ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Sistemas de Información Gerencial

APLICACIÓN Y USO DE HERRAMIENTA OPEN SOURCE DE DATA MINING PARA OBTENCIÓN PERFILES TRANSACCIONALES DE CLIENTES DE TARJETA DE CRÉDITO.

EXAMEN DE GRADO (COMPLEXIVO)

Previa obtención del grado de:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

GARY GLITTER RIVAS CARRILLO

GUAYAQUIL – ECUADOR

AÑO 2015

AGRADECIMIENTO

El agradecimiento de este presente trabajo es para Dios quien me da fortaleza y guía mi camino por el sendero del bien.

A todos los catedráticos de las Maestría en Sistemas de Información Gerencial XIII Promoción, les agradezco por las enseñanzas y conocimiento impartidos, necesarios para poder obtener este grado de Magister, en especial al Ing. Lenin Freire Cobo - Director del MSIG.

DEDICATORIA

A mis adoradas hijas Miriam Sofía y Luciana Valentina gracias por ser como son, por todo su amor y por todo su infinito entusiasmo.

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Lenin Freire
DIRECTOR MSIG

_____

Mg. JORGE RODRÍGUEZ
PROFESOR DELEGADO
POR LA UNIDAD ACADÉMICA

_____

Mg. CARLOS SALAZAR
PROFESOR DELEGADO
POR LA UNIDAD ACADÉMICA

RESUMEN

El área de Prevención y Control de Fraude Electrónico del Banco ABC con la finalidad de conocer de tener el adecuado conocimiento de sus tarjetahabientes, requiere determinar su perfil transaccional.

El perfil transaccional será de apoyo para la detención de las transacciones inusuales de los clientes, ya que este identificará las inconsistencias entre las transacciones actuales y las obtenidas de su perfil.

Actualmente no se dispone del perfil transaccional por cliente. Se generan alertas que representan inusualidad basados en análisis transaccional por comercio específico, giro de comercio, país, modo de entrada.

Estos “limites transaccionales” son revisados periódicamente según se vayan registrando los intentos o fraude.

Adicionalmente la Resolución de la Junta Bancaria JB-2014-3066 [1] exige que las instituciones financieras establezcan un perfil transaccional por cliente.

El mayor desafío que enfrenta la Gerencia de Prevención de Fraude Electrónico es mantener el equilibrio entre el control del fraude y el negocio, el principal reto es las transacciones con lectura de banda que de presentarse reclamos por parte de los clientes terminan siendo pérdidas para el banco emisor.

Para el presenta trabajo se utilizará una herramienta Open Source para la obtención de los perfiles transaccional de los clientes del Banco ABC.

[1] Resolución 3066 Junta Bancaria del Ecuador, http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2014/resol_JB-2014-3066.pdf, , fecha de consulta julio 2015

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

Banco Adquirente	Es el Banco que afilia los comercios.
Banco Emisor	Es el Banco que emite las tarjetas de crédito a los clientes y les asigna un cupo.
Contracargo	Es el inicio de una controversia, se solicita al Banco Adquirente que nos pague en base a los soportes y tipología del caso.
Controversia	Es el proceso mediante el cual se atiende un reclamo a través de los procedimientos estipulados en los manuales operativos de la franquicia.
Datawarehouse	Es un repositorio de datos corporativo que integra información de fuentes distintas y que ayuda para la toma de decisiones de la empresa.
MCC	Categoría del Comercio (Merchant Commerce Code).
Modo de Entrada	Es la forma en la que validó la tarjeta de crédito, durante la transacción.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El área de Prevención y Control de Fraude Electrónico del Banco ABC con la finalidad de conocer de tener el adecuado conocimiento de sus tarjetahabientes, requiere determinar su perfil transaccional.

El perfil transaccional será de apoyo para la detención de las transacciones inusuales de los clientes, ya que este identificará las inconsistencias entre las transacciones actuales y las obtenidas de su perfil.

CAPITULO 1

ASPECTOS GENERALES

1.1 Descripción del problema

El delito de fraude con tarjetas de crédito constituye un problema para los Bancos y para sus clientes, dado que ocasiona pérdida económica y de imagen, y desconfianza de clientes e inversionistas, esto puede implicar la disminución de las operaciones así como afectar futuros planes de crecimiento y expansión.

En la actualidad con la implementación de la tecnología EMV se ha reducido los fraudes por tarjeta presente, más si se combina la lectura del CHIP y el ingreso del PIN lo que da mayor seguridad a la transacción.

Mientras se continua con la implementación de los comercios que acepen CHIP se continua con la exposición a casos de consumos fraudulentos en los que como método de lectura de utilice la banda magnética.

Esto hace que el fraude migre a canales que no requieren la presentación de la tarjeta como el Internet, saltándose las seguridades que brinda el chip.

La Superintendencia de Bancos como ente regulador durante el año 2014 notifico al Sistema Financiero mediante resolución de la Junta Bancaria JB-2014-3066, cambios a la norma de Riesgo Operativo. Dentro de lo más

relevante consideramos que se encuentra la inclusión de un acápite exclusivo de Seguridad de la Información mismo que incluye las mejores prácticas a implementarse en esta materia.

4.3.5.13 Las instituciones establecer mecanismos que permitan registrar el perfil de cada cliente y procedimientos de control sobre sus comportamientos. Todas las transacciones que impliquen movimiento de dinero en el uso de canales electrónicos y de tarjetas se debe definir procedimientos para el monitoreo en línea, con el fin que se pueda permitir o rechazar de manera oportuna las transacciones que impliquen movimiento de dinero y que estos no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al tarjetahabiente mediante SMS, correo electrónico, u otro medio.

Actualmente el Banco ABC tiene categorizado a sus clientes por segmentos demográfico y socioeconómico que van relacionadas a nivel de ingresos, zona de vivienda, y en base a esto les asigna un cupo.

La categorización que se quiere determinar es en base a lo transaccional, es decir a su comportamiento usual o normal de compras, giros, montos, canales.

El perfil transaccional es importante ya que nos permitirá establecer los niveles transaccionales usuales o acostumbrados por los clientes.

EL perfil transaccional no es lo mismo que la categoría de la tarjeta o BIN, ya que no todas las tarjetas de un mismo BIN tienen un mismo o parecido comportamiento.

Corresponde al Área de Prevención de Fraudes Electrónico establecer los mecanismos para determinar el perfil de riesgos de los clientes del Banco ABC.

1.2 Solución propuesta

En este presenta trabajo se muestra la forma de implementar la obtención del perfil transaccional de los cliente de tarjeta de crédito del Banco ABC a través de minería de datos. Esto ayudará al área de Prevención de Fraude Electrónico a la tarea de disminuir el fraude sin afectar el negocio, brindando toda las seguridad a la transacciones legítimas y parar las transacciones que no fueran legitimas con un mínimo de falso positivo.

CAPÍTULO 2

APLICACIÓN DE TÉCNICA DE MINERÍA DE DATOS PARA LA OBTENCIÓN DEL PERFIL TRANSACCIONAL

2.1 Comprehension del negocio de tarjeta de crédito

La tarjeta de crédito es un medio de pago, esta es emitida por un Banco Emisor, el cual asigna al tarjetahabiente o cliente de tarjeta de crédito un cupo de acuerdo a las políticas de riesgos existentes.

El uso del cupo asignado a la tarjeta de crédito se hace a través de los comercios afiliados que acepten los pagos de la franquicia a la que pertenece la tarjeta de crédito.

Figura 2.1

Flujo básico de autorización de una compra con Tarjeta de Crédito

En el proceso de autorización mínimo Intervienen: el Tarjetahabiente, el Comercio, el Banco Adquirente y El Banco Emisor.

Cuando el tarjetahabiente realiza compras o pagos con su tarjeta de crédito asume la obligación de pagar los montos de estas transacciones, incluido intereses y los demás gastos de comisiones, así como de los avances de dinero obtenidos por medio de los cajeros automáticos.

Entre las franquicias más conocidas en el mercado ecuatoriano están: Visa, MasterCard, American Express, Diners Club.

Figura 2.2

Elementos de seguridad comunes de las tarjetas VISA [2]

[2] Características Básicas de seguridad de las tarjetas Visa, https://www.visaeurope.es/visa-para-comercios/seguridad/transacciones-visa/tarjeta-presente/como-reconocer-tarjetas-visa-electron, fecha de consulta julio 2015

2.1.1 Elementos de Seguridad del Plástico de la Tarjeta de Crédito

1. **Chip Inteligente**.

   Es un circuito integrado que contiene la información necesaria para transaccionar.

2. **Número de tarjeta en relieve o impreso.**

   Por lo general los números de tarjeta son de 16 números empiezan con 4 para VISA y con 5 para Mastercard.

3. **Imagen ultravioleta.**

   Es fluorescente cuando se sitúa la tarjeta bajo una luz ultravioleta, se muestra en el centro de la tarjeta.

4. **Holograma 3D.**

   Contiene un holograma 3D que da un efecto tridimensional cuando la tarjeta se la inclina, tiene forma cuadrangular con la imagen de la paloma Visa o MasterCard.

5. **Logotipo de la marca Visa o MasterCard.**

   Esta aparece en la esquina superior derecha, o esquina inferior derecha es una bandera azul blanca y dorada con el logotipo de la marca Visa.

6. **"V" de seguridad en relieve**

   Aparece la letra V para VISA y la M para las tarjetas Mastercard en relieve.

7. **Fecha de caducidad**

   Debe venir impreso la fecha de caducidad del plástico.

8. **Nombre del tarjetahabiente**

   Debe aparecer el nombre del titular de la tarjeta de crédito, si la tarjeta no es nominada puede aparecer algo como "Tarjeta Club", “Tarjeta Club”, etc.

9. **Primeros cuatro dígitos del número de Tarjeta**

   Estos deben igual que los primeros cuatro dígitos del número de la tarjeta.

10. **Elemento de seguridad numérico (CVV2, CVC2)**

    Es un número de tres dígitos que aparecen junto al espacio que es reservado para la firma del tarjetahabiente.

11. **Espacio para la firma del tarjetahabiente**

    Este espacio es para que el cliente firme. Se muestra en este espacio el logo "Visa" a modo de fondo.

2.1.2 Transacciones

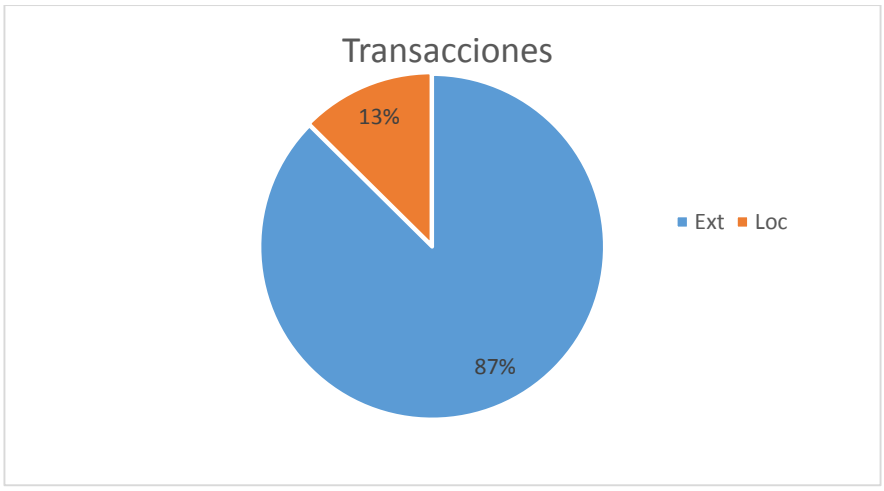
Basado en los elementos de seguridad de las tarjetas de crédito estas pueden ser procedas con los siguientes modos de entrada (Entry Mode).

- **01 Entrada Manual** (Tarjeta ausente), la información es digitada de manera manual principalmente Internet o rastrilladora manual la que se está descontinuando su uso.
- **05 Lectura de CHIP** (Presencia física de la tarjeta), se valida la presencia y lectura del chip, hasta el momento esta tecnología no es clonable, los casos que han existido son por fallas en la implementación de la misma.
- **90 Lectura de Banda Magnética** (Presencia física de la tarjeta), es la forma más común pero es susceptible a clonación por lectura y copia no autorizada de la banda magnética, hoy en día es de bajo costo los equipos para copiar y reproducir las tarjetas de banda.

Según la transaccionalidad analizada el 89% de las transacciones tiene origen en el Exterior y el 11% son de origen local.

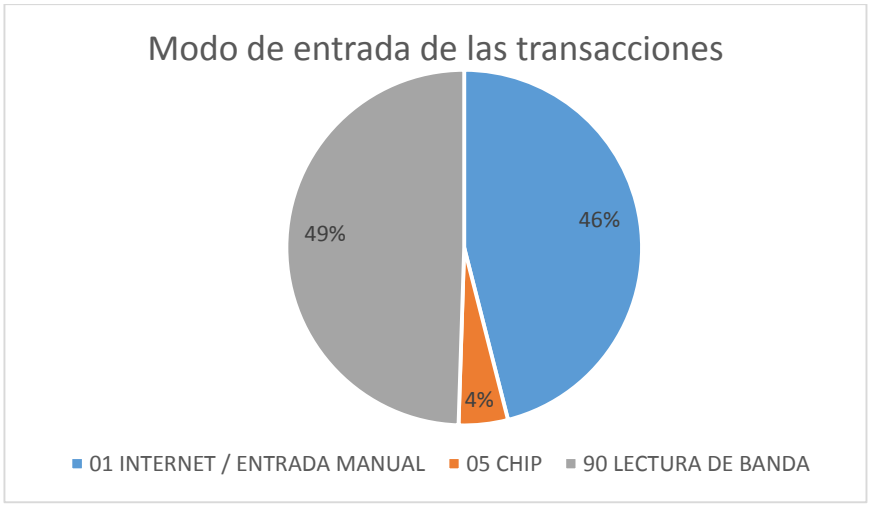
Según el modo de entrada el 49% es con lectura de banda, el 46% es de origen internet y 4% es con lectura de CHIP, la tendencia es que la lectura de banda sea reemplazada con la lectura de CHIP.

Figura 2.3



Transaccionalidad por origen Local/Exterior

Figura 2.4



Comparativo de los modo de entrada de las transacciones

Tabla 2.1 - Top 20 consumos en Internet

MCC	DESCRIPCIÓN DE CÓDIGO DE COMERCIO	%
7311	SERVICIOS DE PUBLICIDAD	17.6%
6300	VENTAS DE SEGUROS	8.7%
8220	UNIVERSIDADES, COLEGIOS PROFESIONALES	5.2%
4722	AGENCIAS Y OPERADOR DE TURISMO	4.6%
5942	LIBRERÍAS	3.4%
5699	ROPA-TIENDAS ESPECIALIDADES BOUTIQUE	3.4%
5719	TIENDA-AMOBLAMIEN. CASERO-ESPECIALIZ.	3.3%
7011	HOTELES,MOTELES,REFUGIOS Y HOSTERIAS	3.2%
4411	BARCOS DE PASAJEROS - CRUCEROS	3.1%
5621	ALMACEN DE ROPA PARA MUJERES	2.8%
5712	MUEBLERIAS Y ALM.PARA AMUEBLAR HOGARES	2.1%
4511	AEROLINEAS - TRANSPORTADORES AEREOS	2.0%
4816	INFORMACIÓN Y SERVICIOS DE COMPUTACION	1.7%
3052	LANCHILE	1.6%
6010	INST.FINANCIERAS-RETIRO MANUAL EFECTIVO	1.5%
5999	TIENDAS AL MINOREO - ESPECIALIDADES	1.4%
3010	KLM	1.4%
8699	ORGANIZACIONES DE MEMBRESIA	1.4%
5732	APARATOS ELECTRONICOS-ELECTRODOMESTI.	1.3%
3219	COPA	1.2%
	….	29.0%
	TOTAL	100.0%

Tabla 2.2 - Transaccionalidad por punto de entrada

Código País	Descripción País	01	05	90	Total
USA	United States of America	853,921	1,612	818,250	1,673,784
ECU	Ecuador	104,937	32,322	178,752	316,012
ESP	Spain	56,293	25,943	41,796	124,032

PAN	Panama	12,233	9,447	42,750	64,430
GBR	United Kingdom	49,616		1,959	51,575
PER	Peru	569	1,987	30,212	32,768
CHL	Chile	4,908	1,101	24,838	30,848
MEX	Mexico	7,570	2,070	15,743	25,383
COL	Colombia	4,731	1,363	18,897	24,991
ITA	Italy	7,076	7,741	8,189	23,006
NLD	Netherlands	7,593	1,837	4,541	13,971
BRA	Brazil	2,317	2,249	9,168	13,734
FRA	France	2,282	549	7,474	10,305
LUX	Luxembourg	7,838			7,838
IND	India	592		7,044	7,636
DEU	Germany	2,840	1,470	3,035	7,345
TUR	Turkey	206	7,041		7,247
CAN	Canada	3,857	238	3,114	7,209
HKG	Hong Kong, Special Administrative Region of China	726	6,264	207	7,197
CHN	China	33	1,032	6,072	7,136
ARG	Argentina	1,427		5,203	6,630
CHE	Switzerland	5,008	369	182	5,559
AND	Andorra	4,393			4,393
NOR	Norway	2,009		1,491	3,500
AUT	Austria	2,044		1,408	3,452
PRI	Puerto Rico	2,019		1,069	3,089
BEL	Belgium	806	1,120	833	2,759
PRT	Portugal	1,461	225	709	2,395
IDN	Indonesia	154	2,059		2,212
TCA	Turks and Caicos Islands	2,105			2,105
VNM	Viet Nam	761	1,103		1,864
ABW	Aruba			1,713	1,713
GRC	Greece		1,601		1,601
KNA	Saint Kitts and Nevis	1,506			1,506
DOM	Dominican Republic		462	876	1,339
CZE	Czech Republic	286		1,020	1,306
ARE	United Arab Emirates		1,002	235	1,237
GTM	Guatemala			1,135	1,135
DNK	Denmark	374		747	1,121
SWE	Sweden	54		932	986
IRL	Ireland	71		831	902

RUS	Russian Federation	46		637	683
POL	Poland			658	658
HUN	Hungary	531			531
URY	Uruguay	325			325
ISR	Israel			268	268
VAT	Holy See (Vatican City State)	66	152	22	240
MLT	Malta			197	197
CRI	Costa Rica			80	80
BHS	Bahamas			53	53
SGP	Singapore		22		22
Total general		**1,155,586**	**112,382**	**1,242,340**	**2,510,308**

2.1.3 Fraudes con Tarjetas de Crédito a Clientes

En la mayoría de casos el fraude de tarjeta de crédito se da cuando el tarjetahabiente entrega su tarjeta de crédito a un desconocido, cuando la extravía o le roban la tarjeta, cuando alguien intercepta el correo o se desvía, o cuando los empleados de un comercio usan un skimmer para copiar la banda magnética de la tarjeta o sencillamente anota los números de la tarjeta de crédito del cliente, código de seguridad y fecha de vencimiento del plástico. [3]

Con esto el delincuente puede:

- Hacer transacciones no autorizadas con los datos obtenidos de la la tarjeta de crédito de la víctima.

[3] Superintendencia de Bancos de Panamá, http://www.superbancos.gob.pa/documentos/temasfreq/Fraude_Tarjeta_Credito.pdf, fecha de consulta julio 2015

- Se reproducen tarjetas clonadas con la información de la banda capturada mediante los skimmers.

Skimming o clonación por copia de banda magnética, es hacer una copia de la información contenida en la banda magnética en un plástico diferente que puede lucir incluso parecido al original.

- Empleados deshonestos usan “skimmers" manuales que funcionan a pilas para robar la información contenida en la banda magnética y revenderlas a delincuentes.

Con esto los delincuentes usan esta información para crear tarjetas clonadas y con estos comprar artículos de gran valor.

El robo de identidad es el uso fraudulento de los datos personales como cedulas de identidad, carnet de conducir o fecha de nacimiento, para cometer fraudes de tipo financiero.

- La persona suplantada puede ser gravemente afectada en su reputación personal, ya que usan su identidad y demás información personal para estafar, haciendo compras, obtener acceso a créditos, los mismos que después caerán en mora.

- Es difícil para a victima de este tipo de fraude después comprobar que es inocente, ya que la información es en muchos casos solo conocida por el perjudicado.

Phishing es el envío indiscriminado de mensajes por correo electrónico haciéndole creer al destinatario que estos mensajes son de un origen verdadero, indicándole que se ha ganado un premio o bajo alguna amenaza quieren conseguir que la víctima entregue la información privada, como coordenadas y claves del banco.

- El Phishing tiene éxito porque los mensajes de correo electrónico parecen ser legítimos, contienen logotipos realistas y los sitios web, lucen muy parecidos a los reales. Hoy en día esta modalidad de fraude se ha convertido en una práctica muy ampliamente utilizada por delincuentes con el fin de robar la información personal de muchas personas.
- Se recomienda que no se abra estos correos electrónicos, y que no se proporcione ninguna información privada, como los números de su tarjeta de crédito, contraseñas, coordenadas, u otra información personal. Los bancos nunca piden información personal de esta forma.

- Si algún titular de cuenta da clic a los links, se los dirige a un sitio web falso con apariencia muy real donde por lo general les solicita números de tarjetas de crédito, contraseñas y demás información personal, en caso de entregar esta información es cuestión de pocos minutos, para que los delincuentes transfieren los saldos a otras cuentas o consuman los cupos usando las contraseñas y demás información proporcionada.
- Aunque usted tenga comunicación legítima vía correo electrónico con algún asesor de su banco nunca envíe información sensible de tarjetas de crédito crédito o contraseñas, porque estos no son seguros y la información puede ser interceptada o cambiada por los delincuentes. En su lugar, acuda en persona a la agencia más cercana, o use el sitio web oficial y seguro que proporcione el banco.

2.1.4 Resolución de un fraude por parte del Banco Emisor

Las franquicias tanto VISA como MasterCard tiene sus propios procedimientos para resolución de controversias, entendiéndose como controversia el proceso que se lleva acabo para resolver todo tipo de reclamo entre el tarjetahabiente y su banco emisor. Están catalogados los más comunes e incluyendo los que tiene que ver con temas de fraude.

Las controversias más comunes iniciadas por los Tarjetahabientes incluyen:

- Insatisfacción en la calidad de la mercancía o servicios recibidos.
- Falta de recepción de las mercancías o servicios.
- Transacciones cuestionables.
- Un procesamiento erróneo por parte del personal del Comercio Afiliado.
- Un uso no autorizado de una Tarjeta de Crédito.

2.1.5 Principales Restricciones para la Resolución

El uso no autorizado de una transacción donde la validación fue de la banda magnética (Entrada 90(no aplica a contracargo, por lo que de no pertenecerle al cliente sería una perdida para el Banco Emisor.

2.2 Entes de Control

Por un lado las franquicias es la que regula el cumplimiento adecuado de los procesos que norman el adecuado uso de la tarjeta de crédito, desde su emisión, procesos de autorización y atención de controversias.

Las franquicias controlan el nivel de transacciones no aprobadas, así como el nivel máximo de contracargo por fraude.

Por lo que el Banco Emisor debe asumir el riesgo hasta los niveles de exposición que sean seguros a fin de tener la menor cantidad de fraudes posibles y a la vez la mayor cantidad de transacciones autorizadas.

2.3 Herramientas Data Mining Open Source

Las franquicias ofrecen diversas herramientas que ayudan y dan asesoría en temas relacionadas a sugerencia de reglas a aplicar. Todas con altos costos de licenciamiento y muchas veces basados en la información de fraude de todos los bancos Emisores de su marca.

2.3.1 Que es Data Mining

Es el proceso extracción de información útil y no evidente de grandes bases de datos como lo son los “data warehouses” [4], es una tecnología que tiene un gran potencial para ayudar a las empresas a encontrar relaciones entre los datos encontrando respuesta y soluciones que de otra forma no son posible.

Claudio Palma en su libro Data Mining el arte de anticipar, haciendo una analogía lo compara a la música y nos dice: [5]

- Música » se escribe de forma extraña pero ilumina la vida.
- Data Mining » se escribe de forma extraña pero ilumina el negocio.

---

[4] Garrido Luis, Aplicaciones Empresariales de Data Mining, http://www.raco.cat/index.php/Questiio/article/download/27010/26844, fecha de consulta julio 2015

[5] Palma Claudio, Data Mining el Arte de Anticipar, RIL Editores, 2009

La acumulación de grandes volúmenes de datos diarios en las empresas auspició el nacimiento de una nueva forma de hacer negocios. Ahora, el cliente que antes era anónimo se hizo visible e identificable, permitiendo desarrollar servicios y atención más a la medida de sus necesidades particulares. Hoy las compañías se adelantan a los requerimientos futuros de sus clientes.

El registro online de información sobre la marcha del negocio está produciendo una acumulación progresiva de grandes masas de datos que, en sí mismos, son una fuente de riqueza para la propia empresa. En los comercio por ejemplo, segundo a segundo se registran los datos de cada venta: el local o agencia donde se realizó, el departamento, el usuario que atendió, el tipo de producto, su color, su precio, su tamaño, el medio de pago (efectivo, tarjeta o cheque). Y si el medio de pago fue tarjeta de crédito de la propia tienda entonces queda registrado sexo, edad y dirección del tarjetahabiente comprador, lo que a su vez permite conectar esta información con su límite de crédito y su comportamiento de pago.

Esta disponibilidad progresiva de grandes volúmenes de información detallada minuto a minuto está abriendo paso a la explotación de información exclusiva y confidencial, con el propósito de sacar ventaja comercial de ella. El uso comercial de la base de datos de una compañía permite limpiar la cartera de clientes de los malos pagadores, anticipar las conductas de riesgo de no pago, profundizar la relación con los diferentes segmentos y hallar

nuevas oportunidades para agregar valor al cliente y hacer nuevos negocios con él o con prospectos del mismo perfil.

El Data Mining surge como una nueva actividad propiciada por la revolución informática y la progresiva profesionalización del análisis computacional de datos. Vamos a pasos agigantados hacia una red de conectividad personal móvil total y permanente, acompañada de un comercio que enriquece sus conceptos de la mano del Data Mining. La informática ha producido un proceso de transformación tan vasto en la sociedad humana que aún no es posible comprender las posibilidades de sus límites los cuales están en constante expansión.

2.3.2 Usos del Data Mining

El Data Mining para generar nuevas oportunidades a un de negocio que posea un “datawarehouse “o base de datos de calidad, dada su capacidad para proporcionar información de relaciones entre los datos: [6]

Predicción de comportamientos.

Estos son tratados como problemas de clasificación. Un caso de marketing dirigido puede ser un ejemplo. Mediante técnicas de Data Mining basada en resultados de campañas anteriores de marketing se puede identificar el perfil de los clientes. De estos obtener la lista de los que son más propensos a

[6] Han Jiawei, Data Mining Concepts and Techniques 2nd Ed.,MK

comprar el producto en los próximos meses y de este modo enviar un correo dirigido en lugar de un correo masivo e ineficiente.

Predicción de tendencias.

Con técnicas de Data Mining se puede crear un modelo para predecir las tendencias. Por ejemplo se puede predecir los flujos de ventas en el futuro o pérdida de clientes. Basándose en información de base de datos históricas.

Descubrimiento de comportamientos desconocidos anteriormente. La visualización de clustering mediante técnicas de Data Mining permite descubrir nuevas y distintas relaciones entre los datos.

2.3.3 Técnicas de Data Mining

Los proyectos de Data Mining se realizan aplicando ciertas técnicas de interés en este campo, las más utilizadas son:

Redes Neuronales.

Se usan generalmente en problemas de clasificación y predicción, consisten en modelos no-lineales basados en las redes de neuronas biológicas.

Arboles de decisión.

Es un modelo de predicción en forma de árbol que representan conjuntos de decisiones capaces de generar reglas para clasificar datos o predecir sobre estos.

Algoritmos genéticos.

Son algoritmos inspirados en la evolución genética de las especies y que se aplican por lo general en problemas de optimización. Son la base y el futuro prometedor de la Inteligencia artificial.

2.4 Clustering.

Es un procedimiento de agrupación de una serie de datos que nos permiten clasificar datos según sus similitudes. El conocimiento de estos grupos son utilizados para entender similitudes naturales de entre distintos clientes en empresas o bancos

2.4.1 Selección de técnica y de herramienta

La técnica que se ha seleccionado es Clustering, es la que más se apega a lo que se requiere obtener como en este caso son los Perfiles Transaccional de los clientes.

La herramienta escogida para Data Mining fue “R” y su ventaja se debe a que es que gran parte de la comunidad académica está desarrollando modelos de análisis de datos muy interesantes en esta plataforma a disposición y alcance de todos en Internet.

2.4.2 Técnica de clasificación y clustering

Esta técnica tiene como finalidad ordenar o particionar fenómenos, a partir de gran cantidad de datos disponibles, en unidades más pequeñas que facilitan su administración, comprensión y entendimiento.

La implementación de esta técnica a datos de transaccionales, facilita la agrupación de los usuarios por su comportamiento transaccional.

CAPITULO 3

ANÁLISIS DE LA SOLUCIÓN DE DATA MINING

3.1 interpretación de los resultados

Para el presente análisis de información se utilizó datos de un solo BIN. Los parámetros utilizados fueron tarjeta de crédito/cliente, montos promedios, montos mínimos y número de MCC en los que se transaccionó.

Solo se consideró las transacciones aprobadas y las efectuadas con entrada 90 (lectura de banda), ya que de suscitarse un fraude cuando se hace con este modo de entrada representa una pérdida para la institución.

3.1.1 Código del Script de R.

```
##leer los datos
BD_Tarjetas<-read.delim("C:/Users/Admin/Documents/PROYECTO
ESPOL/BD_Tarjetas.txt")
## Análisis de Cluster
library(MVA)
library(clúster)
library(HSAUR2)

##Calcular disimilaridades
##Con base a la distancia euclidiana
Tarjetas_Clientes.diss<-daisy(BD_Tarjetas)
```

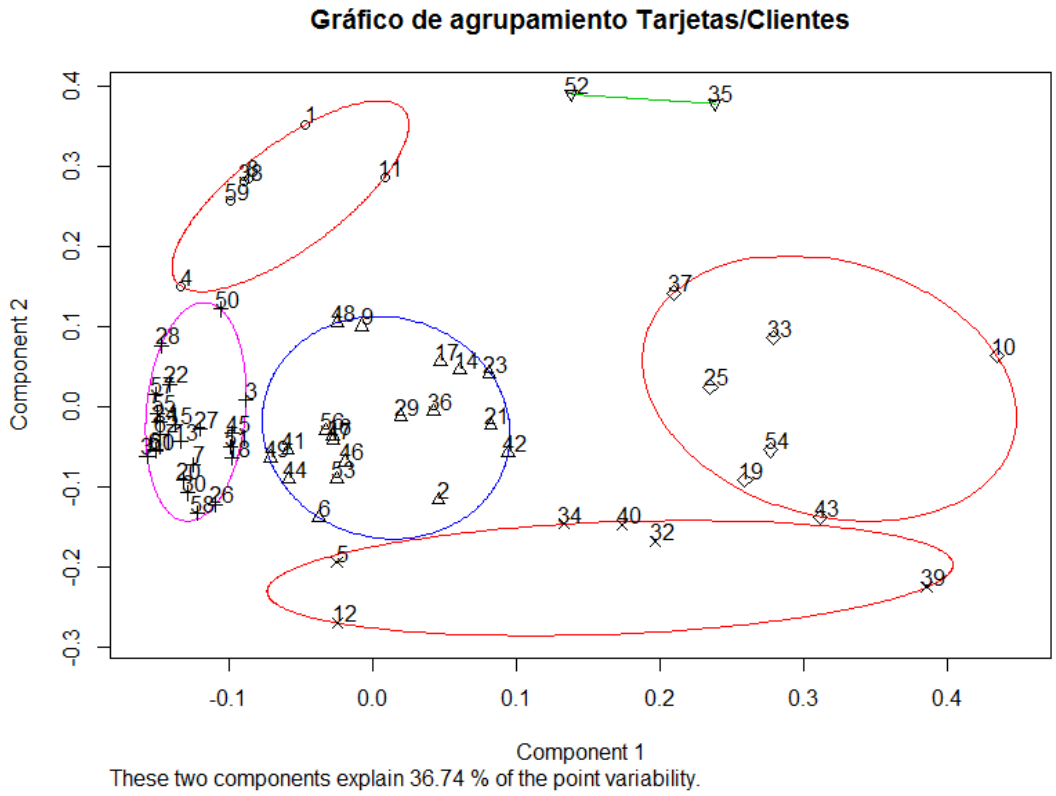
```
##Particionamos en 6 clúster a las Tarjetas/Clientes
##Usando la matriz de disimilaridades y solicitar la
componente clustering

##pam minimiza la suma de las disimilaridades
Tarjetas_Clientes.Cluster<-
pam(Tarjetas_Clientes.diss,6,diss=TRUE)$clustering
## Graficar los clusters identificando interactivamente los
puntos deseados
clusplot(Tarjetas_Clientes.diss,Tarjetas_Clientes.Cluster,main
="Gráfico de agrupamiento
Tarjetas/Clientes",span=TRUE,lines=0,shade=FALSE,diss=TRUE,col
or=TRUE,col.p="black",labels=3)

##Desarrollamos un clúster jerárquico sobre un conjunto de
disimilaridades
##Crear un objeto de clase hclust/método promedio
hc<-hclust(dist(BD_Tarjetas),"ave")
##Graficar el dendrograma correspondiente
plot(hc,main="Dendograma Tarjetas/Clientes(Método del
Promedio)",frame.plot=TRUE,hang=1)

##Desarrollamos un clúster por el método del Centroide
hc.centroide<-hclust(dist(BD_Tarjetas)^2,"cen")
```

```
##Graficar el dendrograma correspondiente para notar las
diferencias
plot(hc.centroide,main="Dendograma Tarjetas/Clientes (método
Centroide)",frame.plot=TRUE,hang=1)
```

3.3 Graficar los clústers identificando interactivamente los puntos deseados.

Se observa los seis clúster o perfiles obtenidos por la técnica.

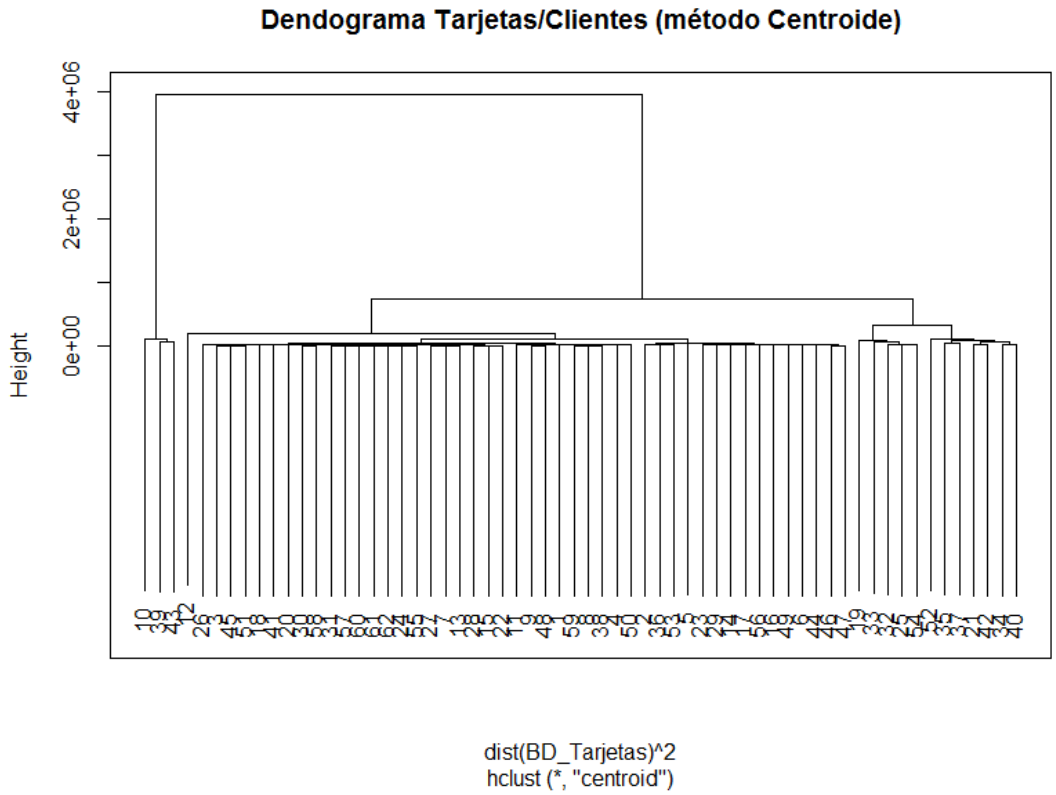
Figura 3.1



Grafica clúster

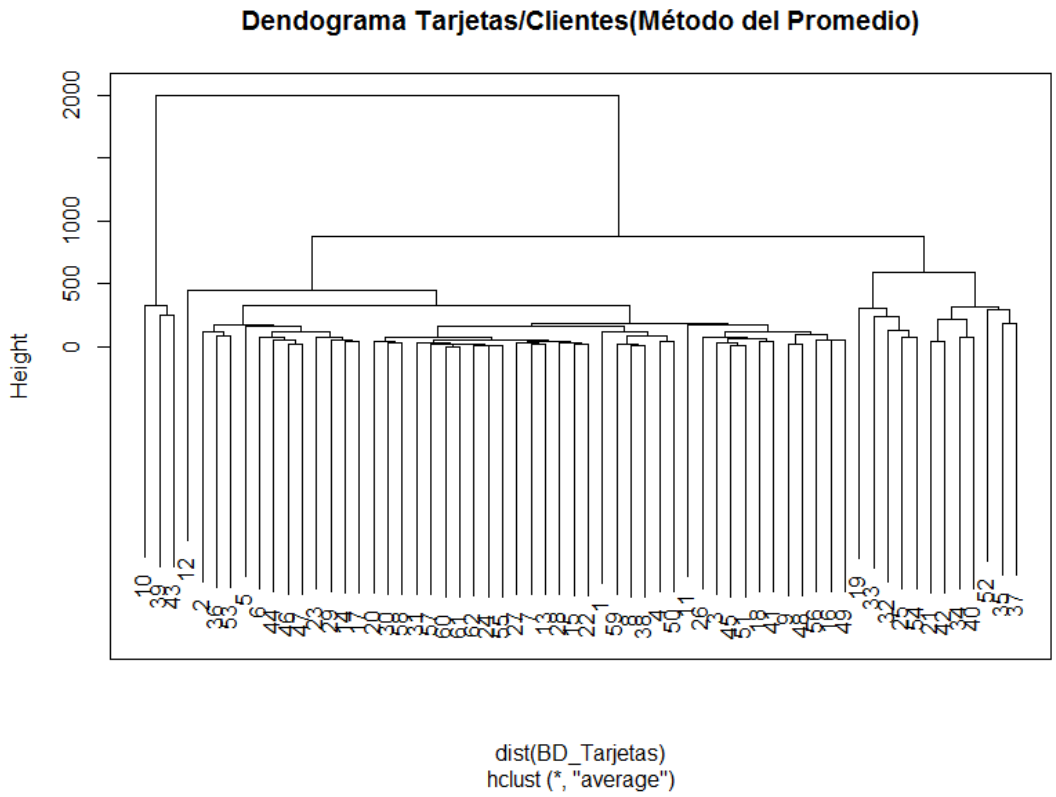
Adicional se generó dos graficas de dendrogramas con dos métodos:

Figura 3.2



Graficar el dendrograma clúster / método centroide

Figura 3.3



Graficar el dendrograma clúster / método promedio

3.3 Ventajas competitivas

La minería de datos está en constante crecimiento y su uso cada vez es más extensivo ya que provee percepciones claves que pueden ser utilizadas para:

- Mejorar el posicionamiento de la marca.
- Mejorar los productos y servicios
- Enfocar los procesos de negocio en los clientes de alto valor

- Resolver problemas difíciles
- Mejorar la relación con el cliente.

Es necesario que una visión de minería de datos este presente siempre en la empresa tomando en cuenta las capacidades que esta puede ofrecer:

- Elementos de datos bien definidos
- Habilidad en el tema al participar en un proyecto
- Datos y resultados históricos suficientes
- Clima organizacional que soporte la toma de riesgos
- Un problema bien definido
- Un equipo altamente capaz
- Herramientas con capacidad para el desarrollo del proyecto

3.5 Usos del perfil transaccional

Un uso común del perfil transaccional es el control de riesgo financiero, se recauda información de la transaccionalidad del cliente y utilizando mecanismo de reglas programadas otorga a cada tarjetahabiente un saldo disponible que pueda ser utilizado mediante su tarjeta de crédito. Se programa el sistema informático de la entidad para no dejar que el cliente gaste más de lo que tiene permitido. Para que no se sobre endeude más de

lo que la entidad ha decidido y que se enmarca dentro de su capacidad de pago.

Las entidades financieras guardan información sobre la transaccionalidad de sus clientes y en base a esta determinan cuales le corresponden según su perfil. Cada uno de los tarjetahabiente de la entidad financiera tiene asignado un perfil, esto lo enmarca en lo que se espera que sea su transaccionalidad normal, en términos cuantificables como tipos de transacciones, montos promedio, velocidad de compra, zona geográfica y crecimiento. El perfil puede comprender operaciones individuales o corresponder a tu rango de tiempo determinado, diario, semanal, mensual, semestral, etc.

Ya con su perfil asignado se inicia el seguimiento transaccional, que no es otra cosa, que comparar las transacciones realizadas con las del perfil asignado. Cuando esta transaccionalidad sobrepasa la que tiene como perfil a esta se la llama transacción inusual, el área de monitoreo es la que llama al cliente, gestiona la alerta, recolectar información y si no lo logra contactarlo determinar si es considerada la operación como sospechosa o inusual, con la finalidad de tomar acción inmediata sobre la misma.

CONCLUSIONES Y RECOMENDACIONES

Los gerentes de prevención de fraudes enfrentan el desafío creciente de mantener el equilibrio entre el control del fraude y el negocio. Al entender la conducta del tarjetahabiente, la distribución en segmento en base a su transaccionalidad le permite tomar mejores medidas y poder llegar a maximizar las ventas y a la vez cumpliendo con los niveles aceptables de pérdidas por fraudes.

Un adecuada segmentación hará que los tarjetahabientes ubicados en el rango de consumo mayor tenga menos negaciones y que a su vez los que menos transaccionan estén menos expuestos al fraude. El índice de fraude sobre ventas es un indicador básico que permite determinar si se están cumpliendo con los objetivos planteados.

Un estudio reciente realizado por MasterCard Advisors demostró el impacto de rechazar una transacción de forma incorrecta debido a una sospecha de fraude: [7]

El gasto general cayó en un promedio del 11 por ciento de los clientes afectados sobre el siguiente período de tres meses.

[7] Mastercard, http://www.mastercard.com/us/wce/PDF/SecurityMatters_2014.pdf , fecha de la consulta julio 2015

Casi el 20 por ciento de los consumidores no tenían gastos en los siguientes seis meses después del rechazo.

Para el presente proyecto la extracción de la información se la realizó desde la herramienta de monitoreo, la limpieza de datos se la realizó utilizando Excel y en ningún caso la información se la consolido en un datawarehouse por lo que a fin académico demostrativo cumple lo requerido.

La implementación de un datawarehouse como repositorio en donde residan los datos históricos le brindaría a este proyecto una mayor escalabilidad a futuro.

BIBLIOGRAFÍA

[1] Resolución 3066 Junta Bancaria del Ecuador, http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2014/resol_JB-2014-3066.pdf, fecha de consulta julio 2015

[2] Características Básicas de seguridad de las tarjetas Visa, https://www.visaeurope.es/visa-para-comercios/seguridad/transacciones-visa/tarjeta-presente/como-reconocer-tarjetas-visa-electron, fecha de consulta julio 2015

[] Superintendencia de Bancos de Panamá, http://www.superbancos.gob.pa/documentos/temasfreq/Fraude_Tarjeta_Credito.pdf, fecha de consulta julio 2015

[4] Garrido Luis, Aplicaciones Empresariales de Data Mining, http://www.raco.cat/index.php/Questiio/article/download/27010/26844, fecha de consulta julio 2015

[5] Palma Claudio, Data Mining el Arte de Anticipar, RIL Editores, 2009

[6] Han Jiawei, Data Mining Concepts and Techniques 2nd Ed.,MK

[7] Mastercard, http://www.mastercard.com/us/wce/PDF/SecurityMatters_2014.pdf , fecha de la consulta julio 2015