UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONOMICAS

"LA AUDITORÍA DE UN BANCO, EN LA PREVENCIÓN Y DETECCIÓN DE FRAUDES, POR LA FALSIFICACIÓN DE LA BANDA MAGNÉTICA DE UNA TARJETA DE CRÉDITO"

PRESENTADA A LA JUNTA DIRECTIVA DE LA

FACULTAD DE CIENCIAS ECONOMICAS

POR

MANUEL FRANCISCO POZ

PREVIO A CONFERIRSELE EL TITULO DE

CONTADOR PUBLICO Y AUDITOR

EN EL GRADO ACADEMICO DE

LICENCIADO

GUATEMALA, MAYO DEL AÑO 2006

JUNTA DIRECTIVA DE LA FACULTAD
DE CIENCIAS ECONOMICAS

Decano	Lic. Eduardo Antonio Velásquez Carrera
Secretario	Lic. Oscar Rolando Zetina Guerra
Vocal I	Lic. Canton Lee Villela
Vocal II	Lic. Albaro Joel Girón Barahona
Vocal III	Lic. Juan Antonio Gómez Monterroso
Vocal IV	P.C. Efrén Arturo Rosales Alvarez
Vocal V	P.C. José Abraham González Lemus

PROFESIONALES QUE REALIZARON LOS EXAMENES
DE AREAS PRACTICAS

Auditoría	Licda. Esperanza Roldán de Morales
Contabilidad	Lic. Hugo Vidal Requena Belteton
Matemática-Estadística	Lic. Carlos Humberto García Alvarez

JURADO QUE PRACTICO EL EXAMEN PRIVADO DE TESIS

Presidente	Lic. Sergio Arturo Sosa Rivas
Examinador	Lic. Olivio Adolfo Cifuentes Morales
Examinador	Lic. Jorge Alberto Trujillo Corzo

ORDEN DE IMPRESION

DEDICATORIA

A Dios Todopoderoso	Por hacer realidad mis sueños, que a través de dificultades en mi vida, con su fortaleza y sabiduría he logrado.
A mi Madre	**LUCIA POZ** Angel que Dios envió y transformó en mi Madre para cuidar y guiar mis pasos, con ejemplo de humildad, gratitud, sacrificio, lucha y coraje, para así afrontar los desafíos de la vida. Infinitas gracias le doy a Dios, por haberme bendecido con tan buena Madre.
A mi Familia	A toda en especial
A mis Amigos	Quienes contribuyeron con sus consejos, apoyo moral y emocional al logro de esta meta.
A la Licenciada	Luisa David de Gidi y familia.
A mi Asesor de Tesis	M.A. Edwin Leonel Martínez Regalado Por su asesoría y orientación en la elaboración de este trabajo.
A la Universidad de San Carlos de Guatemala	Por hacer de mi un profesional útil a la patria.

CONTENDIDO

INTRODUCCION i-iii

CAPITULO I
TARJETA DE CREDITO

1.1	Antecedentes Históricos	01
1.2	Definición de Tarjeta de Crédito	02
1.3	Naturaleza Jurídica	04
1.4	Características de la Tarjeta de Crédito	06
1.5	Sujetos que Conforman la Tarjeta de Crédito	06
1.6	Clasificación de las Tarjetas de Crédito	08
1.7	Actualidad de Transacciones de Tarjetas Visa, en Centro América	10
1.8	Antecedentes Legales y Operativos en Guatemala	11
1.9	Organización de un Departamento de Tarjeta de Crédito en un Banco Privado	13

CAPITULO II
EL FRAUDE EN INSTITUCIONES BANCARIAS EMISORAS DE TARJETAS DE CREDITO

2.1	Concepto de Fraude	16
2.2	Actividad Bancaria	19
2.3	Riesgos en la Actividad Bancaria	19
2.4	Riesgo de Fraude	20
2.5	Situaciones que Facilitan el Fraude	20
2.6	Situaciones Especificas de Fraude	22
2.7	Fraude por Falsificación de la Banda Magnética de una Tarjeta de Crédito	25

CAPITULO III
CLASIFICACION DE RIESGOS EN UNA INSTITUCION BANCARIA EMISORA DE TARJETAS DE CREDITO

3.1	Riesgo	32
3.2	Evaluación del Riesgo Bancario	32
3.3	Riesgo País	33
3.4	Riesgo de Mercado	34
3.5	Riesgo de Operaciones	37
3.6	Riesgo de la Información	38
3.7	Riesgo de Operaciones Ilícitas	40
3.8	Riesgo de Auditoría	41

CAPITULO IV
LA AUDITORIA DE UN BANCO EN LA PREVENCION Y DETECCION DE FRAUDES POR LA FALSIFICACION DE LA BANDA MAGNETICA DE TARJETAS DE CREDITO

4.1	Evaluación del Control Interno	43
4.2	Evaluación del Programa de Control de Fraudes	46
4.3	Normativa Interna y Externa Relacionada al Fraude por Falsificación de Banda Magnética	67
4.4	Nuevas Herramientas a Implementar para la Prevención y Detección de Fraudes	69

CAPITULO V
CASO PRACTICO DE FRAUDE POR LA FALSIFICACION DE LA BANDA MAGNETICA DE UNA TARJETA DE CREDITO

5.1	Area de Auditoría Interna – Revisión de Fraudes por Falsificación de Banda Magnética	70
5.1.1	Programa de Auditoría (controles internos, herramientas y programa control de fraudes)	72
5.1.2	Indice de Marcas de Auditoría Efectuadas en la Revisión	74
5.1.3	Trabajo de Gabinete	75
5.1.4	Informe de Auditoría	84
5.1.5	Resultados del Caso Práctico	88

CONCLUSIONES Y RECOMENDACIONES

Conclusiones	89
Recomendaciones	90
Bibliografía	91
Anexos	94

INDICE DE ESQUEMA

Esquema # 01	Proceso de una Tarjeta de Crédito	04
Esquema # 02	Respaldo de la Marca Internacional VISA	08
Esquema # 03	Organigrama de un Departamento de Tarjeta de Crédito	15
Esquema # 04	Clasificación de Riesgos	42

INDICE DE CUADROS

Cuadro # 01	Estadísticas de Tarjetas VISA y Transacciones en Centro América	11

INDICE DE ANEXOS

Anexo # 01	Solicitud de Tarjeta para Persona o Empresa Individual	95
Anexo # 02	Solicitud de Tarjeta para Persona Jurídica	98
Anexo # 03	Anexo para Solicitud de Tarjeta Adicional Persona o Empresa Individual	101
Anexo # 04	Anexo para Solicitud de Tarjeta Adicional Persona Jurídica	102
Anexo # 05	Contrato para Uso de Línea de Crédito en Tarjeta de Crédito	103
Anexo # 06	Documentación Requerida para Solicitar una Tarjeta de Crédito	107
Anexo # 07	Perfil Requerido para Solicitar una Tarjeta de Crédito	108
Anexo # 08	Proceso Revisión de Documentación del Expediente	109
Anexo # 09	Proceso de Análisis de una Solicitud de Tarjeta de Crédito	110
Anexo # 10	Proceso de Aprobación de Solicitud por Comité de Créditos	111
Anexo # 11	Proceso de Embosado de Tarjetas de Crédito	111
Anexo # 12	Proceso de Entrega de Tarjetas de Crédito	111
Anexo # 13	Formulario de Gestión por Servicio de Tarjeta de Crédito	112
Anexo # 14	Formulario de Gestión por Ajuste Operativo de Tarjeta de Crédito	113
Anexo # 15	Proceso de Atención de Gestiones de los Tarjetahabientes	114
Anexo # 16	Reporte de Requisitos de Información	114
Anexo # 17	Glosario	115

INDICE DE GRAFICAS

Gráfica # 01	Crecimiento de Tarjetas VISA en Centro América	11
Gráfica # 02	Crecimiento de Transacciones con Tarjetas VISA en Centro América	11

INTRODUCCION

El Sistema Bancario de Guatemala esta integrado por un conjunto de instituciones y organizaciones públicas y privadas, que tienen como función principal canalizar los recursos financieros, de personas que tienen excedentes de estos y otras que necesitan de los mismos para financiarse.

El desarrollo de la globalización financiera, ha obligado a los bancos que conforman el Sistema Bancario de Guatemala, a invertir en sistemas, programas y estrategias, para modernizar y diversificar los servicios y productos financieros que ofrecen a sus clientes, con la finalidad de no rezagarse ante la competencia.

Dentro de los servicios financieros más utilizados en la actualidad se menciona el financiamiento o crédito rápido, que se realiza a través del uso de tarjetas de crédito como medio de pago, para la adquisición de bienes y servicios. Este producto se ha incrementado, debido a que representa más riesgo llevar dinero en efectivo para realizar esta serie de transacciones.

Como todo producto financiero, el uso de tarjeta de crédito lleva inherente un riesgo en particular como lo es el de fraude, que puede materializarse a través del robo de la misma, para realizar consumos, ó por medio de la obtención de la información de la banda magnética de una tarjeta, para posteriormente crear una nueva(falsa), con la que se realizan consumos que son cargados a la persona que posee la tarjeta original.

Derivado de lo anterior, es de vital importancia que periódicamente el departamento de auditoría interna de un banco emisor, mediante una auditoría de tipo operacional, evalúe los controles internos, procedimientos y herramientas establecidos para prevenir y detectar fraudes por falsificación de banda magnética de una tarjeta de crédito, con el propósito de mejorar e implementar nuevos mecanismos que permitan monitorear de mejor forma éstos actos delictivos.

Este trabajo de tesis pretende aportar en alguna medida, lineamientos que coadyuven a la gestión de las entidades emisoras, implementando controles internos, procedimientos y herramientas, que les permita prevenir y detectar fraudes en forma oportuna.

El desarrollo de la presente tesis se dividió en seis capítulos, en los cuales se señalan los puntos que se consideraron más importantes y que pueden ser de utilidad al Sistema Bancario Guatemalteco y al profesional de la carrera de Contador Público y Auditor.

En el capitulo primero, se presentan las generalidades de las tarjetas de crédito, se aborda una descripción de los antecedentes del producto, su definición, características, naturaleza y clasificación. Así mismo se describe una forma de como podría integrarse una gerencia de tarjeta de crédito, dentro de una entidad emisora, describiendo cada área que la conformaría.

El segundo capitulo está enfocado en dar a conocer, los diferentes tipos de fraudes a los que están expuestas las actividades, servicios y productos financieros implementados por las entidades bancarias. Se describe a profundidad el fraude por falsificación de la banda magnética de una tarjeta de crédito, comentando sobre los escenarios donde se pueden llevar a cabo, como identificarlos y describiendo estrategias para prevenir y detectar los mismos.

Dentro del tercer capitulo se detallan y describe la clasificación de riesgos a los que se encuentra expuesta una institución bancaria emisora de tarjetas de crédito y algunos efectos de cada uno de ellos, para poder minimizar el margen de probabilidad de ocurrencia.

El capitulo cuarto contiene la parte medular del presente trabajo, pues se detallan los controles internos, procedimientos y programas de control de fraudes, que una institución bancaria emisora debiera poseer para lograr una mayor prevención y detección oportuna de los mismos. Así mismo se dan a conocer la importancia y los métodos de evaluación periódica que debe realizar el departamento de auditoría interna de la entidad para lograr que éstos sean funcionales e implementar nuevos mecanismos cuando así lo requiera la verificación.

En el capitulo quinto se ejemplifica un caso práctico de fraudes cometidos a través de la falsificación de la banda magnética de una tarjeta de crédito, consecuencia de no evaluar oportunamente los controles internos, el programa de control de fraudes y las herramientas electrónicas implementadas para la prevención y detección de esta clase de fraudes.

También dentro de este capitulo, se muestran los documentos que deben verificarse al momento de realizar una investigación de un caso confirmado de fraudes. Los resultados de la evaluación quedan plasmados mediante un informe completo presentado por la auditoría interna, en el que se detallan las conclusiones de la evaluación y las recomendaciones efectuadas con el fin de mejora e implementar nuevas medidas que sean funcionales para la prevención y detección de fraudes por falsificación de la banda magnética de tarjetas de crédito.

Posteriormente se citan las conclusiones y recomendaciones, resultado del contenido del presente trabajo de investigación, las cuales pretenden aportar en alguna medida lineamientos de utilidad tanto para el Sistema Bancario Guatemalteco como para la profesión de Contador Público y Auditor.

Cabe resaltar que en el presente trabajo se intentó cubrir los temas más relevantes, referente al fraude por falsificación de la banda magnética de una tarjeta de crédito, por lo que no se pretende haber agotado el tema, el cual constituye un campo muy amplio de aplicación.

Para este estudio se realizó una investigación en una entidad emisora de tarjetas de crédito, respaldada por la empresa de reconocida trayectoria, en la administración de tarjetas, como lo es **Visa Internacional**, con el objetivo de establecer la importancia que representa para dichas entidades, el contar con políticas, controles internos, programas de control y herramientas electrónicas adecuadas para la prevención y detección de fraudes por la falsificación de la banda magnética de una tarjeta de crédito.

a) Resultados de la Investigación

Con base en la investigación realizada, se desarrollo un caso práctico en el que a través de un trabajo de auditoría en el área de tarjetas de crédito en una institución financiera, se efectuó una investigación de un fraude por falsificación de la banda magnética de una tarjeta que inicialmente fue robada, con el propósito de dar a conocer las inconsistencias y debilidades en procedimientos, controles internos, programas de control de fraudes y herramientas utilizadas, para ejemplificar de mejor forma las causas que provocaron el no prevenir y detectar dicho fraude.

Lo anterior, proporcionó resultados con un grado técnico superior, que muestra nuevos controles, procedimientos internos, programas de control de fraudes y herramientas electrónicas, necesarias para prevenir y detectar esta clase de fraudes, así también permite ampliar el ámbito de inspección por parte del profesional de la carrera de Contador Público y Auditor, en cuanto a esta rama del Sistema Bancario Guatemalteco.

b) Métodos Utilizados

Deductivo
Partiendo de lo general hacia las características particulares de la temática desarrollada.

Indagadora
Al momento de efectuar la presente investigación en el Sistema Bancario Guatemalteco, se utilizaron libros, diccionarios, textos, folletos, seminarios y sitios web que se tuvieron a disposición.

Expositiva
Con base a lo obtenido en la fase indagadora se procedió a la aplicación de los conocimientos y planteamientos establecidos en el plan de investigación, especificado en los capítulos que corresponden.

Concordancias y Diferencias

Con base a la información obtenida a través de los métodos expuestos anteriormente se analizó qué procedimientos teóricos aplican a la realidad que se presenta en está investigación.

c) Técnicas

Se aplicaron técnicas de recopilación de datos bibliográficos, observación, análisis e interpretación de resultados presentados en el trabajo práctico que se desarrollo.

d) Comprobación de la Hipótesis

En el estudio realizado, se logró comprobar la hipótesis planteada al inicio de la investigación, ya que se confirmo, que las entidades emisoras de tarjetas de crédito, deben invertir en mecanismos, controles internos, herramientas electrónicas, que al ser evaluadas periódicamente por el departamento de auditoría interna de cada entidad bancaria, logrará minimizar el riesgo de fraudes por falsificación de banda magnética de tarjeta de crédito, que al final se transforman en perdidas financieras, además de proteger la imagen comercial.

CAPITULO I

TARJETA DE CREDITO

1.1 Antecedentes Históricos

El nacimiento de la tarjeta de crédito ocurrió a mediados del presente siglo, su desarrollo y aceptación mundial han sido rápidos, dejando a los legisladores y autores de la gran mayoría de países completamente rezagados en esta materia; sus orígenes se encuentran en lo que los economistas han llamado “la Sociedad de Consumo”, ya que su extraordinaria difusión ha permitido a los consumidores en forma ágil adquirir un sin número de bienes y servicios.

Las primeras apariciones de tarjetas de crédito similares a las que conocemos en la actualidad, las encontramos en la década de 1920, cuando en los Estados Unidos de Norte América las grandes empresas propietarias de grupos de sociedades controladas y con gran organización, generalmente internacionales, dedicadas al negocio del petróleo, crea una tarjeta que permite a sus clientes obtener crédito en sus diversas empresas, de igual manera, a efecto de aumentar sus ventas, las grandes tiendas llamadas “almacenes por departamentos” deciden adoptar este novedoso sistema de crédito emitiendo tarjetas que permitían a sus clientes predilectos obtener mercancías sin necesidad de cancelarlas al momento de obtenerlas.

En la misma forma las empresas aéreas norteamericanas también comienzan a entregar a sus clientes privilegiados determinadas tarjetas, por medio de las cuales se identificaba a los tenedores, facilitándoles así crédito, sin embargo la función primordial de dichas tarjetas era una identificación concedida por cortesía y se conocían como tarjetas de viaje aéreo (Air Travel Cards).

En el año 1950, un empresario se dio cuenta que podía hacer dinero dejando que otras personas utilizaran su tarjeta aérea cobrándoles por ello algún interés, lo cual le dio la idea de poder organizar una compañía que se dedicara específicamente a negociar con tarjetas de crédito, comercio que en aquel tiempo era desconocido y considerado como mala inversión, esta compañía fue llamada Dinners Club la que continua operando en la gran mayoría de países.

Originalmente las operaciones de esta compañía eran simples y rudimentarias por la cantidad de individuos involucrados, de la manera siguiente: - un poseedor de Dinners Club, consumía en determinado restaurante, y el club pagaría posteriormente al restaurante, descontando un porcentaje que oscilaba entre el 5% y el 7.5% por transacción, a cambio de la prestación del servicio de crédito; lo que seria reembolsado por el poseedor en determinado plazo.

En el año siguiente, 1951, el Franklin National Bank de New York, emite la primera tarjeta de crédito bancaria, acción que fue desarrollada por muchos otros bancos, entre los años 1958 y 1960, la gran mayoría de estos bancos y muchas otras compañías que fueron organizadas para promover estas tarjetas, tuvieron que desistir en su intento de continuar, en vista de las perdidas millonarias que habían sufrido por la falta de suficientes medidas de seguridad, además de haberse iniciado un conflicto de uso, derivado que el servicio no valía la pena para el comerciante a menos que hubiera un gran numero de tenedores de tarjetas de crédito, mientras que por su parte, el tenedor potencial, no tenía interés en la tarjeta de crédito a menos que hubiera un gran número de comerciantes involucrados.

En el año 1961, resurge la idea con mayores medidas de seguridad y más amplitud de funcionamiento, con dos empresas fuertes, siempre dentro de los Estados Unidos de Norte América, que son American Express y Master Charge, ambas con financiamiento bancarios muy fuertes y empresarios muy bien organizados.

Nacen de esta manera dos empresas especializadas en la emisión de tarjetas de crédito, desmembrándose definitivamente la calidad de vendedor y otorgante de crédito en dos personas

distintas; el tratadista argentino Cogorno[1], afirma que este es el verdadero sistema de tarjetas de crédito, indicando lo siguiente: “a través de una firma que sirve de cordón umbilical se unen empresarios totalmente independientes entre sí, y que no cuentan con una organización adecuada para hacer frente a las contingencias de este contrato, acercando bienes y servicios a una demanda que se centra a través de la firma emisora”.

Con la inclusión de un tercero en la relación crediticia, surge un vínculo complejo, en virtud de que mediante la formalización de diversos contratos individuales se forma una comunidad en donde se acepta consensualmente el otorgamiento del crédito, además esa comunidad debe ser lo suficientemente solvente para poder otorgar la más variada calidad y cantidad de bienes y servicios.

Con posterioridad se van internando en el mercado europeo, las ya famosas tarjetas de crédito en el continente Americano, siendo la Carte Bleu de Francia, la que logra su fijación completa en Europa para el año de 1967.

En Guatemala, se inicia en la década de los setentas y su evolución fue más lenta, debido a la economía conservadora que observaba la comunidad, rigiéndose básicamente por el dinero en efectivo; únicamente la empresa Credomatic, logró superar la etapa de introducción, logrando su fijación y aceptación dentro de la comunidad económicamente activa en un porcentaje bastante elevado, y por haber sido una de las pioneras en este campo y por su evidente habilidad para llegar al mercado popular, que es sabido es la gran mayoría y la que engruesa el sector netamente consumista, es que ha alcanzado un auge increíble.

La evolución de las tarjetas de crédito ha sido escabrosa y sólo después de soportar grandes pérdidas ha logrado establecerse este novedoso sistema de crédito. Errores han sido cometidos por las diversas compañías que han intentado estos programas, dentro de los más relevantes se encuentra, el envío en masa de tarjetas de crédito por correo, lo que provoca un sin número de tarjetas robadas, causando descontrol total en los procedimientos de verificación.

En la década de los noventa, se está instaurando un sistema de tarjetas de crédito personalizada, incluyendo una fotografía del tenedor, lo que hace que se llegue a una aceptación satisfactoria en el sistema económico moderno a nivel mundial.

El antecedente histórico obedece a una evolución increpante de nuevos sistemas de adquisición de bienes y servicios, habiendo inventado el sistema de tarjetas de crédito para solucionar momentáneamente el flujo de necesidades crecientes en cierto nivel, clase media y clase alta, en virtud del volumen de consumo y en función de su capacidad de pago.

1.2 Definición de Tarjeta de Crédito

Diversos tratadistas han definido a la tarjeta de crédito, desde distintos tópicos, atendiendo al modelo económico y jurídico existente al momento de crear tales definiciones.

El Jurista guatemalteco Edmundo Vásquez Martínez[2], define a la tarjeta de crédito de la manera siguiente: “La tarjeta de crédito es un documento expedido a favor de una persona determinada, que le da derecho a adquirir bienes al crédito en los establecimientos indicados por el dador”.

La escritora española María Gómez Mendoza[3], la define así: “Tarjeta de crédito es un documento que permite a su titular obtener bienes o servicios sin necesidad de tener que efectuar su pago de inmediato”.

---

[1] (6:190)

[2] (23:696)

[3] (8:391)

Raúl Cervantes Ahumada[4], connotado tratadista mexicano, inicia su definición haciendo una clasificación de la manera siguiente: “Son tarjetas de crédito directas las emitidas por entidades para la compra de artículos en su propio establecimiento exclusivamente, en esta relación, la entidad comercial es a la vez la entidad emisora o creadora de la tarjeta de crédito; son tarjetas de crédito indirectas, las emitidas por bancos o por instituciones especializadas en la comercialización de estos instrumentos, las que operan así: El acreditante abre al acreditado un crédito en cuenta corriente para que por medio de la tarjeta de crédito pueda este último presentarse ante establecimientos comerciales afiliados al creador de la tarjeta, y haciendo uso de su crédito obtengan bienes y servicios que el establecimiento proporcione, el que cobrará al creador de la tarjeta el consumo efectuado por el tenedor, a su vez el mismo creador enviará al acreditado un estado de cuenta mensual, y le cobrará el importe de las disposiciones que haya realizado”.

El tratadista español Rodrigo Uría[5], define la tarjeta de crédito de la manera siguiente: ”Las tarjetas de crédito son documentos generalmente expedidos por grandes bancos o entidades internacionales, para servir por una parte como instrumentos de pago, y en otra como instrumento de crédito de la entidad emisora a favor del titular de la tarjeta”.

Por último tenemos la definición del distinguido jurista Eduardo Guillermo Cogorno[6], quien define la tarjeta de crédito como sigue: “Es un contrato complejo de características propias que establece una relación triangular entre un comprador, un vendedor y una entidad financiera, posibilitando al primero la adquisición de bienes y servicios que ofrece el vendedor, mediante la promesa previa formulada a la entidad emisora de abonar el precio de sus compras en un plazo dado; por su parte el emisor se hará cargo de la deuda abonando inmediatamente el importe al vendedor, previa deducción de las comisiones que hayan estipulado ambos”.

No obstante las diferentes definiciones descritas anteriormente, es importante mencionar que dentro del Código de Comercio, en lo referente a los títulos de crédito, expone lo siguiente:

Se puede definir a la tarjeta de crédito como un documento expedido a favor de una determinada persona denominada tarjetahabiente, a través del cual una institución emisora de tarjetas, otorga un crédito, el cual puede ser utilizado, para la obtención de bienes y servicios, en los establecimientos comerciales afiliados con un ente adquiriente, estableciendo constancia de las condiciones y costos bajo las cuales se regirán estos servicios, en contratos celebrados tanto entre la institución emisora con el tarjetahabiente, así como entre el establecimiento comercial y la entidad emisora de la tarjeta.

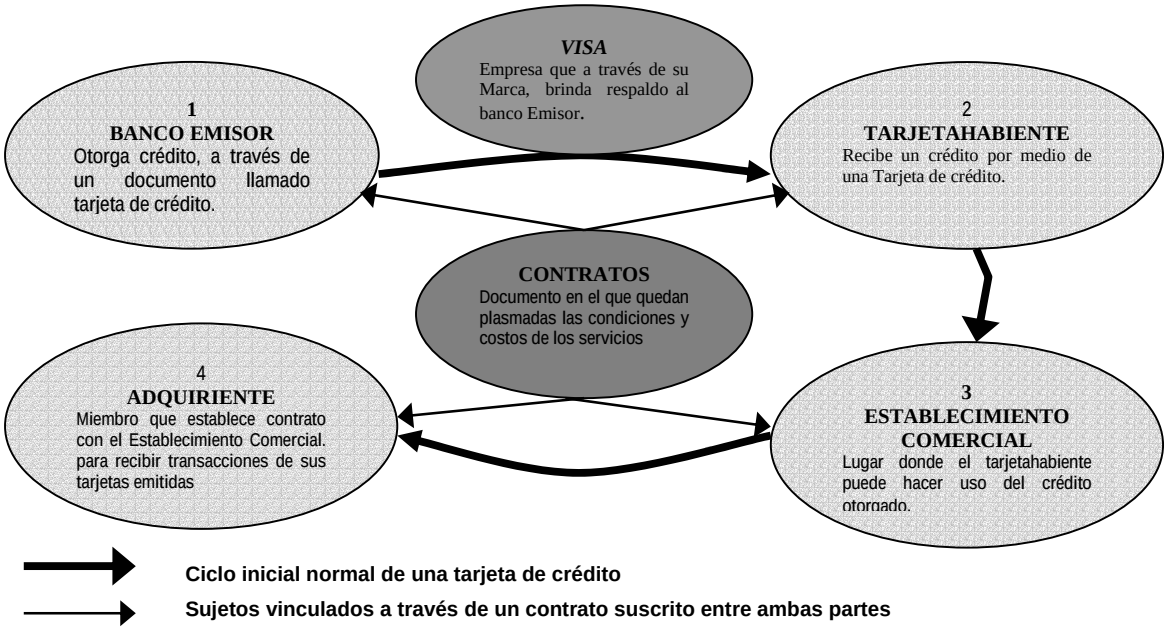
---

[4] (3:145)

[5] (21:687)

[6] (6:205)

Esquema No. 1
Proceso de una Tarjeta de Crédito



1.3 Naturaleza Jurídica

Respecto a la naturaleza jurídica de la tarjeta de crédito, varios autores han afirmado que se trata de un medio de pago, otros la circunscriben como una especie de contrato de aceptación de deuda, mientras otros lo tipifican como un titulo de crédito.

Por su parte la doctrina alemana sostiene que se trata de un titulo valor y aún sin ponerse de acuerdo en cuanto a la naturaleza jurídica de esta institución que crece día con día.

1.3.1 Considerada Como Título de Crédito

Dentro de los exponentes de esta teoría encontramos a Rodrigo Uría y a Edmundo Vásquez Martínez; el primero afirma que hay ciertos documentos configurados según el modelo del título de crédito de que se trate, denominados por el autor español como títulos de legitimación, porque cumplen con la doble función de permitir que el deudor se libere cumpliendo frente al tenedor legítimo del documento, y de facilitar al acreedor la transmisión del crédito legitimando al cesionario mediante la posesión del documento, entre estos se encuentran las cartas de ordenes de crédito y las tarjetas de crédito; por su parte, el jurista guatemalteco, considera a la tarjeta de crédito como un título impropio y como un título de legitimación diciendo, “Mediante la presentación de la tarjeta de crédito, su titular se pone en condición de adquirir el crédito objeto de la tarjeta, al igual que las cartas ordenes de crédito, cuyo régimen se les aplica, la tarjeta de crédito no confiere derecho alguno sobre los destinatarios”.

La corriente italiana se deja sentir en cuanto al contenido del Código de Comercio en Guatemala, particularmente en materia de títulos de crédito, y haciendo una crítica al argumento transcrito anteriormente, vale decir que el hecho de que se considere a la tarjeta de crédito, como un título de crédito impropio e imperfecto, nos da la sensación que no pertenece exclusivamente al campo de las cosas mercantiles en virtud de que si analizamos el articulo 385 del Código de Comercio[7] que literalmente dice: “Son los documentos que incorporan un derecho literal y autónomo, cuyo ejercicio y transferencias son imposibles independientemente del titulo, también tienen la calidad

[7] (5:54)

de bienes muebles". En consecuencia podemos extraer las características que la misma ley le otorga a los títulos de crédito y que parte de ellas hacen falta en la tarjeta de crédito; la incorporación se cumple a cabalidad en la letra de cambio o pagaré, pero definitivamente que en la tarjeta de crédito no se cumple fielmente, porque el derecho no esta solamente en el plástico mismo, que es la parte corporal de la misma, en ésta el derecho y la obligación se encuentra contenido en el contrato previamente suscrito entre el tarjetahabiente y el emisor.

Respecto a la transferencia de la tarjeta de crédito, se anota que ésta es intransferible, toda vez que si el poseedor legítimo de la misma la transfiere a otra persona tendría que ser por la simple tradición, ya que ésta no admite endosos, y quien recibe una tarjeta a nombre de otra, le es imposible hacer alguna gestión lícitamente.

Con referencia a la literalidad, característica cumplida parcialmente en la tarjeta de crédito, ya que si vamos a un documento de crédito perfecto se regirá por lo que diga en su tenor escrito, siendo que lo que no aparezca escrito en el propio título carece de trascendencia jurídica, ejemplo: en la tarjeta de crédito en ningún momento ni en ninguna parte de su estructura física aparece el monto al que estará sujeta, en función de los consumos y pagos hechos en diferentes fechas.

1.3.2 Considerada Como Título Valor

Siguiendo la tendencia de la doctrina alemana, algunos tratadistas ubican la naturaleza jurídica de la tarjeta de crédito como un título valor, derivado de esto es importante mencionar que en el proyecto de Ley Uniforme Centroamericana de Títulos Valores, en el articulo dos, indica que algunos valores no invalidan ni afectan el negocio jurídico que dio origen al documento o al acto, y es precisamente al Acto de Comercio al que atribuyen la naturaleza jurídica de las tarjetas de crédito, ubicándolas como instrumento jurídico, específicamente como un instrumento mercantil.

El insigne tratadista mercantil Joaquín Garriguez[8], expone que son dos las características que originan el derecho mercantil, por una parte el derecho de los comerciantes y por otra el derecho de los actos de comercio, ya que el derecho mercantil nunca ha sido, ni radicalmente subjetivo u objetivo, aunque esta última postura ha sido predominante, ello es porque a través del acto de comercio es que se define el comerciante.

Los códigos de comercio de la mayoría de países, han prescindido de una definición de los que comprende el Acto de Comercio y el nuestro no es la excepción, los legisladores han preferido hacer una enumeración taxativa de las materias que lo conforman, tal como ocurre con el artículo segundo del Código de Comercio; la esencia del mismo la encontramos en el hecho de que se trata de un acto masificado, en una reiteración de la misma operación realizada profesionalmente por distintos entes con ánimo de lucro, derivado de lo anterior se puede decir que la emisión de la tarjeta de crédito, según los parámetros del derecho mercantil, esta comprendida dentro de los actos de comercio.

1.3.3 Considerada Como Medio de Pago

Esta teoría defendida por el Jurista Hernando, Sarmiento Ricaurté[9], que entiende la naturaleza jurídica de tarjeta de crédito, como el medio de pago de que es objeto, en virtud de que ésta tarjeta permite al usuario (tarjetahabiente), adquirir los bienes y servicios que necesita sin pagar su precio en efectivo, siendo que el comprador paga con la exhibición de la tarjeta de crédito y su correspondiente firma; la finalidad del contrato es entonces la sustitución material del dinero, teniendo valor suficiente para extinguir obligaciones, siendo que la tarjeta de crédito se convierte en una especie de dinero (dinero bancario o dinero plástico), con las mismas cualidades.

El hecho de que el comerciante no reciba circulante (dinero) en forma inmediata, y en su lugar reciba un derecho independiente con legitimidad suficiente para lograr el cobro posterior y en

[8] (7:128)
[9] (17:7)

dinero, hace que se confirme que la tarjeta de crédito funge como medio de pago, como consecuencia del convenio celebrado entre el establecimiento y el emisor, según el cual aceptará el pago en forma diferida.

En efecto, el tarjetahabiente no desembolsa efectivo al utilizar su tarjeta de crédito al momento de efectuar su pago con ella, es innegable, con igual efecto liberatorio que el dinero físico o material.

La relación que surge entre el establecimiento y el tarjetahabiente, únicamente pone en marcha efectiva toda la relación jurídica que la tarjeta de crédito implica, siendo que el comerciante practicó una venta o prestó un servicio que le fue pagado a través de una tarjeta, ocurrió de inmediato que se materializa la relación crediticia a favor del tarjetahabiente. La obligación posterior del pago del precio de la mercadería vendida o del servicio prestado será a cargo del emisor, ello a consecuencia de la relación jurídica que atañe al tarjetahabiente, al emisor y al comerciante o proveedor.

1.4 Características de la Tarjeta de Crédito

Las tarjetas de crédito, poseen las características siguientes:

- Son expedidas a favor de una persona determinada, es decir que no pueden extenderse tarjetas de crédito al portador.
- No son negociables, las tarjetas de crédito no pueden ser objeto de ningún traspaso, por lo que no son transferibles.
- Es un documento que identifica al portador del mismo como su propietario, ya que es extendida, por el acreditante a nombre de una persona determinada.
- Permite obtener bienes y servicios en forma inmediata, sin necesidad de efectuar un pago inmediato.
- Es aceptada como medio de compra por los establecimientos que previamente se ha afiliado al sistema tripartito de la tarjeta de crédito.
- El crédito es otorgado por una entidad acreditante, a través de la cual se otorga un crédito rotatorio, por una cuantía y plazo determinados, el que además es prorrogable.

1.4.1 Opciones que brinda una Tarjeta de Crédito

El uso de una tarjeta de crédito, en la actualidad, brinda al tarjetahabiente entre muchas las siguiente opciones:

- Evitar llevar grandes cantidades de efectivo, por lo cual le brinda seguridad.
- Facilitar la adquisición de bienes y servicios, en los establecimientos comerciales afiliados.
- Retirar efectivo en cajeros automáticos, que están al servicio las 24 horas.
- Bloquear la tarjeta rápidamente en caso de extravío o robo.
- Facilitar la reposición en caso de robo o deterioro.
- Evitar el cobro de intereses por financiamiento al realizar el pago del saldo total de la tarjeta, en el tiempo establecido en el estado de cuenta.
- Facilitar el control de saldos y movimientos a través de estados de cuenta.
- Compartir el límite de crédito, con una o varias tarjetas adicionales.
- Utilizar adicional al límite de crédito un porcentaje de sobregiro autorizado por la entidad emisora.

1.5 Sujetos que Conforman la Tarjeta de Crédito

En la tarjeta de crédito considerada como una institución jurídica y no como un mero documento, generalmente intervienen tres sujetos en una geometría triangular, originándose relaciones entre cada una de estos, los cuales son:

1.5.1 Emisor

Considerado el protagonista principal de esta transacción, en virtud de que este sujeto históricamente ha sido el que ha creado y desarrollado este sistema de pago, y desde el punto de vista jurídico son los emisores los que a la fecha establecen los contratos y condiciones bajo las cuales operan las tarjetas de crédito.

De la práctica diaria descubrimos que los emisores de tarjetas de crédito son de tres tipos:

a) **Empresas comerciales** que emiten sus propias tarjetas de crédito a clientes privilegiados, ejemplo de ello en Guatemala: Almacenes Siman, Tiendas Paiz, etc.
b) **Entidades especializadas** que emiten tarjetas de crédito, para ser utilizadas en diferentes establecimientos comerciales afiliados a este emisor, ejemplo en Guatemala: Credomatic, Dinners Club, etc.
c) **Entidades Bancarias**, que emiten tarjetas de crédito como parte de los servicios que ofrecen a sus clientes, ejemplo en Guatemala: Banco Uno, Banco de Comercio, Banco Industrial, etc.

1.5.2 Tarjetahabiente

Básicamente el tarjetahabiente es la persona individual o colectiva que ha solicitado la emisión de una tarjeta de crédito a su nombre, solicitud que tuvo que pasar por una serie de trámites de aprobación previa verificación e investigación de la información de la solicitud, por parte del emisor de la misma.

Las consecuencias jurídicas que se derivan de las relaciones entre el emisor y el tarjetahabiente, principalmente originadas por el contrato que ambos celebran, mediante el cual el emisor confiere la posibilidad de crédito al tarjetahabiente a través del uso de la tarjeta, obligación que inicia desde el momento en que el emisor entrega físicamente la tarjeta.

1.5.3 Establecimiento Afiliado o Proveedor

El establecimiento afiliado, participa en la relación triangular generada por la tarjeta de crédito, constituye el tercer sujeto involucrado, conceptualizándolo de la manera siguiente: Es la persona jurídica individual o colectiva que ha suscrito un contrato con el emisor de la tarjeta de crédito, habiendo cumplido con determinados requisitos, por lo cual deberá aceptar la tarjeta de crédito como medio de pago, en la adquisición de bienes y servicios que preste a los tarjetahabientes, sí este último así lo solicita.

Es importante mencionar que todas las instituciones bancarias emisoras de tarjetas de crédito, deben de asociarse a las Corporaciones Internacionales que Administran Tarjetas de Crédito, de reconocida trayectoria, esto con el fin de tener un buen respaldo de la marca, e incrementar el número de establecimientos comerciales en los que se acepten la tarjeta de crédito emitida por la institución bancaria.

Para la presente tesis, estudiaremos un banco privado que se encuentra afiliado a la Corporación de Administración de Tarjetas más grande y conocida en el ámbito mundial, como lo es **Visa*.***

1.5.4 Adquirente

Se denomina así al miembro que establece contrato con un establecimiento comercial, o desembolsa dinero a un tarjetahabiente en un desembolso de efectivo, y directa o indirectamente entra el recibo de transacción resultante del intercambio.

En el presente trabajo, se tomarán para estudio las tarjetas de crédito emitidas por una entidad respaldada por la marca **Visa**.

1.5.5 ¿Que es VISA?

VISA INTERNATIONAL SERVICE ASSOCIATION (VISA). Es una Corporación de miembros no accionistas formada para dar a través de su marca mundial, respaldo, solidez y fortalecer el respaldo de cualquier entidad emisora de tarjetas de crédito, inicialmente conocido como el programa de Tarjetas Bancarias **Azul, Blanco y Oro.**

En Guatemala, actualmente existen solo dos Adquirentes, ***Visanet,*** respaldado por Visa y ***Credomatic*** respaldado por Visa y Master Card. Las entidades afiliadas a **Visa,** pueden ofrecer a sus tarjetahabientes, una amplia cobertura de aceptación a nivel mundial, un mayor número de establecimientos comerciales afiliados, la red de cajeros automáticos más grande, y la confianza de la mayor cantidad de tarjetahabientes, lo cual se traduce en un mayor, mejor y sólido servicio en cuanto a tarjetas de crédito se refiere.

Lo anterior gracias a que **Visa**, en la actualidad posee la red de Informática y Telemática más grande del mundo**,** la cual esta integrada por lo siguiente:

- 190 países afiliados
- 300 millones de tarjetahabientes
- 10 millones de establecimientos afiliados
- 130,000 cajeros automáticos
- 22,000 instituciones financieras

El estar afiliado a una corporación como la descrita anteriormente, obtiene un gran respaldo de la marca reconocida en el ámbito mundial, como se demuestra en el siguiente diagrama.

Esquema No. 2
Respaldo de la Marca Internacional *VISA*

Fuente: Visa Internacional, Reglamento Operativo para América Latina y el Caribe.

1.6 Clasificación de las Tarjetas de Crédito

El autor Raúl Ahumada[10], distingue dos clases de tarjetas de crédito, las cuales se describen a continuación:

[10] (3:305, 306)

1.6.1 Tarjetas de Crédito Directas

La tarjeta de crédito directa, la define como, “Un documento que acredita a su tenedor como sujeto de crédito para obtener de la entidad comercial creadora o emisora de la tarjeta, mercancías o servicios para pagar al crédito’’. Respecto a este tipo de tarjetas, es la que ordinariamente se clasifica como la tarjeta del sistema bipartito, en el cual la entidad crediticia y el establecimiento comercial, se funden en una sola persona que es la que concede una línea de crédito al tarjetahabiente, para que obtenga en dicho establecimiento comercial, los bienes y servicios que requiera.

1.6.2 Tarjetas de Crédito Indirectas

Respecto a este tipo de tarjetas, Raúl Cervantes la describe diciendo que, “El acreditante que generalmente es un banco, abre al acreditado un crédito por cuenta corriente, para que por medio de la tarjeta pueda el acreditado, presentarse al establecimiento comercial afiliado, y haciendo uso de su crédito obtenga bienes o servicios del establecimiento que los proporcione, el que cobrará al creador de la tarjeta, que a su vez enviará al acreditado un estado de cuenta mensual y le cobrará el importe de las operaciones que haya realizado”.

Respecto a lo anteriormente expuesto, puede afirmarse que existen dos modalidades o sistemas:

1.6.2.1 Sistema de Tarjetas de Crédito Bipartito

El sistema bipartito, es en el cual intervienen únicamente dos partes; un establecimiento comercial, quien otorga el crédito y el tarjetahabiente como el beneficiario del mismo; ejemplo de este tipo de tarjetas, tenemos las que otorgan las empresas como: Almacenes Siman, Almacenes Sears, etc.

1.6.2.2 Sistema de Tarjetas de Crédito Tripartito

El sistema tripartito, es en el cual intervienen tres partes, una Unidad Financiera que puede estar constituida por un banco, siendo su función principal es otorgar una línea de crédito al tarjetahabiente y posteriormente la de realizar los pagos respectivos a los establecimientos que se deriven de la utilización de la tarjeta de crédito, también, participa el establecimiento afiliado, que es la persona individual o jurídica, que realiza la venta o prestación de los servicios que se adquieren a través de una tarjeta de crédito, y acepta que la misma sea obtenida mediante la presentación de la tarjeta y la firma de un comprobante de venta ***(Voucher)*** por parte del titular de la misma.

Dentro del sistema tripartito, existe una división, las cuales por la persona a la que se extiende, se clasifican en:

a) Tarjetas Personales

Es la que se otorga a personas individuales. La responsabilidad del manejo de la cuenta recae directamente sobre ellas. Los tipos de tarjeta personal que se ofrecen son:

- Clásica Local
- Clásica Internacional
- Oro
- Platinum

b) Tarjetas Empresariales

Son emitidas únicamente a empresas de tipo Sociedad Anónima ó de Responsabilidad Limitada. Pueden obtener estas tarjetas los ejecutivos de alto nivel jerárquico dentro de la empresa. Su función principal es cubrir gastos en nombre de la empresa. El límite de crédito

es otorgado a la cuenta, por lo que el mismo es compartido entre todos los ejecutivos. Es aceptada a escala mundial.

c) Tarjetas Adicionales

Son las extensiones otorgadas a las tarjetas de tipo personal, los consumos son desglosados y distribuidos en el mismo estado de cuenta del tarjetahabiente principal. Tanto la tarjeta personal como la adicional comparten el mismo crédito. Las personas facultadas para obtener una tarjeta adicional son los parientes en el primer grado de consanguinidad y de afinidad del tarjetahabiente principal.

Por otra parte, las tarjetas de crédito por su uso se clasifican en:

1.6.3 Tarjetas Locales

Se otorgan a título personal y pueden ser usadas en varios establecimientos comerciales con la limitación, que su uso únicamente puede ser dentro del territorio nacional, en donde fue emitida, en este caso en Guatemala.

1.6.4 Tarjetas Internacionales

Se otorgan de tipo personal o empresarial, pueden utilizarse indistintamente dentro y fuera del territorio nacional en todos los establecimientos afiliados a Visa, son emitidas en un determinado país pero su uso no se limita a éste, sino por el contrario puede adquirirse con esta tarjeta bienes o servicios en otros países, siendo un requisito exigido para poder optar a estas tarjetas, que el tarjetahabiente tenga su domicilio en el país en donde se emite la tarjeta de crédito, las cuales además le dan la oportunidad de adquirir los bienes y servicios en dólares americanos en cualquier lugar del mundo.

1.7. Actualidad de Transacciones de Tarjetas VISA, en Centro América

Es difícil creer que la industria de pagos con tarjeta tenga menos de 30 años, hace sólo unas pocas décadas, los compradores únicamente podían pagar con dinero en efectivo o con cheques.

Hoy en día, las tarjetas de pago se han transformado en una parte integral de nuestras vidas, ya sea que las usemos como crédito o débito, para viajar o en nuestro lugar de residencia, para compras o en los cajeros automáticos ATM ***(Administration Transaction Machine),*** el poseer una tarjeta de pago abre un mundo entero de posibilidades.

Visa es la marca de pagos líder en el mundo, las tarjetas que llevan esta marca, generan un volumen anual de US$ 2.7 billones (millones de millones).

En Centroamérica, **Visa** es un actor importante en el mercado de dinero plástico, aspecto que se ve reflejado en las cifras estadísticas de esta firma en el istmo.

Al mes de septiembre de 2004, el número de tarjetas de crédito y débito **Visa** en la región centroamericana suman más de 3.96 millones, registrando un crecimiento de 23.4% con relación al mismo período de 2003.

En lo que a transacciones en el istmo se refiere, a septiembre del año pasado estas fueron del orden de los 97.8 millones, generando un volumen de ventas de US$ 4,673 millones de manera consolidada.

En la región centroamericana Costa Rica es el país poseedor de mayor número de tarjetas de crédito y débito **Visa** al registrar 1.3 millones en este rubro, al mes de septiembre del 2004. Le sigue en su orden, Guatemala con 865,166 tarjetas, El Salvador con 815,686, Honduras con 629,020, y Nicaragua con 352,900 tarjetas.

Al igual que en el número de tarjetas, Costa Rica ocupa el primer lugar en lo que a transacciones se refiere, al registrar 39 millones de ellas al mes de septiembre del 2004. En este rubro Guatemala ocupa el segundo lugar con 25 millones, El Salvador el tercer lugar con 18.8 millones de transacciones, luego Honduras con 10 millones, y finalmente Nicaragua con 5 millones de transacciones.

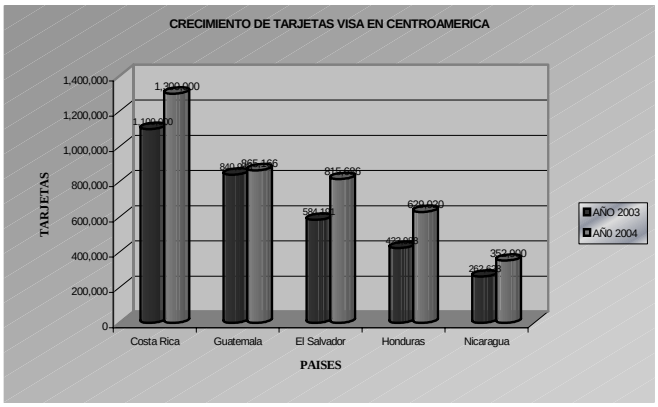
En Centroamérica, los miembros que emiten tarjetas **Visa** suman 47. Costa Rica cuenta con 18 bancos miembros, Guatemala con 21, El Salvador con 8, Honduras con 8, y Nicaragua con 6 emisores principales.

Cuadro No. 1
Estadísticas de Tarjetas VISA y Transacciones en Centroamérica

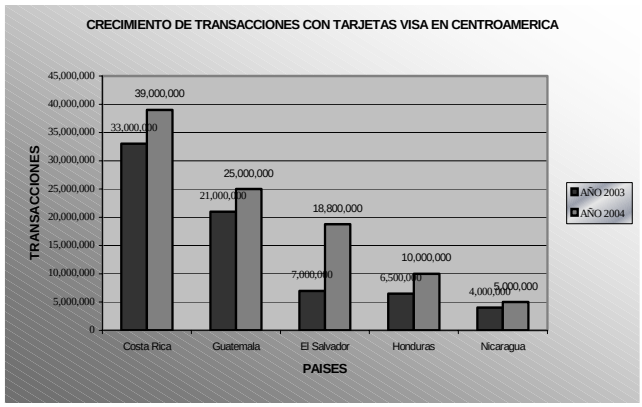
CENTROAMERICA : NUMERO DE TARJETAS VISA Y TRANSACCIONES POR PAIS								
Al 30 de septiembre de cada año								
	Tarjetas (Incluye Crédito y Débito)			Transacciones (Incluye Crédito y Débito)			Transacciones Promedio por Tarjeta	
País	**2003**	**2004**	**% Crecimiento**	**2003**	**2004**	**% Crecimiento**	**2003**	**2004**
Costa Rica	1,100,000	1,300,000	18.2	33,000,000	39,000,000	18.2	30	30
Guatemala	840,943	865,166	2.9	21,000,000	25,000,000	19.0	25	29
El Salvador	584,191	815,686	39.6	7,000,000	18,800,000	168.6	12	23
Honduras	423,988	629,020	48.4	6,500,000	10,000,000	53.8	15	16
Nicaragua	262,628	352,900	34.4	4,000,000	5,000,000	25.0	15	14
Totales	***3,211,750***	***3,962,772***	***23.4***	***71,500,000***	***97,800,000***	***36.8***		

Fuente: Diario Moneda, apartado de Empresas Destacadas, Marzo 29 de 2005, pagina No. 6.

Gráfica No. 1



Gráfica No. 2



Fuente: Diario Moneda, apartado de Empresas Destacadas, Marzo 29 de 2005, pagina No. 6.

Como se puede apreciar en el cuadro anterior, en Centroamérica los principales emisores de tarjetas de crédito lo constituyen los bancos, efecto que se extiende a escala mundial.

1.8 Antecedentes Legales y Operativos en Guatemala

Es importante mencionar que el sistema bancario de cada país, esta íntimamente ligado a la economía y la forma de gobierno de cada uno de ellos, lo cual origina que los bancos adopten diferentes estructuras, derivado del sistema financiero que rija en el mismo.

Los sistemas bancarios de los diversos países varían de uno a otro, pero todos han tendido en las últimas décadas a gravitar alrededor de los sistemas de Banca Central, cuyo arquetipo es el inglés y que se compone de tres partes: el Banco Central, Bancos Comerciales y varias instituciones auxiliares que se dedican a ciertos tipos concretos de crédito. La distinción entre Bancos Centrales y Comerciales radica por esencia en sus objetivos. El Banco Comercial persigue principalmente obtener utilidades, en cambio al Banco Central interesa en primer lugar los efectos que sus operaciones produzcan en el sistema monetario, cambiario y crediticio El Banco Central es uno solo en cada país, sus operaciones son fundamentalmente con el resto del sistema bancario y con el sector público: gobierno central e instituciones estatales descentralizadas. De acuerdo a sus propios principios el Banco central no debe tener accionistas, sino ser un Banco del Estado con la autonomía necesaria para que no sea entorpecida su labor.

El Banco de Guatemala, funciona bajo la dirección general de la Junta Monetaria, la cual tiene como función, normar lo relativo a la operatoria de las entidades que conforman el sistema bancario.

Así también la Superintendencia de Bancos en Guatemala, tiene la función de supervisar, las operaciones que realizan las entidades bancarias.

Es importante mencionar que anteriormente, la Ley de Bancos no permitía que las instituciones bancarias, otorgarán financiamiento a través de tarjetas de crédito, pero si estaba permitido por la legislación general, que se crearan empresas afiliadas, por medio de las cuales prestaban el servicio de tarjetas de crédito.

Derivado de la evolución que mostraba la banca en Guatemala, así como el incremento en la demanda de servicios y productos financieros por parte de los clientes, se evidenció la poca aplicabilidad de la Ley de Bancos anterior.

Por lo anterior, el Congreso de la República de Guatemala, decidió realizar una evaluación a las leyes que regían lo relativo al sector financiero, determinando que era prudente derogar las anteriores, para darle paso a una nueva legislación, más moderna, funcional y aplicable al avance demostrado por las instituciones bancarias.

En Guatemala, el funcionamiento de los Bancos del Sistema, actualmente está regido por la Ley de Bancos y Grupos Financieros, **Decreto número 19-2002**, en lo aplicable por la Ley Orgánica del Banco de Guatemala, **Decreto número 16-2002**, Ley Monetaria, **Decreto número 17-2002**, Ley de Supervisión Financiera, **Decreto número 18-2002**, todos del Congreso de la República de Guatemala, y por las disposiciones emitidas por la Junta Monetaria. En las materias no previstas en estas leyes, se sujetarán a la legislación general de la República en lo que les fuere aplicable.

Cabe mencionar que la Ley de Bancos y Grupos Financiero[11], ***(Decreto No. 19-2002)***, establece en el Titulo I **(Disposiciones Generales)**, en su articulo No. **3 (Intermediación Financiera Bancaria)**, lo siguiente: “Los bancos autorizados conforme esta Ley o leyes especificas podrán realizar intermediación financiera bancaria, consistente en la realización habitual en forma pública o privada, de actividades que consistan en la captación de dinero, o cualquier instrumento representativo del mismo, del público, tales como la recepción de depósitos, colocación de bonos, títulos u otras obligaciones, destinándolo al financiamiento de cualquier naturaleza, sin importar la forma jurídica que adopten dichas captaciones y financiamiento”. Esta misma Ley, en el Titulo IV (**Los Bancos, sus Operaciones y Servicios)**, en su articulo No. 41 (**Operaciones y Servicios)**, establece lo siguiente, “Los bancos autorizados conforme esta Ley podrán efectuar las operaciones en moneda nacional o extranjera y prestar los servicios siguientes”; en el inciso b) **Operaciones Activas**, *numeral 5)* **Emitir y operar tarjetas de crédito.** Adicionalmente a lo anterior, en el último párrafo del mismo articulo, establece lo siguiente ”La Junta Monetaria podrá previa opinión de la Superintendencia de Bancos, autorizar a los bancos a realizar otras operaciones y prestar otros

[11] (9:2)

servicios que no estén contemplados en esta Ley, siempre y cuando los mismos sean compatibles con su naturaleza".

Por lo anterior, nuestro trabajo estará circunscrito a las operaciones de tarjetas de crédito que un banco privado puede realizar en Guatemala, en su calidad de emisor y agente intermediario en este tipo de transacciones. En este contexto, dicha entidad debe desarrollar de manera profesional, el ambiente adecuado para la interacción en el manejo y administración de las tarjetas de crédito, incorporando dentro de su estructura un departamento especializado, responsable y capaz de llevar a cabo sin contratiempos todo este tipo de operaciones, el cual a su vez debe estar integrado administrativamente por diversas áreas de trabajo. Existen innumerables estructuras organizativas sobre las cuales puede girar este negocio, en el siguiente apartado se describe en forma sencilla uno de ellos.

1.9. Organización de un Departamento de Tarjeta de Crédito en un Banco Privado

Se puede identificar dentro de un banco privado, un departamento de tarjeta de crédito, el cual debe estar organizado administrativamente con las siguientes áreas:

1.9.1 Gerencia de Tarjeta de Crédito

Esta área es la responsable de fijar y conducir las políticas de todas las actividades del departamento, debe planificar, dirigir, y coordinar las actividades a corto, mediano y largo plazo, siendo responsable del resultado de las operaciones.

1.9.2 Análisis de Créditos

Esta sección, tiene a su cargo el análisis y la evaluación de la información financiera presentada por el solicitante, para poder determinar la categoría de cliente, la capacidad de pago, los flujos de fondos del mismo. Lo anterior se realiza para poder determinar, según los resultados de la evaluación financiera efectuada, que clase de tarjeta se le puede autorizar, que límite de crédito se le puede asignar, con el fin de que al emitir la tarjeta de crédito, el riesgo en que se incurra sea mínimo y no enfrentar futuras pérdidas financieras para el banco.

El análisis de la información financiera es vital, así como las referencias o su récord crediticio, el cual puede ser consultado a través de los sistemas de información crediticia como por ejemplo el Buró de créditos de la Asociación Bancaria Guatemalteca. Adicionalmente es importante hacer mención que la Superintendencia de Bancos, recientemente implementó un sistema de información de riesgos, para fines de análisis de crédito.

1.9.3 Comité de Riesgos - Autorización de Tarjetas

En algunas instituciones existe más de un comité, encargado de evaluar las solicitudes de tarjetas de crédito, estos comités pueden dividirse, dependiendo del límite de crédito que se esté asignando a las tarjetas. Los integrantes de dicho comité evalúan la intensidad del riesgo al autorizar una tarjeta, tomando en cuenta la categoría del cliente, su capacidad de pago y otros aspectos de su flujo de fondos, para determinar si es factible o no la aprobación respectiva.

1.9.4 Gestión de Cobros

Esta área tienen como finalidad, dar seguimiento a la cartera de tarjetas de crédito en situación de Mora de **30, 60 y 90 días** de atraso, debido a la falta de pago por parte de los tarjetahabientes, realizando las gestiones necesarias para solicitar los pagos atrasados, ya sea por medio telefónico o escrito. Cuando dichos saldos no pueden ser recuperados y pasa **de 90 días hasta un máximo de 180 días**, se convierte en cartera en Cobro Administrativo, momento en que esta sección debe coordinar el cobro de los fondos, a través de una empresa especializada en la recuperación de fondos, y por última instancia, de ser necesario cuando el saldo atrasado pasa de **180 días**, debe

trasladar el caso al departamento jurídico para realizar la gestión de cobro a través de la vía judicial.

1.9.5 Contabilidad e Impuestos

Esta sección tiene la función de llevar el registro contable de las transacciones especificas que realiza el departamento de tarjeta de crédito, desde los gastos administrativos, los financiamientos que integran la cartera de créditos en sus diferentes situaciones, así como el control de efectuar los pagos de impuestos al fisco, adicionalmente se encarga de elaborar los informes requeridos por la Superintendencia de Bancos.

1.9.6 Informática y Desarrollo

Esta área tiene asignado, mantener en buenas condiciones el equipo de informática, así como brindar el soporte técnico en la elaboración de programas que faciliten la labor y que garantice la confiabilidad y oportunidad de la información del sistema de la tarjeta.

1.9.7 Mercadeo y Ventas

Le corresponde planificar, coordinar y supervisar el desarrollo, ejecución de los programas y políticas de mercadeo a efecto de determinar las oportunidades de mercado y los requerimientos para los productos existentes, productos nuevos y otros campos de esfuerzo del departamento.

1.9.8 Supervisión y Seguridad Administrativa

Tiene como función, dar seguimiento a transacciones inusuales de las tarjetas de crédito, que derivado de sus características individuales, difieren de los parámetros establecidos previamente, para que funcione la tarjeta. Para ello se auxilian de herramientas informáticas como lo son las alertas electrónicas que son recibidas de parte de los adquirentes y Visa, con el fin de establecer si éstas transacciones están siendo realizadas por el tarjetahabiente, o son fraudulentas, con lo cual se procede a bloquear inmediatamente la tarjeta y seguir con su investigación.

Adicionalmente esta área tiene a su cargo, el seguimiento de los reclamos formulados por tarjetahabientes, los cuales se basan en procesos y plazos establecidos por Visa, para dar resolución a cada caso.

De las funciones comentadas anteriormente, es importante mencionar que de identificar alguna transacción, con características de Lavado de Dinero, se debe proceder a informar inmediatamente al Oficial de Cumplimiento de la Institución, para que documente el caso e informe a la Superintendencia de Bancos a través de la Intendencia de Verificación Especial.

1.9.9 Auditoría Interna

La auditoría interna, se define como un área de staff, dependiente del Consejo de Administración, con actividad totalmente independiente dentro de una organización, para la revisión de la contabilidad y otras operaciones. Tiene como función, medir y evaluar la efectividad del control interno, asiste a todos los miembros de dirección, con relación al cumplimiento de sus responsabilidades, al facilitarle análisis, evaluaciones, recomendaciones y comentarios pertinentes, relativos a las actividades que revisan. Ayuda a la administración a alcanzar sus metas y objetivos con mayor eficacia, eficiencia y economía, al proporcionar en forma oportuna recomendaciones sobre las operaciones y actividades de la entidad.

1.9.10 Control de Calidad

Esta sección tiene como función, el archivo de los expedientes que incluyen toda la documentación legal, requerida para la apertura de una tarjeta de crédito, también se encarga del envío de los plásticos nuevos a los tarjetahabientes, y custodia de los plásticos vírgenes para futuras tarjetas.

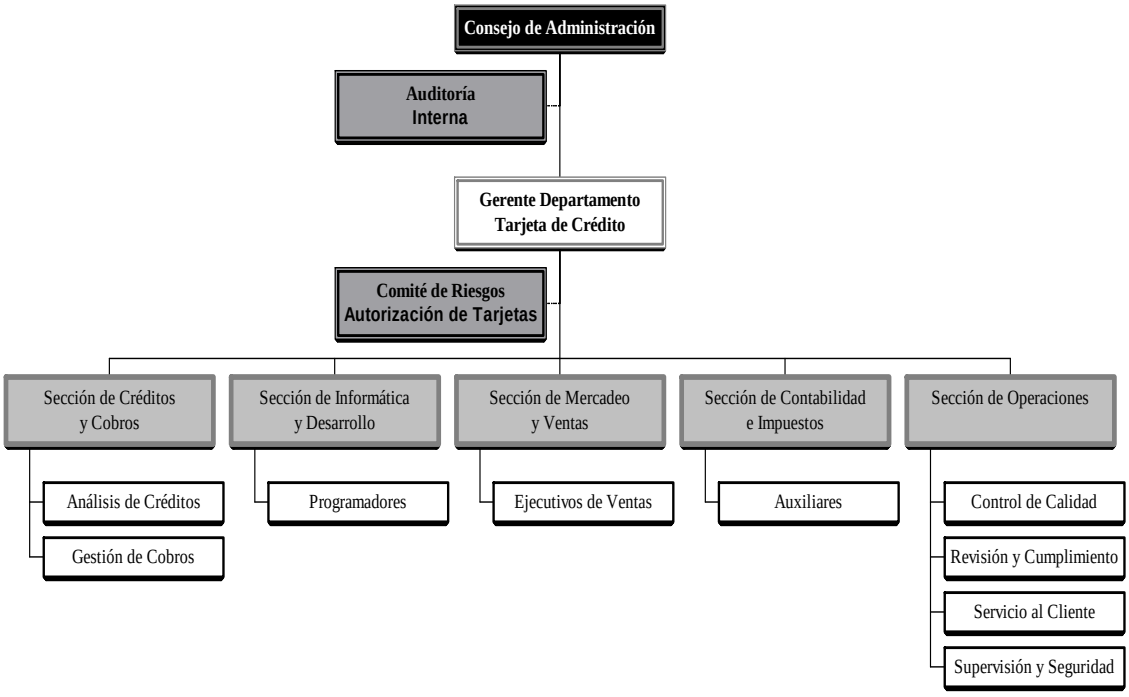
1.9.11 Servicio al Cliente

Es la sección encargada de realizar todas las gestiones para la apertura de tarjetas de crédito, lo cual incluye atender al cliente, para llenar y solicitar toda la documentación necesaria para el trámite respectivo.

1.9.12 Revisión y Cumplimiento

Esta área tienen como función, revisar y evaluar que los expedientes de las tarjetas de crédito, cumplan con toda la documentación requerida internamente por la institución y externamente por lo que exige la Ley de Lavado de Dinero u Otros Activos. También tienen a su cargo la confirmación de referencias personales, familiares, y comerciales, descritas por el cliente en la solicitud de tarjeta de crédito. Además se encarga de listar los estados de cuenta, según las fechas de corte de las mismas, para su posterior envío a los tarjetahabientes.

Esquema No. 3
Organigrama de un Departamento de Tarjeta de Crédito



Fuente: Santiago J. Bullrich
La Tarjeta de Crédito
Abeledo Perrot, Primera Edición

CAPITULO II

EL FRAUDE EN INSTITUCIONES BANCARIAS EMISORAS DE TARJETAS DE CREDITO

Ante la sofisticación tecnológica del crimen organizado, que ha abierto grietas en la seguridad de las operaciones realizadas por las instituciones bancarias, la experiencia nos muestra que la globalización de los mercados financieros ha propiciado colateralmente la internacionalización en la actividad de las bien organizadas bandas de delincuencia.

Por lo anterior, a continuación se comenta brevemente algunos pormenores del fraude, su concepto y modalidades del mismo.

2.1 Concepto de Fraude[12]

Es el engaño de que se vale una persona para hacerse de un objeto de procedencia ajena en perjuicio de otra. En el caso de los cheques y tarjetas de crédito el fraude se clasifica en:

- **Alteración de la Información**. Sin importar como sean llenados los cheques - a mano, máquina de escribir o impresora -, alterar, agregar o quitar información puede ser más sencillo de lo que aparenta.
- **Duplicación de Documentos**. Las nuevas tecnologías como escaneadores y fotocopiadoras a color permiten a la delincuencia generar una reproducción casi idéntica de cualquier documento.
- **Robo de Cheques en Blanco**. No obstante todas las medidas que podamos tomar para evitar perder cheques, desafortunadamente llegan a pasar por muchas manos antes de ser llenados y pagados. Por eso nunca estará de más tomar un tipo de precauciones para evitar estas situaciones.
- **Falsificación de Firma en Documentos**. El sistema financiero mundial se atiene a una firma autógrafa para el pago de documentos.
- **Alteración de Caracteres Magnéticos**. Hoy día nuestro sistema financiero utiliza tecnología para facilitar el proceso de captura de la información de los cheques, como lo es la banda de caracteres magnéticos. Si esta misma se llegara a cambiar o alterar, ya no estaríamos hablando del mismo cheque, sino de otro totalmente distinto.
- **Transferencias Electrónicas**. Con la nueva tendencia de las empresas a realizar sus pagos mediante transferencias electrónicas, cada vez es más frecuente que se realicen fraudes internos o robo de la información al momento de transferirse los datos de la operación.

En nuestra legislación, se puede mencionar que el Código Penal ***(Decreto No. 17-73),*** establece en su Titulo VI **(De los delitos contra el patrimonio)** y Capitulo V (**De la Estafa**), articulo No. 263 (**Estafa Propia**), lo siguiente: "***Comete estafa quien, induciendo a error a otro, mediante ardid o engaño, lo defraudare en su patrimonio en perjuicio propio o ajeno***".

También se entiende por fraude[13], cualquier engaño, maniobra o ardid destinado a producir un beneficio al agente y una pérdida (daño) a la víctima. De modo que involucramos tanto a "actos" aislados como a un conjunto de "actos" concatenados para producir el aludido efecto.

Entre los actos fraudulentos que se manifiestan a escala mundial, se incluyen aquellos por los cuales los delincuentes obtienen el ingreso al mercado financiero de los fondos obtenidos de actividades ilícitas, más específicamente en los últimos años, los provenientes del narcotráfico.

Esa acción de hacer ingresar tales fondos en este mercado para después darles una utilización lícita, se conoce hoy en día con el nombre de "Lavado de Dinero".

---

12 (14:4)

13 (24:197)

2.1.1 El Fraude Global

Desde hace tiempo, la falsificación de billetes dejó de ser un buen negocio para la delincuencia organizada. Y es que los avances tecnológicos están siendo bien aprovechados por los "Cerebros" de estas bandas en la producción de cheques y tarjetas de crédito apócrifos (es decir que son emitidos a nombres de personas que no existen).

Nos enfrentamos a organizaciones criminales profesionales muy complejas y con gran capacidad tecnológica para desarrollar esquemas de fraude a escala internacional. La tecnología que utilizan los grupos delictivos organizados en todo el mundo para falsificar cualquier tipo de documento principalmente cheques, billetes y tarjetas de crédito, es del más alto nivel. Es tal la magnitud de casos de fraude que ocurren actualmente, que la competencia entre documentos buenos y malos se da todos los días.

2.1.2 La Estafa – Consideraciones[14]

La estafa es el perjuicio económico-patrimonial realizado con ánimo de lucro mediante engaño.

Cometen estafa los que, con ánimo de lucro, utilizan el engaño para producir error en otro, induciéndole a realizar un acto de disposición en perjuicio de sí mismo o de un tercero.

Algunos de los motivos que justificarían el incremento evidenciado en la cantidad de maniobras estafadoras, son los siguientes:

- En una economía más saneada, las empresas son más propensas a pasar por alto transacciones dudosas, inadmisibles en periodos de recesión.
- El fraude se esta convirtiendo en un negocio para las organizaciones delictivas locales, nacionales e internacionales.
- La tecnología facilita la falsificación, imitación y cambios documentales.
- Algunas modificaciones legislativas a favor de los usuarios, favorecen involuntariamente al delincuente y perjudican a autoridades y empresas.
- Las probabilidades de obtener grandes beneficios han aumentado notoriamente.
- La prioridad social se centra en la erradicación de los delitos violentos.

2.1.3 Acción Delincuencial – Modalidades

La falsificación es la alteración o modificación realizada en un documento autentico, mediante la supresión mecánica (borrados o respados) o química (lavado); la adición y el retoque, indistintamente, la imitación es la reproducción de un documento autentico.

2.1.3.1 Falsificación

Los mecanismos delictivos para materializar las falsificaciones pueden resumirse sintéticamente en tres procedimientos de matiz genético.

a) Procedimiento de Sustracción

Una vez más, el desarrollo de la tecnología ha facilitado la ampliación de los sistemas utilizados en este procedimiento, no siendo posible descartar ninguno, pues por el contrario, son aplicados en forma indistinta por los falsificadores. Estos sistemas se concretan en el raspado, borrado o lavado químico de los documentos.

La técnica del raspado es quizá la más antigua y ha venido siendo aplicada a una variedad de documentos, ya que son únicamente necesarios para su práctica elementos metálicos afiliados,

[14] (12:1)

como cuchillas o estilizados punzones, los que auxiliados por lupas permitirán erosionar los lugares deseados de la superficie. Una restauración posterior, tan minuciosa como precisa sea la habilidad del delincuente, intentara hacer frente a comprobaciones más o menos rigurosas.

Las entidades financieras vienen combatiendo esta técnica con la incorporación de medidas de seguridad en el entramado del documento, lo que permite no solo su detección en una posición de contraluz, sino que dificultara la restauración del falsificador y facilitara el descubrimiento en un examen visual ordinario.

Estas medidas de seguridad se localizan en las zonas de mayor riesgo del documento, consistiendo en un entramado de líneas que de manera individualizada son casi imperceptibles, pero que en su conjunto conforman un fondo que sirve de soporte a los contenidos fundamentales del documento.

En los últimos años han venido completándose estas franjas microlineales con el empleo de tintas fluorescentes, pues la acción mecánica desfigura los colores y facilita su detección a través del empleo de lamparas de luz ultravioleta.

b) Procedimiento por Adición

Básicamente, es el empleo de las técnicas del añadido o enmienda.

La primera, el añadido, consiste en la inclusión de cifras o letras en un texto sin ninguna otra modificación en su desarrollo. Es común a la mayoría de las falsificaciones que este añadido se produzca en fechas o cantidades, siendo particularmente difíciles de detectar dada la metodicidad en el uso de las tintas y dibujos por los falsificadores.

La segunda, la enmienda, se realiza a partir de la superposición de un texto falso a otro verdadero, actuación que provocara su equivocada interpretación en beneficio del falsificador. Es también de difícil detección a simple vista, siendo necesaria la utilización de medios ópticos especiales o químicos.

La superposición de trazos manuscritos o mecanografiados o la mezcla de ambos, es uno de los retos que hoy plantea la realidad de los fraudes.

c) Procedimiento de Sustitución

Considerado de alto riesgo por los falsificadores más expertos debido a la mayor facilidad en ser detectado, combina de los anteriores procedimientos de sustracción y adición. Se logra mediante la eliminación de una parte del texto y la inclusión de otro falseado, lo que es conocido entre los expertos como la técnica del “injerto”, consistente en la extracción de los números o letras del documento autentico y reemplazarlos, generalmente, por otros provenientes también de documentos similares.

2.1.3.2 Imitación

Si cuando se refirieron las falsificaciones tenían cabida gran variedad de tipos de delincuentes, en las imitaciones (la reproducción integral de un documento, a partir de un soporte en blanco) solo sobreviven los mejores.

Los altos costos de cualesquiera de los métodos de impresión inhabilitan a los menos organizados o inexpertos, convirtiendo los resultados de las falsificaciones por este procedimiento en un grave problema internacional.

Documentos de identidad, cheques y documentación bancaria en general y moneda de todos los países del mundo – en especial dólares estadounidenses -, son sistemáticamente reproducidos día

tras día en todo el mundo. En ocasiones estas imitaciones están a cargo de redes delictivas, algunas de las cuales son todo un "'ejemplo" de organizaciones bien estructuradas.

2.1.3.3 Creación

A pesar que esta modalidad viene siendo utilizada desde hace años con mayor frecuencia que otras, la necesidad de precisar con mayor claridad las distintas técnicas utilizadas por los falsificadores, en aras del perfeccionamiento de los mecanismos de prevención, ha provocado el crecimiento de este concepto del anteriormente apuntado (la imitación), ante la desproporcionada magnitud que esta adquiriendo recientemente.

Por creación se designa a la elaboración de documentos falsos, sin que ello signifique que su reproducción se practique a partir de modelos gubernamentales u oficiales. Es el caso, por ejemplo, de los pasaportes supuestamente pertenecientes a países cuyos documentos oficiales son poco conocidos y que los falsificadores crean integralmente, o el de los documentos bancarios y financieros internacionales desarrollados por los delincuentes a partir de su propia imaginación.

Como se pudo observar, ningún sector esta libre de operaciones fraudulentas, debido a la gran organización de las bandas de defraudadores, así como a la variedad de formas, por medio de las cuales pueden realizar las mismas, de esa cuenta es importante mencionar que nuestro estudio, esta enfocado a los fraudes, que pueden ser objeto las tarjetas de crédito, que es un producto más que ofrecen instituciones que se dedican a las actividades bancarias.

2.2 Actividad Bancaria[15]

Se entiende que es la actividad que realizan los Bancos del Sistema Financiero, no limitadas a la mera intermediación de recursos financieros en el mercado del dinero, sino comprensivas de su actuación en el mercado de capitales.

Los bancos actúan hoy decididamente en el mercado de capitales, operando con títulos mobiliarios, derechos de futuro y opciones. Además realizan operaciones cambiarias y vinculadas con el comercio exterior.

Toda esta actuación los ha convertido en el instrumento ideal para lavar el dinero sucio provenientes de las actividades ilícitas.

2.2.1 Antecedentes de Fraude en la Actividad Bancaria

En el ámbito de la actividad bancaria y financiera estas maniobras o actos fraudulentos han sido y son muy frecuentes desde la maniobra urdida por John Law, un aventurero escocés que creó el Banco General, en Francia en 1716, hasta las maniobras detectadas en Estados Unidos de Norteamérica en los años 1985 y siguientes relacionados con los Savings Banks, pasando por las detectadas en bancos liquidados en la década del '80 y '90, se revela que infinidad de aventureros actúan en el mercado financiero y resultan incontables las maniobras ardidosas creadas para obtener beneficios y perjudicar a terceros.

Entre los actos fraudulentos incluimos aquellos por los cuales los delincuentes obtienen el ingreso al mercado financiero de los fondos obtenidos en sus actividades ilícitas y, más específicamente en los últimos años, los provenientes del narcotráfico.

2.3 Riesgos en la Actividad Bancaria

Es sabido que la actividad bancaria involucra importantes riesgos, porque la materia prima con la que estas entidades realizan sus actividades es por demás peligrosa: el dinero, en sus diversas formas y representaciones.

---

[15] (24:198)

Operar con recursos financieros, con numerario y distintos instrumentos representativos del dinero, ha constituido desde la antigüedad y constituye ahora un elevado riesgo.
De los distintos riesgos vinculados a esta actividad cabe citar el clásico riesgo de crédito, pero además está el riesgo de liquidez, el de inversiones, el de ganancias, etc., y entre otros el de fraude.

2.4 Riesgo de Fraude

Miles de maniobras tienen por finalidad obtener beneficios para el agente, y tienen como efecto generar un daño a la empresa bancaria o a sus clientes.

Este riesgo se combate con una combinación de medidas preventivas que llegan a disminuir su intensidad, pero nunca se podrá eliminar porque resultan ilimitados los medios y actos de fraude, es más, cada nueva operatoria que se incorpora en la actividad bancaria, cada nuevo servicio, introduce nuevas variantes y posibilidades de este riesgo.

En general se aconsejan medidas administrativas y de organización tendientes a aplicar los principios de:

a) División de Funciones

- Una correcta definición de las funciones de los distintos departamentos y áreas del banco;
- Una correcta política que norme la asignación de funciones al personal, definiendo con precisión sus responsabilidades;
- La separación de funciones, evitando la incompatibilidad entre las funciones adjudicadas;
- Rotación del personal.

b) Control Dual

El trabajo de una persona debe ser controlado o verificado por otra, a fin de asegurarse:

- Que se han aplicado los procedimientos internos en materia de ejecución de las operaciones y cumplido las reglas de autorización;
- Que las operaciones han sido correctamente registradas;
- Que una misma persona no realiza dos tareas incompatibles;
- Que han participado por lo menos dos personas en aquellas transacciones que implican pagos, liberación de fondos, transferencias, y en general salida o egreso de fondos o valores.

c) Controles Físicos

- Existencia de arqueos y controles sorpresivos y periódicos de numerario y valores.

No obstante que las instituciones implementen de buena forma, las recomendaciones descritas anteriormente, no implica que se elimine radicalmente el fraude, dado que cada uno de los productos que se ofrecen a los clientes, conllevan una serie de procedimientos, los cuales en cierta forma pueden generar situaciones que facilite el fraude, como las que se mencionan a continuación.

2.5 Situaciones que Facilitan el Fraude

Derivado de la diversidad de operaciones y servicios, que se realizan en la actividad bancaria, también así es el número de situaciones que facilitan el fraude, entre las cuales podemos enunciar las siguientes:

2.5.1 Falta de una Adecuada Reglamentación Preventiva

Como primera situación favorecedora de los fraudes, se cita la ausencia de adecuadas reglamentaciones de carácter preventivo.

Cuando la situación de los bancos e instituciones financieras es crítica, el fraude aparece como una consecuencia. Los problemas de liquidez y solvencia llevan muchas veces a que bancos buenos se conviertan en bancos malos. El comportamiento fraudulento a veces es la causa de las pérdidas iniciales, pero una vez que la falta de liquidez parece inevitable, el fraude es muy común.

A medida que se acerca el fin, los banqueros se sienten tentados de otorgarse a si mismos préstamos que es probable no vayan a reembolsar.

Otro fraude es el de la propiedad oscilante, de compañías parcialmente de propiedad del banco o de su director, si una compañía deja ganancias, el banquero tratará de comprársela al banco a un precio bajo, y si la compañía no es rentable, el banquero se la venderá al banco a un precio elevado.

2.5.2 Excesiva Intervención del Estado en la Actividad Bancaria

Cuando el estado interfiere en la libre actuación de los agentes, se amplía considerablemente la posibilidad de fraudes.

Nuestra experiencia reciente en el país, exhibe ciertos fraudes cometidos contra el Estado por parte de banqueros inescrupulosos y de otros agentes.

2.5.3 La Complejidad y Tecnicismo de la Actividad de los Bancos

También contribuyen a la mayor existencia y variedad de fraudes la complejidad de esta actividad, producto de su elevado tecnicismo. De modo que quienes conocen el funcionamiento de los mercados, por ser sus operadores, o haber realizado antes esta actividad, tienen adquirido el dominio de las reglas de funcionamiento y ello les facilita enormemente la comisión de fraudes.

2.5.4 Falta de Controles Internos Adecuados

La falta de adecuados controles internos en las entidades constituye una peligrosa grieta por donde se filtran actos de fraude y maniobras ardidosas tendientes a perjudicar a las entidades o a sus clientes.

Si los mecanismos internos de control no funcionan correctamente, si existe por ejemplo, una inadecuada distribución de funciones, de modo que quienes realizan una determinada operatoria son quienes efectúan los registros contables de esas operaciones, o quienes realizan los registros son, a su vez quienes los verifican, será muy difícil detectar dichos actos y maniobras.

2.5.5 Falta de Rotación de Personal

Se ha advertido a través de las crisis generalizadas en las entidades de ahorro y crédito norteamericanas de los años ochenta, que una de las causas más comunes de fraudes a las entidades fue la falta de rotación del personal.

Aquel funcionario que nunca falta ni se toma licencia, que siempre realiza la misma tarea, especialmente los gerentes o encargados de sucursales en áreas suburbanas y pequeñas localidades del interior, ha sido el típico defraudador, mediante maniobras como el no ingreso de depósitos importantes o el desvío de depósitos a otras cuentas manejadas por él.

2.6 Situaciones Específicas de Fraude

La actividad bancaria esta influenciada por varios factores, los cuales se conforman de una gran variedad de actividades y situaciones, que son las que inciden en el desarrollo de la misma.

2.6.1 Fraudes al Banco o Utilizando al Banco

Numerosos casos de fraudes se cometen contra los bancos, sea por terceros, por sus clientes o por su personal. Hay también diversos casos de fraude cometidos por terceros, utilizando al banco como vía necesaria para la maniobra ardidosa.

Por ello distinguiremos los fraudes cometidos por terceros, generalmente utilizando al banco como medio o vía para defraudar a clientes del mismo, pero donde siempre juega la responsabilidad del banco que interviene.

Los casos de fraudes cometidos por terceros adquieren variadas formas y se utilizan distintos medios, por lo que sólo mencionaremos los más comunes.

- **Adulteración de Cheques y Otros Documentos**

  El caso más frecuente resulta de la adulteración de cheques, previamente sustraídos y lavados o sometidos a procedimientos especiales por los que se borran los importes y el beneficiario, que son nuevamente integrados por mayor suma y a nombre del presentante.

- **Integración de Certificados de Depósitos en Blanco**

  Otro medio de fraude, es la sustracción de formularios de certificados de depósitos en blanco, que por descuido o en complicidad con el agente, son dejados al alcance del público.

- **Ordenes Falsas de Transferencias de Fondos**

  Los grandes pagos y cobros se realizan hoy en todo el mundo, utilizando la actuación de los bancos como intermediarios, por medio de transferencias electrónicas de fondos. Si se adulteran las órdenes de pago o depósitos, se puede obtener que los fondos que estaban destinados a una determinada cuenta, vayan a parar a otra cuenta, generalmente la del defraudador o un cómplice.

  Este tipo de fraudes, es cada día más frecuente y los bancos deben tomar medidas al respecto, debido a la voluminosa masa de transferencias que efectúan diariamente.

- **Obtención de Cartas de Crédito con Promesa de Envío de Fondos**

  Una forma reciente de fraude es cometido desde el extranjero, donde personas que alegan supuestos contactos e influencias con grandes bancos y financieras del exterior, ofrecen créditos a tasas muy bajas a entidades financieras locales.

  Por un lado requieren la entrega de cartas de crédito "***stand by***", con la promesa de ser utilizadas sólo como garantía del supuesto préstamo.

  Obtenida la carta de crédito de tal naturaleza, cuyo pago se supedita comúnmente a la presentación de algún reclamo del beneficiario indicado, los supuestos influyentes desaparecen, luego aparecen en el país mandatarios (abogados) extranjeros, pretendiendo cobrar la carta de crédito y alegando su naturaleza abstracta y desvinculada de toda operación de crédito o mercadería. El reclamo se formula por terceros (cesionarios) del beneficiario.

  Vinculado con esta operatoria fraudulenta está también la actuación de supuestas consultorías extranjeras que se ofrecen para tramitar créditos en el exterior que demandan largas tratativas,

finalmente infructuosas, pero que acarrean la demanda de importantes honorarios de los intermediarios.

2.6.2 Fraudes de Clientes

También existen los fraudes, realizados por personas inescrupulosas, las cuales para llevar a cabo su cometido, primero tienen que transformarse en clientes de una entidad bancaria, para luego realizar sus delitos utilizando al mismo.

- **Vinculación al Banco con Identidad Falsa**

  Normalmente una maniobra defraudatoria mediante el uso de instrumentos bancarios, comienza con la utilización de una identidad falsa por parte del agente. Si el banco es poco precavido, con un documento falso el agente abrirá una cuenta corriente y obtendrá una chequera con la que luego concretará su maniobra entregando cheques sin fondos a proveedores de buena fe que le entregarán mercaderías a cambio.

- **Información Falsa sobre Solvencia**

  La falsa apariencia de fortuna es otro medio de estafa a un banco por su cliente, que obtiene créditos denunciando bienes que no posee o exagerando sus activos, resulta una maniobra típica en épocas de tasas de interés reguladas, cuando el crédito estaba relacionado. Hoy en cambio con un régimen de tasas libres de interés, es la maniobra de quién no piensa pagar su crédito.

  Son numerosos los casos que han llegado a la justicia, los bancos y entidades financieras han denunciado a los agentes por supuesto delito de defraudación. Reiteradamente también los tribunales han resuelto que no existió delito porque la maniobra defraudatoria no era idónea para consumarlo y que si ello ocurrió, se debió a la negligencia del banco, al no verificar tal información falsa.

  La falta de control y revisión por parte de las entidades, en cuanto a la verificación de la información patrimonial que presentan los clientes, excluye el ilícito.

- **Garantías Sobrevaluadas**

  La sobrevaluación de un bien inmueble sobre el que se constituye una hipoteca o de bienes muebles objeto de una prenda, resulta también una maniobra de fraude común a las entidades financieras, especialmente cuando los bienes están ubicados fuera del ámbito de actuación de la entidad y se procede por medio de tasaciones efectuadas por supuestos peritos particulares.

  La sobrevaluación de la garantía constituye una maniobra defraudatoria porque ante el incumplimiento del pago del préstamo, la ejecución de ella no cubrirá el crédito y no habrá otros bienes con que cobrarse.

2.6.3 Fraudes Internos del Banco (Colaboradores y Funcionarios)

Dentro de una entidad financiera, existen clientes externos que son los cuentabientes, inversionistas, los deudores por préstamos, etc., pero también existen los clientes internos, que lo conforman los colaboradores y funcionarios, que dan funcionamiento a la entidad, pero que también en determinado momento pueden estar involucrados en determinadas actividades fraudulentas, como por ejemplo:

- **No Ingreso de una Transacción**

  Este tipo de fraude, se concreta en el área de caja, cuando la persona encargada de recibir transacciones en efectivo o su equivalente, no ingresa los valores recibidos, o los ingresa a otra

cuenta que ya tiene destinada para realzar el fraude. Para que el cliente externo no se percate de que su transacción no fue realizada correctamente, el empleado de la entidad financiera solo coloca sello y firma a los documentos y no los certifica por la caja, lo cual implica que al final del día no tenga ningún descuadre y se apropie de los fondos.

- **Desviación de Cuentas de Depósito**

El empleado encargado de registrar los depósitos efectuados en la entidad, cuando no tiene sobre si un supervisor que debe realizar el control o la verificación de esos asientos en forma permanente, es candidato al desvío de los fondos depositados, sea en forma total o parcial, registrándolos en otra cuenta que él maneja o que corresponde a un cómplice de dicha maniobra. El empleado del banco que siempre realiza una misma tarea y que, a su vez es quien tiene la posibilidad del control de esa tarea, constituye el ejemplo clásico de este tipo de fraudes.

- **Manejo Fraudulento de Cuentas con Corresponsales**

Entre las cuentas cuya conciliación debe ser permanente por la importancia de los montos que se manejan, están las cuentas con bancos corresponsales del exterior e interior.

Numerosos casos de fraudes han ocurrido por parte de funcionarios y empleados de bancos que manejaban esas cuentas, cuando por falta de personal o adecuados controles internos, no se cumplían las reglas administrativas y de organización tendientes a evitar este tipo de fraudes. El desvío de fondos desde esas cuentas a otras cuentas manejadas por los agentes del fraude, puede resultar muy sencillo.

- **Liquidación de Créditos Personales**

En el mismo orden de ideas se inscriben los fraudes mediante la autoconcesión o autoliquidación de créditos personales por parte de empleados de bancos.

Empleados sobre los que no existe control dual en la ejecución de tareas, pueden proceder a otorgarse un crédito o cancelarlo. De allí la necesidad de que la concesión de créditos, su liquidación y autorización para el pago sean etapas diferenciadas a cargo de distintas personas, de modo que no pueda darse un caso de fraude como el referido, salvo la actuación concertada de los mismos.

- **Sustracción de Formularios de Cheques**

Las chequeras conteniendo los formularios de cheques para ser entregados a los cuentahabientes de cuentas corrientes, deben ser mantenidos en lugar seguro y sobre ellos deben practicarse arqueos periódicos, de lo contrario puede resultar muy probable que se sustraigan, sin que el cuentahabiente advierta su falta al retirarlos, si no procede a contarlos al momento de recibirlos.

Este peligro es mayor para aquellas firmas que requieren muchas chequeras que son retiradas por empleados, quienes comúnmente no proceden a efectuar el proceso del conteo.

- **Sustracción de Tarjetas de Crédito para Entregar**

El caso de las tarjetas de crédito, es similar al de las chequeras, derivado que si no existen adecuados controles internos, esas tarjetas pueden ser entregadas a terceras personas o retiradas por empleados infieles y utilizarlas en comercios o cajeros automáticos, generando un grave perjuicio al titular, máxime que dichas tarjetas aun no tienen firma, de modo que es posible su integración con la firma de quien procederá a utilizarla. Los comercios no son muy exigentes en materia de identificación del titular de la tarjeta y a lo sumo piden un número de documento que hacen constar en el formulario de pago.

- **Operaciones en Compraventa de Bienes**

  Otra maniobra fraudulenta ha sido la compra - venta de bienes entre la entidad y alguna persona o empresa vinculada, con la finalidad de hacer figurar ganancias contables importantes en el estado de resultados de la entidad en crisis. De ese modo el estado de resultados reflejará ganancias inexistentes que luego se incorporarán al patrimonio neto de la entidad como resultado positivo del ejercicio.

  En el mismo sentido, otra maniobra detectada es la realizada por directivos de entidades en crisis que han comprado bienes por valores irrisorios o, al contrario, le han vendido bienes a la entidad por sumas exageradas, en ambos casos en fraude de los intereses de los demás accionistas de la entidad y de sus acreedores.

2.6.4 Fraudes Hechos al Cliente

En estos últimos años se acentúa una tendencia hacia la protección del consumidor del servicio bancario en todo el mundo.

- **Cobro de Intereses Encubiertos, Comisiones y Gastos**

  En este sentido corresponde señalar entre los casos de fraude al consumidor bancario los referidos al cobro de sobreprecios en el crédito otorgado o servicio prestado, mediante la utilización del cobro de comisiones que disfrazan una sobretasa de intereses, o de gastos inexistentes o exagerados, además de cargos excesivos, por el mantenimiento de cuentas, etc.

- **Inclusión de Cláusulas Vejatorias en Formulación de Contratos**

  Es común en toda contratación, que el preferente incluya cláusulas vejatorias aprovechándose de su posición contractual dominante. En tal sentido se citan las de "Exoneración de Responsabilidad": de "Renuncias de Derechos por parte del Adherente; de renuncias a oponer defensas; de constitución de domicilios falsos, etc.

  Este tipo de cláusulas es utilizado en los formularios de contratación que utilizan los bancos en todo el mundo y ello ha dado lugar a una directiva expresa en la Comunidad Económica Europea, en defensa del consumidor bancario, en el sentido de que el cliente sea perfectamente informado sobre el alcance de todas y cada una de las cláusulas incorporadas al contrato.

2.7 Fraude por Falsificación de la Banda Magnética de una Tarjeta de Crédito[16]

En 1989, Visa introdujo, el Programa de Valor de Verificación de Tarjetas (CVV-Card Verification Value), como una forma para contrarrestar la epidemia de fraude provocada por la falsificación de la banda magnética.

El programa mencionado anteriormente, es un código numérico singular que se graba en la banda magnética de la tarjeta. La autorización de transacciones originadas en terminales de lectura de bandas magnéticas incluye la verificación del código, para garantizar que dicho valor coincida con el que tiene el emisor en el archivo correspondiente a esa cuenta.

Hasta la fecha, esta característica ha sido extremadamente exitosa en la reducción de pérdidas por falsificación, sin embargo, no es infalible. Los delincuentes pueden lograr que la verificación del CVV resulte ineficaz con un nuevo método de falsificación denominado "***Skimming***", que significa falsificación de la banda magnética, que comenzara varios años atrás con la utilización de terminales anticuados de escritura/lectura. Recientemente, la falsificación de banda magnética, sé esta haciendo cada vez más sofisticada, hasta el punto de generarle a Visa y a sus miembros un

[16] (25:2)

creciente problema de seguridad de datos. Con las computadoras personales "***laptop***" y otros artículos electrónicos, en la actualidad pueden sustraerse información de cuentas y duplicarse en prácticamente cualquier punto del proceso de autorización, desde las terminales del punto de venta donde se pasan las tarjetas válidas, hasta en cualquiera de los innumerables sistemas que se utilizan en la transmisión y el almacenamiento de datos.

A medida que se siguen incrementando las pérdidas atribuibles a la falsificación de la banda magnética, son grandes los esfuerzos para desarrollar nuevas estrategias tendientes a combatir este problema.

2.7.1 Falsificación de la Banda Magnética

Es un método de falsificación desarrollado por delincuentes, para que el Programa de Valor de Verificación de Tarjetas, resulte ineficaz en la identificación de tarjetas inválidas o falsificadas.

En el ambiente de **VISA**, este tipo de fraude se conoce con el nombre de "***Skimming***", que se entiende como la duplicación de los datos de la banda magnética con el fin de obtener autorizaciones de consumos inválidas.

Los delincuentes copian toda la información contenida en las Pistas 1 y 2 de la banda magnética de una tarjeta válida, para posteriormente grabar estos datos, en tarjetas robadas o falsificadas, lo cual da como resultado la aprobación por parte del emisor de transacciones fraudulentas.

Como este método ha evolucionado, en la actualidad el término "Falsificación de Banda Magnética" se refiere a cualquier situación en la cual se copian datos de cuentas electrónicamente transmitidos o almacenados que se utilizan para crear tarjetas falsas con bandas magnéticas aparentemente válidas.

2.7.2 Escenarios para la Falsificación de la Banda Magnética

A medida que los delincuentes y los sistemas de procesamiento de transacciones se hacen más sofisticados, se multiplican las oportunidades para obtener acceso a información valiosa de cuentas.

Los escenarios para la falsificación de banda magnética abarcan desde comercios falsos o locales preparados con el expreso propósito de obtener datos de bandas magnéticas válidas, hasta conexiones telefónicas para capturar datos de cuentas durante bajadas de carga de terminales o autorizaciones. Cualquier lugar, desde la terminal del punto de venta de un comercio hasta el sistema principal de un adquirente o emisor, puede resultar vulnerable y ni siquiera es necesario que haya una tarjeta válida.

Si bien pueden variar los detalles de las estafas individuales, por lo general, los escenarios para la falsificación de la banda magnética de una tarjeta de crédito, abarcan tres categorías básicas donde se comprometen datos de bandas magnéticas, a saber:

- En un Comercio
- Cuando pasan de una organización a otra durante la autorización
- Cuando se almacenan.

A continuación se describe cada escenario con más detalle.

- **Datos de Pistas Comprometidos en un Comercio**

  El escenario para este tipo de falsificación más común implica datos de banda magnética comprometidos en un comercio - el dueño o un empleado conveniente, copia datos de pistas completos durante una transacción legítima. El hurto de datos tiene lugar en el momento en que se pasa una tarjeta legítima para autorización mediante el uso de una "laptop" u otro

dispositivo electrónico enlazado a la terminal del punto de venta para capturar información de la banda magnética – o bien inmediatamente después, con un segundo intento de autorización de la tarjeta a través de un dispositivo separado e independiente. Los datos de pistas completos obtenidos de esta manera pueden bajarse y volverse a codificar en una tarjeta robada o falsificada.

Los comercios minoristas considerados de alto riesgo para este tipo de falsificación, son aquellos donde la tarjeta queda temporalmente fuera de la vista del tarjetahabiente, como por ejemplo los restaurantes y las estaciones de servicio, se encuentran entre los comercios más vulnerables para que los delincuentes realicen su cometido.

- **Datos de Banda Magnética Comprometidos cuando pasan de una Organización a otra durante la Autorización**

  En este escenario, los datos de banda magnética quedan comprometidos una vez que dejan el comercio, cuando pasan entre diversas partes relacionadas con el proceso de autorización, a saber:

  ⇒ El sistema principal de un Comercio
  ⇒ El sistema principal de un Emisor o de un Adquirente
  ⇒ El procesador de un Emisor o de un Adquirente.

  La información de la cuenta se obtiene por conexión con las líneas telefónicas o mediante la captura de transmisores vía satélite. Los empleados convenientes en estos lugares pueden, aunque no necesariamente, estar involucrados y el personal de dirección puede estar totalmente ajeno a cualquier violación de la información.

- **Datos de Banda Magnética Comprometidos durante el Almacenamiento**

  Otros puntos potenciales de compromisos para la falsificación de la banda magnética de una tarjeta de crédito, incluyen cualquier lugar donde se almacena información de cuentas, ya sea a corto o largo plazo; lo cual abarca terminales de captura de datos electrónicos, computadoras personales y sistemas de computación. Al igual que en los otros escenarios de esta clase de falsificación, los delincuentes irrumpen en estos sistemas de almacenamiento de datos para recuperar y copiar información de cuentas válidas, que posteriormente se codifica en tarjetas falsas o en tarjetas robadas.

  Los puntos potenciales de compromiso de la información en estas estafas incluyen:

  ⇒ Terminales de captura electrónica o activadas por el tarjetahabiente, previo a la operación de cierre diario.
  ⇒ Sistemas de computación del comercio
  ⇒ Sistemas del Emisor o del Adquirente
  ⇒ Sistemas de terceros
  ⇒ Sistemas de respaldo de cualquiera de los anteriormente enumerados.

  Al igual que en el escenario anterior, los empleados y comercios convenientes pueden, aunque no necesariamente, estar involucrados.

2.7.3 Identificación de Transacciones por Falsificación de Banda Magnética

La naturaleza misma de la falsificación de banda magnética de tarjetas de crédito, puede hacer que este tipo de fraude sea particularmente difícil de identificar. Es posible que no se puedan distinguir los registros de autorizaciones por transacciones válidas y por falsificación de banda magnética y es probable que los emisores no sepan qué buscar.

Las estrategias básicas para la identificación de transacciones falsificadas no difieren de las que emplean los emisores para otros tipos de fraude. Las transacciones sospechosas pueden identificarse a través de: **a)** Programas de detección rápida de fraudes implementados por emisores y posteriores llamadas al tarjetahabiente; o **b)** Una llamada al emisor iniciada por un tarjetahabiente.

El personal responsable del manejo de llamadas de los tarjetahabientes, debe estar capacitado para determinar si una transacción fraudulenta, puede ser el resultado de datos de banda magnética comprometidos; lo cual incluye:

- Verificación de que los datos de autorización incorporen el Código de Modo de Entrada del POS (máquina por medio de la cual se procesa la autorización de una transacción), en todas las transacciones en disputa;
- Confirmación de que el Programa de Valor de Verificación de Tarjetas, haya sido verificado al momento de la autorización;
- Verificación de que el tarjetahabiente está en posesión de todas las tarjetas válidas de su cuenta y de que la transacción sospechosa no fue realizada por el tarjetahabiente ni por nadie que tuviere acceso a tarjetas válidas, como por ejemplo, un miembro o amigo de la familia.

Suponiendo que se cumplan las condiciones antes enumeradas, entre los factores que pueden ayudar a confirmar fraude por falsificación de banda magnética, cabe mencionar los siguientes:

- Nombre en el registro de autorización diferente del correspondiente al cliente. Con frecuencia, los delincuentes cambian el nombre del tarjetahabiente en la pista 1 de la banda magnética para hacer coincidir la identificación ficticia. En muchos casos se utiliza el mismo nombre en múltiples tarjetas falsificadas.
- Nombre o número de cuenta impreso en el recibo por la terminal del punto de venta (impresión electrónica) diferente del nombre o número de cuenta del cliente.
- Nombre, número de cuenta u otro dato grabado (como ejemplo una “V” estilizada de Visa) en una impresión manual faltante o diferente de los datos grabados en la tarjeta genuina.
- Múltiples transacciones con tarjetas en áreas geográficas ampliamente separadas que tienen lugar prácticamente al mismo tiempo.

Otros esfuerzos investigativos que pueden ayudar a los emisores a reconocer el fraude por falsificación de la banda magnética de una tarjeta de crédito, son los siguientes:

- Revisar diariamente las transacciones que involucren tarjetas falsificadas y que hayan sido aprobadas. Múltiples cuentas con el mismo patrón de fraude pueden ayudar a detectar un caso de este tipo de fraude.
- Revisar mensualmente los casos de fraude por falsificación con Código de Modalidad de Entrada del POS de grandes montos en dólares a fin de reconocer los patrones de actividades fraudulentas que pueden no ser reconocidos en las revisiones diarias. Ello ayudará a vincular cuentas comprometidas y puntos de compra comunes.
- Analizar patrones de fraude por zona geográfica versus historial de la cuenta. Es más probable que se produzca este tipo de fraude, si los patrones de gasto del cliente indican el uso frecuente de la tarjeta en restaurantes y estaciones de servicio.

Los procedimientos para identificar, investigar y confirmar transacciones por falsificación de banda magnética, varían de un emisor a otro, dependiendo de los tipos específicos de información y demás recursos disponibles. Cuantos más emisores conozcan las características del fraude por falsificación de la banda magnética, mejor podrán reducir y evitar transacciones fraudulentas por esta clase de fraudes.

2.7.4 Identificación del Punto Común de Compra

La investigación de cuentas falsificadas realizada por los emisores también debe incluir esfuerzos para la identificación del punto común de compra, del lugar donde se copiaron originalmente los

datos de la banda magnética. Para identificar un potencial punto común de compra se deberán revisar los registros de transacciones legítimas de varias cuentas falsificadas a los efectos de observar si se puede detectar un punto común de compra.

Se recomienda efectuar las siguientes acciones para la identificación del punto común de compra sospechoso. Al verificar los registros de cuentas, los emisores deberán extraer la información de autorizaciones y ventas correspondiente a los últimos seis meses o más, previos a la primera transacción falsificada confirmada. Para identificarse como punto común de compra, el comercio debe ser el punto de compra de, por lo menos, tres cuentas falsificadas confirmadas. Dos cuentas pueden resultar suficientes en algunos casos, dependiendo de los detalles del fraude y de la investigación.

Una vez identificado el punto común de compra, los emisores deberán verificar sus registros a efecto de detectar otras transacciones legítimas en el comercio que pudieren estar comprometidas. Verificar con los tarjetahabientes y determinar si existen otras transacciones fraudulentas o actividad sospechosa que todavía no ha sido informada. Se evaluará cuidadosamente el riesgo de fraudes adicionales en otras cuentas, y los emisores deberán considerar las acciones que habrá que tomar a los efectos de reducir al mínimo las pérdidas. Dichas acciones pueden variar desde el monitoreo especial de cuentas en riesgo hasta el cierre de una cuenta potencialmente comprometida y la emisión de una tarjeta nueva.

Los emisores deberán informar acerca de un potencial punto común de compra tanto al Adquirente como a Visa con la suficiente información para poder iniciar una investigación. La información mínima sugerida deberá incluir números de cuenta, números de referencia, transacciones legítimas efectuadas antes de las fraudulentas para poder identificar el posible punto común de compra y transacciones que se sospecha fueron hechas por falsificación de banda magnética. Los emisores también deberán reportar el fraude total que hubiere resultado como consecuencia del compromiso de datos de una cuenta.

2.7.5 Estrategias de Prevención y Disminución de Perdidas para los Adquirentes

Los esfuerzos tendientes a combatir el fraude por la falsificación de la banda magnética, no son exclusivos de los emisores. La participación de los adquirentes también resulta esencial para prevenir y disminuir pérdidas por falsificación de banda magnética.

El adquirente debe concentrarse en cuidadosas prácticas de seguridad en la educación de los comercios, con especial énfasis en la seguridad de los datos y en los procedimientos adecuados para la aceptación de tarjetas. Asimismo, deben investigar los comercios que se sospecha son un punto común de compra.

La prevención comienza con cuidadosas prácticas de seguridad para evitar la afiliación de “comercios falsos”. El material para capacitación de comercios debe incorporar un capitulo que trate acerca de la importancia de la seguridad de los datos. Los puntos específicos que debe tratar son indicados a continuación:

- Los comercios no pueden retener ni almacenar datos de banda magnética, una vez autorizada una transacción. Al hacerlo, los comercios se ponen en peligro ellos mismos, como también al adquirente y al sistema de pagos.
- Los comercios o los agentes de éstos deben almacenar todo el material que contenga números de cuentas de tarjetahabientes en un área segura con acceso limitado a personal seleccionado.
- Los datos de cuentas deberán quedar ilegibles antes de ser descartados.
- Los comercios no están autorizados a ofrecer información de tarjetahabientes o de transacciones a ningún tercero, a menos que fuere necesario divulgar dicha información para completar la transacción o si así lo requiere la ley.
- Las solicitudes sospechosas de información de cuentas deberán ser notificadas de inmediato al adquirente del comercio o a Visa.

- Los comercios deben vigilar a los empleados que utilizan “laptop” u otro dispositivo electrónico para trabajar.
- Los comercios deben garantizar que el programa de Valor de Verificación de tarjetas, no pueda ser visualizado en los sistemas de procesamientos que tienen.
- La duplicación de datos de banda magnética con el propósito de la falsificación es un delito federal investigado por el servicio secreto, e inspectores postales, ambos de los Estados Unidos, las agencias locales de aplicación de la ley y los investigadores de bancos.

2.7.6 Investigación de Puntos Comunes de Compra Potenciales

En vista del riesgo significado que presenta la actividad de falsificación, los Adquirentes deben ejercer un mayor esfuerzo en la investigación de puntos comunes de compra.

Como mínimo, las investigaciones deberán determinar la cantidad de datos de cuenta comprometidos, quien fue responsable, el periodo de tiempo durante el cual los datos estuvieron comprometidos y qué se ha hecho para detener el problema. Las siguientes acciones ayudarán a los adquirentes en sus investigaciones.

- Examinar el perfil del comercio.
  - Fecha de apertura
  - Tipo de actividad
  - Cantidad de empleados
  - Cantidad de terminales
  - Tipo de terminales
  - Flujo de datos de autorización
  - ¿En algún momento quedan fuera de la vista de los clientes las tarjetas?
  - Volumen promedio
  - Historial de actividad de excepciones (fraudes, contracargos, solicitudes de copias)

- Examinar el detalle de las transacciones comprometidas para detectar características comunes.
  - Tiempo de la transacción (hora, local del comercio)
  - Tiempo de la terminal.

- Examinar el problema potencial y el detalle de las transacciones comprometidas con el dueño/gerente del comercio a fin de detectar otras características comunes.
  - Turno
  - Empleado
  - Otros denominadores comunes

- Obtener información adicional.
  - ¿Cómo se almacenan los registros de datos?
  - ¿Quién tiene acceso a la información?
  - ¿Algún empleado tiene una “laptop” o algún otro dispositivo electrónico?
  - ¿Qué datos de la banda magnética visualiza el sistema del punto de venta del comercio?

- Trabajar con el comercio para detener otros puntos de compra comunes y, de ser necesario, ponerse en contacto con las autoridades.

  Además de los puntos relativos a la seguridad de los datos, la capacitación de los comercios deberá concentrarse en las funciones y procedimientos de seguridad de tarjetas que hayan resultado exitosas en la disminución de fraudes, como por ejemplo los indicados a continuación:

  ⇒ Garantizar que los cuatro números impresos arriba o debajo del número de cuenta coincidan con los primeros cuatro números grabados
  ⇒ Garantizar que la “V” estilizada este grabada en la tarjeta cerca de la fecha de vencimiento
  ⇒ Garantizar que el panel para la firma no haya sido alterado
  ⇒ Comparar la firma que figura en la tarjeta con la del recibo

Visa tiene a disposición de los Adquirentes videos y volantes que destacan funciones de seguridad y procedimientos relacionados.

Entre las acciones que pueden realizar los adquirentes para ayudar a prevenir el fraude por falsificación de banda magnética, cabe mencionar las siguientes:

- Implementar la comparación de los últimos cuatro dígitos de la cuenta en las terminales de lectura. Esta estrategia es muy eficaz en evitar transacciones fraudulentas en tarjetas robadas nuevamente codificadas con datos de pistas falsificados.
- Los comercios sin terminales de lectura y comparación deberán comparar visualmente los últimos cuatro dígitos grabados en la tarjeta con los últimos cuatro dígitos impresos en el recibo de ventas.
- Los comercios con terminales que imprimen el nombre del tarjetahabiente de la pista 1 en el recibo, deben comparar visualmente el nombre grabado en la tarjeta con el impreso en el recibo.
- Implementar que los comercios de alto riesgo transmitan el contenido de la pista 1, para disminuir el fraude, los emisores pueden crear programas para reconocer transacciones donde el nombre de la pista 1 no coincida con el del tarjetahabiente.

CAPITULO III

CLASIFICACION DE RIESGOS EN UNA INSTITUCION BANCARIA EMISORA DE TARJETAS DE CREDITO

La naturaleza de las actividades realizadas por las entidades bancarias (Depósitos, Inversiones, financiamientos, etc.), involucra de manera inherente, una serie de riesgos que pueden resultar en pérdidas financieras y afectar las ganancias y el capital de las mismas.

Por lo expuesto anteriormente, es de vital importancia comprender las siguientes definiciones:

3.1 Riesgo

En sentido gramatical, se define como, la contingencia o proximidad de un daño.[17]

3.1.1 Riesgo General

Corresponden a los riesgos globales de cada forma de operar, en las diferentes actividades.[17]

3.1.2 Definición de Riesgo Bancario[18]

Se puede definir como la probabilidad que ocurra una contingencia negativa, en cada una de las áreas operativas que conforman una institución bancaria, perjudicando los intereses de los accionistas y del público en general.

3.1.3 Administración del Riesgo de acuerdo a la Ley de Bancos y Grupos Financieros *(Decreto 19-2002)*

Dicha ley establece en su Titulo VI, (***Administración de Riesgos***), artículo No. 55 (***Riesgos***), lo siguiente: "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 tasas de interés, de liquidez, cambiario, de transferencias, operacional y otros** a que estén expuestos, que contengan sistemas de información y un comité de gestión de riesgos, todo ello con el propósito de identificar, medir, monitorear, controlar y prevenir los riesgos.

Adicionalmente es importante mencionar, que la Junta Monetaria emitió la Resolución JM-**93-2005** (**Reglamento para la Administración del Riesgo de Crédito**), que en su articulo No. **01 (Objeto)**, establece "El presente reglamento tiene por objeto normar aspectos que deben observar los bancos, las entidades fuera de plaza o entidades off shore y las empresas de un grupo financiero que otorguen financiamiento, relativos al proceso de crédito, a la información mínima de los solicitantes de financiamiento y de los deudores y a la valuación de activos crediticios".

Lo anterior tiene su base legal en los artículos 50,51,52,53,55,56 y 57 de la Ley de Bancos y Grupos Financieros **(Decreto 19-2002)**, la cual recoge el principio, de que los bancos del sistema precisan de una normativa moderna, que les permita seguir desarrollándose para realizar más eficazmente sus operaciones y prestar mejores servicios, derivado de las tendencias de globalización y el desarrollo de los mercados financieros internacionales.

3.2 Evaluación del Riesgo Bancario

Es la identificación y el análisis de los riesgos relevantes de la institución, para determinar como se deben minimizar los mismos. A continuación se indica en que consiste cada uno de estos términos.

---

17 (1:78)

18 (18:263)

3.2.1 Identificación del Riesgo Bancario

Para la identificación de este riesgo, es indispensable que el banco cuente con técnicas adecuadas para evaluarlo oportunamente, dado que las economías, las industrias, las regulaciones y condiciones de operación continuarán cambiando. Es muy importante que se identifiquen a tiempo los riesgos que surjan con los cambios mencionados.

Por ejemplo, para identificar el riesgo bancario de mercado, en cuanto a la variación de cambios en precios de los productos que se ofrecen al cliente, así como las tasas que la entidad cobra sobre los mismos, se puede utilizar la técnica de comparar los índices promedio del mercado, con los índices de la institución, a efecto de medir su magnitud potencial y la probabilidad de ocurrencia.

Mediante la variación de ciertas suposiciones sobre los precios y tasas de mercado, una entidad puede ser capaz de identificar oportunamente, si puede existir un impacto inaceptable sobre los resultados de operación.

3.2.2 Análisis del Riesgo Bancario

Consiste en el análisis practicado sobre una base de juicio, simplemente centrándose en las áreas claves de operación que contribuyen al riesgo dado.

Por ejemplo al efectuar el análisis de riesgo en el departamento extranjero de un banco, se determina que existe la amenaza latente del lavado de dinero, falsificación de moneda extranjera, falsificación de giros, etc.

Se puede decir, que cada banco enfrenta una variedad de riesgos de fuentes internas y externas, las cuales deben identificarse y analizarse oportunamente, siendo una condición previa el establecimiento de objetivos de cada una de las áreas del banco, enlazados en distintos niveles consistentemente.

Las instituciones bancarias a través de los riesgos, miden y administran adecuadamente las operaciones, efectuando una distinción de estos, para determinar los de mayor relevancia que la entidad enfrentara, analizando su misión de negocios, actividades básicas y los principales procesos. Algunos de los riesgos genéricos más importantes frecuentemente identificados, son aquellos relacionados con el crédito, liquidez, tasas de interés, tasas de cambio, precios de activos financieros, sistemas y operaciones, contabilidad e información, actividad criminal, actividades fiduciarias, procesos gerenciales/administrativos, la estructura legal, reglamentaria, judicial y la propia reputación del banco en el mercado.

En ese sentido, la gama de operaciones en una institución bancaria no son mutuamente excluyentes y cualquier producto o servicio que el banco provee, pueden exponerlo a múltiples riesgos, por lo que como hecho principal para justificar sus ganancias y sus prospectos de viabilidad de largo plazo depende de la habilidad de la gerencia para administrar y controlar exitosamente los mismos.

Basados principalmente en los riesgos que afectan a las instituciones bancarias, se citan a continuación aquellos que se consideran más frecuentes:

3.3 Riesgo País[19]

Se refiere a identificar, evaluar y cuantificar las situaciones que, tanto en Guatemala como en otros países pueden ocurrir, localidades donde residen clientes o emisores, con los cuales se efectúen transacciones transfronterizas, de manera que permitan a la administración adoptar decisiones de negocios adecuados al sector.

---

[19] (22:437)

La ponderación de cada riesgo, determinará un mayor porcentaje de previsiones que por este concepto deban constituir las entidades bancarias que prestan servicios en el extranjero. Este riesgo se divide en:

3.3.1 Riesgo Sistemático

Es aquel que afecta a todo el Sistema Financiero en un momento dado y con grandes consecuencias para él. Ha ocurrido en algunos países, siendo esporádicos.

En el caso de las tarjetas que pueden ser utilizadas a nivel mundial, es importante recordar que la moneda predominante y en la cual se realizan todas las transacciones que efectúan los tarjetahabientes, es el dólar americano, por lo que su posición depende de la economía y sistema financiero del país emisor. Cuando la tarjeta que se utiliza en otro país es emitida en Guatemala, provoca que cualquier cambio que se produzca con el dólar, tenga incidencia en el sistema financiero nacional, que es donde se procesan todas las transacciones efectuadas en el extranjero.

3.3.2 Riesgo Macroeconómico

Dependiendo de la evolución que tengan las economías, de o los países que intervienen en la transacción transfronteriza, se determinarán las situaciones de riesgo que afectan las operaciones del banco.

Es evidente que las economías de los diferentes países a escala mundial, juegan un papel preponderante para incentivar el uso de las tarjetas, que a la postre es el negocio propio de las empresas emisoras, por lo que si la economía del país donde se pretende utilizar es inestable, su uso y aceptación será bajo, por consiguiente eso se transforma en posibles pérdidas para los emisores a nivel nacional, incrementando este riesgo.

3.3.3 Riesgo de Convertibilidad

Este tipo de riesgo se refiere a cuantificar la factibilidad, que pudiera surgir restricciones en cualquiera de los países participantes, respecto a rigidez o congelación de la libre convertibilidad cambiaria de la moneda local, a dólares norteamericanos u otra moneda dura. También deberá cuantificarse la factibilidad de la devaluación de la moneda local.

Esta clase de riesgo se incrementa para los emisores de tarjetas de crédito, al momento que en un determinado país, se tuvieran restricciones en cuanto al uso del dólar, derivado que la empresa líder en respaldo y solidez en esta materia, lo constituye **VISA**, que es una empresa norteamericana, lo cual basa sus operaciones extranjeras en esa moneda, trayendo cono consecuencia que no se pudieran utilizar estas tarjetas en un país con esta situación.

3.3.4 Riesgo de Influencia Externa

Se refiere a conocer previamente los posibles efectos que puedan surgir ante cualquier consecuencia negativa, derivado de la conversión que hagan los bancos de cada país a sus estados financieros, aplicando las normas del país con que se desee comparar.

Para dar un ejemplo, se puede mencionar que si existieran cambios en las normas o en las políticas contables de Estados Unidos, que es donde radica la empresa **VISA**, marca que respalda tarjetas de crédito, es evidente que puede cambiar procedimientos, precios, condiciones, que actualmente se manejan entre ellos y la empresa emisora en nuestro país, lo cual podría incrementar este tipo de riesgo.

3.4 Riesgo de Mercado

Dentro del mercado financiero intervienen varios agentes, los cuales realizan diversas transacciones con el fin de obtener beneficios, provocando que cada uno de ellos cuide y vele por

sus intereses, lo cual se convierte en expectativas a futuro, que de resultar favorables contribuye a cumplir con obligaciones obtenidas, pero de lo contrario incrementa este riesgo, ya que no se podrá cumplir con las obligaciones acordadas. El riesgo de mercado, se divide en:

3.4.1 Riesgo de Crédito

Es aquel que permite cuantificar el grado de solvencia de los clientes, mediante la evaluación de su capacidad para la generación de los flujos necesarios que le permitan cumplir con los términos de pago de sus créditos. Este riesgo es el que tradicionalmente más se administra y conoce, el cual se subdivide en los siguientes:

3.4.1.1 Riesgo de Crédito General

Es aquel al cual está asociada la clasificación de los deudores en distintas categorías según sea el resultado de la evaluación, y que determinará la constitución de provisiones, para cuentas insolventes.

3.4.1.2 Riesgo de Actividad Económica

Es la posibilidad de que ocurra el deterioro de un sector económico determinado, propio del giro del cliente (Agricultura, ganadería, pesca, transporte, construcción, etc.).

En la actualidad es de vital importancia para otorgar créditos a través de tarjetas de crédito, los bancos cuenten con un adecuado departamento de análisis de riesgos, con lo cual se pretende minimizar el riesgo de posibles pérdidas, derivado de la falta de recuperación de los fondos, lo que incrementaría la cartera en mora, en cobro administrativo, prejurídico y jurídico.

Aunado a lo anterior, es conveniente comentar que el incremento en la cartera con poca posibilidad de recuperación, origina que la entidad emisora realice mayores provisiones para saldos con poca o ninguna oportunidad de cobro.

El riesgo de mercado esta íntimamente ligado al desarrollo o deterioro que sufra algún sector económico del país, se puede mencionar a manera de ejemplo que se hayan otorgado tarjetas de crédito de clase oro a empresarios que se dediquen al sector del café, el cual se vio afectado por la economía nacional, lo cual podría provocar en un momento determinado que los saldos de estas tarjetas, se trasladen de vigente al día a mora y posteriormente a jurídico, incrementando este tipo de riesgo para la entidad emisora.

3.4.2 Riesgo Financiero

Es la cuantificación del incremento o decremento desproporcionado entre activos y pasivos (calce de fondos entre activos y pasivos), en términos de una misma moneda, tasa y plazo. Se expresará en cuadro de flujos de vencimiento por plazos de activos y pasivos, por moneda. Este riesgo, se integra por los siguientes:

3.4.2.1 Riesgo de Liquidez

Se refiere a la cuantificación de los superávit o déficit acumulados resultantes de los flujos de cajas proyectados, por distintas paridades monetarias, según sean los vencimientos de los activos y pasivos del banco, que permitan adoptar las acciones pertinentes con la necesaria antelación, para maximizar la rentabilidad.

3.4.2.2 Riesgo de Tasa de Interés

Es la posibilidad que se produzca un eventual descalce entre las tasas de interés pasivas y activas en las que se han invertido los recursos. Dicho efecto en resultados dependerá del estado de la posición financiera mantenida por la institución.

3.4.2.3 Riesgo de Tipo de Cambio

Este riesgo se deriva de mantener posiciones en monedas extranjera abiertas, sea por sobrecompra o sobreventa, los cuales están expuestos a una fluctuación de cambios, con efectos positivos o negativos en resultados.

3.4.2.4 Riesgo de Precio

Corresponde a cuantificar la diferencia entre el valor de compra y el valor de cotización de mercado, correspondiente a los instrumentos mantenidos en el portafolio de inversiones del banco y su efecto en los resultados del mismo.

3.4.2.5 Riesgo de Cobertura de Capital Aportado

Se refiere a verificar que las correspondientes cuentas del activo como contraparte del patrimonio de los accionistas, salvaguarden debidamente el capital aportado. Para la cuantificación de este riesgo, será necesario medir mensualmente dicha cobertura.

No obstante que este riesgo se cuantifica en forma global, por todas las operaciones en conjunto que realiza una institución emisora de tarjetas de crédito, para comentar a manera de ejemplo, se pudo evidenciar que cuando el Congreso de la República decretó un tope límite en las tasas de intereses que podían cobrar estas entidades sobre esta clase de financiamiento, incremento el riesgo financiero, derivado que al cobrar la tasa máxima que permitía la ley, esta clase de negocio no era rentable para los resultados esperados por esta clase de emisores, provocando que este riesgo se transformara en pérdidas para la entidad.

3.4.3 Riesgo de Gestión

Representa la calidad de toda la información que se produce en la institución, en cuanto a estados financieros, cédula de variaciones, índices financieros, presupuesto, cuadros estadísticos, etc., con la finalidad de efectuar evaluaciones periódicas a la situación del banco, en cuanto a sus perspectivas financieras, de clientes, de eficiencia, etc.

Cada institución bancaria que dentro de sus productos se encuentre el financiamiento a través de tarjetas de crédito, debe contemplar el elaborar reportes separados (estados financieros, presupuesto, categorización de clientes, niveles de mora, etc.), de este producto financiero, con el fin de llevar un estricto control de la rentabilidad, eficiencia, categoría de clientes, cartera en mora, de los clientes que conforman el departamento de tarjeta de crédito.

3.4.4 Riesgo de Transformación

Corresponde al riesgo existente en las transformaciones que deba tener la institución, para enfrentar las necesidades del mercado, como por ejemplo: el lanzamiento de nuevos productos, suficiencias de sistemas y tecnología, capacitación del personal, nueva imagen corporativa, campaña de Marketing, etc.

En lo referente a las tarjetas de crédito, cuando se habla de lanzar al mercado nuevos productos, por ejemplo podemos mencionar, la creación de una tarjeta virtual para realizar compras a través de internet, también se puede mencionar el crear un plan de acumulación de puntos por los consumos con la tarjeta, los cuales posteriormente pueden ser canjeados por electrodomésticos, viajes, joyería, etc, con lo anterior se pretende dar más y mejores alternativas financieras al cliente.

Las entidades emisoras de tarjetas de crédito, deben monitorear los sistemas informáticos utilizados, para llevar los registros de los tarjetahabientes, procesar los movimientos diarios de las mismas, con la finalidad de prestar un mejor servicio a los tarjetahabientes, lo cual se transformará en una mejor imagen para la institución.

3.4.5 Riesgo de Competencia

Se refiere al riesgo que representan los productos y cambios estructurales de la competencia, teniendo particular importancia la dinámica o direccionamiento del mercado y la velocidad de respuesta con que el banco pueda reaccionar ante ellos.

Derivado de la evolución que ha tenido el mercado de tarjetas de crédito, es evidente que la competencia es mucha, por lo que éstas entidades tienen que intensificar e implementar promociones, para incrementar la venta del producto y motivar el uso para los que ya lo posean, con el fin de no rezagarse ante la competencia que existe en cuanto a este producto financiero.

3.4.6 Riesgo de Imagen

Es el riesgo derivado del grado de aceptación que la opinión pública tenga del banco, lo que afectará positiva o negativamente su capacidad para establecer nuevas relaciones.

Este riesgo se mide a nivel global de la institución, para lo cual influyen varios factores, como la publicidad, la calidad del servicio que se presta, la diversificación de productos que se ofrezcan, la fidelización que se haya realizado de los clientes, etc., con lo cual se busca crear un buena imagen de la institución.

3.5 Riesgo de Operaciones

Este riesgo está presente en todas las operaciones y servicios que otorga el banco. Es el que se deriva de la calidad de los controles operacionales, del diseño y construcción de los sistemas y procesos, así como la integridad y ética de los funcionarios. Los riesgos de operaciones, se conforman por los siguientes:

3.5.1 Riesgo de Cumplimiento

Corresponde al riesgo ante un incumplimiento de las leyes, normas y disposiciones que regulan el funcionamiento del banco, exponiéndolo a sanciones, multas y efectos negativos en sus resultados e imagen corporativa.

Las instituciones bancarias están sujetas a diferentes actividades periódicas de cumplimiento, como es efectuar pagos de impuestos, enviar información financiera en forma periódica a la Superintendencia de Bancos, contestar requerimientos del ministerio público, etc., de lo contrario, la entidad esta sujeta a sanciones monetarias, que se transformarán en pérdidas para la entidad.

3.5.2 Riesgo de Errores

Son aquellos que surgen como consecuencia de procesar o registrar erróneamente una transacción y no detectarla oportunamente. Como ejemplo están los abonos a cuentas corrientes que no corresponden, cancelación de créditos indebidamente, alzamiento no autorizado de garantías, mayor exposición de riesgo por exceder límites autorizados de líneas de créditos, cobro de intereses en exceso, cuentas con saldo irregular, etc.

Este riesgo se puede evidenciar cuando los cobros de cargos por servicios de las tarjetas de crédito, no pasan por una revisión previa a su procesamiento, provocando que el estado de cuenta del tarjetahabiente refleje saldos incorrectos y por consiguiente reclamos innecesarios, además de una mala imagen de la entidad ante sus clientes.

3.5.3 Riesgo de Información Financiera

Corresponde a los efectos de sanciones o multas (por efectos de envío de información a organismos externos), así como adoptar decisiones erróneas (información interna), derivados de proporcionar información de mala calidad, insuficiente, extemporánea o incompleta.

Toda entidad bancaria, esta sujeta a enviar periódicamente información financiera en forma de reportes, informes, etc., a la Superintendencia de Bancos, de lo contrario estaría expuesta a sanciones monetarias, que se reflejara en el estado de perdidas y ganancias de la entidad.

También el preparar reportes internos incorrectos, repercutirá en la toma de decisiones por parte de las máximas autoridades de la institución, lo cual incrementaría esta clase de riesgos provocando posibles pérdidas para la entidad.

3.5.4 Riesgo de Entes Externos

Es el que surge por una inadecuada interacción (reciprocidad), combinada con los organismos e instituciones que regulan y controlan la industria financiera, tales como auditores externos, contratos de asesorías, contratos por servicios con empresas externas (servicios Outsourcing), etc.

Las instituciones bancarias por el mismo entorno de su actividad económica, tiene que utilizar diferentes clases de servicios por parte de entidades externas, como por ejemplo, una firma de auditoría externa, una entidad de asesoría, una empresa de cobro administrativo y jurídico de cartera, etc., para lo cual firman contratos, en los cuales quedan plasmadas los acuerdos y las condiciones que regirán estas actividades. Por lo cual es de vital importancia que dichos contratos sean revisados cuidadosamente, con el objeto de salvaguardar los intereses de la institución y minimizar este tipo de riesgos.

3.5.5 Riesgo de Recursos Humanos

Es el que surge por el manejo inadecuado de los distintos procesos operativos que realiza la unidad de personal, en cuanto a retenciones y pagos a entidades, remuneraciones, licencias por vacaciones, ausentismo, provisiones, procesos de liquidación, proceso de evaluación de desempeño, etc.

Toda entidad bancaria cuenta con un departamento de recursos humanos, el cual tiene a su cargo primeramente la adecuada selección de personal que formara parte de la institución, así también tiene a su cargo otra serie de actividades que se derivan de la relación entre el colaborador y el patrono, como lo es el procesamiento de salarios, vacaciones y prestaciones laborales.

Por lo anterior, el funcionamiento de este departamento es de vital importancia, para no incrementar el riesgo de contratar personal no calificado, o de posibles intervenciones de la inspección general del trabajo, por faltas en cuanto a las prestaciones que tiene derecho el trabajador.

3.5.6 Riesgo de Seguridad Física

Corresponde a la catástrofe que se puede dar dentro de la institución, afectando a personas, documentos, información y el patrimonio del banco, sin contar con los elementos preventivos de incendios, asaltos y coberturas vigentes de los seguros.

El ejemplo más sencillo, es la información que manejan los bancos, respecto de sus clientes, la cual es de carácter confidencial y se debe resguardar con una copia de seguridad, para evitar su perdida debido a una posible situación de catástrofe, con lo cual la institución no podría seguir operando y sobre todo no tendría el control de sus cuentahabientes y los productos adquiridos por cada uno de ellos, lo que incrementaría el riesgo de seguridad física.

3.6 Riesgo de la Información

Se refiere a las posibles pérdidas de información de la institución, midiendo su magnitud en los aspectos siguientes:

3.6.1 Riesgo de Tecnología

Es la posible contingencia, por no contar con un centro de procesamiento de datos de respaldo, ubicado en un edificio distinto al cual funciona el centro principal, así como la falta de procedimientos para restauración de archivos y datos ante una eventual catástrofe. En materia de tarjetas de crédito es primordial implementar medidas de seguridad para salvaguardar la información de los tarjetahabientes, así como de los estados de cuenta de cada uno de ellos. En la actualidad existen entidades que cuentan con su propio procesador de datos, los cuales deben realizar copias de seguridad y custodiarlas en otra institución para tener la seguridad que en caso de accidente no se pierda la misma.

Otras entidades no cuentan con un centro de procesamiento de datos, por lo cual deben contratar los servicios de una empresa que se dedique a esta actividad, dicha entidad tiene la obligación de crear sus propias medidas de seguridad, ya que además de enviar una copia de seguridad de la información en forma diaria a la institución que requirió de sus servicios, debe custodiar una copia de esta, en alguna otra instalación ajena al edificio que ellos ocupan.

3.6.2 Riesgo Físico del Centro de Computo

Consiste en ocasionar un daño al centro de cómputo por no contar con un control de acceso físico, detectores de humo, extinguidores, etc.

Con el fin de minimizar este riesgo, toda institución bancaria, debe de invertir en equipo de seguridad, para hacer frente a cualquier evento que se pueda dar en el centro de computo, por lo general esta área es restringida a personal debidamente autorizado.

3.6.3 Riesgo de Privacidad de la Información

Corresponde al riesgo que la información pudiera ser sustraída, para luego ser utilizada en forma indebida o divulgada, por lo cual deben existir niveles de las claves de acceso a usuarios, debidamente controlados.

Para minimizar este riesgo, generalmente las instituciones, utilizan claves de acceso, bitácoras de operaciones, y el área es de acceso restringido solo al personal autorizado, por lo cual cualquier anomalía puede ser sujeta de investigación, ya que existe un registro de las operaciones que realiza cada uno según su clave.

3.6.4 Riesgo de Integridad de la Información

Obedece a la posibilidad que la información pudiere ser dañada accidental o intencionalmente.

Es por ello que deben de crearse copias de seguridad, las cuales deben ser cuidadosamente custodiadas, para poder utilizarlas en caso de cualquier accidente o intención de dañarla.

3.6.5 Riesgo de Calidad de la Información

Corresponde a la posibilidad que la información no sea exacta, precisa y confiable, con los riesgos inherentes que ello implica, tanto interna como externamente.

Es sabido que parte fundamental de toda entidad es que procese su información financiera en forma exacta y oportuna, ya que es la base para la toma de decisiones importantes, por parte de las autoridades administrativas de la misma, por lo cual se debe de contar con mecanismos que ejecuten los procesos en forma oportuna y que además genere información confiable, para minimizar este tipo de riesgo.

3.6.6 Riesgo de Transferencia Electrónica de Fondos

Se refiere a la volatilidad de la información en ambientes de operaciones electrónicas de fondos, tales como Swift (System Worldwide International Financial Transactions – Sistema de Transacciones Financieras Internacionales alrededor del mundo), telex, cajeros automáticos, etc.

En el caso de las tarjetas de crédito, es inminente que el uso de cajeros automáticos esta a la orden del día, por lo que se debe de contar con un procesador de datos de muy alta calidad, debido que al momento de solicitar autorizaciones para el uso de una tarjeta, cuenta en mucho el tiempo en que se confirmen los datos y se de respuesta a esta solicitud, de parte del centro procesador de datos, lo que podría repercutir en el servicio al cliente, la imagen de la institución y sobre todo lo útil del producto adquirido por el cliente.

3.7 Riesgo de Operaciones Ilícitas

Se refiere a aquellos riesgos que son causados por operaciones realizadas en contra de la ley, tales como:

3.7.1 Riesgo de Lavado de Dinero

Corresponde a no detectar oportunamente operaciones bancarias que pudieran ser efectuadas a través del banco, tendientes al blanqueo y legitimación de dinero, proveniente de transacciones ilícitas.

El lavado de dinero es un delito que en Guatemala esta regulado el decreto No. 67-2001 **(Ley Contra el Lavado de Dinero u Otros Activos)**, dicha ley exige que toda institución establezca procedimientos de control, capacitación al personal, programas de auditoría y mejorar el conocimiento del cliente.

Adicionalmente a lo descrito anteriormente, la Superintendencia de Bancos, a través de la Intendencia de Verificación Especial, diseñó formularios para el inicio de relaciones con personas individuales o jurídicas, para cuando se realicen operaciones mayores a US$ 10,000.00 o su equivalente en moneda nacional o extranjera, solicitando mensualmente un informe con el detalle de dichas operaciones.

Aunado a lo anterior, es importante mencionar que el Departamento de Auditoria Interna de cada institución bancaria, tiene que implementar un programa que como mínimo debe incluir lo siguiente:

- Conocimiento de los antecedentes personales, laborales, penales, estado patrimonial de los colaboradores que integran la entidad.
- Verificación del conocimiento de los colaboradores, respecto al tema de lavado de dinero, además de las capacitaciones que debe de impartirles el oficial de cumplimiento de la entidad.
- Revisión de las medidas adoptadas por la institución, para incrementar el conocimiento del cliente, y así poderlos categorizar.
- Implementacion por parte de la institución, de un código de conducta y de ética, que sea del conocimiento de todo el personal.
- Verificación de que en todo expediente de los clientes por inicio de relaciones, se encuentre adjunto el formulario IVE requerido, así como toda la demás documentación requerida para poder venderle algún producto financiero.
- Creación de nuevas herramientas para minimizar el riesgo de lavado de dinero, como lo pueden ser las alertas informáticas, las cuales son oportunas para detectar cualquier transacción sospechosa.

En el caso de tarjetas es muy característico que la forma más usada para lavar dinero, es realizando pagos por cantidades mayores al saldo de la misma, por lo que las instituciones deben implementar alertas informáticas, para que al momento de darse estas situaciones, exista una

persona encargada de dar seguimiento, para comprobar si el pago efectuado se encuentra con normalidad.

3.7.2 Riesgo de Fraude

Se refiere a los eventuales fraudes que pudieren existir, por la falta de funcionalidad del control interno, tendiente a evitar su ocurrencia, esto incluye la falsificación, el fraude propiamente, malversación, robo, transacciones de personas de adentro (insiders), vandalismo, extorsión, etc.

Cuando hablamos de tarjetas de crédito, es importante mencionar que los fraudes más comunes se dan por el pago de consumos, con una tarjeta robada o extraviada, así también existe un fraude más complejo, que se da a través de la falsificación de la banda magnética, por medio de una máquina que se encarga de copiar todos los códigos que en esa banda se encuentran, para luego trasladárselos a una tarjeta robada, o bien a una tarjeta nueva falsa.

Por lo anterior, se han creado diferentes patronos de parámetros de usos de las tarjetas, con el objeto que cuando alguna de ellas se salga de estos, se reporte al banco a través de alertas informáticas por medio de correo electrónico y así poder confirmar las transacciones con los tarjetahabientes o bien bloquear la cuenta.

3.8 Riesgo de Auditoría

Comprende los riesgos relacionados con omisiones en el programa de auditoría, tales como:

3.8.1 Riesgo Inherente

Representa la susceptibilidad de una aseveración en una declaración incorrecta, en el supuesto que no existan procedimientos y políticas de estructura de control interno relacionados. Consiste en la posibilidad que en el proceso contable ocurran errores sustanciales antes de considerar la efectividad de los sistemas de control.

Al iniciar una auditoría, es sabido que antes se debe realizar una planificación de los procedimientos que se van a utilizar, dicho trabajo se debe realizar a una fecha determinada sobre la que se evaluará la información, con esto se trata de reducir al máximo este riesgo. Pero tratándose de tarjetas de crédito, es importante señalar que se trata de un tipo de financiamiento muy revolvente, por lo tanto día con día sufre de muchos cambios, lo que viene a incrementar esta clase de riesgo derivado que se pueden obtener resultados satisfactorios, pero al día siguiente puede tener otra perspectiva haciendo que se produzca este riesgo.

3.8.2 Riesgo de Control Interno

Es aquel que comprende a la fragilidad por la ausencia de un control interno preventivo. Uno de los puntos inexistentes en todo informe de auditoría, corresponde a la evaluación del control interno y recomendaciones sobre el mismo. También se refiere a la incapacidad de los controles internos de detectar errores o irregularidades sustanciales en la institución.

Al momento de realizar una auditoría, es evaluado el control interno de la entidad que se esta interviniendo, con el objeto de establecer las deficiencias y por recomendar, que implementen nuevos controles o se mejoren los existentes, todo esto a través de las recomendaciones que plasme el auditor en su informe final.

En lo referente a las tarjetas de crédito, es evidente que se debe llevar un control interno estricto, el cual debe evaluarse constantemente, para minimizar este riesgo, derivado que por tratarse de un tipo de crédito muy activo y por la forma de operar de la misma además de este riesgo, está expuesto a otros riesgos, los cuales se derivan de tener un control interno débil dentro de la institución.

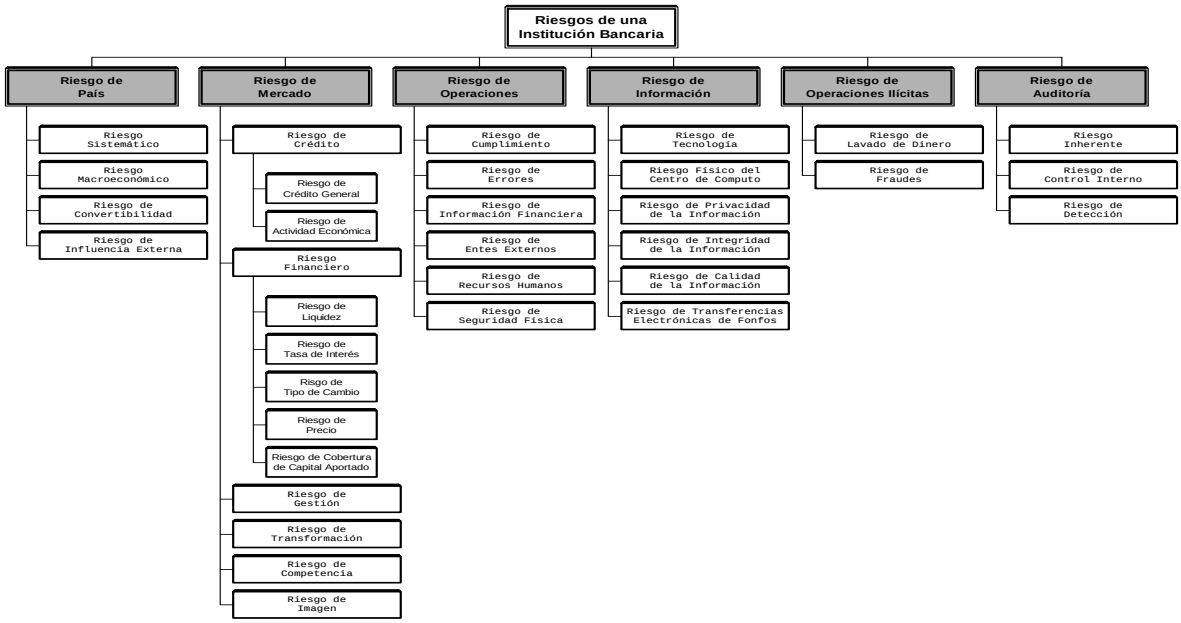
3.8.3 Riesgo de Detección

Es genérico y corresponde a aquel que resulta de una omisión en el proceso de auditoría. Estriba en la posibilidad de que hayan ocurrido errores importantes en el proceso administrativo – contable, y que no fueron detectados por el control interno, ni tampoco por las pruebas, procedimientos diseñados y realizados por el auditor.

Este riesgo tiende a incrementarse o disminuirse, dependiendo de los procedimientos y pruebas se planifiquen, además del alcance que pretendan darles a las mismas, en la ejecución de lo planificado para iniciar la auditoría.

Para una mejor apreciación de lo citado, a continuación se presenta el siguiente diagrama:

Esquema No. 4
Clasificación de Riesgos



Fuente: Carlos Valdivieso
Décimo Primer Simposio de Auditoría Interna
El Nuevo Estándar Internacional de Control Interno C.O.S.O. y su Aplicación Basado en Riesgos

CAPITULO IV

LA AUDITORIA DE UN BANCO EN LA PREVENCION Y DETECCION DE FRAUDES POR LA FALSIFICACION DE LA BANDA MAGNETICA DE TARJETAS DE CREDITO

4.1 Evaluación del Control Interno

El control interno es siempre un proceso fundamental en la actividad bancaria, en virtud de la necesidad de verificar el adecuado funcionamiento de una organización. Involucra a diversos niveles jerárquicos dentro de una institución.

A continuación se describe un sistema de control interno, relacionado a la solicitud, análisis, emisión, atención de gestiones de los tarjetahabientes, dentro de una institución bancaria emisora de tarjetas de crédito.

4.1.1 Proceso de Solicitud y Emisión de una Tarjeta de Crédito

Este proceso se inicia en la sección de servicio al cliente, la cual es de vital importancia debido a que son las personas que tienen el primer contacto con el cliente, al cual le informan sobre los beneficios y las ventajas del producto, le explican su funcionamiento y asesoran cuál es la mejor opción que se adapte a las necesidades y perfil del mismo.

También le indican que formularios y documentos debe presentar para proceder a ingresar su solicitud, la cual posteriormente es trasladada a la sección de Revisión y Cumplimiento.

El proceso de emisión de una tarjeta de crédito, esta integrado por varias etapas, en las cuales deben estar establecidos adecuada y en forma clara, los lineamientos que faciliten la obtención de la información, para lograr realizar un mejor análisis del cliente y fundamentar el riesgo inherente de las solicitudes, que mejorará la calidad global de la cartera crediticia. El proceso de solicitud se divide en:

4.1.1.1 Solicitud de Tarjeta de Crédito

Toda entidad bancaria que dentro de su portafolio de productos, incluya el financiamiento a través de tarjetas de crédito, debe contar con un formato estándar, para la solicitud de la misma, la cual incluye información básica y clave de la persona interesada.

Es importante mencionar que derivado de la Ley de Lavado de Dinero u Otros Activos (Decreto 67-2001), la Superintendencia de Bancos, a través de la Intendencia de Verificación Especial, diseño formularios específicos, para el inicio de relaciones con personas individuales y jurídicas ***(Formularios IVE TC-01 Y TC-02 respectivamente)***. Dichos formatos exigen suficiente información del solicitante, es por ello que la mayoría de entidades emisoras de tarjetas de crédito, optaron por utilizar estos formularios como solicitud de tarjeta de crédito, únicamente adjuntándole el contrato, en el cual el solicitante acepta las condiciones establecidas por el banco, debido que llenar una solicitud y luego el formulario IVE correspondiente, es demasiado trámite para el cliente.

En el apartado de anexos se muestran los formularios IVE utilizados para la solicitud de tarjeta de crédito, anexos para solicitud de tarjeta adicional y contrato para el uso de la línea**. (Ver Anexos 1,2,3,4 y 5)**

4.1.1.2 Documentación Complementaria Requerida para la Solicitud

Adicional a la solicitud de tarjeta, es necesario que el solicitante facilite documentación complementaria, con la cual se conocerá mejor el perfil del mismo, así también se podrá confirmar la información descrita en la solicitud ***(Formularios IVE)***, y otros datos de interés, para el análisis de riesgo.

Otro aspecto relevante es que la información requerida debe cumplir con lo estipulado en el Reglamento para la Administración del Riesgo de Crédito ***(Resolución de la Junta Monetaria JM-93-2005, de fecha 25 de mayo de 2005)***, la cual puede variar dependiendo de la clase de tarjeta para la que este calificando el solicitante. **(Ver Anexo 6)**

4.1.1.3 Perfil de la Persona Solicitante de Tarjeta de Crédito

Adicional a la solicitud de crédito y la documentación complementaria requerida es necesario que el solicitante cumpla con ciertas condiciones que reflejarán su perfil, las cuales pueden variar dependiendo la tarjeta que este solicitando.

Con toda la documentación reunida, según los numerales (4.1.1.1, 4.1.1.2 y 4.1.1.3), se prepara un expediente del cliente el cual debe ser trasladado por esta sección al área de Revisión y Cumplimiento, para la verificación y confirmación de la información respectiva. **(Ver Anexo 7)**

4.1.1.4 Revisión y Cumplimiento

Esta sección tiene como función, verificar que los expedientes contengan los requisitos y documentación complementaria establecida en las solicitudes de crédito. Además se encargan de confirmar la información detallada en la solicitud, como por ejemplo las referencias personales y bancarias. Posteriormente si todo se encuentra en orden se procede a trasladar el expediente a la sección de análisis de riesgos. **(Ver Anexo 8)**

4.1.1.5 Análisis de Riesgos de Solicitudes

Parte fundamental de un proceso de aprobación de tarjetas de crédito, es que dentro de la institución emisora, exista una sección encargada del análisis de riesgo crediticio, la cual basada en la información reunida en el expediente, podrá verificar y evaluar la razonabilidad de aprobar o no la tarjeta solicitada, dejando constancia de la resolución mediante un dictamen que velará porque siempre prevalezca la protección a los intereses de la institución. **(Ver Anexo 9)**

4.1.1.6 Comité de Créditos

Este comité tiene por objeto aprobar operaciones, emitir las actas del comité y preparar las resoluciones (Puntos de Acta) del Consejo de Administración y Gerencia. **(Ver Anexo 10)**

Como se pudo apreciar en los anexos descritos en los apartados anteriores, para que una tarjeta de crédito sea aprobada debe cumplir con ciertos requisitos, los cuales son evaluados y verificados con la finalidad de fundamentar la aprobación de la misma.

Por lo anterior, es de vital importancia que constantemente la auditoría interna de la entidad, realice revisiones periódicas para asegurarse de que se estén cumpliendo con las políticas establecidas dentro de la entidad, con la legislación guatemalteca aplicable, y asegurar un alto nivel en la selección de los clientes, a los cuales se les aprueban las tarjetas, para minimizar el riesgo de posibles cuentas malas que a la larga se vuelven pérdidas para la institución.

4.1.1.7 Embosado de Tarjetas

Mediante este proceso se proceden a grabar en los plásticos vírgenes, el nombre, número de identificación del Banco (Bin) según el tipo de tarjeta aprobada, número de cuenta con que se identificará la tarjeta en el sistema de la entidad emisora, las fechas de emisión y vencimiento de la misma.

También se graba en la banda magnética de la tarjeta, el código de verificación, con el cual se validarán las autorizaciones que solicite el establecimiento afiliado donde sea utilizada. Dicho código, es establecido a través de un logaritmo que establece la institución encargada del embosado.

En el caso que se expone a continuación, la entidad emisora de tarjetas de crédito, no posee una sección encargada del embosado de tarjetas, por lo que utiliza los servicios de una empresa de reconocida trayectoria en este tipo de actividad.

Por lo anterior, es importante comentar que la institución emisora debe custodiar los plásticos vírgenes, los cuales se trasladan periódicamente a la empresa contratada para el embosado, dependiendo de la cantidad de tarjetas que se necesiten emitir. **(Ver Anexo 11)**

4.1.1.8 Entrega de Tarjetas de Crédito

Como último proceso, después de emitida una tarjeta de crédito, se realiza la entrega de la misma al tarjetahabiente, la cual puede ser enviada directamente a la dirección proporcionada por el solicitante o si lo prefiere pasar a recogerla en la agencia del banco más cercana. **(Ver Anexo 12)**

4.1.2 Procesos de Atención y Servicio al Tarjetahabiente

En cualquier entidad emisora de tarjetas de crédito, es imprescindible prestar un excelente servicio, a través de la atención y solución a los requerimientos de los tarjetahabientes. Así mismo dentro de la calidad de este servicio como complemento, las instituciones cuentan con una sección de seguridad que tiene a su cargo la supervisión de los movimientos diarios y el comportamiento de las tarjetas de crédito.

Por lo anterior, a continuación se detallan las actividades específicas que incluyen estos procesos:

4.1.2.1 Análisis Gestiones de Tarjeta de Crédito

Dentro de las funciones que realiza la sección de análisis de riesgo, se incluye la evaluación y verificación de gestiones realizadas por los tarjetahabientes, las cuales se pueden dar por distintas razones, como solicitud de incremento de límite de crédito, cambio de clase de tarjeta, reposición por deterioro, reporte de tarjeta perdida o robada, etc.

También es importante comentar que existen gestiones que se ingresan con el objeto de solicitar revisión de alguna transacción operada a determinada tarjeta, con la que el tarjetahabiente no esta de acuerdo, con la finalidad de que se puedan realizar ajustes o correcciones a los movimientos de la cuenta. **(Ver Anexo 13 y 14)**

4.1.2.2 Seguridad y Vigilancia de las Tarjetas de Crédito

Es importante mencionar que dentro de la atención y servicio que se brinda al tarjetahabiente, se encuentra el monitoreo y supervisión de los movimientos que realizan las tarjetas de crédito, además de brindar la atención a las gestiones ingresadas por los tarjetahabientes las cuales pueden darse por las siguientes situaciones: **(Ver Anexo 15)**

- Reclamos de clientes, por inconformidad con los cargos por servicios efectuados en su estado de cuenta.
- Solicitud de investigación de movimientos no efectuados por el tarjetahabiente.

Adicionalmente a lo anterior, esta sección, tienen a su cargo la constante supervisión de los movimientos de las tarjetas, para lo cual se basa en alertas electrónicas que pueden ser enviadas mediante programas específicos diseñados por VISA o bien por los adquirentes autorizados.

Dichas alertas, son enviadas cuando una determinada tarjeta muestra transacciones poco usuales, respecto al movimiento habitual del tarjetahabiente. Es por ello que pueden haber un sin número de clases de alertas, las cuales pueden estar determinadas entre otras condiciones por las siguientes:

- Cantidad de transacciones efectuada en una hora, o en un día.
- Un límite en el monto de los consumos en el día.
- Consumos en lugares poco frecuentados por el tarjetahabiente.
- Transacciones efectuadas casi a la misma hora, pero en lugares distantes.

Por lo anterior, esta sección debe analizar cada alerta que recibe, con el fin de establecer si las transacciones, se encuentra dentro de los parámetros normales del tarjetahabiente y de ser necesario contactar al tarjetahabiente con el fin de confirmar el movimiento efectuado.

4.1.3 Intervención de la Auditoria Interna

Como parte fundamental de la administración de una determinada entidad, es contar con el apoyo y asesoría de su departamento de auditoría interna, el cual dentro de sus funciones debe velar por que dentro de la institución se cumplan con todos los procesos de controles internos, para minimizar al máximo los diferentes riesgos a los que esta expuesta.

Por lo anterior, la auditoría interna realiza revisiones periódicas de emisiones, seguimiento de gestiones, cobros de cargos por servicios, arqueos de tarjetas, etc., con lo cual se determina el nivel de cumplimiento de los controles internos, además de establecer deficiencias en los mismos, las cuales son informadas a las áreas que corresponden, con el fin de que éstas, sean corregidas oportunamente.

Adicionalmente la auditoría interna tienen como función, revisar que los controles internos existentes, cubran todos los riesgos posibles, de lo contrarío debe evaluarse la forma de cambiarlos o modificarlos, para mantenerlos actualizados, de acuerdo a las exigencias de los cambios constantes, que sufre el mercado y la tecnología.

4.2 Evaluación del Programa de Control de Fraude

Dentro de una entidad emisora de tarjetas de crédito, es de vital importancia que se cuente con un programa de control de fraude, el cual periódicamente debe ser evaluado por el departamento de auditoría interna, con el fin de verificar si aún es funcional, o si bien, deben hacerse enmiendas e implementar nuevos puntos a cubrir dentro del mismo.

4.2.1 Programa de Control de Fraude

La finalidad del control del fraude es prevenir y minimizar las pérdidas causadas por abusos intencionales de los tarjetahabientes, usuarios no autorizados y usuarios o comercios fraudulentos. Para que dicho programa resulte eficaz, las actividades de control de fraude requieren de una interacción entre el departamento de tarjeta de crédito, con el resto que integran la entidad.

4.2.1.1 Funciones

Dentro de las principales funciones de control de fraude, se mencionan las siguientes:

- Prevenir e investigar las actividades efectuadas con tarjetas fraudulentas.
- Prevenir e investigar la copia o el robo de información, relacionada con cuentas, transacciones, en que la seguridad de la misma se vea comprometida.
- Supervisar las cuentas en las que se hayan reportado tarjetas robadas o perdidas.
- Planificar y supervisar la seguridad de las tarjetas, durante el proceso de fabricación, entrega, así como de las existencias de las mismas.
- Mantener en el archivo de excepción, cuentas de tarjetas perdidas y robadas, para que sean retiradas del mercado y en el boletín de tarjetas canceladas, las reportadas como perdidas, robadas o falsificadas.
- Servir de enlace con las autoridades de la policía y funcionarios del ministerio público.
- Planificar y supervisar la seguridad, en las instalaciones físicas de la entidad emisora.
- Mantener un plan de educación para los tarjetahabientes y comercios, con relación a la prevención del fraude.

4.2.1.2 Posición en la Estructura Organizativa de la Entidad Emisora

Toda entidad emisora de tarjetas de crédito, debe implementar dentro de su estructura, un departamento encargado del control de fraude, en el que sus funciones dependerán de varios factores, tales como el volumen de tarjetas Visa que posea, su estructura organizativa actual, las instalaciones físicas, los recursos humanos y económicos con que dispone la misma.

A continuación se muestran algunas opciones utilizadas, con relación a la posición que debe adoptar la función de control de fraude, dentro de la estructura organizativa de la misma.

- **Una división de control de fraude –** En esta opción se utiliza al personal existente y además proporciona independencia del departamento de tarjetas de crédito.

- **Un departamento separado en el centro de Visa** – Con esta opción se establece una línea de comunicación directa con el gerente del departamento de tarjetas de crédito, así también se establecen en forma clara, el control, la responsabilidad y la capacidad de responder por las acciones tomadas o no, lo cual aumenta la capacidad de este departamento, para lograr los resultados esperados.

- **Una función dividida con el departamento de crédito o de cobros** - Cuando dentro de la entidad emisora, el número y la frecuencia de las operaciones de fraude son menores, lo que no justifica contar con personal a jornada completa para realizar estas funciones, frecuentemente consolidan estas tareas, con las actividades del departamento de créditos o cobros. En estos casos, el personal que conforma el departamento debe incluir a personas que hayan recibido una capacitación especial en el área de control e investigación de fraudes.

4.2.2 Personal de la Entidad Emisora

Para prevenir y detectar rápidamente los fraudes, se requiere contar con personal que esté específicamente disponible para cumplir con las responsabilidades asignadas. Dicho personal estará generalmente integrado por investigadores de fraude y personal de apoyo.

4.2.2.1 Investigadores

Las personas que laboran como investigadores, por lo general deben tener las siguientes responsabilidades:

- Comunicarse con las áreas del banco, colaborar con las autoridades de la policía, entrevistar a clientes, comercios y sospechosos, con el fin de recabar la información relacionada con la actividad de fraudes con tarjetas Visa.
- Examinar los recibos o voucher de venta para detectar cualquier pista que pueda revelar la identidad de una persona que esté utilizando una tarjeta, para realizar un fraude, y las áreas donde se está utilizando dicha tarjeta.
- Firmar por parte de la entidad emisora, los documentos relacionados con algún proceso judicial que se siga, contra los defraudadores y comparecer ante los tribunales correspondientes.
- Preparar los reportes de la actividad de fraude, para el gerente del departamento de tarjeta de crédito y otros funcionarios de la gerencia general.
- Preparar los reportes donde se describen los fraudes, los documentos que servirán de pruebas, para las autoridades policíacas, fiscales y procuradores que intervengan en un proceso.
- Emplear a investigadores y personal con experiencia en el área de seguridad de tarjetas de crédito, para los puestos relacionados con el control de fraude. No obstante, los investigadores deben tener las siguientes calificaciones básicas:

  ⇒ Conocimiento de las operaciones con tarjetas, como de todos los procedimientos que incluye ésta actividad financiera.
  ⇒ Experiencia previa en la labor de investigadores.
  ⇒ Conocimiento de las leyes que regulan lo relativo a la actividad de tarjetas de crédito, los fraudes, y los procesos judiciales que se puedan seguir ante los tribunales.
  ⇒ Destrezas de investigación, interrogación y obtención de pruebas, incluyendo la habilidad de seguir pistas.
  ⇒ Capacidad de análisis, toma de decisiones y buen juicio.
  ⇒ Conocimientos y destreza en el manejo de computadoras y sus diversas aplicaciones, el procesamiento de textos, el uso de hojas de cálculo y programas de bases de datos.
  ⇒ Destreza en la comunicación oral y escrita.

4.2.2.2 Niveles de Personal de la Entidad Emisora

Debido a que la incidencia del fraude fluctúa en forma impredecible, se deben hacer periódicamente, revisiones de los niveles de personal.

Los factores que influyen en los requisitos de personal incluyen:

- Volumen de la cartera de tarjetahabientes y comercios.
- Volumen de ventas de tarjetas y de comercios.
- Volumen y tipo de actividad delictiva en los principales mercados del emisor.
- Eficacia de los programas de educación a tarjetahabientes y comercios.
- Eficacia y cooperación de las autoridades policíacas y postales.
- Calidad y desempeño del personal de control de fraude.
- Procedimientos de distribución de tarjetas.
- Penalidades legales establecidas para los delitos relacionados con fraudes cometidos mediante el uso de tarjetas.
- Cooperación de otros centros de Visa.

4.2.2.3 Capacitación del Personal

El personal de control de fraude debe estar capacitado en las siguientes áreas de experiencia y contar con ciertas habilidades:

- Herramientas de reducción de fraudes y uso de las mismas.
- Técnicas y procedimientos de investigación.
- Técnicas de educación a tarjetahabientes y comercios para prevenir el fraude.
- Reglamentos Operativos de Visa.
- Procesamiento y análisis de datos.
- Procedimientos de distribución de tarjetas.
- Cómo servir de enlace con otros centros de tarjetas bancarias y contactos regionales de control de fraude de Visa y comunicarse con los mismos.
- Cómo servir de enlace con las autoridades, funcionarios judiciales y comunicarse con ellos.
- Leyes y reglamentos, relacionados con el fraude de tarjetas.
- Seguridad física del centro de tarjetas bancarias e instalaciones relacionadas.
- Sistema y procedimientos de la actividad de tarjetas de crédito Visa.

La capacitación continua y la educación con respecto a las técnicas de prevención e investigación de fraudes deben mejorar la eficacia del personal relacionado.

4.2.2.4 Metas de Desempeño

Las evaluaciones periódicas de desempeño también contribuyen a mejorar la eficacia del personal.

Las normas de evaluación deben incluir las siguientes:

- Una comparación entre las pérdidas netas anuales debidas al fraude y las estadísticas de pérdidas por fraude locales, regionales y nacionales.
- Una revisión del tiempo requerido para detener la actividad fraudulenta después de detectarse o notificarse la misma.
- Revisiones periódicas de la iniciativa y esfuerzo demostrado por los investigadores en el manejo de los casos asignados.

4.2.3 Herramientas de Control de Fraudes

La idea de eliminar completamente los fraudes a través del uso de tarjetas Visa, es imposible y resulta económicamente cara. No obstante, el fraude y las pérdidas que el mismo ocasiona se pueden manejar y controlar para mantenerlas dentro de límites aceptables. Las siguientes

herramientas pueden ayudar a minimizar la exposición al fraude y contribuir a brindar protección a los tarjetahabientes y comercios.

4.2.3.1 Boletín de Tarjetas Canceladas

El boletín de tarjetas canceladas, es un listado de tarjetas que ya no son válidas, las cuales deben ser rechazadas y retiradas de circulación, al momento de presentarlas en un establecimiento comercial. Para incluir un número de cuenta de tarjeta en el boletín de tarjetas canceladas, primero se debe listar el mismo en el Archivo de Excepción de Visa (Visa Exception File) con el código "recoger tarjeta" y los códigos regionales correspondientes. Las tarjetas que se pueden listar con instrucciones para que sean recogidas y retiradas de circulación incluyen:

- Tarjetas robadas
- Tarjetas falsificadas
- Tarjetas y/o cuentas que registran un número excesivo de compras en un corto plazo o repentinamente.
- Tarjetas o cuentas en las que se ha falsificado la firma del tarjetahabiente
- Cuentas morosas, en las que iniciado el proceso de cobranza, no se pueden establecer comunicación con los tarjetahabientes
- Tarjetas extremadamente morosas en los pagos
- Tarjetas vencidas

El Boletín de Tarjetas Canceladas se emite tanto en formato impreso como en formatos electrónicos, y está disponible en los siguientes medios, dependiendo de los requisitos regionales establecidos por Visa.

- Edición en papel
- Cinta magnética
- CD ROM
- Formato electrónico en línea, los miembros pueden designar a los comercios afiliados a su programa de adquirente que deban recibir copia del boletín de tarjetas canceladas. Dichas copias se pueden enviar a:

  - Todos los establecimientos
  - Establecimientos en determinadas áreas seleccionadas
  - Determinadas categorías específicas de comercios
  - Comercios que tengan una alta incidencia de actividad fraudulenta

Los comercios que reciben dicho boletín, lo utilizan para verificar los números de cuenta en todas las transacciones por debajo de su límite de piso (importe de transacción por encima del cual se requiere al comercio llamar a su centro de autorización y solicitar la misma por voz). Sí el número de cuenta correcto a una transacción específica aparece dentro del boletín, el comercio debe rechazar la tarjeta y, si es posible, retenerla. Los comercios devuelven las tarjetas recuperadas al emisor y pueden tener derecho a una compensación en efectivo.

4.2.3.2 Recompensas a Comercios

Existen entidades emisoras de tarjetas de crédito, que ofrecen a los establecimientos afiliados, una recompensa monetaria por recoger las tarjetas fraudulentas, lo cual motiva y aumenta la disposición de éstos, para utilizar el boletín, particularmente en el caso de las transacciones que estén por debajo de su límite de piso individual.

4.2.3.3 Educación a los Tarjetahabientes y Comercios

Educar a los tarjetahabientes y comercios en el control y la prevención de fraudes, debe ser una tarea continua, para lo cual deben diseñarse materiales que lleven a los tarjetahabientes y

comercios a cobrar conciencia de sus responsabilidades, respecto a la prevención y el control del fraude con tarjetas de crédito.

a) Educación a los tarjetahabientes sobre la Prevención del Fraude

Los materiales diseñados para educar al tarjetahabiente con respecto a la prevención del fraude deben contener información relacionada con los siguientes temas:

- Cómo evitar que se pierdan las tarjetas (las reglas básicas para usar las tarjetas y proteger su seguridad), incluyendo información sobre la seguridad del Número de Identificación Personal o PIN.
- Cómo proteger del número de cuenta, para que este no se vea comprometido.
- Cuales son los procedimientos para reportar las tarjetas perdidas y robadas, incluyendo el número de teléfono del centro de Visa del emisor.
- Cual es la responsabilidad financiera del tarjetahabiente, en caso del uso fraudulento de su tarjeta de crédito.

Preparar y distribuir los materiales descritos anteriormente a los tarjetahabientes, no debe ser una inversión costosa en fondos y tiempo. Se recomienda incluir los materiales con los estados mensuales de la cuenta, o con otros tipos de comunicaciones que se envíen a los tarjetahabientes. Los formatos utilizados pueden ser:

- Envío de estados de cuenta por correo.
- Documentación enviada para cuentas nuevas.
- Documentación enviada cuando se vuelve a emitir la tarjeta.
- Publicidad local.

b) Educación a Comercios sobre Prevención del Fraude

Los programas y materiales educacionales diseñados para los comercios, deben darles las instrucciones apropiadas para que puedan:

- Reconocer las características de un usuario fraudulento, tales como:
  - Carecer de documento de identificación.
  - Nerviosismo al momento de la compra.
  - Mostrar demasiada prisa (cuando los clientes dicen, por ejemplo, que no tienen tiempo para esperar a que se le empaquen los artículos comprados)
  - Compras justamente por debajo del límite de piso.
  - Hacer compras en forma indiscriminada, sin atender al color, tamaño o calidad de los artículos.
  - Comprar piezas o partes para automóviles (por ejemplo, neumáticos) y no instalarlas en el momento de efectuar la compra.
- Reconocer los patrones de las compras sospechosas.
- Comprender la importancia que tiene el utilizar las publicaciones y los sistemas de control de fraude establecidos (notificaciones de alerta sobre tarjetas fraudulentas, boletines, autorizaciones, etc.).
- Reconocer una tarjeta falsificada y un panel de firma alterado.
- Reconocer los dispositivos y métodos utilizados para copiar el contenido de la banda magnética.

Los materiales de educación sobre la prevención de fraudes, se pueden presentar en diversos formatos que incluyen los siguientes:

- Llamadas periódicas de servicio a los establecimientos afiliados.
- Boletines varios de información.
- Seminarios de capacitación

4.2.3.4 Límites de Piso del Comercio

Se debe utilizar la asignación de límites de piso y hacerlos cumplir en forma eficaz para identificar y supervisar a los establecimientos, con mayor riesgo de fraude y en las áreas que tienen una alta incidencia de actividad fraudulenta. Por ejemplo, se puede asignar un límite de piso cero a los establecimientos descritos anteriormente, a fin de requerirles que obtengan autorización para todas las transacciones que realicen. En los casos en que un defraudador haga consumos rutinariamente por un importe que esté justo por debajo del límite de piso asignado, se debe reducir temporalmente ese límite para permitir a la entidad emisora, identificar y capturar al sospechoso.

4.2.3.5 Autorizaciones y Supervisión de Depósitos de los Comercios

La autorización y supervisión de los depósitos de los comercios, sirven de herramientas muy poderosas para identificar los patrones de actividad irregular o sospechosa en el establecimiento, con el fin de detectar y controlar rápidamente las pérdidas originadas por el fraude.

Los reportes de excepción de autorizaciones se pueden utilizar para detectar cualquier actividad poco usual y con gran posibilidad de ser un fraude relacionado con tarjeta de crédito. Entre los ejemplos de parámetros críticos que pueden incluirse en los reportes de excepción de autorizaciones diarias y que pueden utilizar otros adquirentes, se pueden mencionar:

- Varias solicitudes de autorización individuales, que en su conjunto sobrepasen un valor predefinido.
- Varias autorizaciones de una misma cuenta en un establecimiento.
- Consumos con valores que sigan un patrón descendente con el mismo número de cuenta.
- Número excesivo de solicitudes de autorizaciones rechazadas en relación con las aprobadas.
- Gran cantidad de respuestas “Recoger Tarjeta”.
- Cantidad total de autorizaciones, superior a la norma diaria establecida.
- Valor total de autorizaciones, por encima de la norma diaria establecida.
- Un establecimiento que no haya procesado transacciones en los últimos dos meses.
- Ventas fraccionadas y divididas.

Las Normas de Supervisión de Depósitos de los Comercios de Visa, requieren a las entidades emisoras de tarjetas, establecer parámetros de actividad diaria normal para todos los establecimientos afiliados a sus programas de adquirente.

Los parámetros de actividad requeridos, incluyen los siguientes:

- Volumen bruto semanal de ventas.
- Valor promedio de transacción semanal.
- Cantidad por semana de recibos de venta.
- Promedio semanal de tiempo transcurrido entre la fecha de transacción y la fecha de procesamiento del emisor (la fecha de transacción y la fecha de procesamiento cuentan como un día cada una.)
- Número de contracargos por semana (Transacción fraudulenta o de otro tipo, por la cual no se ha recibido pago y la cual el emisor devuelve al adquirente).

Establecidos los parámetros de actividad semanal normal, cualquier cambio repentino o drástico en los depósitos del comercio debe dar lugar a que se genere una alerta u otro tipo de acción investigativa. Los depósitos deben supervisarse como mínimo semanalmente.

4.2.3.6 Servicios de Control de Fraude de Visa

Visa realiza un constante esfuerzo para minimizar las pérdidas ocasionadas por los fraudes y apoyar a través de programas individuales de control de fraude de los emisores, desarrollando un conjunto de servicios automatizados de reportes e información, orientados a prevenir e identificar los fraudes. Con lo anterior se pretende mejorar la capacidad de las instituciones para identificar la

procedencia de los fraudes, investigar los probables esquemas que el mismo va adoptando, y controlar las pérdidas.

A continuación se describen algunos de los servicios de control de fraude que Visa ofrece en la actualidad.

a) Valor de Verificación de Tarjeta

En los últimos años, la alteración y falsificación de la banda magnética de las tarjetas de crédito se ha convertido en una amenaza para la seguridad e integridad de la marca Visa, las entidades emisoras y los establecimientos afiliados, en el mundo entero. Por lo anterior, Visa desarrolló el Valor de Verificación de Tarjeta (Card Verification Value CVV), que es una tecnología de control de riesgos destinada a identificar las tarjetas falsificadas en el punto de venta.

Dicha herramienta, utiliza un proceso criptográfico seguro para codificar un número de verificación único de tres dígitos en la banda magnética de todas las tarjetas Visa válidas, el cual se calcula mediante la aplicación de un algoritmo (una fórmula matemática), a otros datos de la cuenta codificados en la banda magnética. El número se vuelve a calcular y se verifica en línea al mismo tiempo que el terminal autoriza la transacción.

Después de que el terminal verifica el código, el comercio recibe un mensaje que autoriza la transacción. Si al momento de la autorización no pasa la verificación del código, el establecimiento recibe instrucciones de denegar la transacción y recoger la tarjeta.

Dicha herramienta fue implementada en el año de 1991, desde entonces se ha logrado reducir el aumento en el uso de tarjetas con banda magnética falsificada, economizando a emisores y adquirentes alrededor del mundo, grandes cantidades de dinero en posibles pérdidas debidas a este tipo de fraude.

Para que las entidades emisoras logren la certificación para utilizar el Valor de Verificación de Tarjeta, deben primero contar con la capacidad de poder codificar este valor de verificación en las tarjetas que emiten, además de poder responder a las solicitudes de confirmación del mismo en línea a los comercios.

b) Valor de Verificación de Tarjeta 2 (CVV2)

Como el mercado de compras y consumos se ha modernizado con el pasar de los años, así también Visa ha creado servicios que se adapten a esta necesidad, como lo es el servicio de Valor de Verificación de Tarjeta 2 (Card Verification Value 2, CVV2), la cual es una herramienta de verificación de tarjetas diseñada para reducir las pérdidas por fraude relacionadas principalmente con las transacciones de ordenes por correo y teléfono. Este servicio proporciona a los comercios, adquirentes y emisores, datos adicionales en las solicitudes de autorización, identificando posibles actividades de falsificación.

Este código, es un número de tres dígitos que se imprime al dorso de la tarjeta Visa en un tipo de letra distintivo inclinado hacia atrás. Este código se coloca al final del número de cuenta y se calcula utilizando los datos de la cuenta y claves de encripción únicas. El valor, que el comercio obtiene del tarjetahabiente, se verifica entonces en la autorización.

c) Servicio de Identificación de Riesgos del Tarjetahabiente

Derivado que en la actualidad se ha observado que los nuevos esquemas de fraude, pueden originarse y migrar rápidamente y sin previo aviso de una ciudad a país a otro, detectar e identificar lo más rápido posible los patrones que adopta la actividad fraudulenta resulta primordial para controlar las pérdidas. Para todo esto, Visa ha desarrollado el Servicio de

Identificación de Riesgos del Tarjetahabiente (Cardholder Risk Identification Service, CRIS), destinado a mejorar la capacidad de los Miembros, en la identificación de las formas que adoptan los fraudes, para iniciar los esfuerzos de control lo más tempranamente posible.

Este servicio combina la avanzada tecnología de redes neuronales, con los datos de fraude reportados a escala mundial, a fin de generar una calificación de riesgo para cada transacción autorizada a través del sistema VisaNet. Cuando la calificación de riesgo supera los límites designados por los emisores, el servicio genera un reporte de alerta y lo transmite a estos varias veces al día, frecuentemente dentro de un plazo de unas pocas horas de identificada la transacción sospechosa, para que se pueda responder rápidamente y tomar medidas eficaces.

Este servicio ha probado ser sumamente preciso y ha permitido a las entidades emisoras reducir las pérdidas, así como el tiempo que se dedica a investigar las falsas alertas de fraude, además que es muy flexible y los emisores pueden utilizarlo como sistema independiente o como una mejora a su programa de control de fraude existente.

d) Información de Desempeño de los Comercios

Otro servicio diseñado por Visa, es el de Información de Desempeño de los Comercios (Merchant Performance Reporting, MPR), el cual sirve como dos herramientas de control de fraude. Este servicio apoya en la evaluación de los comercios por parte del adquirente, proporcionando información esencial sobre el desempeño de los establecimientos en el área de tarjetas bancarias. Así también hace posible la supervisión más amplia de los establecimientos afiliados por medio de los perfiles de actividad de comercios y reportes comparativos.

El Servicio descrito anteriormente, combina los datos de las transacciones de los comercios individuales, con los datos y patrones de fraude presentes en toda la industria, con el fin de proporcionar a los miembros, información actualizada sobre las actividades y situación crediticia de sus comercios. Para los adquirentes que investigan a posibles comercios con la intención de afiliarlos, el servicio les genera un reporte donde se indica si éstos están sujetos a alguna prohibición con respecto a participar en el sistema Visa, si se encuentran involucrados en algún litigio pendiente de resolver, o si Visa lo tiene registrado como comercio de telemercadeo de alto riesgo.

Las capacidades de generar reportes de administración de cartera disponible a través de este servicio incluyen:

- Alertas que indican si el establecimiento ha sido identificado como comercio de alto riesgo dos o más veces en los últimos seis meses.

- Perfiles de comercios que trazan el desempeño de los establecimientos en el área de tarjetas bancarias en los últimos cinco trimestres. Los perfiles incluyen información sobre la actividad de intercambio de los establecimientos, el importe promedio de su recibo de venta y la actividad de fraude.

- Información que permite comparar a determinados establecimientos con otros negocios en el mismo sector del mercado o zona geográfica.

e) Servicio Nacional de Alerta de Comercios

Como otra herramienta, Visa ofrece el Servicio Nacional de Alerta de Comercios (National Merchant Alert Service, NMAS), para investigar y garantizar el buen crédito de los posibles comercios afiliados. Consiste en una base de datos electrónica que permite a los adquirentes en distintos países incluir y obtener acceso a la información relativa a comercios considerados

de alto riesgo, o cuyos contratos de afiliación han sido cancelados debido a actividades fraudulentas.

Los adquirentes están obligados a consultar este servicio, a fin de determinar si el establecimiento ha sido cancelado anteriormente, o si ha sido identificado como de alto riesgo, esto se realiza a través de enviar sus consultas al servicio por medio de su interfaz existente con el Sistema de Compensación y Liquidación BASE II de VisaNet (*Sistema de procesamiento de datos, redes y operaciones que utiliza VisaNet, para brindar apoyo a los servicios relacionados con el intercambio, compensación y liquidación de las transacciones autorizadas*).

Si el comercio aparece listado en la base de datos del NMAS, el adquirente recibe un mensaje de alerta y se debe comunicar con la entidad que incluyó al comercio en la lista para obtener más información acerca de las razones por las cuales se incluyo. El hecho de que el comercio aparezca en este listado no impide automáticamente al adquirente afiliar al comercio, la intención de este programa es proporcionar a los miembros información pertinente que los ayude a evaluar los riesgos que podría implicar el comercio para la institución.

f) Servicio de Identificación de Riesgos

Como otro componente integral de cualquier programa de control de fraude, se utiliza el servicio de Identificación de Riesgos (Risk Identification Service, RIS), que brinda a los miembros un paquete integrado de capacidades de supervisión, información y generación de reportes, promoviendo, al mismo tiempo, la prevención y el control del fraude en forma oportuna y eficaz.

El servicio recaba y analiza los datos de las transacciones de los comercios y genera reportes sobre las actividades que pueden implicar un riesgo, como un número excesivo de contracargos o cantidades poco usuales en los montos de los depósitos. Estos reportes se encuentran disponibles en forma diaria, semanal, mensual y trimestral, además incluye alertas sobre situaciones específicas de actividad riesgosa y perfiles completos de los comercios.

Cuando este servicio detecta alguna prueba o actividad con alto grado de riesgo, se puede llegar a requerir de los adquirentes y comercios, iniciar acciones para corregir el problema. Por ejemplo, se pueden realizar revisiones de los procedimientos de aceptación de tarjetas con el comercio, en ciertos casos se puede bajar el límite de piso asignado, o cancelar el contrato de afiliación del establecimiento.

Las capacidades de supervisión e información de este servicio, se continúan expandiendo y afinándose, con la finalidad de ofrecer una gama de opciones flexibles y eficaces para identificar y controlar el fraude. Dependiendo de los mercados y de las condiciones de cada país, se pueden ajustar los límites de supervisión.

4.2.4 Investigaciones de Fraudes

Toda investigación tiene como finalidad, reunir suficiente evidencia e información para detener cualquier actividad de fraude, así como de recuperar la tarjeta o número de cuenta involucrado. Las pruebas e información que se recaben durante la investigación, se deben documentar cuidadosamente y se debe proporcionar una copia a las autoridades policíacas y judiciales, para arrestar y condenar a los hechores de estos delitos.

Toda entidad emisora de tarjetas, debe mantener políticas que requieran realizar investigaciones rigurosas, cuidadosas y exhaustivas, para contribuir a obtener toda la información, a efecto de poder tomar medidas severas en contra de los defraudadores. Se dice que una investigación es exitosa, cuando esta puede conducir a la captura de los delincuentes y abrir el camino para investigar otros casos.

4.2.5 Componentes de una Investigación Exitosa

Para obtener una investigación exitosa, se requiere realizar una búsqueda planificada y sistemática de los hechos y las pruebas. Dentro de las habilidades y destrezas básicas que debe tener un investigador, se pueden mencionar:

- Habilidad para realizar entrevistas e interrogar a personas.
- Destreza para examinar registros y documentos relacionados con el fraude.
- Capacidad de observación y análisis de las pruebas encontradas.

Adicionalmente, cada investigación debe incluir cinco pasos básicos:

- **Análisis** – Al momento de revisar la documentación disponible (tales como el reporte de tarjetas perdidas y robadas, la declaración jurada del tarjetahabiente y los recibos de venta) correspondientes a las transacciones fraudulentas.

- **Planificación** – Al iniciar una investigación se debe crear un plan que facilite la adquisición de información y la compilación de pruebas, que conduzcan a identificar al delincuente, arrestarlo y condenarlo.

- **Averiguación de los Hechos** – Debe reunir toda la información y las pruebas de acuerdo con el plan diseñado. La averiguación de los hechos normalmente conlleva entrevistas con testigos por teléfono y en el campo, así como la tarea de verificar y corroborar las pruebas siempre que sea posible.

Cuando se realicen las entrevistas con los testigos, los investigadores deben obtener suficientes datos personales, de manera que se pueda localizar a las personas, como mínimo, un año después de ocurrir la transacción fraudulenta.

- **Documentación** - Documentar los hechos y mantener los resultados de la investigación para referencias futuras.

- **Resolución** – Al momento de resolver, se deben tomar las medidas necesarias, para resolver el caso una vez. Esta resolución se pude dar de las formas siguientes:

  - Entregando las pruebas disponibles a las autoridades, para que ellos realicen su labor.

  - Procurando obtener restitución de los consumos efectuados, cuando no se obtengan suficientes pruebas, para iniciar un proceso judicial.

  - Cerrando el caso, debido a la falta de pruebas suficientes para proceder judicialmente.

4.2.6 Proceso Judicial

Cuando el país donde se tipifique que los fraudes a través de tarjetas de crédito son un delito, las autoridades judiciales, puede solicitar colaboración alguna, para iniciar acción contra los delincuentes.

Es importante que toda entidad emisora de tarjetas de crédito incluya dentro de sus políticas, que al momento de investigarse un caso de fraude, se inicie con un proceso judicial, esto con el fin de proporcionar a la entidad una imagen de seriedad y rigurosidad. Con lo anterior, también se logra crear un freno para otros delincuentes que intenten realizar lo mismo y se obtiene un mayor respeto por parte de las autoridades judiciales, con lo cual se garantiza su colaboración en el futuro.

4.2.7 Tarjetas Pérdidas y Robadas

A continuación se describen los procedimientos que se deben aplicar a las tarjetas Visa perdidas y robadas.

a) Notificación a los Emisores

Las entidades emisoras, reciben las notificaciones relacionadas con las tarjetas perdidas y robadas por vía telefónica, también se puede recibir por telefacsímil, carta, telegrama, y hasta en persona, o ser enviadas por otros a través de VisaNet. Cada notificación debe manejarse en forma individual y registrarse en el formulario designado para reportar las tarjetas perdidas y robadas.

b) Contenido del Formulario de Reporte

El reporte de tarjetas perdidas y robadas requiere la siguiente información:

- Fecha en que se recibió la notificación y se preparó el reporte
- Nombre, dirección y número de teléfono del tarjetahabiente
- Número de cuenta y fecha de vencimiento de la tarjeta
- Fecha en que se descubrió que la tarjeta se había perdido o fue robada
- Circunstancias que rodean la pérdida o robo
- Descripción del ladrón si la tarjeta fue robada
- Fecha, ubicación y valor de la última compra
- Lista de otras pertenencias perdidas o robadas junto con la tarjeta
- Nombre de la persona que reporta la pérdida o robo
- Fecha en que se notificó a la policía que la tarjeta había sido robada

c) Preparación y Ruta a Través del Sistema

Normalmente, una persona de investigación debidamente capacitada para obtener información completa y correcta del tarjetahabiente, puede preparar el reporte de tarjetas perdidas o robadas, para posteriormente trasladar este al personal apropiado, que se encargará de realizar la investigación respectiva.

d) Actualización de Reportes

Cuando el tarjetahabiente proporcione más información con respecto al robo de su tarjeta, o se logren establecer otros hechos relacionados, se debe actualizar el reporte de tarjetas perdidas y robadas, con el fin de asegurar que los expedientes relacionados al caso, se mantengan actualizados en caso de alguna consulta que se quiera realizar.

e) Respuesta del Emisor

Cuando el emisor recibe la notificación de una tarjeta pérdida o robada, debe responder en forma inmediata para documentar y controlar las posibles pérdidas que puedan resultar, además de asegurarse que el tarjetahabiente tenga la reposición de su tarjeta en pocos días, con el fin de causar pocos inconvenientes al mismo.

Para lo anterior, se deben tomar las siguientes medidas:

- **Bloquear la cuenta** – Se deben bloquear todas las cuentas en las que se haya reportado una tarjeta perdida o robada, con el fin de evitar transacciones fraudulentas, éste bloqueo debe generar algún tipo de alerta, si ocurre alguna actividad en la misma.
- **Obtener una declaración jurada del tarjetahabiente** – Se debe obtener una declaración jurada firmada por el tarjetahabiente como prueba, de que él mismo no efectuó ni autorizó las transacciones fraudulentas.

- **Emitir una tarjeta de reposición** – Lo recomendable es enviar por mensajero interno, las tarjetas de reposición para garantizar al tarjetahabiente un mínimo de molestia.

- **Preparar un expediente del caso** – Con las tarjetas de crédito, que se hayan reportado como perdidas o robadas, se debe preparar un expediente, el cual se mantendrá actualizado y será guardado en un lugar seguro.

4.2.8 Instrucciones a los Tarjetahabientes

En el caso de una tarjeta reportada como perdida o robada, se debe asegurar al tarjetahabiente que no será afectado como consecuencia del uso no autorizado de la misma y se debe solicitar que notifique de forma inmediata al banco, si obtienen alguna información adicional.

Así mismo, es importante discutir con el tarjetahabiente los siguientes puntos:

- **Procedimientos relacionados con tarjetas perdidas y robadas** – Se informa al tarjetahabiente del bloqueo de su tarjeta, que toda transacción operada a la misma se revisará para determinar si pudiera ser fraudulenta, así también que toda la información se mantendrá con la debida confidencialidad, salvo que se inicie algún proceso judicial, contra el responsable de los hechos.

- **Tarjeta de reposición y políticas relacionadas con la nueva cuenta** – Establecer la política de la institución para abrir una nueva cuenta, con el objeto de reemplazar la tarjeta perdida o robada, además se informará al tarjetahabiente que la nueva tarjeta, llevará un nuevo número de cuenta, y que no debe utilizar más la cuenta anterior, además que el saldo de la cuenta anterior se trasladará a la reposición.

- **Notificación a la policía** – Se debe indicar al tarjetahabiente que debe dar parte a la policía del robo o perdida de su tarjeta.

4.2.9 Supervisión de las Cuentas

Se deben supervisar las cuentas en las cuales se reporten tarjetas perdidas o robadas, con el fin de detectar cualquier señal de actividad posterior. Dicha supervisión de cuentas puede incluir lo siguiente:

- **Investigar posibles actividades fraudulentas** – De establecerse que la cuenta de la tarjeta, muestra alguna actividad sospechosa de fraude, se debe remitir el expediente del caso con la información relacionada a un investigador capacitado, para que inicie el mismo, el cual será responsable de supervisar la cuenta, actualizar el expediente y mantener comunicación con el tarjetahabiente.

- **Desbloquear la cuenta** – En algunas entidades emisoras, utilizan la política de bloquear temporalmente las cuentas de las tarjeta reportadas como perdidas o robadas, con el fin de dar un tiempo prudencial de seguimiento, el cual al vencer y observar que la tarjeta no ha reflejado movimientos, se desbloquea para que el tarjetahabiente pueda seguir usando la misma tarjeta. Es importante mencionar que en el tiempo prudencial de seguimiento, se le habilita un número temporal de tarjeta para que pueda seguir realizando sus operaciones cotidianas. El plazo temporal puede variar según la entidad emisora.

a) Reportes de Otros Centros de Visa

Un tarjetahabiente puede reportar el robo o pérdida de su tarjeta a cualquier entidad emisora, independientemente de que dicho banco sea o no el emisor de su tarjeta, el cual debe aceptar el reporte y notificar inmediatamente al emisor que corresponda por vía telefónica.

En el caso que el emisor de la tarjeta se encuentra cerrado, la entidad que recibió la notificación la envía a través de la BASE I (Sistema de procesamiento de datos, redes y operaciones de VisaNet que brindan apoyo y proporcionan servicios relacionados con la autorización de las transacciones), para que se incluya la información relativa a la tarjeta perdida o robada en el archivo de excepción correspondiente a dicho centro emisor. Cuando el centro emisor que corresponda reanude sus labores, recibirá un reporte de BASE II con toda la información de la tarjeta perdida o robada.

b) Pérdida o Robo de Tarjetas Sin Grabar

Cuando las tarjetas perdidas o robadas no se encuentre grabadas como en los casos que se describen más adelante, se debe notificar inmediatamente a la Oficina Regional de Visa.

- Cuando las tarjetas se encuentren en posesión de la empresa que las fabrica.
- Mientras las tarjetas se encuentren en tránsito de las instalaciones de la empresa fabricante, a las instalaciones de la entidad emisora.
- Mientras las tarjetas se encuentren en posesión de la entidad emisora.

Dicho reporte debe transmitirse solamente por vía telefónica o por telefacsímil.

4.2.10 Tarjetas Falsificadas

Las tarjetas falsificadas se dividen en dos categorías principales:

- Una tarjeta impresa, grabada o codificada para que parezca una tarjeta Visa válida sin la autorización del emisor.
- Una tarjeta válida emitida por una entidad que ha sido alterada o refabricada. En esta categoría no se incluyen las tarjetas que han sido alteradas solamente con la intención de cambiar o dañar el panel de firma (Ubicación de la firma del tarjetahabiente al dorso de la tarjeta), o la firma del tarjetahabiente.

En este apartado se describen diversos aspectos de las tarjetas falsificadas.

a) Notificación de Pérdidas Relacionadas con Tarjetas Falsificadas

Se debe notificar inmediatamente a Visa si se sospecha o confirma el uso de una tarjeta falsificada, por medio telefónico, telefacsímil y confirmar por escrito en un plazo de dos días laborales.

b) Copia de la Banda Magnética

Este tipo de fraude se da cuando alguien logra copiar en forma no autorizada, el contenido íntegro de la banda magnética de una tarjeta válida debidamente emitida, la cual es utilizada posteriormente para efectuar transacciones fraudulentas en las cuales el terminal lee completamente la banda magnética.

En esencia, este tipo de fraude requiere lo siguiente:

- Que se confirme la transacción sospechosa como una transacción con Código de Entrada POS 90 (*Este código de entrada corresponde cuando el lector de banda, puede leer completamente la información grabada en la misma*).
- Cuando el valor de verificación de tarjeta o CVV, presentado en el mensaje de autorización coincida con el que aparece en la copia o voucher del emisor.
- Sí el tarjetahabiente tiene en su poder la tarjeta legítima.

c) Identificación de Cuentas Falsificadas por Copia de la Banda Magnética

A continuación se describirán algunas instrucciones, que permitirán identificar las cuentas en las cuales se ha copiado el contenido de la banda magnética de la tarjeta:

- **Referencias Investigativas -** Estas referencias se aplican tanto a las investigaciones internas como a las investigaciones realizadas en el campo, por lo general la gente de afuera (de la calle) conoce bien los casos de delitos por la falsificación de la banda magnética de una tarjeta de crédito.

- **Calificación de las Redes Neuronales** – Son modelos de análisis de comportamiento que identifican el fraude con tarjetas falsificadas y pueden detectar alguna señal de que se ha copiado la banda magnética de una tarjeta, éstos análisis muestran el impacto del fraude relacionado por esta vía, que en su mayoría se presenta en los comercios de alto valor, dentro de un plazo breve de tiempo.

- **Revisión diaria de las cuentas castigadas por altos montos debido a falsificación con el Modo de Entrada POS 90** – Derivado de los valores altos de transacciones que generan las cuentas falsificadas debido a la copia de la banda magnética, una revisión caso por caso de las cuentas sospechosas podría revelar otras actividades de este tipo.

- **Revisión mensual de las cuentas castigadas por más US$ 500.00 debido a falsificación, Modo de Entrada POS 90 y fallo en la verificación del CVV** – Se ha observado que las pérdidas promedio por cuenta falsificada debido a la copia de la banda magnética, son más altas que las pérdidas ocasionadas por las falsificaciones tradicionales de tarjetas.

Realizar una revisión de la actividad sospechosa cada fin de mes, permitirá a los analistas de la entidad, localizar las concentraciones de cuentas en zonas geográficas similares. Cualquier número de cuenta identificado por medio de este proceso se considera un caso potencial de copia de banda magnética.

d) Verificación de las Cuentas Falsificadas por Copia de la Banda Magnética

Las cuentas falsificadas se pueden verificar, siguiendo las instrucciones que se describen a continuación:

- **Se debe verificar para detectar cualquier señal de alteración de la banda magnética** – Muchos emisores de tarjetas de crédito, han comprobado al leer la pista 1 de muchas bandas magnéticas copiadas, que el nombre del tarjetahabiente aparece alterado. Además si las transacciones del fraude, se realizan a la misma cuenta y la lectura de la pista 2 muestra que no ha sido alterada, por medio del análisis se pude verificar si se trata de un caso de copia de la banda magnética.

- **Cuando la cuenta presenta cargos coincidentes en áreas geográficas diferentes** - Las transacciones que ocurren dentro de un mismo período de tiempo, pero en diferentes ubicaciones geográficas, deben dar lugar a que se sospeche de la cuenta. En ocasiones el encontrar transacciones de este tipo, no por fuerza es un fraude, derivado que los establecimientos minoristas y estaciones de gasolina, dan proceso a sus autorizaciones desde una sola ubicación centralizada.

- **Tipo de fraude similar** – Es importante verificar por medio del análisis del punto de compra común ***(Common Point of Purchase o CPP),*** que no se están realizando al mismo tiempo, un mismo tipo de fraude con múltiples cuentas y en una determinada zona geográfica.

- **Revisar las ventas efectuadas en un Punto de Compra Común sospechoso** – Cuando se determine que los fraudes de una determinada cuenta, son realizados en el mismo punto de compra común, es importante evaluar otras cuentas que tengan transacciones en el mismo lugar, para confirmar que la cuenta no es sujeta de operaciones fraudulentas. Al

finalizar de completar el análisis y confirmar que la banda magnética ha sido copiada, se debe reportar a Visa para que se hagan otros tipos de análisis.

e) Requisitos de Información

Es importante comentar que para determinar si se debe reportar la cuenta como un caso de copia de la banda magnética, existe un reporte diseñado por Visa, el que deberá cumplir con que todas las preguntas deben tener una respuesta afirmativa, en caso de haber negativas se debe volver a evaluar para confirmar las respuestas. **(Ver Anexo 16)**

f) Soluciones a los Fraudes

En la actualidad aun no se cuenta con una estrategia que de una solución total al problema del fraude por copia de la banda magnética de una tarjeta de crédito. Lo anterior debido a la falta de datos, con lo que resulta imposible justificar el costo de cualquier programa o servicio que se quiera iniciar, respecto a los procesos de fabricación y actualización de los dispositivos utilizados en los puntos de venta. La mejor arma contra este tipo de fraudes, lo constituyen los servicios y programas basados en tecnologías implementadas en el mercado, o las que examinan los datos en forma central.

En la actualidad, Visa está tomando las siguientes medidas para controlar las falsificaciones por copia de la banda magnética:

- **Mejorar el proceso de análisis** - Significa asegurar la integridad y coherencia de los datos de las tarjetas de crédito.

- **Examinar el impacto del fraude en las cuentas potencialmente falsificadas por copia de la banda Magnética** – Se requiere determinar si las demás cuentas utilizadas en puntos de compra comunes, muestran patrones similares de fraude o pruebas de autorización.

- **Evaluar el uso de las redes neuronales** - Las aplicaciones como el Servicio de Identificación de Riesgos del Tarjetahabiente (Cardholder Risk Identification Service, CRIS) proporcionar a los emisores la capacidad de detectar oportunamente los fraudes, dada la frecuencia con que ocurren éstos.

g) Punto de Compra Común (CPP)

Para que un establecimiento comercial se catalogue de esta forma, deben haber ocurrido tres o más transacciones de un tarjetahabiente legítimo, en un plazo de 30 días consecutivos o menos, y que en cada una se haya confirmado posteriormente, que es una actividad fraudulenta por falsificación de la banda magnética.

La información contenida en la banda magnética de una tarjeta de crédito, se puede ver comprometida en establecimientos comerciales, o en cualquier lugar donde se almacenen y transmitan datos, por lo cual la seguridad de esta información tiene una importancia fundamental y forma parte integral de la investigación de los Puntos de Compra Comunes, con el fin de determinar si se vio arriesgada la seguridad de la información.

h) Requisitos del Emisor

Los adquirentes dependen de los datos proporcionados por las entidades emisoras, por lo que éstas últimas deben contar con un proceso, que sirva para confirmar la actividad de transacciones con tarjetas falsificadas que incluya determinados criterios mínimos como:

- Modo de Entrada POS 90
- El Valor de Verificación de Tarjeta coincide

- El tarjetahabiente legítimo tiene las tarjetas en su posesión
- Se han eliminado razonablemente los tipos de fraude alternativos, incluyendo los fraudes cometidos por amistades y familiares

La institución emisora, debe preparar la documentación que haga constar la forma en que se identificó el punto de compra común y enviarla al adquirente y a la región de Visa de dicho adquirente.

La documentación debe proporcionar al adquirente la información siguiente:

- Nombre del Emisor
- Contacto del Emisor, incluyendo
  - Nombre
  - Número de teléfono
  - Número de telefacsímil
- Número de Identificación Bancaria del adquirente (BIN)
- Nombre y número de teléfono del comercio
- Ciudad del comercio
- Estado, provincia, departamento o país del comercio
- Número de cuentas con actividad fraudulenta confirmada (hasta la fecha)
- Monto del fraude confirmado como resultado de este punto de compra común (hasta la fecha)
- Ubicación primaria donde ocurrieron las transacciones fraudulentas
- Lista de transacciones legítimas con fraudes confirmados por copia de la banda magnética, incluyendo:
  - Número de cuenta
  - Importe de la transacción
  - Hora de la autorización
  - Número de Referencia del adquirente (ARN) de 23 dígitos

i) Requisitos del Adquirente

El adquirente tiene la responsabilidad de llevar a cabo una investigación exhaustiva y deben hacer las siguientes preguntas:

- ¿ Cómo se comprometió la seguridad de la cuenta?
- ¿ Quién fue el responsable?
- ¿ En qué se basa la determinación?

Los adquirentes tienen la responsabilidad de presentar los siguientes reportes:

- Un reporte preliminar requerido dentro de un plazo de 10 días calendario consecutivos a partir de la fecha en que el emisor o la región de Visa notificó al adquirente
- Un reporte final requerido dentro de un plazo de 30 días calendario consecutivos a partir de la fecha en que el adquirente haya tomado las medidas necesarias.

Si el adquirente cancela al comercio por la actividad de falsificación por copia de la banda magnética de una tarjeta de crédito, éste deberá listar al comercio en el archivo de comercios cancelados.

4.2.11 Seguridad de las Tarjetas

El departamento de control de fraude de cada entidad emisora, tiene la responsabilidad de desarrollar y mantener procedimientos de seguridad, destinados a proteger las existencias de tarjetas plásticas vírgenes que se encuentren por emitir, así como custodiar bajo un control dual, las tarjetas emitidas que aún no se han entregado.

Se describen algunos procedimientos de seguridad, que pueden ayudar a proteger las tarjetas de crédito:

a) Control de Existencias

El control de existencias debe mantener un inventario y conteo físico de todas las tarjetas a medida que el emisor las recibe, procesa y envía por mensajero a los tarjetahabientes.

Los registros de control de existencias de tarjetas, deben documentar las siguientes etapas del procesamiento de las mismas:

- Recibir del fabricante y almacenar las tarjetas plásticas sin grabar
- Retirar las tarjetas del área de almacenamiento para grabarlas
- Identificar y destruir las tarjetas que se hayan grabado erróneamente o se hayan dañado o estropeado durante el proceso
- Almacenar las tarjetas grabadas antes de enviarlas por mensajero
- Enviar las tarjetas por medio de mensajeros
- Mantener un expediente de auditoría, del personal que tiene acceso a las tarjetas

b) Proceso de Grabación

Los procesos relacionados con la grabación al relieve de las tarjetas, deben llevarse a cabo en una área especial y segura, además se requiere tomar las medidas necesarias para garantizar la seguridad física de dicha área, entre las que se pueden mencionar:

- El acceso al área debe ser limitado exclusivamente al personal autorizado.
- El área debe estar rodeada de ventanas de cristal, con el objeto de que los supervisores puedan observar con facilidad su interior.

Se deben utilizar procedimientos de control dual, para garantizar la seguridad de las tarjetas durante todas las etapas del proceso de grabación y envío por mensajero. Cuando se realice el conteo para mantener existencias, se deben triturar de forma inmediata las tarjetas grabadas erróneamente, dañadas o estropeadas.

c) Envío por Mensajeros Internos

Se deben anotar cuidadosamente los envíos de tarjetas, en los registros de control de existencias, toda la información específica sobre cada una, la cual debe incluir los números de cuenta de las tarjetas, la ubicación desde la cual se enviaron las mismas, la fecha y hora del envío.

Es importante evaluar los aspectos, que se muestran a continuación, con la finalidad de minimizar el riesgo de perdidas y mejorar el control de las tarjetas enviadas.

- **Aviso previo al envío** – El aviso previo (llamado “premaileer”), es una notificación que se envía al tarjetahabiente antes de enviarle la tarjeta. Este aviso cumple dos funciones principales:

  - Primeramente alerta al tarjetahabiente de que la tarjeta se le va a enviar por mensajero interno y debe de recibirla para una determinada fecha. Si el tarjetahabiente no recibe la misma, puede suponer que ha sido robada y notificar al emisor.
  - En segundo lugar, el aviso previo garantiza que las tarjetas no se envíen a una dirección incorrecta.

- **Horario para enviar las tarjetas -** Si es posible, las tarjetas se deben enviar en las horas cuando el volumen de correspondencia sea más ligero. Es recomendable no enviar tarjetas en la tarde o en la noche, cuando el volumen de correspondencia tiende a ser mucho más alto y los mensajeros se conducen con más premura para finalizar su turno de trabajo.

- **Días para enviar las tarjetas -** Evitar enviar tarjetas en ciertos días de la semana en que el servicio procesa altos volúmenes de correspondencia, o en que las tarjetas podrían permanecer un tiempo prolongado en tránsito. Por ejemplo, enviarse el viernes o un día antes de un feriado, lo que reduce el tiempo en que se ven expuestas a robo o extravío.

- **Entrega en el departamento de Mensajería -** Haga las coordinaciones necesarias para entregar las tarjetas que se vayan a enviar, a un empleado designado, a fin de evitar un manejo excesivo por parte de los colaboradores de dicha sección.

- **Correspondencia no entregada -** La correspondencia que no se puede entregar está expuesta a un mayor grado de riesgo de robo y pérdida. Para reducir este riesgo, se sugiere solicitar que el sobre con las tarjetas bancarias se remita automáticamente, al departamento de tarjetas de crédito, a fin de garantizar que se devuelva la correspondencia cuando no sea posible entregarla. Se recomienda además verificar los sobres devueltos para detectar cualquier error o problema durante el proceso de preparación del envío.

- **Tarjetas enviadas con un portador erróneo -** Un problema que ocurre muy comúnmente al preparar los envíos de tarjetas es, el incluir las tarjetas con la dirección de otro tarjetahabiente. La manera más fácil de evitar este problema es colocar una etiqueta con el nombre y la dirección del tarjetahabiente, imprimiéndola directamente en la computadora o imprimiendo la etiqueta por adelantado, posteriormente cotejar dichos datos con listados, para así reducir las probabilidades de que se produzcan errores de cotejo.

- **Sobres opacos** - Cerciórese de que los sobres utilizados para enviar las tarjetas sean opacos y que el contenido de los mismos no se transparente a través del papel de manera que permita leerlo. Los sobres de colores oscuros o los sobres forrados por dentro se consideran sobres opacos.

- **Color y tamaño del sobre** - Cambie periódicamente el color y el tamaño de los sobres para que los empleados de mensajería no puedan asociar un determinado estilo de sobre con los envíos de tarjetas. Al mismo tiempo, utilice sobres que no llamen la atención y evite usar sobres que sean poco usuales en algún sentido (por ejemplo, de un tamaño, color o forma que no sean los de uso común).

- **Sobres para enviar los estados o extractos de cuenta** - Considere enviar las tarjetas en el mismo tipo de sobre que utiliza para enviar los estados o extractos de cuenta mensuales a los tarjetahabientes. Si se utilizan sobres parecidos, los mensajeros u otros empleados, posibles no podrán distinguir fácilmente los envíos de estados de cuenta y los de tarjetas.

- **Aviso posterior** - El aviso posterior (llamado “postmailer”) es una carta de seguimiento que se envía unos días después de la tarjeta, a fin de confirmar que el tarjetahabiente la ha recibido. Dar al tarjetahabiente instrucciones de comunicarse inmediatamente con el emisor si no ha recibido la tarjeta.

- **Activación de la cuenta** - Los programas de activación de cuentas o tarjetas ayudan a los emisores a prevenir las pérdidas causadas por el robo de éstas. Las nuevas o remitidas se bloquean en el momento de enviarlas y la información incluida en el sobre da al tarjetahabiente instrucciones de llamar al centro de tarjetas al momento de recibirla, con el objeto de confirmar su identidad y activar la misma.

d) Tarjetas Devueltas

Cuando no se pueden entregar las tarjetas, es necesario devolverlas lo más pronto posible, para disminuir el riesgo de que se pierdan o sean robadas. Es importante designar una persona responsable en la sección de mensajería, de recibir las tarjetas que no fue posible entregar.

e) Fabricantes y Servicios de Grabación de Tarjetas

El departamento de control de fraude tiene también la responsabilidad de confirmar y supervisar la confiabilidad, buena reputación y estabilidad financiera del fabricante de tarjetas seleccionado para producir, grabar y codificar las tarjetas. Visa recomienda una inspección de las instalaciones de producción y personalización del fabricante, y que se mantengan registros para verificar la implementación de medidas de seguridad adecuadas durante la producción, almacenamiento, personalización y envío de las tarjetas.

Igualmente, deben documentarse las políticas establecidas para garantizar el control de las existencias de tarjetas y plásticos, la integridad de los empleados encargados de realizar las tareas relacionadas con el procesamiento de las mismas. Sí se utiliza el servicio de una tercera empresa para alguna de estas actividades, se deben seguir los mismos procedimientos de investigación y supervisión.

4.2.12 Relaciones con los Funcionarios Judiciales

Cada departamento de control de fraude de una entidad emisora, tiene la responsabilidad de mantener una buena relación de trabajo, con las autoridades judiciales que lleven las investigaciones de delitos relacionados con fraudes a través de tarjetas de crédito.

La colaboración mutua que deben mantener el departamento de control de fraude y las autoridades judiciales, se deben enfocar a las siguientes áreas y debe incluir:

- **Investigación de los fraudes y proceso judicial contra los defraudadores** – Cada investigación que realiza el departamento de control de fraude, es con el objeto de obtener documentos y pruebas, los cuales pueden resultar determinantes para capturar y procesar a los sospechosos.

- **Capacitación** – El realizar seminarios de capacitación sobre el fraude con tarjetas, es una forma de impulsar mejores relaciones entre el personal del departamento de control de fraude y las autoridades judiciales. Es posible que el costo de estos seminarios, corran por cuenta de las entidades emisoras, los que deben ser impartidos a colaboradores del emisor, como a personal de las autoridades judiciales

4.2.13 Seguridad del Centro de Tarjetas

A continuación se describen brevemente los requisitos de seguridad, que deben ser evaluados dentro del centro de tarjetas.

a) Seguridad Física

La seguridad física del centro de tarjetas de crédito de una entidad emisora, debe incluir la vigilancia y supervisión de las siguientes áreas operativas:

- Acceso al edificio, incluidas las entradas y salidas.
- Áreas donde se localizan los archivos de la documentación de las investigaciones de fraudes, y los documentos propios de la emisión de la tarjeta de crédito.
- Área de procesamiento de datos.
- Área de procesamiento de pagos.
- Área de grabación de tarjetas.
- Área de preparación de envíos por mensajeros.

También se deben desarrollar y establecer procedimientos de seguridad, para garantizar la protección del centro de tarjetas en caso de incendio, desastre natural, amenaza de bomba o cualquier clase de disturbio.

b) Personal del Centro

Se debe realizar una verificación exhaustiva de la selección de personal, con el fin de minimizar la posibilidad de contratar a alguien con antecedentes no deseables. Para realizar esta labor, de ser posible se pueden utilizar registros de la policía, sistemas de información creditícia, referencias personales y laborales anteriores.

4.2.14 Controles Administrativos

En lo referente a este tema, se recomiendan verificar los controles que se describen a continuación:

a) Revisión de Desempeño Eficaz del Personal

Periódicamente se debe evaluar el desempeño del personal, para obtener una revisión administrativa de las funciones de seguridad, que se traducirá en oportunidades de establecer sugerencias constructivas que contribuyan a mejorar su desempeño. Adicionalmente como parte de esta verificación, se deben examinar los expedientes de los casos, llevados por los colaboradores, con el objeto de establecer lo siguiente:

- Documentación de los casos, que incluye:
  - Investigación
  - Entrevistas
  - Otros contactos
  - Pruebas físicas
- Ingeniosidad e iniciativa del investigador.
- Respuesta oportuna del investigador.
- Selección de procedimientos para reducir el fraude.
- Grado de alcance y profundidad de la investigación.
- Tiempo total empleado en el caso antes de cerrarlo.
- Resultado de la investigación, que debe incluir:
  - Fondos que se haya logrado recuperar
  - Resultados del proceso judicial contra el defraudador

b) Información de Fraude

Para proporcionar a los emisores información sobre la administración de riesgos y servicios encaminados a combatir los fraudes a través de tarjetas de crédito, así como las pérdidas ocasionadas por los mismos, Visa ha desarrollado el Programa de Información de Fraude ***(Fraud Reporting Program)***. Para cumplir con lo anterior, es de vital importancia que los emisores proporcionen información exacta y precisa con respecto a la clasificación del fraude, al reportarlo.

El proceso para reportar los fraudes, se inicia cuando un tarjetahabiente se comunica con el emisor de la tarjeta, con el objeto de disputar una transacción en su cuenta Visa, con la que él no esta de acuerdo, la cual puede ser una transacción fraudulenta, que el emisor debe reporta a Visa con todos los detalles posibles.

El reporte del fraude, debe incluir información del tarjetahabiente, el comercio, así como la forma en que se procesó la transacción. El emisor identifica el tipo de fraude cometido, utilizando una de las siguientes categorías:

- Tarjeta Perdida / Lost
- Tarjeta Robada / Stolen
- Tarjeta No Recibida / Not received
- Solicitud Fraudulenta / Fraudulent application
- Falsificación / Counterfeit

- Uso fraudulento de un número de cuenta / Fraudulent use of an account number
- Misceláneo o no definido / Miscellaneous-undefined

Basándose en el fraude reportado, Visa envía reportes de actividad fraudulenta a los demás emisores, en forma diaria, semanal, mensual y trimestralmente, los cuales deben notificar si se han aceptado los reportes presentados y si estos se registraron exacta y correctamente en el sistema, para brindar resúmenes de los fraude reportados hasta la fecha.

Si los reportes mencionados anteriormente, indican un nivel alto de fraude en determinadas categorías, es posible que Visa requiera a los emisores tomar medidas con respecto a las transacciones o comercios que dieron origen a los fraudes.

Toda la información que proporciona el Programa de Información de Fraude, se mantiene archivada en la División de Administración de Riesgos y Seguridad de Visa International (IRMS) y en las oficinas regionales. Dicha información se puede utilizar para los siguientes propósitos:

- Analizar las concentraciones del fraude
- Analizar las tendencias que adopta el fraude
- Medir el desempeño de los programas de administración de riesgos y seguridad
- Administrar los reportes de fraude
- Supervisar el cumplimiento de los requisitos de información por parte de los Miembros
- Brindar apoyo a la información de los programas de administración de riesgos y seguridad
- Responder a las consultas y solicitudes de información de las entidades emisoras
- Proporcionar la información y los análisis especiales que se soliciten
- Generar reportes regionales específicos para su distribución a los miembros

La información obtenida de este programa, apoya a otros de administración de riesgos de Visa, incluyendo el Servicio de Identificación de Riesgos (Risk Identification Service, RIS) y el Servicio de Identificación de Riesgos del Tarjetahabiente (Cardholder Risk Identification Service, CRIS), que se describieron a lo largo del presente capitulo.

Cada emisor debe mantener un compromiso constante y riguroso, en el afán de presentar la información más precisa y exacta sobre el fraude, el cual servirá para proteger a todos los demás integrantes del sistema Visa y evitará que sufran pérdidas excesivas debidas al mismo.

El análisis del comportamiento que adoptan los fraudes a escala mundial, permitirán a Visa desarrollar nuevas estrategias para controlarlos, además de colaborar con los emisores, las autoridades policíacas, en la tarea de identificar y contenerlos en la medida que van surgiendo.

Los emisores se benefician al reportar la información de las transacciones correctamente, ya que esto les otorga el derecho de contracargo, con relación a las transacciones fraudulentas.

Como se observo anteriormente, un programa para el control del fraude, debe ser bastante completo, el cual debe incluir cada una de las áreas, procesos, políticas que intervienen en el manejo de tarjetas de crédito. Dicho programa debe ser evaluado periódicamente, con el objeto de establecer deficiencias o aspectos a implementar, a fin de realizar las enmiendas y modificaciones necesarias, para mantener un programa completo, eficiente y actualizado, de acuerdo a las nuevas herramientas que desarrolla VISA.

4.3 Normativa Interna y Externa relacionada al Fraude por Falsificación de la Banda Magnética

Es importante mencionar que toda entidad bancaria, que dentro del portafolio de productos financieros que ofrece a sus clientes, incluya el financiamiento a través de tarjeta de crédito, debe mantener un adecuado control de las operaciones, gestiones y actividades, que conlleva el manejo y procesamiento de una cartera de tarjetas, las cuales además se encuentran regidas por normas internas creadas por la propia entidad, para mantener un supervisión y seguimiento de dicha actividad, pero también existen normas externas las cuales se describen a continuación.

4.3.1 Normativas Internas

Toda entidad bancaria que maneja una cartera de tarjetas de crédito, se ve expuesta a varios riesgos inherentes derivados de la propia actividad, es por ello que para mantener un control adecuado del funcionamiento del departamento encargado de dicha actividad, se auxilia de políticas, normas, reglamentos y procedimientos de control interno, los cuales son creados, con la finalidad de que estos sean las bases para las evaluaciones periódicas que realiza el departamento de auditoría interna, para establecer debilidades de control interno y poderlas corregir en forma oportuna, además de minimizar los riesgos. Entre las normativas internas que puede implementar una entidad bancaria, se puede mencionar las siguientes:

4.3.1.1 Circulares Normativas

Las políticas y procedimientos de control interno, se pueden crear en forma de circulares u oficios de observancia general, las cuales pueden enumerarse correlativamente desde el inicio de la primera, por cada año de ejercicio laboral. Estas circulares son diseñadas por un departamento especialmente creado para realizar esta labor, luego la traslada al departamento o área encargada de realizar la labor, para que la revise y de sus comentarios. Luego de obtener el visto bueno de área encargada, es trasladada al departamento de auditoría interna, para que sea nuevamente revisado y se otorgue otro visto bueno, con lo que se da por finalizada la revisión, para que posteriormente se obtengan las firmas del Gerente General y de las demás personas involucradas. Un diseño de una circular normativa puede ser de la siguiente forma:

CIRCULAR NORMATIVA No. 1 – 2005	
DE: Gerente General	PARA: Todos los Colaboradores del banco Emisor
FECHA DE PUBLICACION: 10 de enero de 2005	ASUNTO: Requisitos Mínimos a Satisfacer para las Solicitudes de Tarjetas de Crédito

Después del encabezado de la circular, en el cuerpo del documento, transcriben las definiciones, requisitos, normas, procesos y procedimientos establecidos para normar una determinada actividad.

4.3.1.2 Manuales Operativos

En algunas instituciones prefieren utilizar Manuales Operativos, los cuales son como una especie de folleto, en el cual se recopilan todas las definiciones, procesos, normas y procedimientos establecidos, referentes a una determinada actividad, los cuales son de observancia general para los colaboradores, en especial para las personas que desarrollen la actividad, basándose en los lineamientos establecidos para el efecto.

4.3.2 Normativas Externas

Es importante comentar que toda entidad bancaria emisora de tarjetas de crédito, no obstante que emita sus propias normas internas, para mantener un control adecuado de la actividad de financiamiento a través de tarjetas de crédito, se ve obligada a observar ciertas normas externas, las cuales pueden constituirse como las requeridas por la empresa que le otorga el respaldo a la tarjeta de crédito, así como las leyes nacionales que regulan las actividades derivadas del uso de tarjetas de crédito.

4.3.2.1 Normas Estipuladas por VISA

Derivado que en presente trabajo de investigación, se tomo como base de estudio, una entidad bancaria emisora de tarjetas de crédito, con el respaldo de la marca internacional **VISA**, es importante comentar que dicha empresa para poder otorgar dicho respaldo, estipula ciertos reglamentos, manuales de observancia obligatoria, los cuales se describen a continuación:

a) **Reglamento Regional de VISA –** Dentro de este reglamento se encuentran normados los estándares establecidos para los miembros de la región, pero como esta marca es de reconocimiento a nivel mundial, ha dividido los países por áreas geográficas, con el fin de facilitar su comunicación con los mismos, así como de mantener un mejor control estadístico de sus operaciones, es por ello que **Guatemala** se encuentra ubicada para VISA, dentro del área Regional para América Latina y el Caribe.

b) **Reglamento Operativo de VISA -** Dentro de este reglamento se encuentra normado lo relativo a la operatoria de las tarjetas de crédito **VISA,** como lo son las transacciones derivadas del uso de las mismas, así como de los procedimientos a seguir en caso de posibles fraudes realizados a través de la falsificación de la banda magnética de una determinada tarjeta de crédito. También se encuentra normado lo relacionado a, dónde, cómo y cuándo puede ser utilizada la marca.

c) **Estatutos de VISA –** Dicha empresa ha creado ciertos estatutos de observancia obligatoria para los miembros de la marca, como por ejemplo, las medidas a las que se atienen estas entidades, por el uso indebido de la marca, las comisiones y cargos que cobra ésta por las mismas, el uso de la marca y las diferentes intervenciones que lleva a cabo, para ayudar en la recopilación de información, para el esclarecimiento de un fraude realizado a través de la falsificación de la tarjeta de crédito, el costo de los programas creados por **VISA**, para mantener mejores controles de los fraudes, autorizaciones, etc.

Es importante comentar que no obstante los reglamentos y estatutos descritos anteriormente, **VISA** ha creado varios manuales, programas, seminarios, publicaciones, etc., que se encuentran a la disposición de cualquier miembro, con el fin de ayudar a éstos, a mantener mejores controles, dar mayor seguridad y brindar un mejor servicio a los tarjetahabientes.

4.3.2.2 Normas Legales Guatemaltecas

Como toda entidad bancaria, además de crear normas internas, para mantener un control interno adecuado en la gestión del financiamiento a través de tarjetas de crédito, también debe observar las leyes guatemaltecas que están relacionadas con dicha actividad.

Cuando una entidad bancaria detecta un fraude por falsificación de la banda magnética de una tarjeta de crédito, tiene la obligación de realizar una investigación exhaustiva, con el propósito de determinar las responsabilidades, por parte del tarjetahabiente y de la propia entidad.

Además, de lograr esclarecer la o las personas responsables de cometer dicho fraude, esta en el derecho de iniciar una demanda judicial, para lo cual puede apoyarse en el Código Penal (Decreto 17-73), que establece lo siguiente:

"**Articulo 263.- (Estafa Propia).** Comete estafa quien induciendo a error a otro, mediante ardid o engaño, lo defraudare en su patrimonio en perjuicio propio o ajeno".

"**Articulo 264.- (Casos Especiales de Estafa)**. Incurrirá en las sanciones señaladas en el articulo anterior", y **numeral 23** "Quien defraudare o perjudicare a otro, usando de cualquier ardid o engaño, que no se haya expresado en los incisos anteriores".

Es importante comentar que dentro de la legislación guatemalteca, no existe una ley específica que regule lo relacionado al uso de tarjetas de crédito y sus actividades derivadas, es por ello que al momento de iniciar alguna demanda por algún fraude cometido a través de la falsificación de la

banda magnética de una determinada tarjeta, se debe de enfocar como un tipo de defraudación o estafa, lo cual esta regulado por el Código Penal, descrito anteriormente.

4.4 Nuevas Herramientas a Implementar para la Prevención y Detección de Fraudes

El incremento de los fraudes cometidos por la falsificación de la banda magnética de tarjetas de crédito a escala mundial, ha originado que las entidades bancarias emisoras, busquen nuevas alternativas de herramientas a implementar, para poder contrarrestar esta situación, con el fin de minimizar al máximo el riesgo de que suceda este tipo de fraude.

Por lo anterior, la empresa encargada de dar el respaldo de las tarjetas de crédito, a través de su marca reconocida a nivel mundial como lo es **VISA,** constantemente se mantiene creando nuevos programas y sistemas, que permitan a las instituciones bancarias emisoras de tarjetas, auxiliarse con el fin de fortalecer sus controles internos, a fin de mantener un mejor control de las transacciones que realizan sus tarjetahabientes. A continuación se describe uno de los últimos programas creados con el fin de ayudar a los miembros que la integran, a administrar el riesgo de fraudes:

4.4.1 Detección de Fraude Emisor IFD

Para ofrecer un mejor servicio a sus miembros, el equipo de Administración de Riesgos de VISA Internacional, está llevando a cabo varias iniciativas proactivas, para poner a disposición nuevas herramientas que ayuden a reducir el fraude. Una de estas herramientas recientes es el servicio llamado “Detección de Fraude Emisor – IFD”, el cual cuenta con características especiales para ayudar a prevenir el fraude y aumentar la rentabilidad de los miembros y la marca.

Esta herramienta reemplazará a los servicios CRIS y CRIS Online, que era otra herramienta que anteriormente se utilizaba para la reducción del fraude, las cuales en la última década fueron exitosas, apoyando a sus emisores y disminuyendo sus pérdidas por fraudes.

Debido a los distintos tipos de fraudes, entre los que se encuentra la falsificación de la banda magnética de las tarjetas de crédito, que la región de América Latina y el Caribe está experimentando y a la acelerada evolución de la tecnología de riesgo en el campo de la inteligencia artificial, VISA Internacional, esta migrando a una nueva plataforma llamada Detección de Fraude Emisor – IFD “***Issuer Fraud Detection***”.

La estrategia de VISA es de proveerle a los miembros una metodología eficiente y expedita de envío de alertas que le ofrezca a los emisores la oportunidad de responder rápidamente ante la posibilidad de actividad fraudulenta y reducir la exposición al riesgo.

Es muy importante comentar que todos estos servicios creados por Visa, son ofrecidos a los miembros que la integran, con un valor en dólares, el cual deben de observar las entidades emisoras como inversión, para implementar herramientas que disminuyan la posibilidad de fraudes,

además de brindar un mejor servicio a sus clientes.

CAPITULO V

CASO PRACTICO DEL PAPEL DE LA AUDITORIA INTERNA DE UNA ENTIDAD BANCARIA EMISORA DE TARJETAS DE CREDITO, EN LA PREVENCION Y DETECCION DE FRAUDES POR LA FALSIFICACION DE LA BANDA MAGNETICA

A manera de ejemplificar el papel de la auditoría interna de una entidad bancaria en la prevención y detección de fraudes por la falsificación de la banda magnética de tarjetas de crédito bajo el respaldo de la marca **VISA Internacional,** a continuación se desarrolla un caso práctico que pretende incorporar los lineamientos descritos en los capítulos anteriores, con el objeto de localizar las posibles causas, debilidades de controles internos; que pueden facilitar éste tipo de actividad ilícita.

5.1 Area de Auditoría Interna – Revisión de Fraudes por Falsificación de Banda Magnética de Tarjetas de Crédito

Toda entidad bancaria que dentro de su portafolio de productos financieros incluya el financiamiento a través de tarjetas de crédito, en este caso con el respaldo de la marca internacional **VISA**, debe de contar con procedimientos, medidas de seguridad y controles internos proactivos, que ayuden a minimizar el riesgo de posibles fraudes por medio de la falsificación de la banda magnética de la tarjeta, lo cual se traduce en seguridad para los tarjetahabientes de la entidad emisora.

Como la modernización y crecimiento constante de los sistemas informáticos de información, están siendo utilizados por los defraudadores, en el diseño y creación de programas, sistemas y máquinas electrónicas, mediante los cuales obtienen información resguardada por las entidades emisoras respecto a su cartera de tarjetas, para crear nuevas y con éstas lograr realizar consumos o transacciones fraudulentas, que a la larga se traducen en pérdidas, ya sea para la entidad o para el tarjetahabiente.

Por lo anterior, Visa constantemente se encuentra desarrollando herramientas electrónicas que aunadas a las políticas administrativas y los controles internos de la entidad, se logre mantener un control de los fraudes, a través de la prevención y detección de los mismos.

Es de vital importancia que el departamento de auditoría interna de la entidad emisora, realice revisiones y verificaciones periódicas de los controles internos, políticas y herramientas, con la finalidad de establecer deficiencias y debilidades, las que puedan ser corregidas e implementar nuevas para minimizar las posibilidades de dichos actos ilícitos.

Por todo lo anterior, a continuación se presenta un caso práctico en el cual se simulan varias transacciones fraudulentas, las cuales tuvieron su origen en distintas circunstancias.

Dichas transacciones son investigadas por el departamento de auditoría interna, basados en una evaluación de controles internos, políticas y medidas administrativas, y las herramientas implementadas, con el fin de mantener el control de los fraudes por la falsificación de la banda magnética de tarjetas de crédito.

Con la evaluación mencionada en el párrafo anterior, se logro determinar el origen de las mismas, la responsabilidad de las partes (Banco – Tarjetahabiente), con el objeto de cuantificar y dejar reflejadas las deficiencias localizadas, a través de un informe de auditoría.

A continuación se muestra el bosquejo del caso práctico a desarrollar:

INDICE DEL CASO PRACTICO

Número	Descripción	# de Cédula	# Página
a)	Cartera Total de Tarjetas de Crédito	**A**	**75**
5.1.1	Programa de auditoría, para la revisión de transacciones fraudulentas por medio de la falsificación de la banda magnética	**A.1**	**72**

	de tarjetas de crédito		
5.1.2	Indice de Marcas de Auditoría Efectuadas en la Revisión	**A.2**	**74**
5.1.3	Trabajo de Gabinete		
b)	Tarjetas de Crédito con Transacciones Fraudulentas por Falsificación de la Banda Magnética	**A.3**	**76**
c)	Identificación de los Saldos Fraudulentos de las Tarjetas de Crédito	**A.4**	**77**
d)	Transacciones Fraudulentas por Falsificación de Banda Magnética de Tarjetas de Crédito	**A.5**	**78**
e)	Evaluación Cumplimiento de Controles Internos del Banco	**A.6**	**80**
f)	Revisión Funcionalidad de las Herramientas Utilizadas por el Banco	**A.7**	**81**
g)	Verificación Cumplimiento del Programa de Control de Fraudes del Banco	**A.8**	**82**
h)	Resolución de Casos de Transacciones Fraudulentas Investigadas	**A.9**	**83**
5.1.4	Informe de Auditoría	**A.10**	**84**
5.1.5	Resultados del Caso Práctico	**A.10**	**88**

5.1.1 Programa de Auditoría para la Revisión de Fraudes por Falsificación de la Banda Magnética de Tarjetas de Crédito

BANCO UNIVERSIDAD, S. A.
Indice de Marcas de Auditoría

Cédula No.	**A.1**
Hecho Por	**M.M.C.**
Revisado Por	**M.F.P.**
Fecha Inicio	**27-12-2005**
Fecha Fin	**01-01-2006**

PROGRAMA DE TRABAJO PARA LA REVISIÓN DE FRAUDES POR FALSIFICACION DE LA BANDA MAGNETICA DE TARJETAS DE CREDITO

I Objetivos de la Revisión:

1. Evaluar el cumplimiento de los controles internos establecidos, para minimizar el riesgo de posibles fraudes por falsificación de banda magnética.
2. Verificar la efectividad de las herramientas electrónicas adquiridas para ayudar en la prevención y detección de fraudes por la falsificación de la banda magnética.
3. Establecer el cumplimiento con el programa de control de fraudes implementado por la entidad.

II Procedimiento

1. Verificar la información de las bases de datos de las tarjetas de crédito.
2. Solicitar el control electrónico de las gestiones operativas atendidas por el personal del área de Seguridad y Vigilancia de tarjetas de crédito.
3. Observar el comportamiento de los tarjetahabientes en el uso de las tarjetas de crédito.
4. Realizar el análisis y verificaciones necesarias para comprobar que son transacciones fraudulentas.

III Trabajo a Efectuar

1. Extraer de las bases de datos el total de la cartera de tarjetas de crédito vigentes a la fecha de la revisión.
2. Determinar las tarjetas de crédito que fueron objeto de transacciones fraudulentas, por medio de la revisión de gestiones operativas, cartas físicas y correos electrónicos recibidos en el área de Seguridad y Vigilancia del Departamento de Tarjeta de Crédito, en el cual consten los reclamos por transacciones que en ningún momento fueron realizadas ni autorizadas por el tarjetahabiente.
3. Identificar las transacciones fraudulentas, realizando las siguientes revisiones:

   - Determinar las transacciones que reclama el tarjetahabiente;
   - Revisar contra estados de cuenta que efectivamente fueron realizadas las transacciones;
   - Verificar contra copias de los comprobantes de consumos (Voucher), que los datos de las transacciones, corresponden al tarjetahabiente titular y no estén cambiados;
   - Revisar contra detalle del listado de incoming (movimientos diarios), el origen de las transacciones, para determinar el modo de entrada y autorización del consumo, el país y ciudad donde se efectuó, clase de establecimiento, hora y fecha.

4. Evaluar el cumplimiento de los controles internos establecidos para el análisis, aprobación, emisión y entrega de las tarjetas con transacciones fraudulentas.
5. Revisar la funcionalidad de las herramientas electrónicas implementadas para prevenir y detectar fraudes por la falsificación de la banda magnética de tarjetas de crédito y el porque no fueron detectados los consumos investigados.
6. Derivado de las revisiones efectuadas analizar cada caso de transacciones fraudulentas, con la finalidad de determinar responsabilidades para el tarjetahabiente o para el emisor.

IV Cronograma de Trabajo

Esta revisión se debe realizar normalmente en forma mensual, pero esto no representa que en caso de incrementarse el nivel de operaciones fraudulentas, se pueda minimizar el período en que se realice esta revisión, con el objeto de contrarrestar los mismos.

Del trabajo realizado se deberá dejar evidencia en cédulas de auditoría, debidamente identificadas para facilitar la revisión del trabajo efectuado, vigilando en la elaboración de la mismas, orden, limpieza, claridad en su interpretación e identificación mediante de marcas de auditoría utilizadas.

Concluida la revisión, se debe preparar un informe el cual debe dirigirse al Gerente del Departamento de Tarjeta de Crédito, con copia al Gerente General de la entidad, el cual previamente debe estar revisado por el Auditor Interno de la entidad.

Manuel Francisco Poz
Auditor Interno

El presente programa tiene vigencia a partir del 01/01/2006.

5.1.2 Indice de Marcas de Auditoría Efectuadas en la Revisión

A continuación se presenta el índice de marcas de auditoría elaboradas en la revisión efectuada, sobre las transacciones fraudulentas por medio de la falsificación de la banda magnética de tarjetas de crédito.

BANCO UNIVERSIDAD, S. A.
Indice de Marcas de Auditoría

Cédula No.	**A.2**
Hecho Por	**M.M.C.**
Revisado Por	**M.F.P.**
Fecha Inicio	**13-03-2006**
Fecha Fin	**13-03-2006**

En la revisión efectuada se utilizaron las siguientes marcas para referenciar las cédulas de trabajo:

Marca de Auditoría	Descripción de la Marca de Auditoría
√	Información cuadrada contra la contabilidad
Σ	Cálculos efectuados y verificados
∂	Información revisada contra gestión operativa, carta o correo electrónico recibido para el reclamo.
ƒ	Información revisada en el expediente físico de la tarjeta de crédito.
β	Datos verificados contra boletín de tarjetas canceladas.
∅	Datos verificados contra el control electrónico de alertas recibidas.
∃	Comunicación telefónica establecida con el tarjetahabiente.
ψ	Revisión de los parámetros establecidos para la generación de alertas.
⊗	Información cotejada contra estados de cuentas de tarjetas de crédito.
≠	Información verificada contra listado de movimientos (Incomming).
↵	Consumos verificados contra copias físicas de boletas de consumos.

5.1.3 Trabajo de Gabinete

BANCO UNIVERSIDAD, S. A.

Cartera Total de Tarjetas de Crédito
Saldos al 28/02/2006

Cédula No.	**A**
Hecho Por	**M.M.C.**

Revisado Por	**M.F.P.**
Fecha Inicio	**01-03-2006**
Fecha Fin	**01-03-2006**

Se procedió a extraer de la base de datos del procesador de tarjetas de crédito, el total de la cartera vigente al 28 de febrero de 2006, las cuales se describen a continuación:

Tarjeta	Saldo Q.	Ref.	Tarjeta	Saldo Q.	Ref.	Tarjeta	Saldo Q.	Ref.	Tarjeta	Saldo Q.	Ref.
123456789123456	825.33		234567898765432	3,817.54		345678912345321	18,745.25		456789876543219	26,785.45	
123456789123458	453.97		234567898765437	2,834.87		345678912345324	12,489.58		456789876543223	10,584.56	
123456789123460	1,213.34		234567898765439	4,800.56		345678912345327	4,682.58		456789876543227	24,785.65	A.2
123456789123462	634.00		234567898765441	5,102.53		345678912345330	10,587.54		456789876543231	89,911.54	
123456789123464	285.79		234567898765443	1,256.87		345678912345333	14,756.25		456789876543235	40,689.57	
123456789123465	327.46		234567898765445	2,842.45		345678912345336	16,895.47		456789876543239	54,685.78	
123456789123466	1,005.22		234567898765447	3,471.54		345678912345339	15,478.23		456789876543243	14,728.64	
123456789123467	984.21		234567898765449	558.47		345678912345342	23,874.56		456789876543247	41,587.58	
123456789123468	159.12		234567898765451	6,543.58	A.2	345678912345345	20,458.74		456789876543251	20,456.58	
123456789123469	753.85		234567898765453	7,892.41		345678912345348	34,587.54	A.2	456789876543255	81,874.89	A.2
123456789123470	47.52		234567898765455	9,423.14		345678912345351	35,214.25		456789876543259	45,765.23	
123456789123471	258.63		234567898765457	5,874.26		345678912345354	18,745.89		456789876543263	64,523.58	
123456789123472	1,120.00		234567898765459	1,185.47		345678912345357	8,951.74		456789876543267	13,587.64	
123456789123473	445.12		234567898765461	2,654.58		345678912345360	25,874.63		456789876543271	105,487.56	
123456789123474	854.35		234567898765463	4,587.54		345678912345363	31,879.54		456789876543275	51,468.57	
123456789123475	564.88		234567898765465	4,689.54		345678912345366	33,548.52		456789876543279	66,452.35	
123456789123476	999.44		234567898765467	2,365.21		345678912345369	34,689.54		456789876543283	74,856.23	
123456789123477	1,000.00		234567898765469	7,542.39		345678912345372	39,899.54		456789876543287	75,635.84	
123456789123478	110.24		234567898765471	5,482.14		345678912345375	41,587.54		456789876543291	97,582.54	
123456789123479	767.08		234567898765473	7,862.89		345678912345378	23,456.87		456789876543295	94,563.58	
123456789123480	621.87		234567898765475	9,942.87		345678912345381	12,586.57		456789876543299	96,358.79	
123456789123481	521.46		234567898765477	10,000.00		345678912345384	17,893.54		456789876543303	88,639.54	
123456789123482	746.85		234567898765479	1,254.21		345678912345387	19,487.58		456789876543307	50,879.52	
123456789123483	158.45		234567898765481	4,487.98		345678912345390	20,145.25		456789876543311	123,589.56	
123456789123484	279.42		234567898765483	8,765.25	A.2	345678912345393	5,428.58		456789876543315	69,879.46	
123456789123485	1,000.35		234567898765485	3,489.52		345678912345396	34,879.50	A.2	456789876543319	66,874.54	
123456789123486	1,106.87		234567898765487	2,528.56		345678912345399	3,487.52		456789876543323	85,468.58	
123456789123487	365.82		234567898765489	6,584.87		345678912345402	38,965.58		456789876543327	35,879.56	
123456789123488	439.87		234567898765491	4,528.30		345678912345405	1,234.58		456789876543331	110,548.68	
123456789123489	482.71		234567898765493	487.25		345678912345408	12,548.75		456789876543335	60,423.58	
123456789123490	358.93		234567898765495	4,897.25		345678912345411	11,584.58		456789876543339	48,723.54	
123456789123491	936.66		234567898765497	4,568.54		345678912345414	12,500.47		456789876543343	75,315.87	
123456789123492	1,123.33		234567898765499	4,876.23		345678912345417	7,654.25		456789876543347	83,456.76	A.2
123456789123493	444.55		234567898765501	2,358.14		345678912345420	10,639.82		456789876543351	75,846.87	A.2
123456789123494	805.72		234567898765503	1,400.48		345678912345423	27,854.88		456789876543355	45,685.89	
123456789123495	681.24		234567898765505	987.54		345678912345426	29,358.47		456789876543359	68,235.74	
123456789123496	209.78		234567898765507	9,845.28		345678912345429	36,874.52		456789876543363	84,578.88	
123456789123497	1,500.00	A.2	234567898765509	2,800.45		345678912345432	11,117.45		456789876543367	18,756.58	
123456789123498	947.66		234567898765511	6,784.58		345678912345435	8,456.25		456789876543371	56,500.72	A.2
123456789123499	880.43		234567898765513	8,999.58		345678912345438	14,725.89		456789876543375	15,127.44	
123456789123500	1,157.54		234567898765515	9,548.71	A.2	345678912345441	36,985.47		456789876543379	97,845.58	
123456789123501	853.21		234567898765517	2,201.25		345678912345444	8,523.58		456789876543383	34,568.57	
123456789123502	935.24		234567898765519	3,584.78		345678912345447	21,756.25		456789876543387	45,892.58	
123456789123503	184.99		234567898765521	4,652.58		345678912345450	32,456.87	A.2	456789876543391	27,458.69	A.2
123456789123504	123.49		234567898765523	5,784.25		345678912345453	38,741.25		456789876543395	88,699.78	
123456789123505	634.87		234567898765525	6,789.54		345678912345456	40,125.47		456789876543399	98,989.98	
123456789123506	878.42		234567898765527	7,845.45		345678912345459	23,487.52		456789876543403	9,784.56	
123456789123507	550.42		234567898765529	8,792.58		345678912345462	16,753.58		456789876543407	95,487.52	
123456789123508	870.75		234567898765531	9,965.71		345678912345465	13,753.33	A.2	456789876543411	32,456.87	
123456789123509	63.67		234567898765533	10,125.35	A.2	345678912345468	9,854.78		456789876543415	101,547.56	
Totales	32,674.12	√Σ		259,665.06	√Σ		1,046,265.93	√Σ		3,089,515.15	√Σ

BANCO UNIVERSIDAD, S. A.

Tarjetas de Crédito con Transacciones Fraudulentas por Falsificación de la Banda Magnética
Saldos al 28/02/2006

Cédula No.	**A.3**
Hecho Por	**M.M.C.**

Revisado Por	**M.F.P.**
Fecha Inicio	**02-03-2006**
Fecha Fin	**02-03-2006**

Por medio de la revisión de gestiones operativas físicas, cartas y correos electrónicos de reclamos recibidos de parte de los tarjetahabientes, se pudo identificar que 15 tarjetas fueron objeto de transacciones fraudulentas por la falsificación de la banda magnética, derivado que las operaciones en ningún momento fueron realizadas, ni autorizadas por el tarjetahabiente titular, por lo que solicitan les sea acreditado a su cuenta el valor de los mismos.

Dichas tarjetas se detallan a continuación:

No.	Clase de Tarjeta	Tarjeta	Nombre del Tarjetahabiente	Cant. Trans.	Monto Q. Transacc.	Ref	Marca Auditoría	Medio de Reclamo
1	Local	123456789123497	Roberto Enrique Suarez Mallo	01	554.89	**A.2**	∂	Gestión operativa ingresada
2	Internacional	234567898765451	María del Carmen Arreola Mejia	03	2,275.99	**A.2**	∂	Gestión operativa ingresada
3	Internacional	234567898765483	Eriberto Haroldo Barreondo Paz	02	4,155.75	**A.2**	∂	Correo electrónico recibido
4	Internacional	234567898765515	Benedicto Lucas Garrido Ajanel	02	5,129.92	**A.2**	∂	Carta de reclamo recibida
5	Internacional	234567898765533	Anibal Ernesto Pineda Morataya	04	6,161.31	**A.2**	∂	Correo electrónico recibido
6	Oro	345678912345348	Miguel Angel Zamora Acuña	04	15,905.13	**A.2**	∂	Gestión operativa ingresada
7	Oro	345678912345396	Eugenia Magaly Trejo Abularach	03	12,635.12	**A.2**	∂	Correo electrónico recibido
8	Oro	345678912345450	Oscar Fernando Morales Patzun	02	11,756.04	**A.2**	∂	Correo electrónico recibido
9	Oro	345678912345465	Pancracio Etelvino Jerez Tobar	03	5,609.26	**A.2**	∂	Gestión operativa ingresada
10	Platinum	456789876543227	Desiderio Alberto Cozzi Zaneti	01	12,383.12	**A.2**	∂	Gestión operativa ingresada
11	Platinum	456789876543255	Mónica Ester Galantes Retana	06	46,699.04	**A.2**	∂	Carta de reclamo recibida
12	Platinum	456789876543347	Gianluigi Paolo Cassano Tominni	04	40,800.00	**A.2**	∂	Gestión operativa ingresada
13	Platinum	456789876543391	Wilfredo Antonio Rosales Altan	02	16,101.69	**A.2**	∂	Correo electrónico recibido
14	Platinum	456789876543371	Julio César MirafloresHurtado	03	22,120.64	**A.2**	∂	Gestión operativa ingresada
15	Platinum	456789876543351	Bertha Etelvina Carrasco Morales	03	36,014.00	**A.2**	∂	Carta de reclamo recibida
	Totales			**43**	**238,301.90**	**A.2**		
				Σ	**Σ**			

BANCO UNIVERSIDAD, S. A.

Identificación de los Saldos Fraudulentos de las Tarjetas de Crédito
Saldos al 28/02/2006

Cédula No.	**A.4**
Hecho Por	**M.M.C.**
Revisado Por	**M.F.P.**

Fecha Inicio	**02-03-2006**
Fecha Fin	**02-03-2006**

Como se puede apreciar en el siguiente cuadro el valor de las transacciones fraudulentas, no necesariamente representa el total del saldo de la tarjetas, como se puede apreciar al referirse a la cédula **"A"**. El detalle de las tarjetas identificadas, se muestra a continuación:

No.	Clase de Tarjeta	Tarjeta	Nombre del Tarjetahabiente	Saldo al 28/02/06 Q.	Ref.	Valor de Consumos Fraudulentos Q.	Ref.	% Fraudulento	Saldo Libre de Fraudes Q.
1	Local	123456789123497	Roberto Enrique Suarez Mallo	1,500.00	**A**	554.89	**A.1**	37.00	945.11
2	Internacional	234567898765451	María del Carmen Arreola Mejía	6,543.58	**A**	2,275.99	**A.1**	5.31	4,267.59
3	Internacional	234567898765483	Eriberto Haroldo Barreondo Paz	8,765.25	**A**	4,155.75	**A.1**	47.41	4,609.50
4	Internacional	234567898765515	Benedicto Lucas Garrido Ajanel	9,548.71	**A**	5,129.92	**A.1**	53.72	4,418.79
5	Internacional	234567898765533	Anibal Ernesto Pineda Morataya	10,125.35	**A**	6,161.31	**A.1**	60.85	3,964.04
6	Oro	345678912345348	Miguel Angel Zamora Acuña	34,587.54	**A**	15,905.13	**A.1**	45.99	18,682.41
7	Oro	345678912345396	Eugenia Magaly Trejo Abularach	34,879.50	**A**	12,635.12	**A.1**	36.23	22,244.38
8	Oro	345678912345450	Oscar Fernando Morales Patzun	32,456.87	**A**	11,756.04	**A.1**	36.22	20,700.83
9	Oro	345678912345465	Pancracio Etelvino Jerez Tobar	13,753.33	**A**	5,609.26	**A.1**	40.78	8,144.07
8	Platinum	456789876543227	Desiderio Alberto Cozzi Zaneti	24,785.65	**A**	12,383.12	**A.1**	49.96	12,402.53
11	Platinum	456789876543255	Mónica Ester Galantes Retana	81,874.89	**A**	46,699.04	**A.1**	75.48	20,071.85
12	Platinum	456789876543347	Gianluigi Paolo Cassano Tominni	83,456.76	**A**	40,800.00	**A.1**	28.28	59,856.76
13	Platinum	456789876543391	Wilfredo Antonio Rosales Altan	27,458.69	**A**	16,101.69	**A.1**	58.64	11,357.00
14	Platinum	456789876543371	Julio César MirafloresHurtado	56,500.72	**A**	22,120.64	**A.1**	57.56	23,980.08
15	Platinum	456789876543351	Bertha Etelvina Carrasco Morales	75,846.87	**A**	36,014.00	**A.1**	47.48	39,832.87
		Totales		**502,083.71**		**238,301.90**	**A.1, A,3**		**263,781.81**
				Σ		**Σ**			

BANCO UNIVERSIDAD, S. A.

Transacciones Fraudulentas por Falsificación de la Banda Magnética de Tarjetas de Crédito
Durante el período del 01/01/2006 al 28/02/2006

Cédula No.	**A.5**
Hecho Por	**M.M.C.**
Revisado Por	**M.F.P.**
Fecha Inicio	**03-03-2006**
Fecha Fin	**03-03-2006**

Después de haber revisado las gestiones operativas, cartas y correos de reclamos recibidos, se procedió a verificar cada transacción, contra los estados de cuenta, los comprobantes de pagos y el listado de incoming (Detalle de Movimientos Diarios), para determinar las transacciones que se originaron por fraude de banda magnética de la tarjeta de crédito, además de obtener las siguiente información:

- Clases de tarjetas que fueron afectadas por transacciones fraudulentas.
- Cuantificación del monto total que suman las transacciones fraudulentas.
- Factores por medio de los cuales se autorizaron las transacciones.
- País y Estado donde se efectuaron las transacciones.
- Identificación de los establecimientos donde se realizaron los consumos.

De la revisión efectuada se identificaron 43 operaciones fraudulentas, las cuales se describen a continuación:

				ORIGEN		DESTINO				DATOS DE LA AUTORIZACION							
No.	Tarjeta	Ref.	Fecha Transacción	Moneda	Monto	Moneda	Monto	Establecimiento	País	Estado	CC	MCC	Code	Ind.	POS EM	Rason	CDP
1	123456789123497	A.1	02/01/2006	1	554.89	1	554.89	ESTABLECIMIENTO # A	Guatemala	Guatemala	GT	42	012345	N	90	00	602
2	234567898765451	A.1	03/01/2006	1	687.52	1	687.52	ESTABLECIMIENTO # L	Guatemala	Guatemala	GT	54	067890	N	90	00	603
3			12/01/2006	1	842.58	1	842.58	ESTABLECIMIENTO # H	Guatemala	Guatemala	GT	28	159753	N	90	00	612
4			18/01/2006	1	745.89	1	745.89	ESTABLECIMIENTO # X	Guatemala	Guatemala	GT	73	423879	N	90	00	618
5	234567898765483	A.1	04/01/2006	1	1,258.52	1	1,258.52	ESTABLECIMIENTO # B	Guatemala	Guatemala	GT	92	352479	N	90	00	604
6			10/01/2006	1	2,897.23	1	2,897.23	ESTABLECIMIENTO # C	Guatemala	Guatemala	GT	83	952413	N	90	00	610
7	234567898765515	A.1	22/01/2006	2	271.43	1	2,171.44	ESTABLECIMIENTO # M	México	Monterrey	MX	38	043210	N	90	00	622
8			22/01/2006	2	369.81	1	2,958.48	ESTABLECIMIENTO # F	México	Toluca	MX	56	456789	N	90	00	622
9	234567898765533	A.1	10/01/2006	1	554.56	1	554.56	ESTABLECIMIENTO # K	Guatemala	Guatemala	GT	91	846032	N	90	00	610
10			17/01/2006	1	874.29	1	874.29	ESTABLECIMIENTO # L	Guatemala	Guatemala	GT	73	756821	N	90	00	617
11			24/01/2006	1	1,125.42	1	1,125.42	ESTABLECIMIENTO # G	Guatemala	Guatemala	GT	17	129864	N	90	00	624
12			01/02/2006	2	450.88	1	3,607.04	ESTABLECIMIENTO # T	Estados Unidos	New York	US	36	743859	N	90	00	632
13	345678912345348	A.1	05/02/2006	1	2,496.57	1	2,496.57	ESTABLECIMIENTO # V	Guatemala	Guatemala	GT	29	746935	N	90	00	636
14			05/02/2006	2	570.42	1	4,563.36	ESTABLECIMIENTO # V	Estados Unidos	Dallas	US	29	102478	N	90	00	636
15			10/02/2006	2	823.33	1	6,586.64	ESTABLECIMIENTO # R	Estados Unidos	Dallas	US	44	369201	N	90	00	641
16			15/02/2006	1	2,258.56	1	2,258.56	ESTABLECIMIENTO # Q	Guatemala	Guatemala	GT	79	704893	N	90	00	646
17	345678912345396	A.1	04/02/2006	1	3,575.81	1	3,575.81	ESTABLECIMIENTO # H	Guatemala	Guatemala	GT	28	749038	N	90	00	635
18			05/02/2006	1	4,269.87	1	4,269.87	ESTABLECIMIENTO # H	Guatemala	Guatemala	GT	28	401308	N	90	00	636
19			06/02/2006	1	4,789.44	1	4,789.44	ESTABLECIMIENTO # H	Guatemala	Guatemala	GT	28	789658	N	90	00	637
20	345678912345450	A.1	17/02/2006	1	4,863.57	1	4,863.57	ESTABLECIMIENTO # X	Guatemala	Guatemala	GT	54	104863	N	90	00	648
21			17/02/2006	1	6,892.47	1	6,892.47	ESTABLECIMIENTO # Z	Guatemala	Guatemala	GT	15	487638	N	90	00	648

22	345678912345465	A.1	14/02/2006	1	1,234.56	1	1,234.56	ESTABLECIMIENTO # F	Guatemala	Guatemala	GT	56	146823	N	90	00	645
23			20/02/2006	2	421.89	1	3,375.12	ESTABLECIMIENTO # T	Guatemala	Guatemala	GT	36	746523	N	90	00	651
24			26/02/2006	1	999.58	1	999.58	ESTABLECIMIENTO # L	Estados Unidos	Boston	US	73	986304	N	90	00	657
25	456789876543227	A.1	16/02/2006	2	1,547.89	1	12,383.12	ESTABLECIMIENTO # O	Estados Unidos	Boston	US	89	980847	N	90	00	647
26	456789876543255	A.1	18/01/2006	2	942.57	1	7,540.56	ESTABLECIMIENTO # W	Portugal	Lisboa	PG	99	174098	N	90	00	618
27			19/01/2006	2	1,010.74	1	8,085.92	ESTABLECIMIENTO # T	Portugal	Lisboa	PG	36	489306	N	90	00	619
28			20/01/2006	2	1,212.45	1	9,699.60	ESTABLECIMIENTO # R	Portugal	Lisboa	PG	44	489687	N	90	00	620
29			04/02/2006	2	987.52	1	7,900.16	ESTABLECIMIENTO # T	Portugal	Lisboa	PG	36	203698	N	90	00	635
30			05/02/2006	2	547.52	1	4,380.16	ESTABLECIMIENTO # R	Portugal	Lisboa	PG	44	403871	N	90	00	636
31			06/02/2006	2	1,136.58	1	9,092.64	ESTABLECIMIENTO # W	Portugal	Lisboa	PG	99	692501	N	90	00	637
32	456789876543347	A.1	15/01/2006	2	1,200.00	1	9,600.00	ESTABLECIMIENTO # P	Italia	Milán	IT	67	789456	N	90	00	615
33			22/01/2006	2	1,750.00	1	14,000.00	ESTABLECIMIENTO # P	Italia	Milán	IT	67	123456	N	90	00	622
34			01/02/2006	2	1,000.00	1	8,000.00	ESTABLECIMIENTO # R	Holanda	Eindhoven	ND	44	452896	N	90	00	632
35			05/02/2006	2	1,150.00	1	9,200.00	ESTABLECIMIENTO # T	Holanda	Eindhoven	ND	36	489710	N	90	00	636
36	456789876543391	A.1	31/01/2006	1	7,550.80	1	7,550.80	ESTABLECIMIENTO # M	Guatemala	Guatemala	GT	38	489387	N	90	00	631
37			31/01/2006	1	8,550.89	1	8,550.89	ESTABLECIMIENTO # K	Guatemala	Guatemala	GT	91	487638	N	90	00	631
38	456789876543371	A.1	10/02/2006	2	1,125.82	1	9,006.56	ESTABLECIMIENTO # O	Estados Unidos	Texas	US	89	653214	N	90	00	641
39			11/02/2006	2	850.74	1	6,805.92	ESTABLECIMIENTO # Q	Estados Unidos	Denver	US	79	785631	N	90	00	642
40			12/02/2006	2	788.52	1	6,308.16	ESTABLECIMIENTO # P	Estados Unidos	Texas	US	67	445892	N	90	00	643
41	456789876543351	A.1	09/01/2006	2	1,400.50	1	11,204.00	ESTABLECIMIENTO # R	México	Querétaro	MX	44	325871	N	90	00	609
42			13/01/2006	2	1,500.75	1	12,006.00	ESTABLECIMIENTO # R	México	Querétaro	MX	44	324896	N	90	00	613
43			21/01/2006	2	1,600.50	1	12,804.00	ESTABLECIMIENTO # R	México	Querétaro	MX	44	123548	N	90	00	621
							238,301.90	**A.2**									

≠ ⊗ ∑ ∂ ↵

Indice de Códigos de Columnas

CC País donde se realizó la transacción.
MCC Código de categoría del comercio (Restaurantes, Farmacias, Zapaterías, etc.), con que visa identifica a los mismos.
Code Código de autorización (Número de autorización otorgado).
Ind. Indicador de la forma en que se otorgo la autorización de transacción (N = Normal).
POS EM Código de lectura de la banda magnética (Código 90 = Lectura de banda magnética completa).
Rason Código de identificación de la solicitud de la autorización (00 = Solicitud de autorización normal).
CDP Fecha del proceso de la transacción (Ejemplo = Para una transacción del 28/02/06, el código indica que se proceso en el año 6 y que van 59 días del año).

BANCO UNIVERSIDAD, S. A.

Evaluación Cumplimiento de Controles Internos del Banco
Tarjetas Identificadas con Transacciones Fraudulentas al 28/02/2006

Cédula No.	**A.6**
Hecho Por	**M.M.C.**
Revisado Por	**M.F.P.**
Fecha Inicio	**04-03-2006**
Fecha Fin	**05-03-2006**

Identificadas las transacciones fraudulentas efectuadas a través de la falsificación de la banda magnética de las tarjetas de crédito, a continuación se verificó el cumplimiento de los de los controles internos de la entidad bancaria, obteniendo los siguientes resultados:

			Controles Internos del Banco									
No.	**Tarjeta**	**Ref.**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Marca**	**Deficiencia en el Control Interno**
1	123456789123497	**A.1**					**X**				*f*	No se confirmó información relevante del cliente
2	234567898765451	**A.1**				X				X	*f*	No cumple el perfil requerido para el tipo de tarjeta y no se consultó información del sistema público
3	234567898765483	**A.1**		X	I						*f*	Falta contrato entre el Banco y el cliente y fotocopia de cédula
4	234567898765515	**A.1**									*f*	Información Completa
5	234567898765533	**A.1**		I	I		X			X	*f*	Falta firma del cliente en el contrato, no cumple el perfil para el tipo de tarjeta, no se confirmo información
6	345678912345348	**A.1**									*f*	Información Completa
7	345678912345396	**A.1**			I				X		*f*	Falta estados de cuentas bancarias y el sobreflex con firma de recibido de la tarjeta
8	345678912345450	**A.1**									*f*	Información Completa
9	345678912345465	**A.1**									*f*	Información Completa
10	456789876543227	**A.1**									*f*	Información Completa
11	456789876543255	**A.1**			I		I			X	*f*	Falta copia de cédula, no se confirmo información y no se consulto información del sistema público
12	456789876543347	**A.1**		X						X	*f*	Falta contrato y no se consulto información del sistema
13	456789876543391	**A.1**		I							*f*	Falta firma del cliente en el contrato suscrito
14	456789876543371	**A.1**									*f*	Información Completa
15	456789876543351	**A.1**									*f*	Información Completa

Indice de Letras
X Documento o requisito no encontrado
I Documento o requisito incompleto

Indice de Números
1 Solicitud de tarjeta de crédito.
2 Contrato suscrito entre el Banco y el cliente para el uso de la tarjeta de crédito.
3 Documentación complementaria a la solicitud de crédito requerida.
4 Perfil del cliente con relación al tipo de tarjeta autorizado.
5 Constancias de confirmación de información proporcionada por el solicitante.
6 Resolución de la solicitud de tarjeta o Acta del Comité.
7 Sobreflex donde conste la entrega de la tarjeta al cliente.
8 Consulta de referencias personales, bancarias y crediticias, obtenidas de un sistema público de información.

BANCO UNIVERSIDAD, S. A.

Revisión Funcionalidad de las Herramientas Utilizadas por el Banco
Tarjetas Identificadas con Transacciones Fraudulentas al 28/02/2006

Cédula No.	**A.7**
Hecho Por	**M.M.C.**
Revisado Por	**M.F.P.**
Fecha Inicio	**05-03-2006**
Fecha Fin	**06-03-2006**

Con la identificación de las tarjetas de crédito que fueron afectadas por transacciones fraudulentas, se procedió a verificar la eficacia de las herramientas implementadas para la prevención y detección de fraudes, obteniendo los siguientes resultados:

			Herramientas Utilizadas por el Banco											
No.	**Tarjeta**	**Ref.**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Marca**	**Comentario**
1	123456789123497	**A.1**	**NA**					**NA**	**NA**				∃, Ψ	La tarjeta original se encuentra en poder del tarjetahabiente y los consumos se hicieron dentro de los parámetros establecidos.
2	234567898765451	**A.1**	**NA**					**NA**	**NA**				∃, Ψ	La tarjeta original se encuentra en poder del tarjetahabiente y los consumos se hicieron dentro de los parámetros establecidos..
3	234567898765483	**A.1**	**NA**						**NA**				∅	Se recibieron alertas por los consumos, pero no fueron atendidas por el personal del área de seguridad del Banco.
4	234567898765515	**A.1**	**X**						**NA**				∂, ∅, β	La tarjeta se reporto como extraviada, no se incluyo en el boletín. Se recibió dos alertas del adquirente por consumos del mismo día, las que no atendieron.
5	234567898765533	**A.1**	**NA**						**NA**				∅	Se recibió alerta por consumo del 01/02/06, el cual se confirmo con el tarjetahabiente.
6	345678912345348	**A.1**	**X**					**X**	**X**				∂, Ψ, β	La tarjeta se reporto como robada pero no se incluyo en el boletín de tarjetas canceladas. No se recibieron alertas y los consumos estuvieron fuera de los parámetros establecidos.
7	345678912345396	**A.1**	**NA**	**1/**	**2/**	**3/**	**3/**	**NA**	**NA**	**4/**	**3/**	**3/**	∂	La tarjeta fue robada y el tarjetahabiente reportó el suceso fuera de los plazos establecidos en el contrato suscrito con el Banco.
8	345678912345450	**A.1**							**NA**				∅	Se recibió alerta por consumos consecutivos, pero no fueron atendidas por el personal del Banco
9	345678912345465	**A.1**	**NA**					**NA**	**NA**				∂	Tarjeta no reportada como robada, derivado que el tarjetahabiente no se había percatado del suceso.
10	456789876543227	**A.1**	**NA**					**X**	**X**				∂, ∅	No se recibió alerta por el consumo y éste se encuentra parámetrizado para detectarlos.
11	456789876543255	**A.1**	**NA**										∅	Se recibieron alertas por reincidencia de establecimientos pero no se dio seguimiento.
12	456789876543347	**A.1**	**NA**						**NA**				∅	Se recibieron las alertas de los consumos, pero por ser día inhábil no se dio seguimiento a las mismas
13	456789876543391	**A.1**	**NA**						**NA**				∂, β	Se recibió reporte del robo de la tarjeta, pero no se bloqueo en el sistema, ni se incluyó en el boletín lo que provocó el procesamiento de los consumos.
14	456789876543371	**A.1**	**NA**					**NA**	**NA**				∂, β	La tarjeta se reporto como robada pero no se bloqueo ni se incluyó en el boletín de tarjetas.
15	456789876543351	**A.1**	**NA**										∅	Se recibieron alertas y se confirmaron con cliente.

1/ El Banco tiene la política de recompensar a los establecimientos afiliados que retengan una tarjeta reportada en el boletín de tarjetas canceladas**.**

2/ El Banco educa a los tarjetahabientes por medio de publicidad enviada en los estados de cuenta a cada fecha de corte y los adquirentes educan a los comercios afiliados a través de capacitaciones periódicas**.**

3/ Al realizar la evaluación, se pudo constatar que el Banco no ha adquirido ni utilizado las herramientas para ayudar con la prevención y detección de fraudes por medio de la falsificación de la banda magnética de la tarjeta de crédito**.**

4/ Se logro comprobar que el Banco utiliza en todas sus tarjetas emitidas, el código de verificación de tarjeta**.**

Indice de Referencias

Herramienta funcionó en la prevención y detección del fraude por la falsificación de la banda magnética.

X Herramienta implementada NO detectó fraude

NA Derivado del caso revisado, No Aplica la herramienta implementada

Indice de Números

1 Boletín de Tarjetas Canceladas
2 Recompensa a Comercios
3 Educación a Tarjetahabientes y Comercios
4 Límites de Piso de Comercios
5 Autorizaciones y Supervisión de Depósitos de los Comercios
6 Alertas electrónicas recibida de los Adquirentes
7 Alertas electrónicas recibida del programa de VISA
8 Códigos de Verificación de Tarjetas
9 Servicio Nacional de Alerta de Comercio
10 Servicio de Identificación de Riesgos

BANCO UNIVERSIDAD, S. A.

Verificación Cumplimiento del Programa de Control de Fraudes, del Banco
AL 28/02/2006

Cédula No.	**A.8**
Hecho Por	**M.M.C.**
Revisado Por	**M.F.P.**
Fecha Inicio	**06-03-2006**
Fecha Fin	**07-03-2006**

Se procedió a revisar el grado de cumplimiento por parte del Banco, del programa diseñado para el control de fraudes por la falsificación de la banda magnética de tarjetas de crédito, determinando los siguientes resultados:

No.	Programa de Control de Fraudes	1	2	Observaciones
1	Departamento de Control de Fraudes	X		Solo se cuenta con una sección encargada de la Vigilancia y Seguridad de tarjetas de crédito
	Personal del Banco para el Control de Fraudes			
2	Poseen experiencia para la investigación de fraudes	X		El personal encargado posee cierta experiencia, pero el número de colaboradores no se encuentra acorde a la cantidad de fraudes que se deben investigar.
3	Se tiene un programa de capacitación continua	X		No se cuenta con un programa continúo de capacitación para el personal que tiene a su cargo la vigilancia y seguimiento de fraudes.
	Herramientas de Control de Fraudes			
4	Boletín de tarjetas canceladas		X	Las tarjetas canceladas se incluyen en el boletín de tarjetas canceladas.
5	Recompensa a los comercios		X	Se ofrece recompensa a los establecimientos que retienen tarjetas canceladas.
6	Educación a los tarjetahabientes y comercios		X	Se mantiene una educación a los tarjetahabientes y comercios, a través de publicidad en los estados de cuenta y seminarios a los comercios.
7	Límites de piso a los comercios	X		No se utiliza la información de los comercios fraudulentos, por eso no se implemento el límite de piso en los mismos.
8	Autorización y supervisión depósitos de comercios	X		No se implemento el control de los depósitos que realizan los comercios.
9	Servicios de control de fraude de VISA (Alertas Electrónicas)		X	Se utiliza el servicio de alertas electrónicas de los adquirentes y del programa de VISA adquirido.

Indice de Números
1 Herramienta NO implementada
2 Herramienta Implementada

g) Resolución Casos de Transacciones Fraudulentas Investigadas

Terminada la fase de investigación de las transacciones fraudulentas, se procedió a verificar el grado de responsabilidad que tuvo el tarjetahabiente y el Banco emisor, con el objeto de establecer la resolución de cada caso.

Adicionalmente es importante determinar a cuanto ascienden las transacciones en las cuales la responsabilidad corre por parte del Banco, con el fin de realizar una provisión para absorber el monto, ya que esto tendrá un impacto directo en los resultados de la entidad emisora.

Para una mejor apreciación de los factores que originaron la responsabilidad de los consumos, a continuación se muestra detalle de las deficiencias detectadas:

BANCO UNIVERSIDAD, S. A.

Resolución de Casos de Transacciones Fraudulentas Investigadas Realizadas Durante el Período del 01 de enero al 28 de febrero de 2006

Cédula No.	**A.9**
Hecho Por	**M.M.C.**
Revisado Por	**M.F.P.**
Fecha Inicio	**08-03-2006**
Fecha Fin	**10-03-2006**

No.	Tarjeta	Valor Q. Transacc.	Ref.	Control Interno (Banco Emisor)	Ref.	Herramientas (Banco Emisor)	Ref.	Origen del Fraude (Tarjetahabiente)	Ref.	Resolución del Caso (Responsable)
1	123456789123497	554.89	**A.1**	Satisfactorio	**A.4**	Satisfactorio	**A.5**	Uso normal	**A.5**	Banco
2	234567898765451	687.52	**A.1**	Deficiente	**A.4**	Satisfactorio	**A.5**	Uso normal	**A.5**	Banco
3		842.58								
4		745.89								
5	234567898765483	1,258.52	**A.1**	Deficiente	**A.4**	Deficiente	**A.5**	Uso normal	**A.5**	Banco
6		2,897.23								
7	234567898765515	2,171.44	**A.1**	Satisfactorio	**A.4**	Deficiente	**A.5**	Uso normal	**A.5**	Banco
8		2,958.48								
9	234567898765533	554.56	**A.1**	Deficiente	**A.4**	Deficiente	**A.5**	Uso normal	**A.5**	Banco y Tarjetahabiente por la transacción de Q. 1,125.42
10		874.29								
11		1,125.42								
12		3,607.04								
13	345678912345348	2,496.57	**A.1**	Satisfactorio	**A.4**	Deficiente	**A.5**	Uso normal	**A.5**	Banco
14		4,563.36								
15		6,586.64								
16		2,258.56								
17	345678912345396	3,575.81	**A.1**	Deficiente	**A.4**	Satisfactorio	**A.5**	Incumplimiento	**A.5**	Tarjetahabiente
18		4,269.87								
19		4,789.44								
20	345678912345450	4,863.57	**A.1**	Satisfactorio	**A.4**	Deficiente	**A.5**	Uso normal	**A.5**	Banco
21		6,892.47								
22	345678912345465	1,234.56	**A.1**	Satisfactorio	**A.4**	Satisfactorio	**A.5**	Incumplimiento	**A.5**	Tarjetahabiente
23		3,375.12								
24		999.58								
25	456789876543227	12,383.12	**A.1**	Satisfactorio	**A.4**	Deficiente	**A.5**	Uso normal	**A.5**	Banco
26	456789876543255	7,540.56	**A.1**	Deficiente	**A.4**	Deficiente	**A.5**	Uso normal	**A.5**	Banco
27		8,085.92								
28		9,699.60								
29		7,900.16								
30		4,380.16								
31		9,092.64								
32	456789876543347	9,600.00	**A.1**	Deficiente	**A.4**	Deficiente	**A.5**	Uso normal	**A.5**	Banco
33		14,000.00								
34		8,000.00								
35		9,200.00								
36	456789876543391	7,550.80	**A.1**	Deficiente	**A.4**	Deficiente	**A.5**	Uso normal	**A.5**	Banco
37		8,550.89								
38	456789876543371	9,006.56	**A.1**	Satisfactorio	**A.4**	Deficiente	**A.5**	Uso Normal	**A.5**	Banco
39		6,805.92								
40		6,308.16								
41	456789876543351	11,204.00	**A.1**	Satisfactorio	**A.4**	Satisfactorio	**A.5**	Uso normal	**A.5**	Tarjetahabiente
42		12,006.00								
43		12,804.00								

Adicionalmente a lo descrito en el cuadro anterior, cabe mencionar que aunado a las deficiencias localizadas en los controles internos y herramientas para la prevención y detección de fraudes por la falsificación de la banda magnética de tarjetas de crédito, se añaden las del programa del control de fraudes que afectan en forma general, las cuales se pueden observar en la cédula **A.6** (Evaluación Cumplimiento del Programa del Control de Fraudes).

RESUMEN DE CUANTIFICACION DE TRANSACCIONES FRAUDULENTAS

DESCRIPCION	CANTIDAD TRANSACC.	MONTO Q.	%
Responsable Tarjetahabiente	10	55,383.80	23.24
Responsable Banco Emisor	33	182,918.10	76.76
TOTALES	**43**	**238,301.90**	**100.00**

5.1.4 Informe de Auditoría

BU **Banco Universidad, S. A.**

Departamento de Auditoría Interna

Cédula No.	**A.10**
Hecho Por	**M.M.C.**
Revisado Por	**M.F.P.**
Fecha Inicio	**11/03/2006**
Fecha Fin	**24/03/2006**

PARA: Gerente Departamento de Tarjeta de Crédito

DE: Auditoría Interna

ASUNTO: **Investigación Fraudes por la Falsificación de la Banda Magnética de Tarjetas de Crédito, durante Enero Y Febrero de 2006**

FECHA: Marzo 25 de 2006

Como parte de la programación que desarrolla el departamento de auditoría interna, se procedió a revisar las tarjetas de crédito que fueron objeto de transacciones fraudulentas, por medio de la falsificación de la banda magnética, con el objeto de establecer debilidades de control interno, de herramientas electrónicas y falta de cumplimiento con el programa, diseñados para la prevención y detección de éste tipo de operaciones ilícitas.

El trabajo se desarrollo de la siguiente forma:

a) Determinación de la Cartera Total de Tarjetas de Crédito, por Clase y Fecha de Corte

Se procedió a establecer la cartera total de tarjetas vigentes a los meses de enero y febrero de 2006, a través de la revisión y extracción de la base de datos del sistema de tarjetas de crédito. Con lo anterior se pudo verificar que el banco cuenta con una cartera total de 200 tarjetas emitidas de distintas clases, las cuales se resumen a continuación:

No.	Clase de Tarjeta Emitida	Cantidad de Tarjetas	Saldo Global al 28/02/2006 Q.
1	Local	50	32,674.12
2	Internacional	50	259,665.06
3	Oro	50	1,046,265.93
4	Platinum	50	3,089,515.15
	TOTALES	**200**	**4,428,120.26**

b) Detección de las Tarjetas con Transacciones Fraudulentas

Basados en el control electrónico de gestiones operativas, correos electrónicos y cartas físicas de reclamos recibidas, se procedió a tabular las tarjetas que muestran consumos no autorizados por los tarjetahabientes. Con lo anterior se pudo establecer que clases y cantidad de tarjetas fueron afectadas, y a cuanto asciende el monto quetzalizado de las mismas, determinando lo siguiente:

No.	Clase de Tarjeta	Cantidad de Tarjetas	Monto de Consumos en Q.
1	Local	01	554.89
2	Internacional	04	17,722.97
3	Oro	04	45,905.55
4	Platinum	06	174,118.49
	Totales	**15**	**238,301.90**

c) Identificación de transacciones fraudulentas por falsificación de la banda magnética

Con las tarjetas de crédito con transacciones fraudulentas plenamente identificadas, se procedió a revisar el total de transacciones efectuadas a través de las mismas. Dichas operaciones fueron revisadas y verificadas para tener la certeza de que correspondían a los tarjetahabientes que efectuaron los reclamos y que las mismas no fueron autorizadas por ellos. Para la revisión, se verificaron contra la siguiente información:

- Estado de cuenta de los cortes de enero y febrero de 2006.
- Listado detallado de movimientos autorizados (Incomming)
- Gestiones operativas por reclamos de cargos fraudulentos.
- Copia Físicas de boletas de transacciones efectuadas (Slips).

De la revisión efectuada se obtuvieron los siguientes resultados:

No.	Clase de Tarjeta	Cantidad Transacc. Q.	Monto Q.	Cantidad Transacc. US$	Monto US$	Monto 1/ Quetzalizado	Monto Global en Q.
1	Local	01	554.89	N/A	N/A	N/A	554.89
2	Internacional	08	8,986.01	03	1,092.12	8,736.96	17,722.97
3	Oro	09	31,380.43	03	1,815.64	14,525.12	45,905.55
4	Platinum	02	16,101.69	17	19,752.10	158,016.80	174,118.49
	Totales	**20**	**90,964.22**	**23**	**22,659.86**	**181,278.88**	**238,301.90**

1/ El tipo de cambio utilizado para quetzalizar las operaciones en moneda extranjera, es de Q. 8.00 por US$ 1.00.

d) Verificación cumplimiento de controles internos para emisión de tarjetas de crédito

Se procedió a revisar la efectividad de los controles internos implementados por la entidad bancaria, para la emisión de la tarjeta de crédito objeto de las transacciones fraudulentas, con la finalidad de asegurarse por parte del banco, de lo siguiente:

- El contrato suscrito entre el tarjetahabiente y el Banco, por el uso de la línea de crédito a través del financiamiento por medio de tarjeta de crédito, debidamente firmado, ya que en este se contemplan las condiciones que acepta el solicitante.
- La documentación requerida para la solicitud de la tarjeta, así como verificar que haya cumplido con el perfil deseado, para mantener conocimiento general del tarjetahabiente.
- Resolución de la solicitud de tarjeta o acta de autorización cuando así lo amerite el caso, para tener la certeza que se realizo el análisis respectivo para aprobar la tarjeta.
- Copia del sobreflex en el cual haya quedado la evidencia de la entrega de la tarjeta, por medio de la firma y número de documento de identificación del tarjetahabiente.
- Constancia de consulta de referencias personales, bancarias y crediticias del tarjetahabiente, en las que se haya establecido, que la persona a la que le fue autorizada la tarjeta, es honorable y con buen récord en sus referencias.

Los resultados de la revisión de las 15 tarjetas identificadas, se resumen en el siguiente cuadro:

	Cantidad de Tarjetas	
Descripción	Satisfactoria	Deficiente
Tarjetas de crédito verificadas	08	07

Como se puede observar en el cuadro anterior los resultados evidencian varias deficiencias, las que son causas que facilitan la ejecución de fraudes, que se convierten en pérdidas para la entidad.

e) Revisión Funcionalidad de herramientas electrónicas utilizadas por la entidad emisora

Se procedió a revisar que las transacciones de las tarjetas investigadas, hayan sido detectadas por medio de las herramientas implementadas por el Banco, para la prevención y detección de las mismas. De la revisión efectuada, se pudieron obtener los siguientes resultados:

Descripción	Cantidad de Tarjetas con Posibilidad	
	Satisfactorio	Deficiente
Tarjetas de crédito verificadas	05	10

Como se puede apreciar en el cuadro anterior, de las tarjetas que tuvieron posibilidad de ser detectadas por cualquiera de las herramientas utilizadas por el Banco, fueron pocas las que presentaron algún tipo de advertencia para que el personal de la entidad emisora, hiciera las gestiones necesarias con el fin de neutralizar las transacciones efectuadas.

f) Verificación Cumplimiento del Programa de Control de Fraude

Se procedió a evaluar el grado de avance que se tiene en la implementación y cumplimiento del programa de control de fraudes, el cual contempla varios aspectos enfocados en diferentes área, con el objeto de manejar con mayor control, los posibles fraudes que se pueden presentar partiendo de la premisa que la actividad del financiamiento a través de tarjeta de crédito, lleva inherente el riesgo de fraude.

Derivado de la evaluación efectuada, se pudieron observar varias deficiencias, las cuales se detallan a continuación:

- Dentro de la estructura organizativa del Banco, no se ha implementado un departamento específico para el control de fraudes a través de tarjetas de crédito.
- El personal encargado de las investigaciones de fraudes a través de tarjetas de crédito, no cuenta con una amplia experiencia en la materia, ya que lo han ido adquiriendo del trabajo diario.
- No se tiene implementado un programa permanente de capacitación específica, para el personal relacionado al control de fraudes por medio de tarjetas de crédito.
- No se ha implementado la herramienta referente a la información de los establecimientos afiliados, lo que origina que no se manejen límites de piso para los de alto riesgo de posibles fraudes.
- Derivado que la mayoría de los establecimientos afiliados, no manejan cuentas monetarias en el Banco, no se ha implementado el control de depósitos que realizan los mismos.
- No se han implementado más herramientas de control, debido a que el tamaño de la cartera no lo amerita, además de que cada una representa una fuerte inversión para el Banco.

Lo anterior muestra que el Banco, necesita realizar ciertos cambios dentro de sus políticas y medidas de control, para poder fortalecer sus diferentes áreas y con ello lograr minimizar el riesgo de fraude a través de su cartera de tarjetas de crédito.

g) Determinación de Responsabilidades de las Transacciones Fraudulentas Investigadas

Terminada la investigación de las transacciones fraudulentas de las tarjetas de crédito identificadas, se realizó una verificación de las debilidades localizadas, tanto por parte del tarjetahabiente como del Banco, para así determinar la responsabilidad de las mismas, con el objeto de cuantificar el costo de lo que tendría que asumir cada una de las partes involucradas.

A continuación se presenta un resumen de las responsabilidades determinadas y de sus respectivos costos:

Descripción	Cantidad De Transacciones	Monto Q.	%
Responsable Tarjetahabiente	10	55,383.80	23.24
Responsable Banco Emisor	33	182,918.10	76.76
TOTALES	**75**	**238,301.90**	**100.00**

Como se observa en el cuadro anterior, la mayor parte de las responsabilidades fueron por parte de la entidad bancaria, debido a que se tuvieron varias deficiencias de control interno, las herramientas no detectaron los consumos, en otros casos sí detecto pero el personal de la entidad no le dio el seguimiento oportuno y la falta de cumplimiento con lo establecido dentro del programa de control de fraudes instituido por la entidad.

En el caso de la responsabilidad de los tarjetahabientes, sobresale el descuido al utilizar su tarjeta, el reportar el robo o extravío de la misma fuera de tiempo o el que no se detectaron porque las transacciones fueron realizadas justo por debajo del monto parametrizado en el sistema y en las herramientas utilizadas.

CONCLUSIONES DEL CASO PRACTICO

De acuerdo a la evaluación de controles interno, herramientas utilizadas y programa de control de fraude, efectuada con relación a los casos de tarjetas que presentaron transacciones fraudulentas, se concluye lo siguiente:

1. Se pudo establecer que existen deficiencias en los controles internos, en la funcionalidad de las herramientas electrónicas adquiridas y en el poco grado de avance en la implementacion del programa de control de fraudes por falsificación de banda magnética de tarjetas de crédito, las cuales se tradujeron en la no detección de los fraudes evaluados.

2. Se localizaron fuertes debilidades de control interno, respecto a la documentación, información y perfiles requeridos para la emisión de tarjetas de crédito, las cuales resultaron perjudiciales al momento de determinar las responsabilidades de las operaciones fraudulentas.

3. Se evidenció la falta de un programa de capacitación continuo para el personal encargado del seguimiento de alertas y avisos de las herramientas implementadas, así como de las investigaciones de fraudes por la falsificación de la banda magnética de tarjetas de crédito.

4. Se observaron debilidades en el seguimiento de alertas o avisos recibidos por medio de las herramientas implementadas por el Banco, de parte del personal encargado del control de fraudes.

5. Se constato la falta de incorporación de otras herramientas de control de fraudes, puestas a disposición de parte de Visa Internacional Región América Latina y el Caribe.

6. Se detectaron deficiencias en la recepción y registro en el sistema de tarjetas de crédito reportadas como robadas, lo que automáticamente favorece al tarjetahabiente al momento del reclamo correspondiente.

7. Se evidenció deficiencia en la implementacion y cumplimiento del programa de control de fraudes diseñado por el Banco, lo cual sumo como factor en contra al momento de revisar y dar seguimiento a cada una de las transacciones fraudulentas detectadas.

8. Se observaron incumplimientos por parte de los tarjetahabientes, respecto a las condiciones establecidas en el contrato suscrito y firmado con el Banco.

9. Se detectaron casos de falta de responsabilidad del tarjetahabiente, con relación al cuidado del uso de su tarjeta de crédito.

RECOMENDACIONES DEL CASO PRACTICO

Para mejorar los aspectos descritos anteriormente, se sugiere atender las siguientes recomendaciones, con la finalidad de fortalecer los controles internos, dar mayor funcionalidad a las herramientas electrónicas utilizadas y mejorar el avance en la implementacion del programa de control de fraudes:

1. Realizar las gestiones necesarias, a efecto de vigilar el estricto cumplimiento de controles internos establecidos mediante las circulares normativas, analizar la parametrización y adecuar de mejor forma las herramientas utilizadas, así como evaluar las causas y vigilar el debido cumplimiento con el cronograma de implementacion del programa de control de fraude, con el fin de minimizar el riesgo de posibles fraudes por falsificación de banda magnética de tarjetas de crédito.

2. Fortalecer los controles internos establecidos, para el análisis y aprobación de solicitudes de tarjetas de crédito, con la finalidad de mantener toda la información necesaria al momento de presentarse casos de reclamos por fraudes de tarjetas de crédito.

3. Evaluar la posibilidad de invertir en la adquisición de nuevas herramientas, con el objeto de ampliar las posibilidades de prevenir y detectar fraudes por medio de la falsificación de la banda magnética de tarjetas de crédito.

4. Realizar una verificación de los parámetros establecidos en las herramientas que actualmente se utilizan, con el objeto de modificarlas y hacerlas más rigurosas, para lograr una mayor cobertura en la detección y prevención de fraudes por esta vía

5. Realizar las gestiones necesarias, a efecto de mejorar y avanzar en la implementación de las políticas y procedimientos establecidos, en el programa de control de fraude diseñado para el Banco.

6. Implementar a la brevedad posible un programa continuo de capacitación, respecto a temas relacionados a la prevención, detección, control, seguimiento e investigación de fraudes por medio de la falsificación de tarjetas de crédito.

5.1.5 Resultados del Caso Práctico

Como se pudo observar en el caso práctico presentado existen muchos medios que facilitan el uso de tarjetas de crédito para realizar operaciones fraudulentas, pero al referirnos a la falsificación de la banda magnética, nos concretamos a que los defraudadores tuvieron acceso y copiaron los datos establecidos en dicha banda, lo cual es complicado poder establecer el momento y lugar exacto en que se realizó la copia.

En el caso desarrollado se observa que derivado de las deficiencias de control interno, las pocas herramientas de control utilizadas, la falta de una adecuada parámetrización de las mismas y la no eficiente implementacion del las políticas y medidas establecidas dentro del programa de control de fraudes diseñado para la entidad, se incrementa el riesgo de fraudes a través de la falsificación de la banda magnética de tarjetas de crédito, lo que repercute directamente en los resultados de la entidad, ya que éstos en su mayoría deben ser absorbidos por la misma.

La aplicación y modificación de procedimientos de control interno, la mejora en los parámetros establecidos para las herramientas utilizadas, la incorporación de nuevas y la eficiente implementacion del programa de control de fraudes diseñado, contribuirá en el fortalecimiento de la prevención y detección de los fraudes ya que se incrementará el campo de acción de las medidas utilizadas y se minimizará el riesgo de posibles operaciones fraudulentas, lo que repercute en los resultados de la entidad emisora, al no tener operaciones que tengan que ser absorbidas por la misma.

Sin embargo no existen controles, medidas y herramientas electrónicas infalibles para evitar que el riesgo de este tipo de fraude, sea asumidos por las entidades que se dedican a este tipo de financiamiento, no obstante que la adopción de medidas de control y una supervisión periódica adecuada por parte del departamento de auditoría interna, contribuirá a mejorar los resultados de prevención y detección de fraudes por la falsificación de la banda magnética de tarjetas de crédito.

Manuel Francisco Poz
Auditor Interno

MFP/khl
c.c Gerente General
Gerente División de Riesgos
Archivo

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Toda entidad bancaria que dentro de los servicios financieros que ofrezca, incluya el financiamiento a través de la emisión de tarjetas de crédito, debe mantener políticas, procedimientos y auxiliarse de herramientas, para minimizar el riesgo de fraude por la falsificación de la banda magnética de tarjetas, que están expuestas en forma inherente.

2. El manejo y control de los fraudes a través de tarjetas de crédito, es responsabilidad de la administración de la entidad emisora, no obstante el Auditor debe apoyar a ésta, mediante la revisión periódica de los controles internos, procedimientos y herramientas, con el fin de identificar debilidades que puedan ser corregidas oportunamente.

3. Los fraudes realizados a través de la falsificación de la banda magnética de una tarjeta de crédito, se traducen en pérdidas financieras, las cuales dependiendo de los factores bajo los cuales se haya cometido, deben ser absorbidos por el tarjetahabiente o la entidad emisora.

4. La empresa **Visa Internacional**, constantemente se encuentra diseñando herramientas electrónicas que ayuden a minimizar los niveles de fraudes a través de tarjetas de crédito, las cuales pone a disposición de las entidades emisoras a cambio de una inversión económica. De esa cuenta dichas entidades determinan la adquisición de herramientas, basadas en el volumen de transacciones que realicen los tarjetahabientes y el tamaño de cartera que administren.

5. Cuando se presentan operaciones de transacciones fraudulentas, es necesario realizar una investigación exhaustiva, con la finalidad de determinar las responsabilidades de parte del tarjetahabiente o la entidad emisora, con el fin de determinar quien absorberá el costo de las mismas.

6. El desarrollo de la tecnología informática ha provocado que ésta sea utilizada por personas dedicadas a realizar actos ilícitos o fraudes, en la creación de mecanismos eficientes, con el propósito de obtener información de las bandas magnéticas de tarjetas y poder llevar a cabo su cometido.

RECOMENDACIONES

1. En el ámbito de la banca, es imposible que una institución emisora de tarjetas de crédito pueda operar sin asumir algunos niveles de riesgos de fraudes. En tal virtud es importante que las entidades emisoras, a través de la alta dirección, establezcan políticas y procedimientos de controles adecuados, los que deben ser revisados y aprobados por el consejo de administración, comunicados al gerente del departamento de tarjeta de crédito y evaluados periódicamente por la auditoría interna de la entidad.

2. La auditoría interna de la entidad emisora de tarjetas de crédito, debe ser la que proporcione el mayor apoyo a la gerencia general, en la prevención y detección de fraudes, contando para ello con políticas, controles internos, procedimientos y herramientas necesarias que permitan llevar a cabo y de manera eficaz, ésta labor.

   Por esta razón se requiere que las auditorías internas de las entidades emisoras, cuenten con personal calificado, al cual se debe brindar el apoyo necesario, para mantenerlo en constante capacitación.

3. Dentro de toda entidad emisora de tarjetas de crédito, existe una gerencia encargada de administrar los diferentes tipos de riesgos a los que esta expuesta la misma. Dicha sección conjuntamente con el apoyo de la administración y la auditoría interna, deben velar para que las políticas y medidas fijadas se cumplan a cabalidad, con el propósito de poder justificar de mejor forma los reclamos hechos por los tarjetahabientes, a fin de no incurrir en responsabilidad y absorber costos de las transacciones fraudulentas.

4. Es importante que el área de tarjetas de crédito, con el apoyo de la auditoría interna de la entidad, evalúen periódicamente el tamaño de la cartera de tarjetas, el volumen de las transacciones en cantidad y valor, a efecto de implementar nuevas herramientas electrónicas, diseñadas y puestas a disposición por **Visa Internacional**.

5. Dentro del área de tarjetas de crédito, de una entidad, es de vital importancia que se implemente una sección específica para el control e investigación de fraudes, la cual debe estar integrado por personal capacitado y experimentado en ésta clase de operaciones, con el fin de obtener resultados oportunos en la resolución de casos y determinar responsabilidades.

6. Dado el crecimiento de la tecnología informática y su utilización en este tipo de fraudes, es necesario que las entidades emisoras de tarjetas de crédito, realicen constantemente campañas de educación a los tarjetahabientes y establecimientos afiliados, con el fin de concienciar a los mismos, sobre el cuidado y control que se debe mantener al utilizar las tarjetas.

BIBLIOGRAFIA

1. Alcibar, J.R. – H.A. Binda
   TECNICAS Y ORGANIZACIÓN BANCARIA
   Ediciones Macchl
   Argentina, 1980.

2. Bullrich, Santiago J
   LA TARJETA DE CREDITO
   Abeledo Perrot, Primera Edición
   Argentina, 1971.

3. Cervantes Ahumada, Raúl
   TITULOS Y OPERACIONES DE CREDITO
   Ediciones Herrero, S.A., 10ma. Edición.
   México, 1978.

4. Chicas Hernández, Jaime Humberto
   Del Aguila de Reyes, Evelyn
   MATERIAL DE APOYO PARA LAS PLATICAS DE ORIENTANCION DE ELABORACION DE TESIS
   Universidad de San Carlos de Guatemala
   Guatemala, Julio 2000.

5. **CODIGO DE COMERCIO**
   Decreto No. 2-70 del Congreso de la República de Guatemala

6. Cogorno, Eduardo Guillermo
   TEORIA Y TECNICA DE LOS NUEVOS CONTRATOS COMERCIALES
   Ediciones, Meuri
   Argentina, 1979.

7. Garriguez, Joaquín
   CURSO DE DERECHO MERCANTIL
   Imprenta Aguirre
   Madrid, 1975.

8. Gómez Mendoza, María
   CONSIDERACIONES GENERALES EN TORNO A LAS TARJETAS DE CREDITO
   Estudios Jurídicos en Homenaje a Joaquín Garriguez
   Tomo II, Ediciones Tecnos
   Madrid, 1971.

9. **LEY DE BANCOS Y GRUPOS FINANCIEROS**
   Decreto 19-2002 del Congreso de la República de Guatemala

10. **LEY MONETARIA**
    Decreto 17-2002 del Congreso de la República de Guatemala

11. **LEY ORGANICA DEL BANCO DE GUATEMALA**
    Decreto 16-2002 del Congreso de la República de Guatemala

12. Noguera Blas E.
    PREVENCION DE FRAUDES EN INSTRUMENTOS BANCARIOS
    Decanato del Cuerpo de Peritos Forenses
    Corte Suprema de Justicia
    Argentina, 2001.

13. **PAGINA WEB, SUPERINTENDENCIA DE BANCOS**
http://www.sib.gob.gt/marco legal y normativo/principales leyes/doctos/bancos2/dto

14. **PAGINA WEB, ARTICULOS SOBRE LA ACTIVIDAD FINANCIERA DE DIFERENTES SECTORES**
http://www.condusef.gob.mx/revista/proteja/art bancos/fraudes.htm

15. **PAGINA WEB, ASPECTOS GENERALES Y CRITERIOS BASICOS UTILIZADOS EN LA AUDITORIA OPERACIONAL**
http://www.hacienda.gob.ni/sigfa/audi/vol2/audioperdes/aspgral.htm

16. Price WaterHouse, Firma de Auditoría
DESARROLLO DEL PLAN DE AUDITORIA
Serie de Guías de Auditoría
Bandeirante, Gráfica e Editorial
Sao Bernardo do Campo, 1986.

17. Sarmiento Ricaurté, Hernando
LA TARJETA DE CREDITO, SU ASPECTO JURIDICO Y ECONOMICO
Editorial Temis
Bogotá, 1973.

18. Soler Ramos, José A. – Staking, Kim B. – Ayuso Calle, Alfonso – Beato Paulina – Botin O'Shea, Emilio – Escrig, Meliá Miguel y Falero Carrasco, Fernando.
GESTION DE RIESGOS FINANCIEROS
Banco Interamericano de Desarrollo (BID), Grupo Santander
Washington, D.C. Estados Unidos de América – 1999.

19. Superintendencia de Bancos de Guatemala, - Ponentes: BRIONES, ALDO Y FANKHANEL, ERICK
Segunda Conferencia sobre Supervisión Financiera.
LA ADMINISTRACION Y SUPERVISION DE RIESGOS
Ponencia: Gestión Bancaria y Administración de Riesgos
Guatemala, 21 y 22 de Agosto de 1997

20. Traducción del Instituto de Auditores Internos de España- Coopers & Lybrand, S. A.
LOS NUEVOS CONCEPTOS DE CONTROL INTERNO (INFORME C.O.S.O.)
Ediciones Díaz de Santos, S.A.
Madrid, España, 1997.

21. Uría, Rodrigo
DERECHO MERCANTIL
Imprenta Aguirre, 8va. Edición
Madrid, 1972.

22. Valdivieso Valenzuela, Carlos (Ponente)
DECIMO PRIMER CONGRESO DE AUDITORIA INTERNA – EL NUEVO ESTÁNDAR INTERNACIONAL DE CONTROL INTERNO C.O.S.O. Y SU APLICACIÓN BASADO EN RIESGOS
Universidad de Chile, 1997.

23. Vásquez Martínez, Edmundo
INSTITUCIONES DEL DERECHO MERCANTIL
Serviprensa Centroamericana
Guatemala, 1978.

24. Villegas, Carlos Gilberto
REVISTA DE DERECHO PRIVADO Y COMUNITARIO
Rubinzal-Culzoni Editores
Santa Fe, Argentina;

25. VISA Internacional
GUIA PARA ADMINISTRACION DE RIESGOS Y SEGURIDAD
Región América Latina y el Caribe
Febrero, 2003.

26. VISA Internacional
REGLAMENTO OPERATIVO
Para la Región América Latina y el Caribe
Febrero, 2003.

27. VISA Internacional
SEMINARIO DE PREVENCION DE FRAUDES, NIVEL1
Para la Región de América Latina y el Caribe
Mayo, 1998.

ANEXOS

ANEXO No. 01
Solicitud de Tarjeta para Persona o Empresa Individual

FORMULARIO IVE-TC-01

TARJETAS DE CRÉDITO

FORMULARIO PARA INICIO DE RELACIONES

- Persona o Empresa Individual -

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

RELACION:

DEUDOR ☐ CODEUDOR ☐ No. DE CLIENTE

3	DATOS DEL PRODUCTO O SERVICIO SOLICITADO

3.1 Tipo de tarjeta solicitada:

Local ☐ Internacional ☐ Oro ☐ Otra (especificar): . .

Con Garantía ☐ Monto de la Garantía (Q.):

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:	Número:	Lugar de emisión:

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

4.7 Número de identificación tributaria (NIT):		País del NIT:	

4.8 Teléfonos:	4.9 Fax:	4.10 E-mail:

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

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

4.12 Sexo: M ☐ F ☐	Estado Civil:

4.13 Donde desea recibir su correspondencia:	Casa ☐	Oficina ☐	Otro:

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	Profesión u Oficio:
Sexo M ☐ F ☐			

5.4	Número de Identificación Tributaria (NIT):	País del NIT:	
5.5	Tipo de documento de identificación:	Número:	Lugar de emisión:
5.6	Dirección particular completa (calle o avenida, casa No., colonia, sector, lote, manzana, zona, municipio, departamento y país):		
5.7	Relación con el tarjetahabiente titular:		
5.8	Teléfonos:	5.89 Fax:	5.10 E-mail:
5.11	Nombre que desea en la tarjeta (26 caracteres como máximo)		
	☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐		

NOTA: Cuando el espacio del formulario sea insuficiente, 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.	Teléfonos:
6.2	Nombre del patrono anterior, si su estabilidad laboral es menos a 6 meses:		Teléfonos:
6.3	Personales (nombres de dos personas que no sean familiares):		Teléfonos:
6.4	Familiares (Nombres de dos familiares que no vivan con usted)		Teléfonos:

7.	INFORMACIÓN ECONÓMICO-FINANCIERA DEL SOLICITANTE				
7.1	Actividad económica del solicitante:				
	7.1.1 Origen 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/aaaa):**
7.1.2.2 Dirección completa del trabajo (calle o Ave., casa No., Col., sector, lote, manzana, zona, municipio, Depto. y país):	
7.1.2.3 Teléfonos del trabajo:	**7.1.2.4 Fax del trabajo:**
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 (Calle o Av.,casa No.,colonia,sector,lote,manzana,zona, municipio, departamento y país):	
7.1.3.5. Fecha de inicio de operaciones:	
7.1.3.6. Objeto:	
7.1.3.7. Teléfonos:	**7.1.3.8 Fax:**
7.2 Sector de la economía en que el solicitante desarrolla su actividad (Industria, Comercio, Agricultura, Otros):	
7.3 Ingresos mensuales aproximados:	**7.4 Egresos mensuales aproximados:**

.

DEBITO CUENTA **PAGO CONTADO** ☐ **PAGO MINIMO** ☐

Cta. De Ahorros No.:_____ **Cta. De Monetarios No.** _____

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 o carné.

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

9. OBLIGACIONES DEL SOLICITANTE

9.1 Declaro 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

Firma y código del empleado responsable de la verificación de la información

Firma y código de quien autoriza la operación

BASE LEGAL:

Artículo 21 de la Ley Contra el Lavado de Dinero u Otros Activos, Decreto Número 67-2001 del Congreso de la República y 12 de su Reglamento, contenido en Acuerdo Gubernativo Número 118-2002, de la Presidencia de la República.

ANEXO No. 02
Solicitud de Tarjeta para Persona Jurídica

FORMULARIO IVE - TC - 02

TARJETAS DE CRÉDITO
FORMULARIO PARA INICIO DE RELACIONES
- Persona Jurídica -

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

3	DATOS DEL PRODUCTO O SERVICIO SOLICITADO					
3.1	Tipo de tarjeta solicitada:					
	LOCAL ☐	INTERNACIONAL ☐	ORO ☐	Otra (especificar):		
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 DE LA ENTIDAD SOLICITANTE			
4.1	Tipo de Sociedad o Entidad:			
4.2	Nombre, razón social o denominación completa:			
4.3	Nombre comercial:			
4.4	Actividad económica principal u objeto de la entidad:			
4.5	Número de Identificación Tributaria (NIT):			País del NIT:
4.6	Datos de la escritura pública de constitución de sociedad o entidad:			
	Número:	Fecha:	Notario que la autorizó:	
4.7	Modificaciones a la escritura pública de constitución de sociedad o entidad (de existir más de una, detallar en hojas aparte):			
	Escritura No.:	Fecha:	Notario que la autorizó:	
4.8	Patente de sociedad:			
	No.:	Folio:	Libro:	No. de Exp.:
4.9	Patente de empresa:			
	No.:	Folio:	Libro:	No. de Exp.:
4.10	Si no es una Empresa o Sociedad Mercantil, deberá indicar la información siguiente, del Acuerdo Gubernativo o documento similar:			
	No.:	Fecha (dd/mm/aaaa):	Autoridad:	
4.11	Datos de Registro:			
	Nombre del Registro:	No.:	Folio:	Libro:
4.12	Teléfonos:	4.13 Fax:		
4.14	Dirección completa (calle o avenida, casa No., colonia, sector, lote, manzana, zona, municipio, departamento y país):			

5.	REFERENCIAS DE LA EMPRESA SOLICITANTE	
5.1	Comerciales (nombres de las empresas):	Teléfonos:
5.2	Bancarias (nombres de los bancos):	Teléfonos:

6. DATOS DEL REPRESENTANTE LEGAL SOLICITANTE				
6.1 Primer apellido:	Segundo apellido:		Apellido de casada:	
Primer nombre:	Segundo nombre:			
6.2 Fecha de nacimiento (dd/mm/aaaa):	6.3 Nacionalidad:			
6.4 Tipo de documento de identificación:	Número:	Lugar de emisión:		
Sexo: M ☐ F ☐	6.5 Número de Identificación Tributaria (NIT):	País del NIT:		
6.6 Profesión u oficio:	6.7 Teléfonos particulares:			
6.8 Dirección completa (calle o avenida, casa No., colonia, sector, lote, manzana, zona, municipio, departamento y país):				
6.9 Acta notarial de nombramiento:				
Fecha:	Notario que la autorizó:	Cargo para el que se le nombró:		
6.10 Número de inscripción del nombramiento en el Registro u Oficina respectiva:				
6.11 Para efectos de esta solicitud, actúa únicamente en beneficio de la entidad antes descrita:				
Sí ☐ No ☐				
6.12 Si la respuesta es negativa, proporcionar información de la persona en nombre de quien se actúa:				
6.12.1 Nombre completo de la persona y/o razón social de la entidad:				
6.12.2 Fecha de nacimiento o constitución (dd/mm/aaaa):	6.12.3 Nacionalidad:			
6.12.4 Tipo de documento de identificación:	Número:	Lugar de emisión:		
6.12.5 Número de Identificación Tributaria (NIT):	6.12.6 Teléfonos:			

7. DATOS DE TARJETAS ADICIONALES QUE SE SOLICITEN
Utilice el adendum a este formulario si el caso lo amerita.

8. INFORMACIÓN ECONÓMICO-FINANCIERA DE LA ENTIDAD SOLICITANTE				
8.1 Miembros del Consejo de Administración, Junta Directiva, Administrador Único u otro similar:				
Nombres y apellidos completos				
Nota: Propietarios del 5% o más de las acciones.				
8.2 Datos del gerente y otros funcionarios gerenciales:				
Nombres y apellidos completos:	No.de cédula de vecindad o pasaporte:	Lugar de emisión:	Cargo:	NIT:
8.3 Ubicación de los principales proveedores y clientes:				
PROVEEDORES	CLIENTES			
Ubicación geográfica:	Ubicación geográfica:			

8.4	**Detalles de la actividad:**
	8.4.1 Monto aproximado de ingresos mensuales:
	8.4.2 Monto aproximado de egresos mensuales:
	8.4.3 Número aproximado de empleados:
8.5	**Otros datos de la empresa solicitante:**
Procedencia de los fondos para el pago de la(s) tarjeta(s) de crédito	

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

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

9.1 Fotocopia del primer testimonio de la escritura pública de constitución, debidamente registrada.
9.2 Fotocopia de la Patente de Sociedad.
9.3 Fotocopia de la Patente de Empresa.
9.4 Fotocopia del Acuerdo Gubernativo u otro documento similar (en el caso de Fundaciones, Iglesias, etc.) en el que se autorice su constitución.
9.5 Fotocopia del nombramiento del representante legal, debidamente registrado o primer testimonio de la escritura de mandato debidamente registrado.
9.6 Fotocopia de la cédula de vecindad o pasaporte del representante legal.
9.7 Fotocopia de los documentos de identificación del (los) responsable(s) de la(s) tarjeta(s) de crédito.
9.8 En caso de ser extranjeros, una fotocopia de su documento de identificación y del documento que acredite su condición migratoria, cuando sea aplicable (pasaporte, tarjeta de visitante, pase especial de viaje).

9.9 Sociedades u otras entidades en formación:
9.9.1 Carta de notario que certifique que tiene en proceso la constitución de la sociedad o entidad, en donde se indique, qué persona será designada como representante legal.
9.9.2 En el plazo de 60 días contados a partir de la apertura de la cuenta, deberá presentarse los documentos indicados.
9.9.3 Es responsabilidad de la persona obligada velar por el cumplimiento de lo estipulado en el numeral inmediato anterior

10. OBLIGACIONES DE LA ENTIDAD Y DE LOS FIRMANTES

10.1 Me comprometo a informar de inmediato a la empresa emisora de la tarjeta de crédito cuando se produzca cualquier cambio en la información consignada en este formulario.

10.2 Autorizo a la empresa emisora de la tarjeta de crédito a verificar la información proporcionada en este formulario.

Firma del representante legal

Firma y código del empleado responsable que llenó el formulario

Firma y código del empleado responsable de la verificación de la información

Firma y código de quien autoriza la operación

BASE LEGAL:

Artículo 21 de la Ley Contra el Lavado de Dinero u Otros Activos, Decreto Número 67-2001 del Congreso de la República y 12 de su Reglamento, contenido en el Acuerdo Gubernativo Número 118-2002, de la Presidencia de la República.

ANEXO No. 03
Anexo para Solicitud de Tarjeta Adicional Persona o Empresa Individual

FORMULARIO IVE TC - 01

TARJETAS DE CRÉDITO

FORMULARIO PARA INICIO DE RELACIONES
- Persona o Empresa Individual -
Adendum

LUGAR:	FECHA (dd/mm/aaaa):

CUENTA TITULAR:

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		Profesión u Oficio:
Sexo	M ☐ F ☐			
5.4 Número de Identificación Tributaria (NIT):		País del NIT:		
5.5	Tipo de documento de identificación:	Número:		Lugar de emisión:
5.6	Dirección particular completa (calle o avenida, casa No., colonia, sector, lote, manzana, zona, municipio, departamento y país):			
5.7	Relación con el tarjetahabiente titular:			
5.8	Teléfonos:	5.89 Fax:		5.10 E-mail:
5.11	Nombre que desea en la tarjeta (26 caracteres como máximo)			

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

FIRMA DEL SOLICITANTE

Firma y código del empleado responsable que llenó el formulario

Firma y código del empleado responsable de la verificación de la información

Firma y código de quien autoriza la operación

BASE LEGAL:
Artículo 21 de la Ley Contra el Lavado de Dinero u Otros Activos, Decreto Número 67-2001 del Congreso de la República y 12 de su Reglamento, contenido en Acuerdo Gubernativo Número 118-2002, de la Presidencia de la República.

ANEXO No. 04
Anexo para Solicitud Tarjeta Adicional Persona Jurídica

FORMULARIO IVE TC - 02

TARJETAS DE CRÉDITO
FORMULARIO PARA INICIO DE RELACIONES
- Persona Jurídica -
Adendum

LUGAR:	FECHA (dd/mm/aaaa):

CUENTA TITULAR:	
NOMBRE DE LA EMPRESA:	

7. DATOS DE TARJETAS ADICIONALES QUE SE SOLICITEN

7.1 Primer apellido:	Segundo apellido:	Apellido de casada:

Primer nombre:	Segundo nombre:
7.2 Fecha de nacimiento (dd/mm/aaaa):	7.3 Nacionalidad:

7.4 Tipo de documento de identificación:	Número:	Lugar de emisión:

Sexo M ☐ F ☐	7.5 Número de Identificación Tributaria (NIT):	País del NIT:

7.6 Profesión u oficio:	7.7 Teléfonos paticulares

7.8 Dirección completa (calle o avenida, casa No., colonia, sector, lote, manzana, zona, municipio, departamento y país):

7.9 Cargo o relación que tiene con la entidad solicitante:

Nombre que desea en la tarjeta (26 caracteres como máximo)

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Firma del solicitante

Firma y código del empleado responsable que llenó el formulario

Firma y código del empleado responsable de la verificación de la información

Firma y código de quien autoriza la operación

BASE LEGAL: Artículo 21 de la Ley Contra el Lavado de Dinero u Otros Activos, Decreto Número 67-2001 del Congreso de la República y 12 de su Reglamento, contenido en el Acuerdo Gubernativo Número 118-2002, de la Presidencia de la República.

ANEXO No. 05
CONTRATO PARA USO DE LINEA DE CREDITO EN TARJETA DE CREDITO BANCO UNIVERSIDAD, S.A. CLASICA LOCAL, CLASICA INTERNCIONAL, ORO Y CORPORATIVA

Los suscritos, BANCO UNIVERSIDAD, S.A. que en este documento se denominará "BANCO UNIVERSIDAD, S.A." "El emisor", "El acreditante", representado por _____ y acredita su personería con acta notarial de su nombramiento faccionada en esta ciudad el ____ de_____del año____ por el notario_____ y esta debidamente inscrito en el Registro Mercantil General de la República, y _____, representado por _____ en lo sucesivo de este contrato se denominará "El acreditado", "El Tarjetahabiente", de _____ años de edad, /_____/, (estado civil)/_____/_____/_____/_____/ (nacionalidad) (profesión) (No. De cédula) /_____/ con domicilio en _____ (extendida en) con residencia en_____ quien actúa en su calidad de _____ de la entidad _____, lo que acredita con su nombramiento autorizado en esta ciudad, por el Notario _____ con fecha _____ inscrito en el Registro Mercantil General de la República al número _____ ( ), folio _____( ) del libro_____ ( ) de Auxiliares de Comercio, cuya sede social se encuentra ubicada en la _____, y _____ de _____ años de edad, /_____/,_____ (estado civil) (nacionalidad)_____/_____/_____/_____ (profesión) (No. De cédula) (extendida en) con domicilio en _____ con residencia en _____ lo que acredita con su nombramiento autorizado en esta ciudad, por el Notario _____ con fecha _____inscrito en el Registro Mercantil General de la República al número _____( ), folio _____ ( ) del Libro _____ ( ) de Auxiliares de Comercio, cuya sede social se encuentra ubicada en la _____ a quien en lo sucesivo de este contrato se denominará "El fiador " o "El garante mancomunadamente solidario", convenimos en celebrar el presente contrato de APERTURA DE CREDITO PARA EL USO DE TARJETA DE CREDITO, de conformidad con lo siguiente. PRIMERO: a) DEFINICIONES: Banco Universidad, Sociedad Anónima (Entidad Privada de Depósito y Crédito) denominada en este contrato "El Emisor" o "El Acreditante". Tarjetahabiente: Es la persona natural o jurídica titular de la tarjeta Visa de Banco Universidad, Sociedad Anónima, incluyendo a todas las personas autorizadas para hacer uso de la misma, durante un período establecido para el efecto por el emisor. Tarjeta: Es la Tarjeta de Crédito de Visa emitida por Banco Universidad, Sociedad Anónima, mediante la cual el tarjetahabiente puede adquirir bienes y servicios en los establecimientos afiliados a terceros y se clasifica en "Titulares y "Adicionales". b) APERTURA DE CREDITO. *BANCO UNIVERSIDAD, S.A.* abre un crédito en cuenta corriente hasta por la suma de _____QUETZALES (Q_____) al tarjetahabiente, para pagar por su cuenta bienes, servicios o numerario adquiridos mediante el uso de las tarjetas de crédito que el emisor emita a nombre del acreditado, o la o las personas por él autorizadas y que efectúe o efectúen a terceros o en los establecimientos afiliados, que mediante convenios celebrados para el efecto acepten las tarjetas emitidas por el emisor. El importe de la apertura de crédito podrá aumentarlo o disminuirlo BANCO UNIVERSIDAD, S.A. a su discreción, según el comportamiento y las necesidades del acreditado, para cuyo efecto bastará comunicación escrita en la que se indique el nuevo importe de crédito al acreditado y su fiador, a las direcciones aquí consignadas, en el entendido de que el nuevo importe del crédito, en caso de aumento, entrará en vigor cinco días después de la comunicación, a menos que el acreditado y su fiador soliciten por escrito que el aumento tenga efecto inmediato. En el caso de disminución del importe acreditado éste será siempre de efecto inmediato. Al importe de la apertura del crédito se le denominará "límite de crédito". SEGUNDO: DE LAS TARJETAS. Las tarjetas de Crédito (a las que podrá designárseles indistintamente como "tarjeta" o "tarjetas", según el caso) que *BANCO UNIVERSIDAD, S.A.* emita a favor del acreditado, para que –si es el caso- pueda hacer uso del presente crédito, tendrán las características conforme lo estipula el Código de Comercio. TERCERO: ENTREGA DE TARJETAS (PRIMERA O PRORROGAS) (TITULARES O ADICIONALES), el emisor entregará personalmente al tarjetahabiente las tarjetas o bien podrá enviárselas por correo certificado, mensajería privada, también podrá hacerse la entrega de la tarjeta o tarjetas por medio de pariente o familiar, o persona debidamente identificadas que residan en la dirección reportada en la solicitud o cualquier otra documentación en poder del emisor, en cuyo caso el tarjetahabiente se da por bien recibido de la o las tarjetas. Quedando obligado el tarjetahabiente a firmar la o las tarjetas al recibirlas, siendo responsable desde el momento de la entrega certificada, de las consecuencias que pudiesen derivar por la falta de firma. CUARTO: a) USO DE LA TARJETA: el tarjetahabiente podrá adquirir cualquier bien, servicio o efectivo en los establecimientos afiliados (mismos a los que podrá denominarse simplemente "establecimiento" o establecimientos" o "afiliados", según el caso) mediante el uso de la tarjeta, y desde ya el tarjetahabiente solicita, instruye y autoriza al emisor a pagar por su cuenta los cargos originados por el uso de la tarjeta incluyendo aquellos en los que no exista pagaré o documento firmado, debido al uso de la tarjeta por vía telefónica o por correo o mediante el uso de medios electrónicos o similares. Condición especial de este contrato la constituye el hecho de que, aunque el tarjetahabiente o tarjetahabiente adicional no hubiese firmado este contrato o el original se extraviare, el sólo hecho de que use la tarjeta, firmando un slip de compra o consumo, o exista un acuse de recibo de plástico firmado, presume la existencia de una relación contractual entre emisor y tarjetahabientes, en cuyo caso este último o últimos acepta o aceptan conocer y quedar obligados ante el emisor de todas y cada una de las obligaciones contenidas en este contrato, o copia simple del mismo. b) OBTENCIÓN DE EFECTIVO: El tarjetahabiente podrá disponer del efectivo, ya sea en las oficinas del emisor, en las de otras instituciones autorizadas por el emisor, o a través de los cajeros automáticos que el emisor tenga establecidos o en operación en sucursales de otras instituciones con las que el emisor tenga convenios, así como en equipos automatizados establecidos o en operación de otras instituciones que correspondan a sistemas mundiales para las tarjetas de crédito con los que el emisor tenga celebrados convenios al efecto o por cualquier otro medio que en el futuro habilite o contrate el emisor para este efecto. Lo anterior se hará teniendo en cuenta que el emisor queda relevado de toda responsabilidad en el caso de que por cualquier causa no pudiera prestar el servicio. Sin perjuicio de lo anterior, el tarjetahabiente queda obligado a dar aviso de inmediato y por escrito al emisor en los casos de retención de la tarjeta por parte del cajero automático. Asimismo, el emisor y la o las personas o entidades que presten el servicio, quedan exoneradas de toda responsabilidad, en caso de asalto o robo que pudiera darse en contra del tarjetahabiente en las áreas de acceso a este servicio o fuera de ellas. c) TARJETAS: TITULARES Y ADICIONALES. El emisor emitirá a nombre del tarjetahabiente una tarjeta titular, y además podrá emitir tarjetas a nombre de terceras personas designadas por el tarjetahabiente, mediante las cuales también puede usarse el presente crédito, las cuales serán tarjetas adicionales o suplementarias a cargo del acreditado, o el tarjetahabiente. c.1) OBLIGACIONES DE LOS TARJETAHABIENTES ADICIONALES: Los tarjetahabientes adicionales por ese solo hecho se obligan solidariamente con el tarjetahabiente principal, y el principal de igual forma con el adicional, a favor del emisor, por todas las obligaciones que se deriven del presente contrato. Si el tarjetahabiente adicional fuere menor de edad, el obligado en los términos de este

contrato por el uso de esta tarjeta, será el tarjetahabiente titular e igualmente el Fiador, en las condiciones, obligaciones y estipulaciones pactadas en este contrato. d) ESTADOS DE CUENTA Y OBLIGACIONES DE PAGO. d.1) Estado de cuenta. El emisor enviará mensualmente a la dirección registrada por el tarjetahabiente, el estado de cuenta cortado a un determinado día del mes, (día que se conocerá como "fecha de corte") en el que se indicará lo adeudado al emisor por cada uno de los conceptos que se detallarán en este punto y el saldo total. Los estados de cuenta serán enviados después de la fecha de corte, y se presumen recibidos por el tarjetahabiente quince días después de la fecha de recibido. El tarjetahabiente Titular o Adicional, se obliga a comunicar al Emisor cualquier cambio de dirección que hiciere, en el entendido de que si no le comunica tal cambio, se presume por recibido el estado de cuenta enviado por el emisor. Igualmente el emisor queda facultado para enviar al tarjetahabiente su estado de cuenta o cualquier otra información, a dirección diferente que le constare, a la registrada por el tarjetahabiente. El tarjetahabiente deberá presentar cualquier inconformidad u observación sobre sus estados de cuenta dentro de los quince días contados desde la fecha de corte, y sin ninguna objeción u observaciones recibida por el emisor dentro de dicho plazo, se presumirán totalmente aceptados los estados de cuenta por parte del tarjetahabiente. Si el tarjetahabiente no recibiere su estado de cuenta no lo exime de efectuar el pago correspondiente. d.2) Obligaciones de Pago. El tarjetahabiente queda obligado a pagar al emisor por los siguientes conceptos: 1) una suma anual por la emisión de cada tarjeta titular y una suma anual por la emisión de cada tarjeta suplementaria o adicional. Estas sumas serán determinadas por el emisor y comunicadas al tarjetahabiente al hacer entrega o enviar las tarjetas o estados de cuenta. 2) todas las sumas que el emisor haya pagado a los establecimientos por cuenta del tarjetahabiente; 3) la comisión fijada por el emisor sobre los consumos efectuados en establecimientos localizados dentro y fuera de la República de Guatemala; 4) la comisión fijada por el emisor sobre el numerario adquirido mediante el uso de la tarjeta, que será cargada al efectuar la operación; 5) intereses generados por el pago diferido de cuentas por consumos por el uso de la línea de crédito autorizada para utilización con la tarjeta cuya tasa libre y variable será fijada por el emisor, especialmente se obliga a pagar cualquier costo o intereses en concepto de sobregiro o exceso en el uso de la línea de crédito, cuyo monto o tasa será fijada al sólo criterio del emisor; 6) un recargo calculado a la tasa vigente sobre cargos no pagados en la fecha fijada para el efecto o amortizaciones no cubiertas también en la fecha correspondiente en el caso de pagos diferidos o de intereses. 7) recargo a la tasa fijada por el emisor sobre cargos, provenientes de consumos efectuados en el extranjero, si los mismos no son pagados en la fecha fijada como límite para ello; 8) recargo determinado por el emisor por cada documento de pago que sea rechazado. Cuando el tarjetahabiente en consumos locales cancele el saldo total de su cuenta, antes o en fechas de vencimiento no se le cobrarán intereses. Los porcentajes y sumas a cobrarse por los servicios consignados en el apartado (d.2) podrán ser variados por el emisor dando aviso de ello por cualquier medio que el emisor estime conveniente incluyendo el propio estado de cuenta, asimismo el emisor podrá crear nuevos cargos y cobros que el tarjetahabiente acepta a pagar desde ya. Aunque los mismos no estuvieren previstos en este Contrato o en algún otro documento anexo al mismo. QUINTO: OTRAS OBLIGACIONES DEL TARJETAHABIENTE: Además de las obligaciones contraídas por el tarjetahabiente por virtud de las diferentes estipulaciones del presente Contrato y de la ley que rige las relaciones contractuales, el tarjetahabiente especialmente se obliga a cumplir y a respetar las siguientes obligaciones a) firmar la tarjeta al momento de recibir la misma; b) notificar de inmediato y por escrito al emisor cualquier cambio en la residencia que ha señalado en el presente documento; c) efectuar todos los pagos derivados del presente contrato en los montos, tiempos y lugares que se estipulen en los estados de cuenta o avisos que para el efecto envíe el emisor, según el caso, d) custodiar, guardar y cuidar las tarjetas en forma diligente; e) no hacer uso de la tarjeta en un ámbito temporal o especial diferente al señalado en la misma; f) no hacer uso de la tarjeta cuando el emisor se lo indique mediante el envío de aviso escrito. SEXTO: PLAZO. El plazo del presente contrato será hasta de dos años contados desde la presente fecha. El emisor podrá prorrogar automáticamente dicho plazo por períodos iguales y sucesivos, prórroga que se manifestará mediante la emisión o envío de nuevas tarjetas y quedará aceptada por la recepción de las mismas. SEPTIMO: FORMA DE PAGO. el acreditado queda obligado a pagar al emisor las sumas que le aparezcan como saldos deudores en sus estados de cuenta, aún cuando el total sobrepase el monto máximo fijado en el punto primero (a este respecto si el tarjetahabiente excede de su línea o límite de crédito fijada o autorizada deberá pagar el sobregiro en la forma que el emisor le indique, sin perjuicio de los otros derechos de este como acreedor y mientras no lo pague será considerado en estado de mora con respecto a todo su saldo deudor), cualquier documento donde conste un límite de crédito variado que el originalmente solicitado y autorizado y que consta en este contrato, se tiene como parte de este contrato o sus prórrogas. Los pagos de las referidas sumas deberán efectuarse dentro de las fechas fijadas en los estados de cuenta, los consumos efectuados por el tarjetahabiente podrán pagarse por abonos mensuales fijados por el emisor. Los abonos mínimos y porcentajes podrán ser variados por el emisor en cualquier tiempo. Es entendido que los consumos realizados fuera del territorio de la República de Guatemala, deberán pagarse en la moneda que se indique en los estados de cuenta. OCTAVO: Los gastos extrajudiciales y judiciales que la aplicación de este contrato originen asimismo como el cobro de los adeudos derivados del mismo, serán por única y exclusiva cuenta del tarjetahabiente. NOVENO: IMPUESTOS Y OTROS GASTOS. Si se da el caso de que el emisor se vea obligado a incurrir en gastos de impuestos, retenciones, cargos, tasas, arbitrios o limitación de cualquier género y que corresponden al tarjetahabiente, éste deberá reembolsarlos. Así como cualquiera otro que se genere con motivo de este contrato será por cuenta y cargo del tarjetahabiente. DECIMO: FALTA DE ACEPTACIÓN DE LA TARJETA DE LOS AFILIADOS. "El emisor no garantiza que lo afiliados acepten en casos concretos el uso de la tarjeta que el tarjetahabiente presenta". En consecuencia, el emisor no incurrirá en responsabilidad, si algún afiliado negara al tarjetahabiente el uso de la tarjeta, aun cuando ello obedezca a error o negligencia. DECIMO PRIMERO: DIVERGENCIA CON AFILIADOS. Los derechos del emisor son independientes y autónomos, en consecuencia, no se verán afectados por divergencias en cuando a los negocios realizados por el tarjetahabiente y el afiliado. En consecuencia cualquier reclamo relacionado con los bienes o servicios recibidos deberá formularlo el tarjetahabiente directamente al afiliado, sin que ello lo excuse de su cumplimiento para con el emisor, especialmente de las obligaciones de pago. DECIMO SEGUNDO: DESTRUCCIÓN DE DOCUMENTOS. El tarjetahabiente autoriza expresamente al emisor para destruir los documentos que comprueban el uso de la tarjeta, una vez haya transcurrido el plazo convenido para la impugnación de estados de cuenta. DECIMO TERCERO: PROPIEDAD DE LA TARJETA. La tarjeta es de única y exclusiva propiedad del emisor y el tarjetahabiente únicamente la posee en calidad de depósito por lo que es responsable directo de su guarda, custodia y uso. En consecuencia al darse por terminado el presente contrato por cualquier causa, o al vencer el plazo de vigencia de la tarjeta deberá devolverla de inmediato al emisor, siendo responsabilidad del tarjetahabiente su destrucción y posterior entrega al emisor para su destrucción. El emisor está facultado a recuperar la tarjeta por cualquier medio legal a su alcance. DECIMO CUARTO: EXTRAVIO O SUSTRACCIÓN DE LA TARJETA. En caso de robo, extravío o sustracción de la tarjeta el tarjetahabiente queda obligado a dar aviso de inmediato y por escrito al emisor de tal circunstancia, a denunciar el hecho ante la autoridad competente y a presentar al emisor certificación de denuncia. El tarjetahabiente será responsable del uso que se haga de la tarjeta dentro de los quince días siguientes a la fecha en que haya dado aviso por escrito al emisor, quien

extenderá la constancia respectiva. El emisor resolverá sobre la reposición de la tarjeta y el costo de reposición será cargado al tarjetahabiente, dicho costo será establecido por el emisor en cada caso: además el emisor hará un cargo por los costos que conlleva tomar las medidas necesarias para prevenir el uso fraudulento de la o las tarjetas robadas, extraviadas o sustraídas, cargo que será determinado por el emisor en cada caso y que el tarjetahabiente deberá pagarlo de inmediato. DECIMO QUINTO: IMPUTACION DE PAGOS. Los pagos que efectúe el tarjetahabiente se aplicarán a discreción del emisor y cubrirá los siguientes rubros, sin orden de importancia: a) gastos de cobranza, b) intereses moratorios, c) comisiones y otros cargos d) cuota anual por emisión de la tarjeta, e) adeudo originado por el valor de los consumos efectuados usando la tarjeta, y f) a cualquier otra obligación, aún distinta a la que se origine de este crédito, que el tarjetahabiente tenga con BANCO UNIVERSIDAD, S.A. DECIMO SEXTO: PAGOS EN EXCESO. Si por cualquier razón el tarjetahabiente efectuare pagos en exceso de lo adeudado a determinada fecha de corte, el tarjetahabiente renuncia al cobro de intereses sobre las sumas pagadas en exceso y faculta al emisor para acreditar dichas sumas a futuros cargos a su cuenta, a discreción del emisor. DECIMO SEPTIMO: ACCIONES. Es entendido por el tarjetahabiente que el emisor le expide las tarjetas y le aprueba la apertura del crédito, en base a los bienes e ingresos y/o estado patrimonial que en la solicitud declaró tener y que si dichos bienes e ingresos disminuyeran, fueran grabados y objeto de demanda o fueran falsos, el emisor podrá además de dar por vencido este contrato y cobrar los saldos deudores en totalidad, ejercer las acciones civiles y penales que en derecho correspondan. DECIMO OCTAVO: RESCISION EXTRAJUDICIAL O VENCIMIENTO ANTICIPADO. El emisor podría dar por vencido el plazo original o el de las prórrogas del presente contrato en forma anticipada y sin necesidad de declaración judicial, si el acreditado dejara de cumplir cualesquiera de las obligaciones que impone el presente contrato o violara cualesquiera de las prohibiciones aquí establecidas, si los bienes o ingresos del tarjetahabiente o su fiador disminuyesen, falleciesen o cayesen en insolvencia, concurso, quiebra, fueran declarados en estado de interdicción o si fuesen objeto de demanda o embargo. Una vez vencido el plazo del presente contrato, el tarjetahabiente y las personas poseedoras de tarjetas adicionales quedan obligadas a no continuar usando las mismas a partir de la fecha que se indique en el aviso respectivo que el emisor les envíe, y estarán obligados a devolver de inmediato las tarjetas al emisor. DECIMO NOVENO: CESION DEL CREDITO. El emisor queda autorizado a ceder los créditos y demás derechos provenientes de este contrato, principales o accesorios, sin necesidad de aviso previo o posterior notificación al tarjetahabiente o a su fiador. VIGESIMO: FIANZA. Por su parte el fiador se constituye fiador solidario y mancomunado del tarjetahabiente para el cumplimiento de todas y cada una de las obligaciones que él mismo contrae en este acto y acepta expresamente las prórrogas que se convengan o sucedan aún sin noticia o consentimiento y agrega que la fianza estará vigente hasta que se encuentren totalmente cumplidas todas y cada una de las obligaciones afianzadas, aún después de vencido el contrato y desde ya renuncia en forma expresa al derecho de excusión en virtud de la solidaridad mancomunada y a cualquier otro derecho que pueda invocar frente al acreedor por su calidad de fiador. VIGESIMO PRIMERO: ADMINISTRACIÓN POR ENCARGO. El emisor podrá encargar total o parcialmente la administración de sus operaciones derivadas de la emisión de tarjeta de crédito a cualquier persona individual o jurídica y en dicho caso los derechos del emisor podrán ser ejercitados por dicha persona y las obligaciones del tarjetahabiente y su fiador podrían cumplirse con la misma persona. VIGESIMO SEGUNDO: RENUNCIAS Y OTROS PACTOS. a) el tarjetahabiente y su fiador aceptan como buenas y exactas las cuentas que formule el emisor acerca de este negocio y como líquido y ejecutivo el saldo que en cualquier tiempo les exija. En caso de ventilarse alguna cuestión o reclamación derivada del presente contrato, por vía judicial, el tarjetahabiente como el fiador y tarjetahabiente adicional renuncia al fuero de su domicilio y se someten a los tribunales que el emisor elija y señala la dirección indicada al principio, como lugar para recibir cualquier notificación, aviso, citación o emplazamiento judicial o extrajudicial, obligándose a comunicar al emisor de inmediato cualquier cambio de dirección para dichos efectos, aceptado en caso de no dar en esos avisos, como válidos cualquier aviso, requerimiento o notificación que les hagan en las direcciones que han proporcionado para los efectos de este contrato aún cuando hubiesen cambiado la misma; b) las partes aceptan el presente contrato y que el mismo será titulo ejecutivo suficiente para el cobro de las sumas debitadas por el emisor y de los intereses que en su caso se genere y cualquier otro cobro aquí pactado, o bien acta notarial en la que conste el saldo que existiere en la contabilidad del emisor, derivado de la tenencia y uso de la "tarjeta titular" o de cualquier "tarjeta adicional" o cualquier titulo bancario especialmente la constancia del saldo deudor que extienda la contabilidad de *BANCO UNIVERSIDAD S.A.,* saldo que se considera aceptado extrajudicialmente con base en los registros que obren en poder de *BANCO UNIVERSIDAD, S.A., c)* el tarjetahabiente y su fiador renuncian al derecho de invocar falta de mora si efectuaran abonos parciales sobre saldos vencidos, ya que la mora subsistirá hasta la total cancelación de los saldos vencidos, d) el tarjetahabiente y su fiador asimismo renuncian al requerimiento como condición para incurrir en mora y aceptan que la mora se constituye de acuerdo a lo estipulado en el Código de Comercio. e) el tarjetahabiente y su fiador renuncian al derecho de imputación de pagos y en caso de otras obligaciones en *BANCO UNIVERSIDAD, S.A.,* aceptan que este pueda aplicar al destino que juzgue más conveniente los pagos que se hagan; el deudor y su fiador autorizan a *BANCO UNIVERSIDAD, S.A.* para que pueda debitar cualquier cuenta de depósito bancario que lleven en *BANCO UNIVERSIDAD, S.A.*, las sumas que por cualquier concepto le adeuden a *BANCO UNIVERSIDAD, S.A.* sea que conste o no en este contrato. f) los contratantes aceptamos que cualquier nota, carta, correspondencia o comunicación escrita, telefónica, telegráfica, cablegráfica, vía Internet o cualquier otro medio de comunicación en los que se contenga o conste obligaciones para con el emisor, concedidas por este en alguna de las formas anteriormente mencionadas, se tienen como parte de este contrato o sus prórrogas y obligan al o los tarjetahabientes, y se tienen por incorporadas a este contrato automáticamente y si el emisor lo prefiere, por acta notarial o certificación contable, existan o no los originales o copias de los mismos. Así también aceptamos que cualquier obligación no prevista para el fiador o tarjetahabientes adicionales, se aplicarán las previstas en este contrato para el tarjetahabiente principal. g) los contratantes (tarjetahabiente, fiador y tarjetahabiente adicional), aceptamos el contenido de este contrato, lo leemos íntegramente, aceptamos, ratificamos y firmamos. En la ciudad de _____ del departamento de _____ el ____ del mes de _____ del año _____.

F) _____ F) _____

Por el emisor Tarjetahabiente Titular

F) _____ F) _____ F)_____

Fiador Tarjetahabiente adicional Tarjetahabiente adicional

En la ciudad de _____, del departamento de _____ el día _____ del mes de _____ del año_____ Como Notario DOY FE: a) que las firmas que anteceden son autenticas en virtud de haber sido puestas el día de hoy a mi presencia por los señores _____, persona de mi anterior conocimiento y quien firma en representación de Banco Universidad, Sociedad Anónima y los señores _____, quienes se identifican con las cédulas de vecindad números de orden_____ y de registros_____, extendida(s) por la(s) municipalidad(es) de _____, del (los) departamento(s) de _____, respectivamente. b) Las firmas que legalizo están contenidas en un documento privado que contiene un contrato de apertura de crédito para el uso de tarjeta de crédito. c) los signatarios firman nuevamente la presente acta de legalización juntamente con el infrascrito Notario.

F) _____ F) _____

Por el emisor Tarjetahabiente Titular

F) _____ F)_____ F) _____

Fiador Tarjetahabiente adicional Tarjetahabiente adicional

ANTE MÍ:

ANEXO No. 06
Documentación Complementaria Requerida para Solicitud de Tarjeta

Documentación Requerida	Clase de Tarjeta				
	Local	Inter.	Oro	Corp.	Plat.
Formulario IVE TC – 01	X	X	X		X
Formulario IVE TC – 02				X	
Fotocopia completa de cédula de vecindad del solicitante	X	X	X		X
Fotocopia completa de pasaporte (para extranjeros)	X	X	X		X
Fotocopia completa de documento que acredite condición migratoria (para extranjeros)	X	X	X		X
Estado Patrimonial y Estado de Ingresos y Egresos, con antigüedad máxima de tres (3) meses a la fecha de la solicitud. (créditos mayores a Q.50,000.00)		X	X		X
Estados de cuenta bancarios de los últimos tres (3) meses (original ó copia certificada) de todos los bancos donde maneje cuentas	X	X	X	X	X
Recibo cancelado del último mes de pago de luz, agua ó teléfono	X	X	X	X	X
Constancia de Ingresos para personas con relación de dependencia en iniciativa privada ó último codo de pago para empleados públicos	X	X	X		X
Carta de compromiso de pago (aplicable a colaboradores del banco)	X	X	X		
Últimas 2 boletas de pago (aplicable a colaboradores del banco)	X	X	X		
Estados Financieros correspondientes a los dos (2) últimos ejercicios anteriores y estados financieros al cierre del mes, con antigüedad no mayor a cuatro (4) meses previos a la fecha de solicitud (para propietarios de empresa individual, cuando el crédito sea mayor a Q.50,000.00)		X	X	X	X
Flujo de fondos proyectado para el período del financiamiento, firmado por funcionario responsable y representante legal				X	
Fotocopia completa de cédula de vecindad de (l) los Representante (s) Legal (es) (pasaporte si es extranjero)				X	
Fotocopia del primer testimonio de la escritura pública de constitución, debidamente registrada				X	
Fotocopia de acuerdo gubernativo u otro documento similar (en caso de Fundaciones, Iglesias, etc.)				X	
Fotocopia de Patente de Comercio (en caso de ser persona jurídica)	X	X	X	X	X
Fotocopia de Patente de Sociedad (en caso de ser persona jurídica)				X	
Fotocopia de carné ó constancia de inscripción en la SAT (en caso de ser persona jurídica)	X	X	X	X	X
Acta del Consejo de Administración autorizando al representante legal la solicitud de tarjeta de crédito en nombre de la empresa (si no se indica en el acta de nombramiento del representante legal)				X	
Carta del notario certificando el proceso de la constitución de la sociedad ó entidad, indicando qué persona será designada como representante legal (Sociedades ó Entidades en Formación)				X	
Fotocopia completa de documentos de identificación de los funcionarios responsables del manejo de tarjetas de crédito				X	

ANEXO No. 07
Perfil de la Persona Requerido para Solicitar Tarjeta de Crédito

	Clase de Tarjeta				
Condiciones Requeridas	**Local**	**Inter.**	**Oro**	**Corp.**	**Plat.**
Edad comprendida entre 18 y 65 años	X				
Edad comprendida entre 21 y 65 años		X			
Edad comprendida entre 24 y 65 años			X		
Edad Mínima de 30 años					X
Ingresos Mensuales Mínimos Q.1,800.00 para la capital ó Q.1,500.00 para Deptos.	X				
Ingresos Mensuales Mínimos Q.4,200.00 para la capital ó Q.3,500.00 para Deptos.		X			
Ingresos Mensuales Mínimos Q.14,000.00			X		
Ingresos Mensuales Mínimos Q.50,000.00					X
Estabilidad laboral mínima de 1 año ó 2 años en empleo anterior (de reconocido prestigio para extranjeros)	X	X			
Estabilidad laboral mínima de 3 años (de reconocido prestigio para extranjeros)			X		
Estabilidad de Domicilio mínima de 2 años, ó 2 años en domicilio anterior	X	X			
Estabilidad de Domicilio mínima de 3 años ó 3 años en domicilio anterior			X		
2 Referencias Familiares y 2 Referencias Personales	X	X	X		
Referencias Bancarias y 2 Comerciales (en caso de persona jurídica y comerciante)	X	X	X	X	
3 Años de Constitución				X	
Estabilidad de empresa mínima de 2 años (En caso de ser comerciante propietario)	X	X	X		
Condiciones Adicionales Requeridas, si posee cuentas en el Banco Emisor	**Local**	**Inter.**	**Oro**	**Corp.**	**Plat.**
Cliente Calificado con Categoría 1 (1/)					X
Cliente Calificado con Categoría 1 ó 2 (1/)			X	X	
Cliente Calificado con Categoría 1, 2 ó 3 (1/)	X	X			
Sin cheques rechazados en el último año					X
Máximo de dos (2) cheques rechazados por insuficiencia de fondos ó reserva de cobro en el último año hasta la fecha de la solicitud			X	X	
Máximo de tres (3) cheques rechazados por insuficiencia de fondos ó reserva de cobro en el último año hasta la fecha de la solicitud	X	X			
Saldos Promedio de Q.4,000.00 (en caso de ser persona extranjera)		X			
Saldos Promedio de Q.16,000.00 (en caso de ser persona extranjera)			X		

(1/) Referencias:

Categoría (1) = **Excelente Cliente**
Categoría (2) = **Muy Buen Cliente**
Categoría (3) = **Buen Cliente**

Para obtener la categoría de cliente, deben tomarse en cuenta varios factores, como por ejemplo, el movimiento de las cuentas, la reciprocidad con el banco, el saldo promedio, la cantidad de productos que posee en el banco, etc.

ANEXO No. 08
Proceso Revisión de Documentos en Expediente Físico

No.	Descripción de la Actividad	Responsable
1.	Recibe documentación de expedientes de crédito con acuse de recibido	Revisor y Verificador
2.	Verifica y ordena la documentación	Revisor y Verificador
3.	Revisa que la documentación esté completa y cumpla con todos los requisitos establecidos: • Si la información está completa, continua el proceso • Si la información no está completa, solicita que el expediente sea completado	Revisor y Verificador
4.	Verifica cuentas activas y pasivas del deudor y codeudor con la entidad emisora	Revisor y Verificador
5.	Consulta referencias en el Sistema ORBE e Información Pública.Net (deudor y codeudor), además del sistema que ofrece la Superintendencia de Bancos	Coordinador de Revisión y Cumplimiento
6.	Prepara informe de confirmación de datos y referencias efectuadas, según la información proporcionada y adjunta al expediente	Coordinador de Revisión y Cumplimiento
7.	Prepara expediente adjuntando consultas efectuadas y comentarios y lo remite al Coordinador de la Mesa de Servicio	Coordinador de Revisión y Cumplimiento
8.	Llevar control de los expedientes recibidos y trasladados a la sección de análisis de crédito, para que continúe su trámite	Coordinador de Revisión y Cumplimiento

ANEXO No. 09
Proceso de Análisis de Solicitud Tarjetas de Crédito

No.	Descripción de la Actividad	Responsable
1.	Recibe solicitudes confirmadas del Departamento de Tarjeta de Crédito para que sean analizadas	Analista de Riesgos
2.	Revisa en el expediente que la papelería esté completa con base en los requisitos para cada tipo de tarjeta y que reúna condiciones de legítima	Analista de Riesgos
3.	Revisa el formulario IVE-TC que corresponda, verifica que no tenga tachones ni alteraciones y que la información esté completa	Analista de Riesgos
4.	Evalúa las referencias crediticias que constan en el Sistema de la entidad (de haber tenido crédito anterior), además de iinformación pública; en el sistema central de Riesgos (ORBE) y en el sistema de la Superintendencia de Bancos • Si las referencias son satisfactorias, continua el proceso. • Si no son satisfactorias, se procede a conseguir aclaración ó explicación de los aspectos que hacen que no sean satisfactorias las referencias al Jefe de la Sección de Ventas del Departamento de Tarjeta de Crédito	Analista de Riesgos
5.	Analiza la capacidad de pago, Para personas individuales que laboran en relación de dependencia • Ingresos reportados. • Egresos reportados. • Tarjetas de crédito reportadas. • Préstamos vigentes. • Cargas familiares. Para comerciantes individuales • Consulta el análisis crediticio de la empresa Para empresas • Consulta el análisis crediticio de la empresa	Analista de Riesgos
6.	Analiza factores de riesgo, así: Persona individual • Renta de vivienda. • Estabilidad laboral y domicilio. • Sector de residencia. • Profesión u oficio. • Actividad, ubicación y referencias de la empresa donde labora Para comerciantes individuales • Consulta el análisis crediticio de la empresa Para empresas • Consulta el análisis crediticio de la empresa	Analista de Riesgos
7.	Emite su opinión con base en el análisis efectuado, dejando constancia de la resolución, en un dictamen	Analista de Riesgos
8.	Da trámite a las solicitudes trasladando los expedientes así: • Solicitudes que cumplen con los requisitos; referencias crediticias satisfactorias; reportan capacidad de pago; y, los factores de riesgo permitan recomendar la aprobación, se trasladan para convocatoria de comité de créditos • Solicitudes cuyas referencias no son satisfactorias; no reportan capacidad de pago; y, los factores de riesgo no permitan recomendar la aprobación, se trasladan al Departamento de Tarjeta de Crédito, par avisar al cliente • Solicitudes pendientes por algún requisito, se trasladan al departamento de Tarjeta de Crédito, para ser completados	Analista de Riesgos

ANEXO No. 10
Proceso de Aprobación de Solicitud de Tarjeta de Crédito por Comité de Créditos

No.	Descripción de la Actividad	Responsable
1.	Se presenta el caso ante los miembros del Comité	Jefe de Análisis de Riesgos
2.	Analizan los casos y toman decisión. • Aprueban la operación: Con la opinión favorable de todos los miembros presentes del Comité. (No obstante será admisible un voto en contra) • No aprueban la operación: (Con dos ó más opiniones en contra se rechazará) Razonan voto en caso de existir votos en contra, para hacerlo constar en el Punto de Acta correspondiente	Miembros del Comité
3.	Trasladan comentarios emitidos así: • Comité de Riesgos de Gerencia: A la Secretaría de Gerencia Financiera y de Riesgos • Comité de Riesgos de Consejo: A la Secretaría de Consejo de Administración	Jefe de Análisis de Riesgos

ANEXO No. 11
Proceso de Embosado de Tarjetas de Crédito

No.	Descripción de la Actividad	Responsable
1.	Traslado de plásticos vírgenes a la empresa encargada del embosado, con nota de envío adjunta.	Encargada de Control de Calidad y Bóveda 1/
2.	Recepción de plásticos vírgenes y nota de envío de parte de la entidad emisora de tarjetas y su posterior custodia.	Auxiliar de Custodia de Valores 2/
3.	Elaboración del archivo diario con la información de los registros a embosar, así como su transmisión electrónicamente, envío de copia en diskette y nota indicando el número de registros a embosar, a la empresa contratada para el efecto.	Analista Informático 1/
4.	Recepción de archivo electrónico, el diskette y nota de envío en la que se indica el número de registros a embosar, verificando el cuadre entre estos.	Encargado de Embosar 2/
5.	Embosado de plásticos vírgenes, según el archivo enviado.	Encargado de Embosar 2/
6.	Luego del embosado, imprimir el reporte de los registros procesados, para trasladarlo a la entidad emisora, conjuntamente con los plásticos, a fin de ser verificados por la misma.	Encargado de Embosar 2/
7.	Recepción de plásticos embosados, para su verificación y posterior custodia.	Encargada de Control de Calidad y Bóveda 1/

1/ Actividades realizadas por personal de la entidad emisora de tarjetas.
2/ Actividades realizadas por personal de la empresa encargada de embosar las tarjetas.

ANEXO No. 12
Proceso de Entrega de Tarjetas de Crédito

No.	Descripción de la Actividad	Responsable
1.	Ensobrado de tarjetas en los sobreflex especialmente diseñados, traslado al departamento de mensajería, para el envío directamente al cliente o a la agencia en la cual desea recogerla el mismo.	Encargada de Control de Calidad y Bóveda
2.	Localización del cliente o traslado a la agencia acordada, para la entrega de la tarjeta, en la cual le deben firmar en la nota adjunta al sobreflex.	Mensajeros
3.	Traslado de las notas de entrega debidamente firmadas a la sección de control de calidad, o devolución de las tarjetas no entregadas debido a la falta de localización del tarjetahabiente.	Mensajeros
4.	Adjuntar las notas de entrega de las tarjetas, en el expediente abierto para la emisión.	Encargada de Control de Calidad y Bóveda
5.	Verificar y confirmar el lugar donde el solicitante desea recibir la tarjeta que en un principio no se pudo entregar.	Encargada de Control de Calidad y Bóveda

ANEXO No. 13
Formulario de Gestión por Servicio para Tarjeta de Crédito

CENTRO DE ATENCION AL CLIENTE
FORMULARIO DE GESTIONES DE CREDITO

NOMBRE DE QUIEN ATIENDE LA GESTIÓN _____ **AGENCIA** _____

DATOS GENERALES

Apellidos _____ **Nombres** _____

Identificación: CEDULA / PASAPORTE **Número:** _____ **Medios de Contacto:** Tel. Casa _____

CODIGO(S) DE GESTION _____ Tel Oficina _____ Celular: _____

correo electrónico: _____

Número de Tarjeta _____ Fecha Gestión DIA _____ MES _____ AÑO _____

01. MODIFICACION DE LIMITE DE CREDITO

De:_____A:_____

Permanente ☐ Temporal (Dias) ☐☐☐

02. DEBITO A CUENTA MENSUAL

2.1 Adición (Cuenta) _____ 2.2 Eliminar ☐

2.3 Modificación(Nueva Cuenta) _____

03. CANCELACIONES

3.1Titular ☐ 3.2Adicional* ☐ 3.3 Al Vencimiento** ☐

04. SOLICITUD TARJETA ADICIONAL (Utilice Observaciones Para datos de envío del Plástico)

Llenar Addendum Formulario IVE Adjuntar fotocopia de Cédula completa del Solicitante Adicional Firmar Contrato para Tarjetahabiente Adicional al Anverso)

*Número de Tarjeta _____ **Vencimiento MES _____ AÑO _____

05. CAMBIO DE TIPO DE TARJETA

De:_____A:_____

06. SEGURO INTERVISA

6.1 Adición (Llenar Formulario) ☐ 6.2 Declinación ☐

6.3 Cambio (Llenar Observaciones) ☐

07. CANJE DE INTERPUNTOS

Cantidad _____

Establecimiento _____

Artículo(s) (Llenar observaciones)

Lugar de Entrega Certificado (Llenar Observaciones)

08. MODIFICACION DE DIRECCION CORRESPONDENCIA

Tipo de Dirección: Casa ☐ Trabajo ☐ P.O. Box ☐

_____

_____

_____

CODIGO POSTAL _____

09. CAMBIO DE NOMBRE EN PLASTICO (Indicar en Observaciones el Lugar de Entrega del Plástico)

Máximo 26 caracteres, llenar con letra de molde

Nombre en Plástico _____

10. REPOSICION DE TARJETA (Indicar en Observaciones el Lugar de Entrega del Plástico)

10.1 Deterioro ☐ 10.2 Pérdida o Extravío ☐ 10.3 Banda Magnética ☐ 10.4 Retenida ATM ☐

10.4 Robo ☐ Fecha DIA MES AÑO Hora: _____ País: _____

PERSONA QUE INFORMA SOBRE EL ROBO DE LA TARJETA _____

TELEFONO DE PERSONA QUE INFORMA SOBRE ROBO DE TARJETA _____

11. CAMBIO DE NOMBRE DE TARJETAHABIENTE

Adjuntar copia de Documento de Identificación, Llenar formulario IVE y actualizar información Utilizar espacio de Observaciones

12. CAMBIO DE AFINIDAD

Nueva Afinidad ☐

13. CAMBIO DE FECHA PARA EMISION DE ESTADOS DE CUENTA

Nuevo Día de Emisión ☐

14. RENOVACION DE CUENTA

Actualizar Información Financiera, Adjuntar Documentos

15. OTROS (ESPECIFIQUE)

OBSERVACIONES

Firma Tarjetahabiente | Resolución (A) (D) (P) | Firma Autorizada | Fecha DIA MES AÑO

ANEXO No. 14
Formulario de Gestión por Ajuste Operativo de Tarjeta de Crédito

CENTRO DE ATENCION AL CLIENTE
FORMULARIO DE AJUSTES OPERATIVOS

NOMBRE DE QUIEN ATIENDE LA GESTIÓN _____ **AGENCIA** _____

DATOS GENERALES

Apellidos _____ **Nombres**

Identificación: CEDULA / PASAPORTE **Número:** **Medios de Contacto:** Tel. Casa _____

Tel Oficina _____ Celular: _____

correo electrónico: _____

Número de Tarjeta _____ Fecha de Gestión DIA MES AÑO

001	**Compras**	002	**Retiros**	**USE CUADRO**	003	**Pagos**	**USE CUADRO**
	No Corresponde		No dispensó	A Y C		Aplicar por Débito a Cuenta	C
	Duplicada		Duplicado	A Y C		No Aplicado	C
	Aplicada por otro valor		Dispensó Monto Parcial	A Y C		Mal Aplicado	A Y C
	Fotocopia de Compra					Aplicado por otro Valor	A Y C

004	**Extorno de Cargos**	VALOR		005	**Modificación Interpuntos** C
	Membresia	_____	C		Saldo Actual _____
	Seguro Intervisa	_____	C		(+)Aumento _____
	Cargos por Financiamiento	_____	C		(-)Disminucion _____
	Cargos Moratorios	_____	C		Total _____
	Cargos por Sobregiro	_____	C		
	Cuota de Procesamiento	_____	C	006	**Traslado de Saldos** B
	Cheque Rechazado	_____	C		
	Gastos por Mora	_____	C	007	**Conversion de Saldos** B
	Otros (Especifique en Observaciones)	_____	C		Dolares a Quetzales ☐ Quetzales a Dólares ☐
	TOTAL	_____			**TIPO DE CAMBIO** _____

008 **Devolución de Saldo a Favor*** C

Q. _____ **$.** _____

DEPOSITAR A CUENTA _____

EMITIR CHEQUE ☐

***Se depositará a cuenta o emitirá cheque únicamente a nombre del tarjetahabiente**

009 **OTROS** _____ C

CUADRO A

Fecha Débito o Crédito	No. Referencia	Fecha Transacción	Establecimiento	Valor
DIA MES AÑO		DIA MES AÑO		
DIA MES AÑO		DIA MES AÑO		
DIA MES AÑO		DIA MES AÑO		
DIA MES AÑO		DIA MES AÑO		
DIA MES AÑO		DIA MES AÑO		

CUADRO B

Débito a Cuenta _____ Q. _____ $ _____

Crédito a Cuenta _____ Q. _____ $ _____

CUADRO C

OBSERVACIONES

ANEXO No. 15
Proceso de Atención de Gestiones de los Tarjetahabientes

No.	Descripción de la Actividad	Responsable
1.	Recibe el formato de gestiones de ampliación de limite de crédito y cambio de clase de tarjeta, para ser evaluadas.	Analista de Riesgo
2.	Solicita el expediente del tarjetahabiente para revisar qué información contiene y determinar si es necesario requerir algún documento adicional. • Si no hace falta información, continua el procedimiento. Si hace falta información se devuelve la gestión a la sección de cumplimiento, indicando la información a requerir.	Analista de Riesgo
3	Analiza en la forma siguiente: Ampliación de limite de crédito temporal ó permanente: • Capacidad de pago actual reportada. • Comportamiento de pago de la tarjeta de crédito que consta en la papelería trasladada. • Referencias crediticias trasladadas. Cambio de tipo de tarjeta: • Comportamiento de pago reportado en la gestión. • Referencias crediticias reportadas en la gestión. • Cumplimiento de los requisitos establecidos para la clase de tarjeta de crédito cuyo cambio solicita. • Sueldo actual y edad. Si posee cuentas en la entidad, verifica la categoría del cliente y lo imprime para dejar constancia en su dictamen.	Analista de Riesgo
4.	Da trámite a las gestiones así: • Gestiones que se recomienda aprobar, se trasladan al Departamento de Tarjeta de Crédito para la convocatoria del Comité. • Gestiones que no cumplen con requisitos, ó por algún motivo no es recomendable autorizar, se trasladan al Departamento de Tarjeta de Crédito para su archivo e informe sobre la resolución al Solicitante.	Analista de Riesgo

ANEXO No. 16
Reporte de Requisitos de Información

Numero de Cuenta

SI	NO	CUESTIONAMIENTOS
		¿Es el número de cuenta un número emitido en forma válida?
		¿Estaba la cuenta al día en el momento de ocurrir la transacción?
		¿Se hizo la validación de la fecha de vencimiento?
		¿Tiene el número de cuenta en cuestión un Valor de Verificación de Tarjeta debidamente codificado?
		¿Se ha certificado la transacción en cuestión y participa la tarjeta en el programa del Valor de Verificación de Tarjeta (CVV)?
		¿Validó usted el Valor de Verificación de Tarjeta como un valor correcto?

NOTA: *Si ha respondido afirmativamente a todas estas preguntas, proceda a la próxima sección.*

Tarjetahabiente

SI	NO	CUESTIONAMIENTOS
		¿Ha disputado el tarjetahabiente la transacción?
		¿Tiene el tarjetahabiente todas las tarjetas en su posesión?
		¿Firmó el tarjetahabiente una declaración jurada donde hace constar que la transacción no fue una transacción autorizada?
		¿Estuvo el tarjetahabiente de acuerdo en participar en el proceso judicial que se siga contra los sospechosos de perpetrar el fraude?

NOTA: *Si ha respondido afirmativamente a todas estas preguntas, proceda a la próxima sección.*

Transacción

SI	NO	CUESTIONAMIENTOS
		¿Se recibió la transacción en cuestión por medio del Modo de Entrada POS 90?
		¿Se reportaron todas las transacciones fraudulentas en esta cuenta a Visa como falsificaciones por medio del mensaje TC 40?

ANEXO No. 17
Glosario

Activación de Tarjetas
Un método alternativo que se utiliza al entregar las tarjetas con fines de seguridad. El Emisor espera a que el tarjetahabiente legítimo confirme que ha recibido la tarjeta antes de activar la cuenta. Las tarjetas se bloquean en el momento de enviarlas por correo y el tarjetahabiente debe llamar al Emisor para confirmar que ha recibido la tarjeta y corroborar con pruebas positivas su identidad.

Actividad semanal normal / Normal weekly activity
Parámetros establecidos por los Adquirentes para identificar y supervisar la actividad de transacciones de los comercios y detectar cualquier patrón poco usual o sospechoso en sus depósitos. Se requiere a los Adquirentes establecer parámetros de Actividad Semanal Normal como parte de las normas del programa de Supervisión de Depósitos de Comercios.

Administración de Capacidad de Autorización Positiva / Positive Authorization Capacity Management (PACM)
Un sistema electrónico de administración de autorizaciones que supervisa el número de solicitudes de autorización enviadas a cada Emisor. Cuando el número de solicitudes de autorización que está recibiendo el Emisor se iguala o supera su capacidad para responder a las mismas, el sistema dirige las transacciones de bajo riesgo al Sistema de Procesamiento de Respaldo de Visa (STIP).

Algoritmo del dígito de verificación MOD-10/ MOD-10 check-digit algorithm
La fórmula matemática estándar que se utiliza para crear y verificar la validez de los números de cuenta de las tarjetas de pago Visa.

Archivo de Excepción / Exception File
La base de datos mundial que mantiene Visa con los números de cuenta de las tarjetas perdidas y robadas y otras tarjetas listadas con instrucciones de recoger, referir u otro manejo especial. Los números de cuenta de todas las transacciones dirigidas al sistema de Procesamiento de Respaldo de Visa (Stand-In Processing System, STIP) se verifican contra el Archivo de Excepción.

Autorización / Authorization
La aprobación o denegación de una transacción efectuada con una tarjeta de pago. El comercio u otro Miembro solicita la autorización, que es otorgada o denegada por el Emisor.

Banda magnética / Magnetic stripe o Mag stripe
Una banda de cinta magnética que se coloca al dorso de todas las tarjetas de pago y en la cual se codifican los datos que identifican la cuenta según lo especificado en el Reglamento Operativo de Visa. En una tarjeta válida, la información de la cuenta codificada en la banda magnética coincide con los datos similares grabados en el frente de la tarjeta.

BASE I
Los sistemas de procesamiento de datos, redes y operaciones de VisaNet que brindan apoyo y proporcionan servicios relacionados con la autorización de las transacciones.

BASE II
Los sistemas de procesamiento de datos, redes y operaciones que utiliza VisaNet para brindar apoyo a los servicios relacionados con el intercambio, compensación y liquidación de las transacciones autorizadas.

BIN
Véase Número de Identificación Bancaria/de BASE.

Boletín de Tarjetas Canceladas / Card Recovery Bulletin
Listado internacional impreso de tarjetas perdidas, robadas, falsificadas y otras tarjetas que los Emisores radicados en otros países (fuera de Estados Unidos) han incluido con instrucciones de

recoger la tarjeta. El *Boletín de Tarjetas Canceladas* se imprime solamente para distribución fuera de Estados Unidos.

Captura electrónica de datos / Electronic data capture (EDC)
Un sistema electrónico que utiliza un terminal de captura de datos ubicado en el establecimiento comercial para registrar y autorizar las transacciones. Las transacciones autorizadas se guardan automáticamente y se procesan al concluir el día de trabajo, y los fondos se transfieren directamente a la cuenta del Adquirente, y después al comercio, dentro de un plazo de 48 horas.

Características de seguridad de la tarjeta / Card security features
Elementos alfanuméricos, visuales, de diseño y funcionales que se incluyen en una tarjeta de pago para garantizar la validez del plástico. Las dimensiones físicas exactas y la colocación de estas características en la tarjeta están especificadas en el Reglamento Operativo de Visa, y dificultan la duplicación exacta de los productos. Los comercios y Miembros verifican las características de seguridad de la tarjeta en el punto de transacción, a fin de confirmar la validez de la tarjeta y prevenir las transacciones fraudulentas.

Centro de autorización / Authorization center
Instalaciones que el Miembro establece internamente o en la sede de un tercero procesador para responder a las solicitudes de autorización de transacciones o adelantos de efectivo de los comercios u otros Miembros. Los centros de autorización también pueden responder a los referidos o llamadas “Código 10”.

Código 10 / Code 10
El término utilizado por los comercios y Miembros cuando llaman a un centro de autorización para informar que sospechan de una tarjeta, de un tarjetahabiente o de una transacción específica. Las llamadas Código 10 generalmente se transfieren directamente al Emisor para su manejo especial.

Comercio inactivo / Inactive merchant
Un establecimiento comercial que ha suscrito un contrato válido con un Adquirente pero no ha hecho ningún depósito de recibos de venta a su cuenta durante un largo tiempo.

Contracargo / Chargeback
Una transacción fraudulenta o de otro tipo por la cual no se ha recibido pago y la cual el Emisor devuelve al Adquirente. Dependiendo de las circunstancias, los Adquirentes podrían intentar devolver estas transacciones al comercio que originalmente las aceptó.

Contrato de Comercio / Merchant agreement
Un contrato entre el comercio y el Adquirente donde se establecen sus respectivos derechos, responsabilidades y obligaciones para participar en el programa de tarjetas Visa del Adquirente.

Copia de la banda magnética / Skimming
Un tipo de uso fraudulento en el cual los datos de una tarjeta emitida en forma válida se obtienen por medios ilegales y se utilizan posteriormente para efectuar transacciones fraudulentas en las cuales se lee la banda magnética.

Crédito / Credit
El reembolso o ajuste de precio que un establecimiento comercial acredita a la cuenta de un tarjetahabiente.

Control dual / Dual control
Un procedimiento de administración de riesgos en el cual el acceso a las áreas de alta seguridad tales como la caja fuerte u otros lugares donde se almacenan tarjetas de pago se controla mediante una cerradura, combinación u otro dispositivo de seguridad. Este procedimiento requiere la presencia de dos personas, cada una de las cuales tiene una llave o clave separada, o una parte de la combinación, para poder obtener acceso a dicha área de seguridad.

Digitación / Key entry
El uso de funciones manuales en el terminal de punto de venta o de captura electrónica de datos para ingresar la información de la cuenta en el punto de transacción, en lugar de pasar la tarjeta por el lector de banda magnética del equipo. La digitación es una característica frecuente en ciertos tipos de fraude como el uso fraudulento de números de cuenta.

Fraude de telemercadeo / Telemarketing fraud
Un tipo de uso fraudulento en el cual los perpetradores o sus cómplices hacen por teléfono ofertas falsas o inverosímiles de artículos o servicios como por ejemplo, joyas, vacaciones o premios en efectivo y "venden" los mismos utilizando técnicas para presionar y coaccionar al tarjetahabiente. En muchos casos el verdadero propósito del esquema es engañar al tarjetahabiente para lograr que proporcione el número de su tarjeta. Los perpetradores utilizan entonces estos números de cuenta para cargar transacciones fraudulentas.

Fraudes relacionados con cambios de dirección / Change of address fraud
Un esquema de fraude relacionado con solicitudes fraudulentas en el cual el perpetrador presenta un cambio de dirección y solicita una tarjeta adicional para la cuenta de un tarjetahabiente legítimo. El perpetrador utiliza entonces la tarjeta adicional para hacer cargos fraudulentos a la cuenta.

Grabación / Embossing
El proceso que se utiliza para imprimir la información del tarjetahabiente (por ejemplo, el nombre y el número de cuenta) en caracteres al relieve en una tarjeta Visa.

Holograma / Hologram
Una imagen dos dimensiones que da la impresión de ser tridimensional y que parece moverse al inclinarla de un lado a otro. El holograma de la paloma en vuelo es una de las características de seguridad que tienen todas las tarjetas Visa válidas.

Información de la cuenta / Account information
La información de la cuenta y de la transacción incluye los datos que son necesarios para procesar correctamente las transacciones con tarjetas Visa, incluyendo toda la información registrada en la tarjeta Visa por medios electromecánicos, o por otros medios.

Lavado / Laundering o Factoring
El procesamiento de recibos de venta pertenecientes a un comercio que no ha suscrito un contrato válido con un Adquirente por parte de un establecimiento comercial que sí ha suscrito un contrato válido. Independientemente de que los recibos procesados correspondan o no a transacciones fraudulentas, el lavado de recibos constituye una violación del contrato del comercio y trae como resultado la cancelación del contrato de afiliación.

Límite de piso / Floor limit
El importe de transacción por encima del cual se requiere al comercio llamar a su centro de autorización y solicitar una autorización por voz de la transacción. En Estados Unidos, el límite de piso se utiliza solamente en los comercios que no cuentan con terminales electrónicas, las cuales realizan automáticamente el proceso de autorización de todas las transacciones.

Límite de piso cero / Zero floor limit
Un límite de piso por un importe de cero. Los comercios que tengan un límite de piso cero están obligados a solicitar autorización para todas las transacciones. Todas las transacciones no autorizadas se contracargan.

Número de Identificación Bancaria/de BASE / BIN
Un número de seis dígitos que Visa utiliza para identificar a un Miembro o procesador para fines de procesamiento de autorizaciones, compensación y liquidación de las transacciones. Los primeros cuatro dígitos del Número de Identificación Bancaria/de BASE del Miembro también se imprimen como característica de seguridad en todas las tarjetas Visa válidas emitidas por el Miembro.

Orden por correo/teléfono / Mail order/ telephone order (MO/TO)
Negocios que obtienen una parte sustancial de sus ingresos por medio de ventas de mercancía o servicios por correo o teléfono. Estas transacciones frecuentemente se cargan a la cuenta de tarjeta de pago del cliente.

Panel de firma / Signature panel
La ubicación de la firma del tarjetahabiente al dorso de todas las tarjetas Visa válidas. El panel de firma es una cinta de color blanco que lleva impresa la Palabra Registrada Visa en tinta azul y en un patrón repetitivo inclinado a un ángulo de 45 grados. Una vez firmado el panel, cualquier intento para borrar o alterar la firma dañará o alterará visiblemente el patrón impreso con la Palabra Registrada Visa.

Personalizador / Personalizer
Una instalación en la cual la información del tarjetahabiente (en oposición a otras características de seguridad y diseño) se graba o codifica en las tarjetas. Los Miembros pueden contar con personalizadores internos o pueden contratar los servicios de un tercero.

Plástico en blanco / White plastic
Una tarjeta plástica del mismo tamaño que una tarjeta de pago válida a la cual se ha colocado una banda magnética falsificada. La tarjeta se utiliza para hacer cargos de transacciones fraudulentas. Los esquemas con tarjetas plásticas en blanco normalmente requieren la cooperación de un comercio que participa en la confabulación para cometer el fraude.

Procesamiento de Respaldo / Stand-In Processing (STIP)
Sistema de procesamiento de autorizaciones en línea de Visa que responde a las solicitudes de autorización de transacciones de los comercios cuando el Emisor no está disponible para responder o ha optado por permitir que Visa procese determinadas transacciones.

Programa de Información de Fraude / Fraud Reporting Program
Un sistema de compilación y procesamiento de datos desarrollado por Visa para reunir, compilar y analizar la información relativa a las transacciones fraudulentas confirmadas.

Recibo de transacción / Transaction receipt
Un registro electrónico o en papel de una transacción, o una copia del mismo. Los recibos se generan en el punto de transacción por medios manuales o a través del terminal de punto de venta o captura electrónica de datos.

Servicio de Autorización Positiva al Tarjetahabiente / Positive Cardholder Authorization Service (PCAS)
Un sistema de autorización electrónica que utiliza los límites especificados por los Emisores para determinar cuáles transacciones se pueden dirigir al Sistema de Procesamiento de Respaldo de Visa (STIP) para su autorización, y cuáles se deben dirigir al Emisor. Las transacciones con importes que estén por debajo de los límites especificados por el Emisor se dirigen al Sistema de Procesamiento de Respaldo (STIP) de Visa, mientras que las transacciones que sobrepasan estos límites se dirigen al Emisor.

Servicio Nacional de Alerta de Comercios / National Merchant Alert Service (NMAS)
Bases de datos nacionales que listan la información correspondiente a los comercios cancelados o de alto riesgo. El Servicio Nacional de Alerta de Comercios está disponible solamente en los mercados participantes de las regiones Asia-Pacífico, Europa, Oriente Medio y África y América Latina. Cada país cuenta con su propio servicio. Los Adquirentes ubicados en países que cuentan con el Servicio NMAS pueden consultar el listado para obtener información relevante antes de afiliar a un comercio.

Solicitud del comercio / Merchant application
Un formulario que utilizan los Adquirentes para obtener la información personal y financiera relacionada con un establecimiento comercial antes de suscribir un contrato de afiliación con el

comercio. Según lo especificado en el Reglamento Operativo de Visa, los Adquirentes determinan individualmente el diseño de la solicitud del comercio y el tipo específico de información que requieren en la misma.

Solicitud fraudulenta / Fraudulent application
Presentación de una solicitud para obtener una tarjeta de pago, la cual contiene información personal, financiera y otros datos falsos.

Solicitudes excesivas / Excessive applications
La presentación simultánea de varias solicitudes para obtener tarjetas de pago en un plazo de tiempo corto, particularmente cuando el crédito disponible en todas las tarjetas solicitadas supera la capacidad del solicitante para obtener crédito.

Supervisión de autorizaciones / Authorization monitoring
Sistemas electrónicos que utilizan los Miembros para estudiar las transacciones autorizadas en un determinado plazo (por ejemplo, un día, una semana o un mes) a fin de detectar cualquier señal que indique la posibilidad de actividad fraudulenta.

Tarjeta perdida o robada / Lost or stolen card
La categoría general de fraude que designa todas las situaciones en las cuales las tarjetas legítimas se pierden o son robadas mientras se encuentran en posesión del tarjetahabiente. Con la excepción de las categorías correspondientes a tarjetas no recibidas y solicitudes fraudulentas, las tarjetas perdidas y robadas tienen relación con la mayoría de las situaciones en las cuales se obtiene una tarjeta válida por medios ilegales.

Tarjetas No Recibidas / Not Received Items (NRI)
Pérdida o robo de una tarjeta de pago que se ha enviado por correo a un tarjetahabiente y no ha sido recibida por el mismo ni devuelta al Emisor.

Transacción / Transaction
El intercambio de bienes, servicios o fondos en efectivo entre un tarjetahabiente y un establecimiento comercial o Miembro.

Valor de Verificación de Tarjeta / Card Verification Value (CVV)
Un número de verificación único de tres dígitos que se codifica en la banda magnética de todas las tarjetas válidas. Este número se calcula aplicando un algoritmo—es decir, una fórmula matemática—a la información codificada en la banda magnética, la cual se verifica durante el proceso de autorización de la transacción.

Valor de Verificación de Tarjeta 2 / Card Verification Value 2 (CVV2)
Un número de tres dígitos que se imprime al dorso de la tarjeta Visa en un tipo distintivo de letra itálica inclinada hacia atrás. El número se posiciona al final del número de cuenta. El valor se calcula utilizando los datos de la cuenta y las claves de encripción únicas del Emisor.

Uso no autorizado / Unauthorized use
Un tipo de uso fraudulento en el cual los perpetradores, haciéndose pasar por el tarjetahabiente legítimo, cargan transacciones correspondientes a órdenes por correo y teléfono (MO/TO) a un número de cuenta. En la mayoría de los casos los números de cuenta utilizados en estas transacciones son válidos, pero los perpetradores los han obtenido por medios ilegales.

Uso fraudulento / Fraudulent use
Uso de un número de cuenta obtenido por medios ilegales, en oposición a una tarjeta, con la finalidad de efectuar una transacción fraudulenta. El término se refiere a una gran diversidad de esquemas de fraude en los cuales no es necesario tener la tarjeta física (por ejemplo, uso no autorizado, fraude de telemercadeo y fraude relacionado con la captura electrónica de datos o EDC).