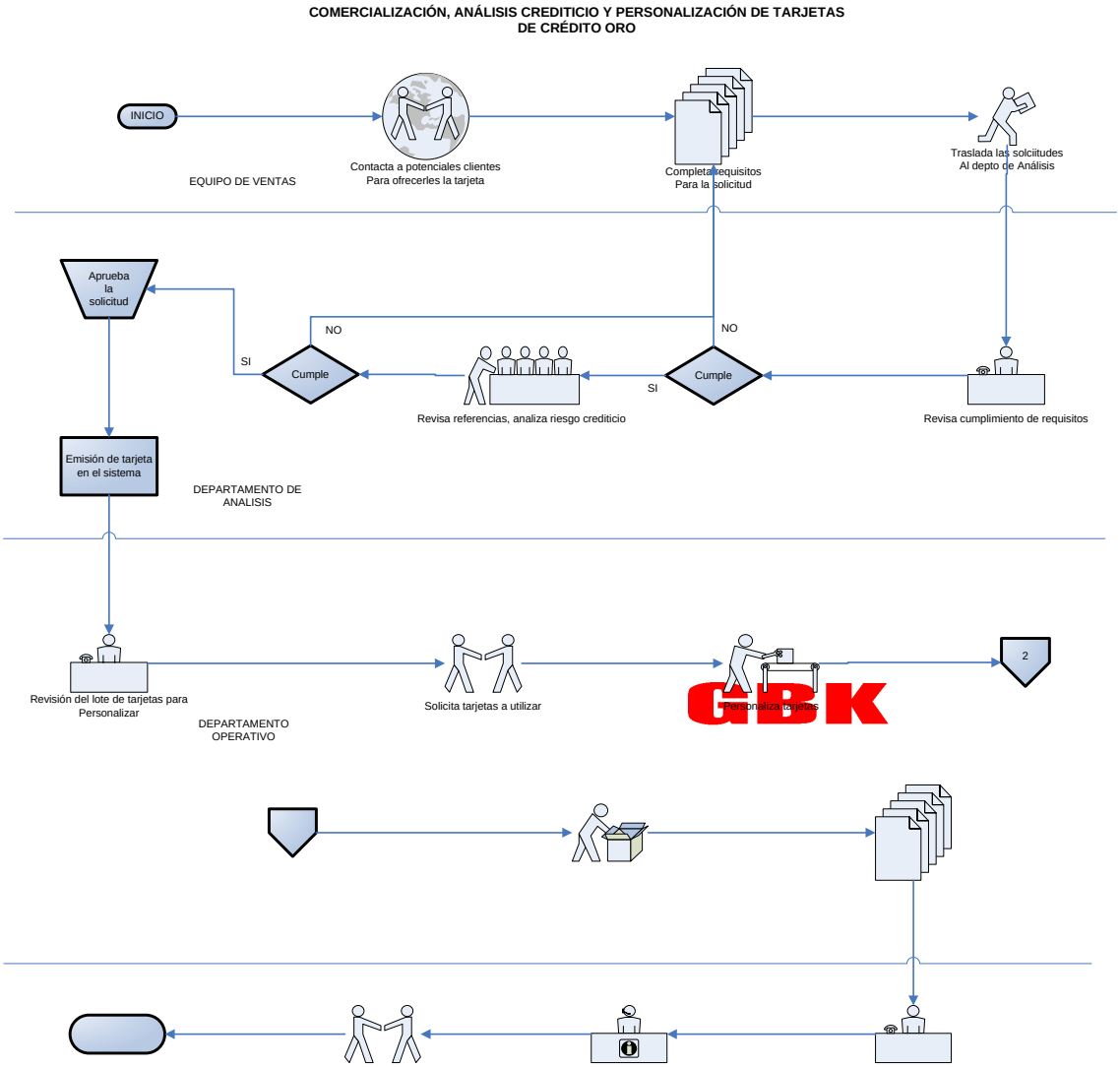
- Ingreso de pólizas contables. Con la información extraída de los reportes de operaciones, se prepara el registro contable. Las pólizas son ingresadas por los auxiliares contables y autorizadas por el jefe del área.
- Archivo de pólizas contables. Cada registro es archivado de manera cronológica y por numeración de cada póliza.

5.2 Trabajo de campo

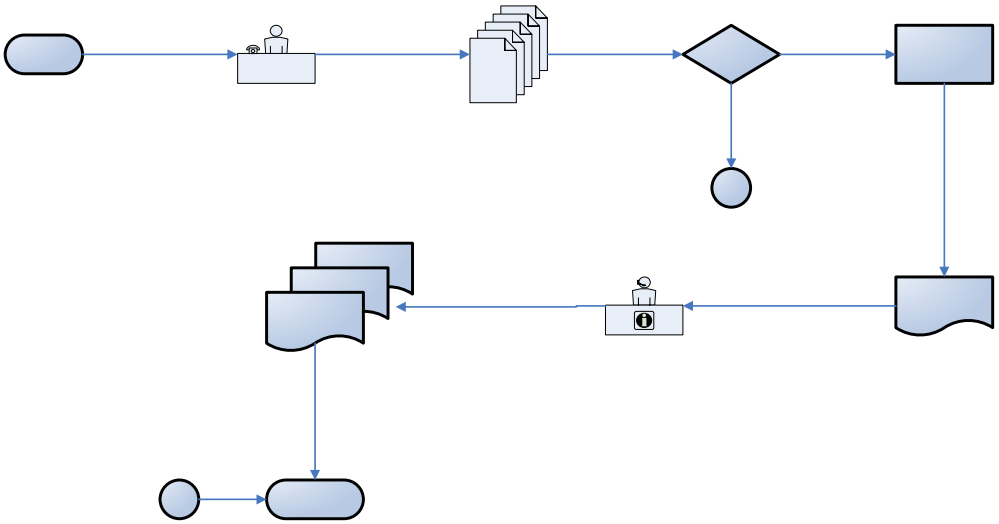
5.2.1 Flujogramas. En el papel de trabajo anterior se describieron cada uno de los procesos que se realizan en el área de tarjetas de Goldbank; sin embargo para mayor comprensión a continuación se presentan de manera visual cada uno de los citados procesos.

GOLDBANK, S.A
FLUJOGRAMAS DE PROCESOS **PT** RO-04
AREA DE TARJETA DE CREDITO **Hecho por** J.I.G.V 05-11-200X
PERIODO REVISADO: Enero a Diciembre 200X **Revisado por** E.L.M.R 15-11-200X

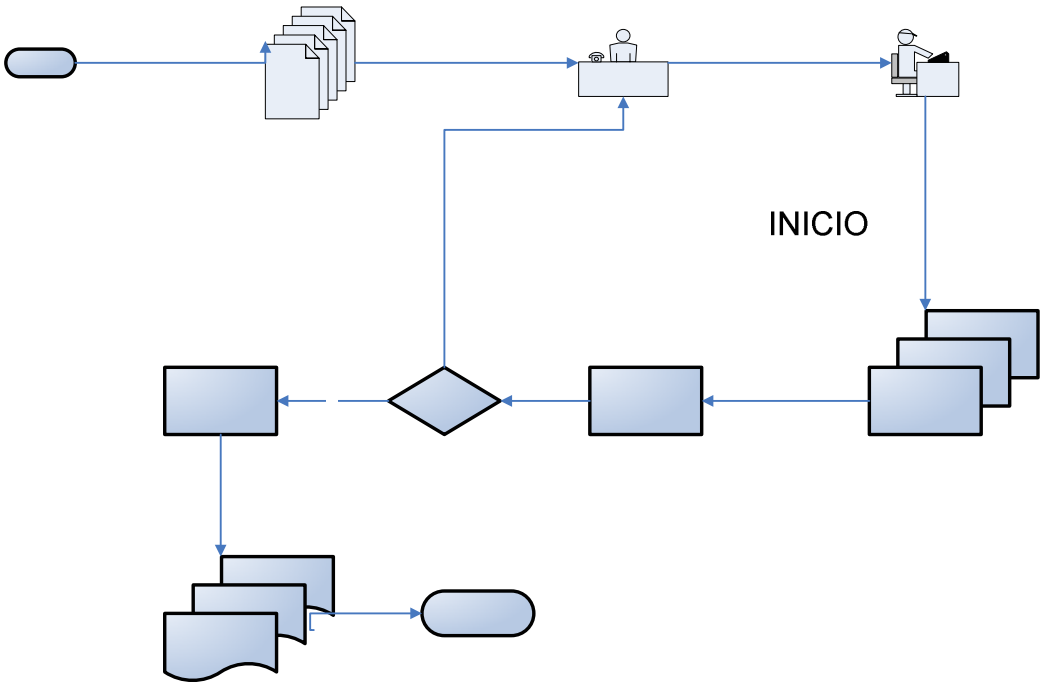
- Comercialización, análisis crediticio y personalización de tarjetas.



- Operación de gestiones.



- Registro contable.



5.2.2 Programa de trabajo para identificación de riesgos.

GOLDBANK, S.A
PROGRAMA DE TRABAJO / EVALUACIÓN DE RIESGOS **PT** RO-05
AREA DE TARJETA DE CREDITO **Hecho por** J.I.G.V 05-11-200X
PERIODO REVISADO: Enero a Diciembre 200X **Revisado por** E.L.M.R 15-11-200X

OBJETIVOS DEL TRABAJO:

- Apoyar la gestión del Comité de Riesgo Operativo y de la Gerencia de TC.
- Identificar los riesgos con mayor grado de posibilidad de ocurrencia y pérdida.
- Identificar las causas que generan la ocurrencia de los riesgos más altos.
- Proponer medidas de control y mitigación de los riesgos identificados.

No	Procedimiento / Actividad	Responsable	Tiempo estimado	Tiempo efectivo
1	Solicite los manuales de políticas y procedimientos del departamento.	Analista 1	2 horas	1.5 horas
2	Analice cada uno de los procedimientos establecidos en el manual y prepare cuestionario	Analista 1	15 horas	16 horas
3	Entreviste al responsable de Análisis crediticio, para comprobar el cumplimiento de las normas establecidas en el manual y normativa de riesgo crediticio de la institución.	Analista 2	12 horas	13 horas
4	Entreviste al responsable de personalización de tarjetas y al Jefe Operativo para comprobar el cumplimiento de los controles establecidos y resguardo de las tarjetas.	Analista 3	4 horas	3 horas
5	Entreviste al Jefe Comercial, además requiera políticas de ventas y control por vendedor.	Analista 2	4 horas	2.5 horas
6	Entreviste al jefe de contabilidad y verifique el adecuado soporte en las pólizas contables.	Analista 3	8 horas	9 horas
7	Revise 2 gestiones de: Cambio de límite de crédito, canje de puntos, cambio de tarjeta, cancelación de tarjeta e intercambio.	Analista 3	4 horas	3.5 horas
8	Presenten resultados de las entrevistas y comentarios del trabajo al Analista 1.	Analista 2 Analista 3	4 horas	6 horas
9	Complete la matriz de identificación de riesgos, basado en el informe presentado por los analistas 1 y 2. Confirme debilidades reportadas.	Analista 1	1 día.	5 horas
10	Analice el comportamiento de los clientes con tarjetas ORO en un período de 3 meses.	Analista 2	16 horas	18 horas
11	Revise ponderación de valores asignados por Analista 1 y compruebe resultados con base en informes estadísticos del departamento.	Grupo de trabajo	1 día	4 horas
12	Discuta el informe con gerente del área y prepare minuta de los acuerdos alcanzados.	Grupo de trabajo	4 horas	6 horas

5.2.3 Cuestionario de Control Interno

BANCO GOLDBANK, S.A. **PT:** RO- 6 1/2
ÁREA: TARJETA DE CRÉDITO *Hecho* JIGV 1510200X
CUESTIONARIO DE CONTROL INTERNO *Rev. P* ELMR 2010200X
PERIODO: ENERO-DICIEMBRE 200X

No	DESCRIPCION	RESPUESTAS	COMENTARIO
I	**Comercialización**		
1	Las bases de datos para la promoción de la tarjeta son provistas en su totalidad por el banco?	☐ SI ☑ NO	
1.1	De ser negativa la respuesta, de donde se obtienen otras bases de datos?	*De empresas relacionadas comercialmente con el banco*	
2	Las bases de datos para promocionar los servicios de tarjeta son revisadas por la gerencia de ventas o queda a discreción del grupo de vendedores?	☑ SI ☐ NO	
3	Se lleva control de las llamadas realizadas para el telemercadeo de la tarjeta de crédito?	☐ SI ☐ NO	
3.1	Si la respuesta es afirmativa, que tipo de control se lleva para el efecto, seleccione:		
	Manual	☐ SI	
	Grabación de llamadas	☑ SI	
	Otro	☐ SI	
4	Se realizan emisiones anticipadas de tarjetas para ser entregadas en la visita al potencial cliente?	☐ SI ☑ NO	
4.1	Si la respuesta es positiva, quién autoriza tales emisiones		
4.2	Qué soporte existe de las emisiones anticipadas?	N/A	
5	Existe una lista de chequeo de requisitos en las visitas a los potenciales clientes?	☑ SI ☐ NO	
6	Es revisada la legitimidad de documentos provistos por los clientes, tales como: Estados de cuenta, copia de cédula, etc.?	☑ SI ☐ NO	
7	Existe control sobre los expedientes trasladados del departamento de ventas a análisis crediticio?	☑ SI ☐ NO	
7.1	Si la respuesta es afirmativa, que tipo de control se lleva para el efecto?	*Acuse de recibo de expedientes (Manual)*	

Comentario(s) de el(los) entrevistado(s)

El departamento de ventas posee manuales para la comercialización de tarjetas. Existe el servicio de personas subcontratadas para la comercialización de tarjetas.

II	**Análisis Crediticio**		
1	Existen responsables de la revisión de los expedientes trasladados del departamento de ventas?	☑ SI ☐ NO	*2 personas responsables*
2	Existen lineamientos establecidos para la apropiada revisión de expedientes, previo al análisis crediticio?	☑ SI ☐ NO	*Manuales de procesos/ Ultima actualización 1505200X*
3	Existe control de los expedientes rechazados por no contener los requisitos mínimos para ser analizados?	☑ SI ☐ NO	
3.1	Que tipo de control existe para el efecto?	*Base de datos en archivo electrónico*	
4	Están normada la confirmación de información en las bases de datos de referencias internas y externas?	☐ SI ☑ NO	
5	En la confirmación de referencias, son validados los siguientes aspectos, seleccione:		
	Endeudamiento total en el sistema regulado	☐ SI	
	Referencias comerciales	☐ SI	
	Procesos judiciales vigentes	☐ SI	
	Todas las anteriores	☑ SI	
5.1	De qué manera se deja evidencia de la validación de los aspectos seleccionados en la pregunta anterior?	*Control en hoja electrónica*	
6	Para la confirmación de referencias personales telefónicamente, existe un control especial para validar la efectiva realización?	☐ SI ☑ NO	
6.1	Cuál?		

BANCO GOLDBANK, S.A. **PT:** RO- 6 2/2
ÁREA: TARJETA DE CRÉDITO *Hecho* JIGV 1510200X
CUESTIONARIO DE CONTROL INTERNO *Rev. P* ELMR 2010200X
PERIODO: ENERO-DICIEMBRE 200X

No	DESCRIPCION	RESPUESTAS	COMENTARIO
II	**Análisis Crediticio (continuación)**		
7	El software empleado para el scoring crediticio genera el mayor indicador para la evaluación del cliente?	☐ SI ☑ NO	
8	Como se distribuye la ponderación de riesgo crediticio en el otorgamiento de una tarjeta de crédito? Expréselo en %		
	Resultado del score proporcionado por el software	40%	
	Indicadores cualitativos del cliente	40%	
	Análisis del comité de créditos o el jefe del departamento	20%	
	Otro (Especifique)		
9	El personal responsable del análisis crediticio, recibe constante capacitación para actualizarlos y tecnificarlos en el tema?	☑ SI ☐ NO	
9.1	Si la respuesta fue positiva, cuál es la periodicidad de las capacitaciones?	*Semestralmente*	
10	Existen registros de errores o fallas en la autorización de créditos anteriores?	☐ SI ☑ NO	*No se considera necesario*
11	Se notifica la resolución de los créditos a los vendedores o a los clientes directamente?	☐ SI ☑ NO	
12	El resguardo de los expedientes se realiza en el propio departamento de análisis crediticio?	☑ SI ☐ NO	*Existen archivos especiales*
III	**Personalización de tarjetas de crédito**		
1	Existe control dual en la administración de las tarjetas vírgenes?	☑ SI ☐ NO	
1.1	Quienes son los responsables del control de tarjetas vírgenes?	*El jefe de operaciones y un asistente*	
2	El registro contable de las tarjetas utilizadas se realiza por persona distinta a la que personaliza las tarjetas?	☑ SI ☐ NO	
2.1	Quién realiza el registro contable?	*El asistente contable de operaciones*	
3	El archivo electrónico que contiene la información para las nuevas emisiones es modificable?	☐ SI ☑ NO	
3.1	Si la respuesta fue positiva, qué información puede modificarse y que niveles de autorización existen para ello?	*N/A*	
4	El equipo de troquelación de tarjetas se encuentra en un lugar y ambiente apropiados?	☑ SI ☐ NO	
5	Quienes tienen acceso al área de personalización de tarjetas?	*Únicamente responsable de troquelación*	
6	Existen planes de contingencia para la personalización de tarjetas en caso de fallas del equipo?	☐ SI ☑ NO	
7	Qué procede con los plásticos que se dañan en el proceso de personalización?	*Se resguardan hasta la destrucción y se registran contablemente*	
8	Cuales son los controles en el envío de tarjetas a la red de agencias para su entrega al cliente, seleccione:		
	Hojas electrónicas de envío	☑ SI	
	Confirmación telefónica de recibo	☑ SI	
	Otro (Especifique)	☐ SI	
IV	**Monitoreo de operaciones con tarjetas de crédito**		
1	Existen políticas definidas para el monitoreo de transacciones	☑ SI ☐ NO	
2	Son considerados los aspectos siguientes en el monitoreo?		
	Frecuencia de las transacciones	☑ SI	
	Límites de crédito	☐ SI	
	Comportamiento habitual del cliente	☑ SI	
	Otro (Especifique)	☐ SI	
3	Existen mecanismos automatizados para el monitoreo?	☑ SI ☐ NO	
4	Existen provisiones para las potenciales pérdidas?	☐ SI ☑ NO	
5	Existen planes de contingencia en caso fallen los programas?	☑ SI ☐ NO	

5.3 Trabajo de gabinete

5.3.1 Identificación y evaluación de riesgos operativos.

Con la información proporcionada, el equipo responsable identifica y evalúa la exposición a riesgos operativos en el área, para lo cual puede utilizar una matriz de identificación de riesgos, la cual está conformada entre algunos elementos importantes por los siguientes:

- Tipología de riesgos. Eventos que pueden representar riesgos en cualquiera de los procesos del departamento o fuera de él.
- Posibilidad de ocurrencia. Probabilidad que el evento desfavorable pueda suscitarse en el proceso o en el uso de la tarjeta de crédito expresada en tiempo. La frecuencia puede establecerse en función a eventos registrados en el pasado o por la experiencia de los evaluadores.
- Impacto del riesgo. Ponderación del impacto que puede generar la ocurrencia del evento desfavorable.
- Responsable de Control. Identificación del puesto responsable por cumplir el proceso y los controles establecidos para el mismo.
- Posibles pérdidas. Cuantificación monetaria de los valores en exposición a riesgos operativos por proceso o eventos relacionados con el uso de tarjetas de crédito.
- Controles existentes. Lista de medidas normadas verbales o escritas a considerarse por los empleados, para el control de las operaciones.
- Calificación del control interno. Con base en la lista de medidas existentes, la revisión de cumplimiento y entrevistas con el personal, se define la calificación de CI.
- Medidas de mitigación. Ponderación a considerar si existen medidas adoptadas para la apropiada mitigación de riesgos operativos en el proceso o evento relacionado con el uso de las tarjetas de crédito. El valor de este campo resta al total de las otras columnas.
- Controles sugeridos. Lista de recomendaciones para mejorar el control.

- Exposición a riesgo. Refleja el resultado de sumar los valores que pudieran ser ponderados a cada elemento de la matriz de acuerdo con la columna seleccionada por ítem, tales valores debieran ser asignados de conformidad con la experiencia de los responsables de análisis de riesgos o con base en datos históricos de eventos registrados.

Ponderación sugerida de exposición a riesgo operativo, matriz RO-7.

COLOR SUGERIDO	PUNTAJE SUGERIDO	EXPLICACIÓN
VERDE	Hasta 50 puntos	Riesgo moderado o bajo. No requiere mayor atención, pero el proceso pudiera ser mejorado.
AMARILLO	De 51 a 70	Riesgo medio o potencial. Los procesos que sean calificados en este segmento pudieran ser sujetos de análisis para la mejora y mitigación de riesgos operativos por la alta posibilidad de ocurrencia.
ROJO	De 71 a 100	Riesgo Alto. Procesos o actividades que requieren un análisis inmediato para la búsqueda de medidas que mitiguen los riesgos operativos.

GOLDBANK, SOCIEDAD ANONIMA
MATRIZ DE IDENTIFICACION DE RIESGO OPERATIVO
AREA EVALUADA: TARJETA DE CREDITO
PERIODO REVISADO: Enero a Diciembre 200X

PT RO-7 1/2
Hecho por J.I.G.V 05-11-200X
Revisado por E.L.M.R 15-11-200X

No.	Descripción del tipo de riesgo (Según clasificación emitido por el Comité de Basilea)	Posibilidad de ocurrencia 15 pts			Impacto del riesgo 25 pts			Responsable de Control	Posibles pérdidas (Directas e indirectas) 30 pts					Controles y medidas Existentes (Descripción)	Calificación del control interno 20 pts				Medidas de Mitigación -10 pts			Controles o medidas Sugeridas (Descripción)	Exposición a Riesgo	OBSERVACIONES
		Muy probable	Probable	Poco Probable	Alto	Medio	Bajo		< Q10mil	>Q10 mil y < 50 mil	> Q50 mil y < Q100mil	> Q100 mil	Imagen o clientes		SI 0pts	NO 10 pts	Bueno	Regular	Malo	Seguros	Provisiones	Planes de Contingencia		BAJO < 50 (verde) MEDIO >50 & < 70 (Amar) ALTO >70 (Rojo)	
1	**EJECUCION DE PROCESOS**																							**54**	
1.1	Errores contables		10				10	Jefe de Contab	5					Revisión de pólizas a cargo de Jefe	0		5						Ninguno	30	
1.2	Inexactitud de informes y datos			5		15		Jefe Comercial	5				5	Ninguno		10		15					Revisión de reportes empleados.	55	
1.3	Falta de soporte de gestiones	15				15		Jefe Operativo		15				Ninguno		10		15					Check list de requisitos.	70	
1.4	Inexistencia de autorización en solicitud de créditos		10		20			Jefe de Análisis				25		Revisión a cargo del Jefe de Análisis	0			15					Requerimiento de dos firmas por montos superiores a Q25mil	70	
1.5	Sanciones por incumplimiento de normativa interna / externa			5		15		Jefe Operativo		15				Ninguno		10		15					Emisión de documento sobre normas internas o externas a considerar.	60	
1.6	Incumplimiento de empresas subcontratadas.			5		15		Jefe Operativo		15				Claúsulas del contrato suscrito con empresas subcontratadas	0		5			(10)				30	
1.7	Errores en la confirmación de referencias.	15				15		Jefe de Análisis	5					Ninguno		10			20				Cruce de casos analizados entre analistas y revisión aleatoria.	65	
2	**FALLOS EN LOS SISTEMAS**																							**52**	
2.1	En el programa de autorizaciones.			5	25			Sistemas	5				10	Back-ups, monitoreo de caídas	0		5					(10)	Centro de replicación y pruebas de stress	40	
2.2	En equipo de cómputo.			5	25			Sistemas	5				10	Ninguno		10		15				(10)	Disponibilidad de técnicos capacitados	60	
2.3	De comunicación		10		25			Sistemas	5				10	Claúsulas de responsabilidad proveedor			5						Considerar proveedor alterno.	55	
3	**DANO A LOS ACTIVOS**																							**55**	
3.1	Desastres naturales		10			15		N/A		15				Ninguno		10		15			(5)		Plan de contingencia	60	
3.2	Delincuencia / Manifestaciones			5			5	N/A		15				Ninguno		10		15					Ninguno	50	

GOLDBANK, SOCIEDAD ANONIMA **PT** RO-7 2/2

MATRIZ DE IDENTIFICACION DE RIESGO OPERATIVO **Hecho por** J.I.G.V 05-11-200X

DEPARTAMENTO: TARJETA DE CREDITO / SEGMENTO ORO **Revisado por** E.L.M.R 15-11-200X

PERIODO REVISADO: Enero a Diciembre 200X

No.	Descripción del tipo de riesgo (Según clasificación emitido por el Comité de Basilea)	Estimación de ocurrencia 15 pts			Impacto del riesgo 20 pts			Responsable de Control	Posibles pérdidas (Directas e indirectas) 25 pts					Controles Existentes (Descripción)	Si 0pts	NO 10 pts	Calificación del control interno 20 pts			Medidas de Mitigación 10 pts			Controles Sugeridos (Descripción)	Exposición a Riesgo	OBSERVACIONES
		Diaria	Semanal	Mensual	Alto	Medio	Bajo		< Q10mil	>Q10 mil y < 50 mil	> Q50 mil y < Q100mil	> Q100 mil	Imagen o clientes				Bueno	Regular	Malo	Seguros	Provisiones	Planes de Contingencia		BAJO < 50 (verde) MEDIO >50 & < 70 (Amar) ALTO >70 (Rojo)	
4	**PRACTICAS EMPRESARIALES**																							**55**	
4.1	Incumplimiento de contrato suscrito en la solicitud de tarjeta			5		15		Jefe Comercial		20			10	Revisión periódica de las claúsulas del contrato con el Depto. Legal.	0		5						Arqueo de contratos y verificación de aceptación por parte del cliente.	55	
4.2	Tarjeta mal diseñada			5			5	Jefe Comercial					15	Ninguno		10		15					Pruebas previas al envío	50	
4.3	Mala asesoría del equipo de ventas sobre funcionalidad de TC	15					5	Jefe Comercial					15	Ninguno		10		15					Capacitación al personal de ventas Encuesta a los principales clientes	60	
5	**RELACIONES Y SEGURIDAD LABORAL**																							**23**	
5.1	Accidentes en el área de trabajo			5			5	N/A	5					Existencia de seguros	0		5			(10)			Ninguno	10	
5.2	Reclamos de indemnización		15			10		Recursos Hms		10				Provisiones contables	0		5				(5)		Ninguno	35	
6	**FRAUDE INTERNO**																							**59**	
6.1	Exoneración de intereses y cargos por comisiones		15			15		Jefe Operativo	5					Revisión de gestiones a cargo del jefe de operaciones, trabajos de auditoría.	0		5						Ninguno	40	
6.2	Modificación de límites de crédito		15		20			Jefe Operativo			20			Revisión de gestiones a cargo del jefe.	0			15					Generación de reporte de cambios	70	
6.3	Aprobación de tarjetas sin considerar las políticas del banco.		15		20			Jefe de Análisis			20			Revisión a cargo del jefe de Análisis y generación de listado de aprobaciones	0		5						Reporte de aprobaciones al Gerente del área y revisiones a cargo de AI	60	
6.4	Robo de tarjetas	15			20			Jefe Operativo		15				Cuadre contable y arqueo de tarjetas			5						Revisiones y arqueos a cargo de AI	55	
6.5	Informes modificados intencionalmente.		15			15		Todos los jefes					10	Ninguno		10			20				Revisión de reportes utilizados para preparar los informes.	70	
7	**FRAUDE EXTERNO**																							70	
7.1	Falsedad en las solicitudes de crédito.	15				15		Jefe de Análisis			20			Confirmación de información en burós de información				15					No aceptación de copias vía fax, capacitación al personal de ventas para la detección de doctos falsos.	65	
7.2	Ataques informáticos			5	25			Sistemas				30		Equipos especializados en detección de ataques informáticos.				15				(10)	Contratación de empresa que certifique la seguridad de los sistemas.	65	
7.3	Copia de tarjetas (Skimming)	15			25			Jefe Operativo				30		Recomendaciones de seguridad a los clientes.					20	(10)			Compra de software para Monitoreo de transacciones y creación de área responsable de efectuar esa actividad.	80	
7.4	Robo y pérdida de tarjetas	15			25			Jefe Operativo		15				Ninguno		10		15		(10)				70	
7.5	Fraudes por Internet y teléfono	15			25			Jefe Operativo		15				Ninguno		10		15		(10)				70	

5.4 Informe de identificación y evaluación de riesgos.

Guatemala,
Noviembre 16 de diciembre año 20XX.

Ref. Evaluación de riesgos operativos en el departamento de Tarjeta de Crédito / Segmento ORO

Señores miembros del
COMITÉ DE RIESGO OPERATIVO
GOLDBANK, Sociedad Anónima
Edificio.

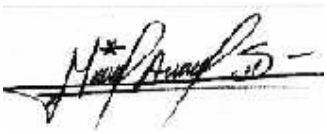
Señores:

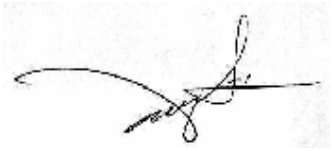
Conforme la asignación que hicieran en su oportunidad al grupo de trabajo conformado por los abajo firmantes, nos permitimos presentar el informe sobre los riesgos identificados y la evaluación correspondiente de las causas que creemos los generan, así como una lista de recomendaciones para el apropiado control y mitigación de los mismos, en el área de tarjetas con énfasis en el segmento ORO.

En tal sentido acompañamos para su pronta aprobación, las medidas de control y mitigación respectivas de riesgo en el área sujeta de evaluación.

Sin otro particular,

Atentamente,





Lic. Fernando Antonio López M
Gerente de Operaciones

Lic. José Danilo Gómez R.
Jefe Administración de Riesgos

Lic. Carlos Miguel Pérez.
Auditor Interno

INFORME

A) RIESGOS IDENTIFICADOS.

Clasificados por el porcentaje de exposición que representan, los riesgos que requieren mayor control y gestión, son los que se detallan a continuación.

% RIESGO	TIPO DE RIESGO	Código (Matriz)	CAUSA (S)
80	Skimming (Fraude Externo)	**7.3**	Legislación sobre el tema y complicidad de empleados de diversos comercios.
70	Robo y pérdida de tarjetas.	**7.4**	Descuido de clientes y débiles fuentes de monitoreo de transacciones.
70	Fraudes por Internet y teléfono.	**7.5**	Uso de tarjetas en sitios inseguros.
70	Informes modificados intencionalmente (Fraude interno)	**6.5**	Concentración de funciones en Jefe Comercial e inexistencia de reportes que validen datos.
70	Modificación de límites de crédito (Fraude interno)	**6.2**	Inexistencia de reporte de cambios efectuados y concentración de funciones en el área operativa.
70	Inexistencia de autorización en solicitud de créditos.	**1.4**	Autorización de tarjetas con la firma de analista.
70	Falta de soporte de las gestiones	**1.3**	Inexistencia de controles
65	Falsedad en las solicitudes de crédito. (Fraude Externo)	**7.1**	Robo de identidad y débiles controles en las entidades responsables de emisión de documentos de identificación.
65	Ataques informáticos (Fraude Externo)	**7.2**	Crecimiento de la cantidad de delincuentes informáticos con capacidad para realizar este tipo de ilícitos.

B) MEDIDAS RECOMENDADAS.

En concordancia con cada uno de los riesgos enumerados en el inciso A, a continuación se presenta una propuesta de medidas de control y mitigación que pudieran implantarse para la apropiada administración de riesgo operativo en el área de tarjetas / Segmento Oro.

Código (Matriz)	RECOMENDACIÓN	MEDIDA DE MITIGACIÓN
7.3	Creación de Unidad especializada y dedicada al monitoreo de transacciones, adquisición de programas informáticos para el efecto.	Renegociar la póliza de seguro Creación de provisiones para pérdidas por éste riesgo.
7.4	Recomendaciones de seguridad a los clientes y monitoreo de transacciones inusuales.	Renegociar la póliza de seguro Ofrecer cobertura a clientes.
7.5	Recomendaciones de seguridad a los clientes y monitoreo de transacciones inusuales.	Renegociar la póliza de seguro Ofrecer cobertura a clientes.
6.5	Requerimiento a Sistemas para la generación de reportes para evitar la preparación de reportes manuales.	Ninguna
6.2	Generación de reporte de cambios y revisión de niveles de autorización en el sistema.	Adquisición de póliza de seguro por fraudes internos.
1.4	Requerimiento de dos firmas –funcionarios- para autorización de límites superiores a Q25mil.	Ninguna
1.3	Generación de check list de requisitos para cada gestión, cuadre de gestiones recibidas y operadas (actividad a cargo de personas diferentes).	Adquisición de póliza de seguro por fraudes internos.
7.1	No aceptación de copias vía fax, capacitación al personal de ventas para la detección de doctos falsos, Unidad especializada en revisión de veracidad de documentos.	Planes de contingencia para la validación de información (visita a municipalidades, confirmación telefónica, etc.)
7.2	Contratación de empresa que certifique la seguridad de los sistemas.	Centro de replicación, en caso ocurra un desastre de grandes consecuencias.

C) MONITOREO DE TRANSACCIONES CON TARJETAS ORO.

No obstante es una medida recomendada en el inciso anterior para el control y mitigación de riesgo por la ocurrencia de una serie de fraudes externos; requiere ahondar en el tema para su mejor comprensión y aprobación.

i. Análisis del Segmento. Una de las actividades efectuadas por el grupo de trabajo consistió en analizar el segmento de clientes que poseen tarjetas Oro en la entidad, llegando a las conclusiones siguientes: Grupo económico al que pertenecen los tarjetahabientes con nivel socioeconómico C1 ó AB (Segmento económico que agrupa personas con ingresos superiores a Q10mil mensuales); principales razones por las que los clientes prefieren este tipo de tarjeta: Distinción y estatus, límite de crédito considerable, beneficios adicionales (Sin cargos por operaciones internacionales, adelantos de efectivo, bonificaciones extras); Operaciones y comercios en donde realizan transacciones con este tipo de tarjeta fuera o dentro del territorio nacional: tiendas de ropa, restaurantes, hoteles, electrónicos y aerolíneas.

ii. Información necesaria para el monitoreo de transacciones. Cada operación realizada con tarjetas del segmento Oro, provee una serie de datos, mismos que puede emplearse para el monitoreo en línea; éstos son: Número de tarjeta, monto de la operación, tipo de operación (Compra-Retiro) código del comercio (MCC), país, moneda, fecha, hora, modo de aprobación (tarjeta presente, Internet, teléfono).

iii. Definición de parámetros para el monitoreo de transacciones. Utilizando un sistema informático denominado **XYZ ®**, pueden definirse una diversidad de parámetros para el monitoreo de transacciones con tarjetas, entre los que sugerimos los siguientes:

- Consumos mayores a Q5mil o equivalente -en divisa- .

- Consumos en dos países diferentes en menos de 3 horas.
- Consumos en Internet por monto superior a Q2mil o equivalente.
- Consumos aprobados telefónicamente superiores a Q1mil o equivalente.
- Dos o más recargas telefónicas o consumos en gasolineras.
- Retiro de fondos por el máximo habilitado en cajeros automáticos.

Guatemala, diciembre del año 20XX

Atentamente,

Grupo de trabajo responsable de la

Identificación y Evaluación de riesgos operativos en el área de TC.

CONCLUSIONES

1. La Superintendencia de Bancos está promoviendo en las entidades bancarias privadas, la observancia de medidas encaminadas a la administración del riesgo operativo, con el objeto de ir avanzando hacia los lineamientos internacionales de supervisión bancaria dictadas por el acuerdo de Basilea II, considerando al riesgo operativo de igual importancia que el de mercado y crédito.

2. El área de tarjeta de crédito de un banco está expuesta a gran cantidad de riesgos operativos, de los cuales sobresalen en orden de impacto: Fraude externo con tarjetas –consistente con el punto de vista de entidades de la región Latinoamericana- en este tipo de riesgo el segmento de tarjeta Oro es el mayor expuesto; Fallos en los sistemas y fraudes internos a causados por empleados infieles.

3. La existencia de un control interno apropiado dentro de la entidad, constituye el elemento fundamental en la administración de riesgo operativo, por las razones siguientes: adecuada segregación de funciones incompatibles, salvaguarda de los bienes mediante la asignación de recursos necesarios, asignación de roles conforme la capacidad y cualidad del puesto.

4. El rol de Auditoría Interna en el marco de las mejores prácticas para la administración de riesgo operativo dictadas por el Comité de Basilea comprende entre otros, los aspectos siguientes: Acompañar y complementar las medidas que considere oportunas el ente responsable de velar por el control del riesgo operativo en la entidad –si existiera-, por tal razón el apoyo de Auditoría es determinante en la gestión del citado riesgo.

5. Una de las actividades centrales para la administración del riesgo, la constituye la identificación de potenciales eventos desfavorables, actividad en la que pueden presentarse dificultades para categorizar el tipo e impacto que genera cada uno de ellos.

6. Los responsables de control de riesgos en el área de tarjetas, de los emisores bancarios poseen poco conocimiento sobre la aplicación del Acuerdo de Basilea II en lo que refiere a riesgo operativo, pero esto no ha impedido iniciar los trabajos para administrarlo.

RECOMENDACIONES

1. Que los funcionarios responsables de control de riesgos en los bancos, dimensionen el impacto que representa el riesgo operativo, independientemente del requerimiento del Supervisor, sino por los beneficios siguientes: reducción de la probabilidad de ocurrencia de eventos desfavorables, mejora de la eficiencia de los procedimientos y mejor calidad de servicio.

2. Que los funcionarios responsables de administrar el riesgo o en su caso el departamento de tarjeta de crédito definan o fortalezcan las actividades de control de fraudes, principalmente para el segmento de tarjetas Oro, de la siguiente manera: definición de limites de riesgo aceptable, medidas de monitoreo oportunas, participación en el comité de seguridad de emisores de tarjetas, etc.

3. Que la Auditoría Interna y los responsables de administración de riesgo operativo –si existiera tal ente en los bancos- analicen la confiabilidad y eficiencia de los controles internos establecidos, enfocándose en que no sean únicamente normas escritas sino de cumplimiento obligatorio por cada colaborador.

4. Que la Auditoría Interna coadyuve con el Directorio y la Alta Gerencia en rol que le corresponde en los aspectos relacionados con la Administración de riesgo operativo, como sigue: alinear los objetivos de la entidad con los del área evaluada, velar por la eficiencia y eficacia de los procesos, supervisar el cumplimiento de las medidas que recomiende el ente responsable del control de riesgo operativo.

5. Que los responsables de realizar la actividad de identificación de riesgos, tomen en cuenta los factores siguientes: interrelación de riesgos, jerarquía de los procesos, responsables de ejecución y herramientas de identificación.

6. Que el Directorio y la Alta Gerencia de las entidades emisoras, promueva la cultura de administración de riesgos, enmarcado en las normas internacionales establecidas por el Comité de Basilea, haciendo conciencia en toda la estructura de la organización aunque no exista requerimiento oficial para ello.

BIBLIOGRAFÍA

1. BESSIS, J. “Risk Management in Banking” Segunda ediciòn 2002. John Wiley Sons Limited.
2. CANO, MIGUEL ANTONIO. “Administración del riesgo en el negocio bancario” III Convención de Usuarios PLUS TI**.**
3. CANO, MIGUEL ANTONIO. “Seminario tarjetas de crédito control y auditoría” Instituto bancario, bursátil y de seguros de Costa Rica año 2000.
4. COMISIÓN NACIONAL BANCARIA Y VALORES DE MÉXICO. “Disposiciones de carácter prudencial en materia de administración integral de riesgos aplicables a las instituciones de crédito” junio 2004.
5. COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA. Página Web Banco de Pagos Internacionales, Basilea Suiza: www.bis.org
6. COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA. “Auditoría interna en bancos y la relación del supervisor con los auditores”. Año 2001.
7. COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA. “Convergencia internacional de medidas y normas de capital”. Junio 2004.
8. COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA. “Marco para la evaluación del control interno” 1998.
9. COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA. “Prácticas sanas para la administración y supervisión del riesgo operativo” Febrero 2003.
10. CONGRESO DE LA REPÚBLICA DE GUATEMALA Decreto número 19-2002. Ley de Bancos y Grupos Financieros.
11. CONGRESO DE LA REPÚBLICA DE GUATEMALA, Decreto número 02-70 y 33-2003. Código de Comercio y sus Reformas.
12. CONGRESO DE LA REPÚBLICA DE GUATEMALA, Decreto número 16-2002. Ley Orgánica del Banco de Guatemala.
13. CONGRESO DE LA REPÚBLICA DE GUATEMALA, Decreto número 18-2002. Ley de Supervisión Financiera.
14. CONGRESO DE LA REPÚBLICA DE GUATEMALA, Decreto número 26-92. Ley del Impuesto Sobre la Renta.
15. CONGRESO DE LA REPÚBLICA DE GUATEMALA, Decreto número 58-2005. Ley para prevenir y reprimir el financiamiento del terrorismo.
16. CONGRESO DE LA REPÚBLICA DE GUATEMALA, Decreto número 67-2001. Ley Contra el Lavado de Dinero u otros activos.

17. CUMES MARISCAL, ANA DAMARIS. “Riesgos Operativos en el proceso de cobro de la cartera vigente en empresas de tarjetas de crédito” Trabajo de tesis, URL 2005.
18. DMR CONSULTING. “El riesgo operacional en las entidades financieras de Latinoamérica. situación actual y tendencias”. Ediciones Cyan, S.A. 2005.
19. ESPIÑERA, SHELDON & ASOCIADOS. “El Riesgo Operacional: Hacia una gerencia proactiva” Julio 2006.
20. ESTRADA VILLALTA, RICARDO AXUÁN, “Organización de la Administración de Riesgos en los Bancos Privados Nacionales” Pág. 25, Impresos La Unión, año 2003.
21. FENTANES, JUAN EDUARDO. “Elementos de Derecho Comercial Tarjeta de Crédito” Monografía.
22. FLORES, ERICK. “Contabilidad Bancaria” curso de 9no semestre Universidad de San Carl.os de Guatemala, segundo semestre año 2002.
23. GARCÍA, COTTY. “Principios básicos de supervisión bancaria, dictados por el comité de Basilea” Trabajo de tesis USAC 2003.
24. GUTIÉRREZ MENESES, RODOLFO ALEJANDRO. “Tarjeta de Crédito y su impacto en la movilidad de las transacciones comerciales” Trabajo de tesis, URL 1997.
25. JUNTA MONETARIA DE GUATEMALA, Resolución JM. 93-2005 Reglamento para la Administración del Riesgo de Crédito.
26. LADINO, ENRIQUE, “Monografía: El Control interno y el informe C.O.S.O”. www.Monografías.com.
27. LARA HARO, ALFONSO. “Medición y control de riesgos financieros”. 3ra edición 2003. Limusa, S.A de CV, Noriega Editores.
28. MOLINA, J ERNESTO. “Contabilidad bancaria Guatemala” Año 2001 impresión en Servitextos Décimo tercer edición.
29. SILVA CUEVA, JOSÉ LUÍS, “Origen de la Tarjeta de Crédito” Monografía del sitio Gestiopolis.com.
30. SPERO, HERBERT, “Moneda y banca”. Impreso por Barnes Noble 1984, Segunda Edición. 236 páginas.
31. SUPERINTENDENCIA DE BANCOS GUATEMALA. Página Web: www.sib.gob.gt
32. THE INSTITUTE OF INTERNAL AUDITORS (Instituto de Auditores Internos). “Normas para el ejercicio profesional de la auditoría interna”. Año 2001.
33. VILARIÑO, A. “Turbulencias Financieras y Riesgo de Mercado”. Primera edición 2001. Editorial Prentice Hall.

ANEXOS

Anexo I.	Encuesta efectuada en seis entidades bancarias privadas nacionales para determinar su actuación en el tema de administración de riesgo operativo.
Anexo II.	Matriz de identificación y evaluación de riesgo operativo.
Anexo III.	Formulario IVE-TC 01, para inicio de relación comercial de un cliente que solicita una tarjeta de crédito en una entidad bancaria.
Anexo IV.	Glosario de términos.

ANEXO I

ENCUESTA SOBRE EL TEMA: " RIESGO OPERATIVO EN EL ÁREA DE TC"

El presente cuestionario es para uso en la preparación de un trabajo que trata el tema de riesgo operacional en las entidades bancarias que emiten tarjetas de crédito, en vísperas de aplicación de los aspectos establecidos en el acuerdo de Basilea II.

Es necesario hacer la aclaración que las preguntas planteadas en la misma, son de carácter general para no comprometer a los entrevistados.

Instrucciones: Por favor contestar en la medida que considere, los siguientes planteamientos sobre el tema del riesgo operativo en el área de tarjetas de crédito de su institución, marcando con una equis (X) las que considere le apliquen.

1) A continuación se describen una serie de eventos que ocurren o pueden ocurrir en el área de tarjetas, de las cuales por favor marque las que considere de mayor importancia o que hayan experimentado en su entidad:

   - Fraudes:

Skimming	☐	Tarjetas robadas	☐
Asalto o fraudes en ATMs	☐	Duplicación de cobros por comercio	☐
Fraude en solicitudes	☐	Robo de plásticos por el personal	☐
Robo de base de datos	☐	Aumentos de límites no autorizados	☐

   Otro (Especificar) _____

   - Procesos (en el área):

Incumplimiento de normas	☐	Mal ingreso de datos al sistema	☐
Errores contables	☐	Expedientes incompletos	☐

   Otro (Especificar) _____

   - Otros eventos:

   Interrupción de los sistemas por tiempos prolongados que afecte el servicio ☐

   Fallas por tarjetas mal diseñadas ☐ Desastres naturales ☐

2) Cuales de las siguientes opciones de control y reembolso manejan para prevenir pérdidas en el caso de fraudes con tarjetas?

Contratación de seguros	☐	Provisiones internas	☐
Monitoreo de transacciones	☐		

   Otro (Especificar) _____

3) Disponen de algún programa (software) que ayude a administrar el riesgo por fraude con tarjetas?

   SI ☐ NO ☐ Cuál (es):_____

4) Poseen manuales de procedimientos que delimiten las responsabilidades y funciones de los que en esta área laboran o las instrucciones son manejadas bajo otro esquema?.

SI ☐ NO ☐ Otro:_____

5) En cuanto a los controles existentes para evitar fraudes o fallas en los procesos, recae la responsabilidad en la Auditoría Interna o existen responsables de prevenir antes de llegar a esta instancia.

SI ☐ NO ☐ Cual dependencia:_____

6) El control de las pérdidas que se hayan registrado por cualquier concepto (Skiminng, robo, pérdida, etc.) se contabiliza en una cuenta específica y/o se lleva control detallado por medio de estadísticas.

a) Sin control separado, ☐

b) Control contable separado ☐ c) Estadístico ☐ Ambas (b y c) ☐

7) Cuál es su conocimiento sobre el tema de riesgo operacional?

Ninguno al respecto ☐ Conocimiento elemental ☐ Experto ☐

Comentario:_____

_____

8) Conoce las implicaciones que conlleva el acuerdo de Basilea II en el contexto de riesgo operacional para las entidades financieras?

SI ☐ NO ☐

Comentario:_____

_____

9) Existen responsables en las medidas de prevención de riesgo operativo en su entidad?

SI ☐ NO ☐ Comentario:_____

ANEXO No. II

EJEMPLO DE MATRIZ PARA IDENTIFICACIÓN Y EVALUACIÓN DE RIESGO OPERATIVO

BANCO: _____

MATRIZ DE IDENTIFICACION DE RIESGO OPERATIVO

DEPARTAMENTO:

No.	Descripción del tipo de riesgo (Según clasificación emitido por el Comité de Basilea)	Posibilidad de ocurrencia 15 pts			Impacto del riesgo 25 pts			Responsable de Control	Posibles pérdidas (Directas e indirectas) 30 pts					Controles y medidas Existentes (Descripción)			Calificación del control interno 20 pts			Medidas de Mitigación -10 pts			Controles o medidas Sugeridas (Descripción)	Exposición a Riesgo	OBSERVACIONES
		Muy probable	Probable	Poco Probable	Alto	Medio	Bajo		< Q10mil	>Q10 mil y < 50 mil	> Q50 mil y < Q100mil	> Q100 mil	Imagen o clientes		Si 0pts	NO 10 pts	Bueno	Regular	Malo	Seguros	Provisiones	Planes de Contingencia		BAJO < 50 (verde) MEDIO >50 & < 70 (Amar) ALTO >70 (Rojo)	

ENTIDAD BANCARIA

FORMULARIO IVE TC - 01

TARJETAS DE CREDITO

FORMULARIO PARA INICIO DE RELACIONES

- Persona o Comerciante Individual -

1. LUGAR	**2. FECHA (dd/mm/aaaa)**

RELACION

DEUDOR ☐ CODEUDOR ☐

3. DATOS DEL PRODUCTO O SERVICIO SOLICITADO

3.1. Tipo de tarjeta solicitada:

Local ☐ Internacional ☐ Oro ☐ Platinum ☐ Marca Compartida: _____

3.2. Otras operaciones con el grupo financiero:

Banco	☐	Empresa de Seguros	☐	Factoraje	☐
Sociedad Financiera	☐	Empresa de Fianzas	☐	Off - Shore	☐
Almacén General de Depósito	☐	Casa de Bolsa	☐	Casa de Cambio	☐

Otros (especifique) _____

3.3. Otras tarjetas de crédito que posee:

Empresa Emisora:	Número:	Límite autorizado:	Fecha de Vencimiento (dd/mm/aaaa):

4. DATOS PERSONALES DEL SOLICITANTE

4.1. Primer apellido:	Segundo apellido:	Apellido de casada:

Primer nombre:	Segundo nombre:

4.2. Fecha de nacimiento (dd/mm/aaaa)	**4.3.** Nacionalidad:	**4.4.** Profesión u oficio

4.5. Tipo de documento de identificación:

Cédula de Vecindad: ☐	No. de orden:	No. de registro:
Departamento:	Municipio:	
Pasaporte: ☐	Número:	País del pasaporte:

4.6. Dirección particular completa (calle o ave., casa No. colonia, sector, lote, manzana, zona, municipio, Depto. y país)

Número o nombre de calle o avenida	Numero (casa)	Apto. o similar	Colonia o barrio

Zona	Municipio	Departamento	País

4.7. Número de identificación tributaria (NIT):		País del NIT:
4.8. Teléfonos:	**4.9.** Fax:	**4.10.** Correo electrónico:

4.11. Nombre que desea en la tarjeta (máximo 26 caracteres):

4.12. Sexo **M** ☐ **F** ☐	**4.13.** Estado civil:		
4.14. Donde desea recibir su correspondencia:	Casa: ☐	Oficina: ☐	Otro: ☐
Número o nombre de calle o avenida	Numero (casa)	Apto. o similar	Colonia o Barrio

Zona	Municipio	Departamento	País

DATOS DEL CONYUGE

4.15. Primer apellido:	Segundo apellido:	Apellido de casada:

Primer nombre:	Segundo nombre:

4.16. Fecha de nacimiento (dd/mm/aaaa)	**4.17.** Nacionalidad:	**4.18.** Profesión u oficio

4.19. Tipo de documento de identificación:

Cédula de Vecindad: ☐	No. de orden:	No. de registro:
Departamento:	Municipio:	
Pasaporte: ☐	Número:	País del pasaporte:

4.20. Empresa donde labora:

4.21. Salario mensual:	Tiempo de trabajar allí:		
4.22. Teléfono Casa:	TeléfonoTrabajo:	Extensión:	Celular:
4.23.Número de Identificación Tributaria (NIT):		País del NIT:	

5.	**DATOS DE TARJETAS ADICIONALES QUE SE SOLICITEN**		
5.1. Primer Apellido:	Segundo apellido:		Apellido de casada:
Primer Nombre:		Segundo Nombre:	
5.2. Fecha de Nacimiento (dd/mm/aaaa)	**5.3.** Nacionalidad:		**5.4.** Profesión u Oficio
5.5. Tipo de documento de identificación:			
Cédula de Vecindad: ☐	No. de orden		No. de registro:
Departamento:		Municipio:	
Pasaporte: ☐	Número:		País del pasaporte:
5.6. Sexo: **M** ☐ **F** ☐	**5.7.** Estado civil:		

Relación con tarjetahabiente titular:	Número de Identificación Tributaria (NIT)	País del NIT:

5.7. Dirección particular completa (calle o ave., casa No. colonia, sector, lote, manzana, zona, municipio, Depto. y país)

Número o nombre de calle o avenida	Numero (casa)	Apto. o similar	Colonia o Barrio

Zona	Municipio	Departamento	País

5.8. Teléfonos:	**5.9.** Fax:	**5.10.** Correo electrónico:

5.11. Nombre que desea en la tarjeta (máximo 26 caracteres):

NOTA: Cuando el espacio del formulario sea insificiente, sírvase incluir la información en hojas por separado, indicando el numeral al que corresponde

6.	**REFERENCIAS DEL SOLICITANTE**		
6.1. Bancarias (nombre de los bancos):	Cuenta No.:		Telefonos:
6.2. Comerciales (nombre del comercio):	Teléfonos:		Año del crédito:

6.3. Personales (nombres de personas que no sean familiares):	Tel. Casa:	Tel. Oficina:	Tel. Celular:
6.4. Familiares (dos personas que no vivan con usted):	Tel. Casa:	Tel. Oficina:	Tel. Celular:

7.	**INFORMACIÓN ECONÓMICO - FINANCIERA DEL SOLICITANTE**		
7.1. Actividad económica del solicitante:			
7.1.1. Orígen de sus ingresos:			
Relación de dependencia ☐	Profesional ☐		Negocio propio ☐
Mixto ☐	Otro especifique _____		
7.1.2 Datos de la empresa o institución donde trabaja:			
7.1.2.1 Puesto que desempeña:			Fecha de ingreso (dd/mm/aaa):

7.1.2.2 Dirección completa del trabajo (calle o ave., casa No. Colonia, sector, lote, manzana, zona, municipio, Depto. y país)

Número o nombre de calle o avenida	Numero (casa)	Apto. o similar	Colonia o Barrio

Zona	Municipio	Departamento	País

7.1.2.3 Teléfonos del trabajo:	**7.1.2.4** Fax de trabajo:	**7.1.2.5** Correo electrónico de trabajo:

7.1.2.6 Nombre del patrono anterior, si su estabilidad laboral es menor a 6 meses:	Teléfonos:
7.1.2.7 Puesto que desempeñó:	Años:

7.1.3 Datos del negocio:			
7.1.3.1 Nombre:			
7.1.3.2 Patente de empresa número:	**7.1.3.3** NIT de la empresa:		País del NIT:

7.1.3.4 Dirección completa del negocio (calle o ave., casa No. Colonia, sector, lote, manzana, zona, municipio, Depto. y país)

Número o nombre de calle o avenida	Numero (casa)	Apto. o similar	Colonia o Barrio

Zona	Municipio	Departamento	País

7.1.3.5 Fecha de inicio de operaciones (dd/mm/aaaa):	
7.1.3.6 Objeto:	

7.1.3.7 Teléfonos:	**7.1.3.8** Fax:	**7.1.3.9** Correo electrónico:

7.2. Sector de la economía en el que el solicitante desarrolla su actividad (Industria, comercio, agricultura, otros):	
7.3. Ingresos mensuales aproximados:	**7.4.** Egresos mensuales aproximados:

7.4. Posee vehículo	**Si** ☐ **No** ☐	Pagado ☐	Amortizándose ☐	Cuota:	Q.

Modelo	Tipo	Marca	Línea	Placas

7.5. Tipo de vivienda Propia ☐ Amortizándose ☐ Familiar ☐ Alquilada ☐

Años de residir en el domicilio:	Monto de alquiler ó pago mensual:	No. de dependientes:

SERVICIOS ADICIONALES SIN COSTO						
Pagos mensuales con Débito a Cuenta:	Si ☐	No ☐	Pago:	Mínimo ☐	De contado ☐
Número de Cuenta:			Tipo:	Ahorros ☐	Monetarios ☐
banca en línea ** Completar contrato*	Si ☐	No ☐	Correo:		

8. DOCUMENTOS QUE SE DEBEN ANEXAR AL FORMULARIO DE INICIO DE RELACIONES

8.1. Fotocopia de los documentos de identificación de los responsables de la(s) tarjeta(s) de crédito.
8.2. En caso de ser extranjeros, una fotocopia del documento que acredite la condición migratoria cuando sea aplicable.
8.3 En caso de poseer negocio propio adjuntar, fotocopia de patente de empresa y del formulario de inscripción en la SAT ó carné.

SI ES NECESARIO UN FIADOR, DEBE LLENAR OTRA SOLICITUD Y ADJUNTAR PAPELERÍA.

9. OBLIGACIONES DEL SOLICITANTE

9.1 Declaro bajo juramento que los datos indicados son verdaderos y autorizo al emisor para su comprobación en fe de lo cual firmo la presente solicitud.
9.2 Me comprometo a informar de inmediato a la compañía emisora de la tarjeta de crédito cuando se produzca cambio en la información consignada en este formulario.

Firma del Solicitante	**Otros Firmantes**
Firma y código del empleado responsable que llenó el formulario	**Vo.Bo Institución**

ANEXO IV: GLOSARIO DE TÉRMINOS

Adquirente: Entidad dedicada a proveer los elementos necesarios a los comercios que se afilien para poder operar y realizar los cobros mediante el uso de tarjetas.

ATM (A teller machine): Dispensador de efectivo o cajero automático.

Autoevaluación de riesgo: Técnica que consiste en realizar un análisis interno de los fraudes que pudiesen ocurrir en determinado proceso, considerando la tipología de riesgos existentes.

Back Office: Definición que se atribuye a los equipos de soporte operativo existentes en las empresas para apoyar los objetivos comerciales.

Banco: Entidad financiera regulada que como principal actividad realiza la intermediación financiera.

BIN (Bank identification number): Representa la identidad del emisor, el país y categoría de la tarjeta, el mismo es de utilidad para el direccionamiento de las transacciones en el proceso de aceptación de la tarjeta.

Cargos: Definición que se otorga a los montos que se incluyen en el estado de cuenta de cada tarjetahabiente, usualmente son: compras, retiros, intereses, comisiones.

Comité de Basilea: Ente internacional creado en 1974 integrado por los presidentes de los bancos centrales de los países más desarrollados en materia financiera (Canadá, Bélgica, Francia, Alemania, Italia, Japón, Estados Unidos, Inglaterra, Holanda, Suiza, Suecia, Luxemburgo y España). Este ente define las recomendaciones o sugerencias en materia bancaria a nivel internacional, las cuales deben ser adoptadas para poder competir de manera globalizada.

Corte: Se denomina de esta manera a la fecha en la cual la entidad financiera computa el monto acumulado durante un periodo de tiempo –usualmente un mes-, saldos deudores, comisiones, intereses, etc., a cargo del tarjetahabiente por el uso de la tarjeta.

Emisor: Entidad bancaria autorizada para emitir tarjetas de crédito, bajo la licencia de marca internacional, por ejemplo: VISA o MasterCard.

Establecimiento Afiliado: Entidad comercial dedicada a la venta de bienes o la prestación de servicios que acepta como medio de pago la tarjeta de crédito.

Exposición a riesgo: Grado de posibilidad de ocurrencia de eventos desfavorables.

Formulario IVE: Documento requerido por la entidad financiera a los clientes que desean efectuar diversas operaciones dentro de la entidad. El objetivo es determinar el grado de confiabilidad de la información y prevenir el lavado de activos.

Hardware: Comprende todos los equipos tecnológicos necesarios para el procesamiento de información a través de sistemas computarizados.

Intermediación financiera: Proceso por medio del cual una entidad financiera autorizada capta recursos del público para otorgarlos bajo la modalidad de préstamos; considerando factores de riesgo en el proceso.

Lavado de dinero: Acto por medio del cual se pretende legitimizar flujos de dinero provenientes de fuentes ilícitas.

Límite de tolerancia a riesgo: Representa por medio de valores monetarios, los montos hasta donde la entidad considera aceptable el riesgo. Pueden definirse límites de tolerancia cero si fuese el caso, pero representa mayor inversión en controles.

Matriz de evaluación de riesgos: Hoja de cálculo que considerando los factores de riesgo que se desean evaluar y las medidas de control existente, determinan el grado de exposición a riesgos operativos.

Mitigar: Amortiguar o prevenir la ocurrencia de riesgos operativos, corresponde a este etapa de la administración de riesgos la generación de provisiones, definir planes de continuidad, entre otros.

NSE (Nivel socioeconómico): Categoría que se asigna a cada individuo considerando sus ingresos y gastos financieros, es de mucha utilidad para la segmentación de mercados objetivos.

Órgano Supervisor: Denominación que se otorga al ente Estatal encargado de supervisar las actividades de las entidades financieras –La Superintendencia de Bancos-.

Outsourcing: Trasladar operaciones de determinada empresa a una tercera por diversas razones, ejemplo: especialización, costos de operación, incremento del servicio, etc. Se denomina también tercerización o subcontratación de servicios.

Parámetro de monitoreo: Expresión que se utiliza para definir los niveles de control que pueden establecerse para el monitoreo de cualquier operación, considerando una diversidad de factores.

Personalización de tarjetas: Proceso de generación de las tarjetas de crédito para su posterior utilización por parte de los clientes. Consiste en la grabación de información en la tarjeta.

PIN (Personal identification number): Código numérico necesario para efectuar operaciones en dispositivos electrónicos habilitados para uso de la tarjeta, ejemplo: cajeros automáticos, kioscos de servicio, etc.

Plan de contingencia: Actividades desarrolladas con el objetivo considerar medidas alternas de continuidad de las operaciones.

POS (Point of sale): Denominada también terminal de venta, consiste en un aparato en donde se procesan las transacciones con tarjetas en los establecimientos afiliados.

Procesador: Es la entidad que posee los medios tecnológicos y la información de cada cuenta (disponibilidad, vencimiento, claves, bases de datos, etc.) para poder autorizar las transacciones que el tarjetahabiente desee efectuar.

Record crediticio: Historial del comportamiento crediticio de cualquier persona (individual o jurìdica), mismo que es de mucha utilidad al momento de realizar análisis para la autorización de créditos bajo cualquier modalidad, incluida la tarjeta.

Riesgo operativo: El riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos.

Riesgo: Palabra proveniente del latín Risicare que significa atreverse o transitar por un sendero peligroso. Puede definirse como la posibilidad de ocurrencia de eventos desfavorables.

Sabotaje: Acto malintencionado para interrumpir la continuidad del negocio, cometido por personal interno de la entidad.

Sistema financiero nacional: Es el conjunto de instituciones y organizaciones públicas y privadas que tienen como función principal otorgar los recursos financieros de ciertas personas que disponen de excedente de dicho recurso, hacia aquellas personas individuales o jurídicas que necesitan del mismo.

Skimming: Denominación que se otorga al fraude cometido mediante la copia de la información contenida en la banda magnética de la tarjeta.

Software: Programas o rutinas informáticas necesarias para el procesamiento de datos en medios computarizados.

Tarjeta virgen: Se denomina de esta manera a aquellas tarjetas que poseen los elementos de arte de la entidad pero que no cuentan con la personalización correspondiente.

Tarjetahabiente (TH): Persona física, que con la autorización y calificación como sujeto de crédito por parte del Emisor, utiliza la tarjeta de crédito para pagar bienes o servicios.

Tipología de riesgos operativos: Clasificación pormenorizada por niveles de riesgos operativos existentes.

VISA®: Ente internacional dedicado a la promoción como medio de pago de las tarjetas de crédito, fundada en 1977 por un grupo de bancos norteamericanos.

Voucher (Comprobante de compra): Documento que extienden los establecimientos comerciales o de servicio a los tarjetahabientes al realizar los pagos por medio de tarjeta de crédito