ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Sistemas de Información Gerencial

"IMPLEMENTACIÓN DE UNA HERRAMIENTA TECNOLÓGICA QUE PERMITA REALIZAR EL MONITOREO CENTRALIZADO QUE APOYE A LA PREVENCIÓN DEL FRAUDE PARA TRANSACCIONES DE INSTITUCIONES FINANCIERAS"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

PAULINA GENOVEVA MORENO COSTALES

GUAYAQUIL-ECUADOR

AÑO 2016

AGRADECIMIENTO

En primer lugar agradezco a Dios, que siempre ha estado a mi lado dándome fuerzas durante todo el proceso de la obtención del título, a mi hermana Adriana Genoveva Moreno Costales ya que muchas veces ella me dio el impulso que necesitaba para seguir adelante, a mi esposo amado, el cual ha sido un eje y ejemplo principal de superación y me ha dado el apoyo necesario cuando más lo necesitaba y desde luego a mis hijos queridos por su comprensión en los muchos momentos en los que no estuve presente.

DEDICATORIA

Dedico este trabajo a mi familia y padres, ya que siempre me comprendieron que el no estar presente no significaba falta de amor, sino más bien, la culminación de esta meta es la aplicación de los valores inculcados por mi padres y un ejemplo valioso para mis hijos.

TRIBUNAL DE SUSTENTACIÓN

MGS. LENIN FREIRE

DIRECTOR DE MSIG

MGS JUAN CARLOS GARCÍA P.

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El principal objetivo de este trabajo es mostrar que los sistemas de información sirven de gran apoyo a gestiones donde es necesario consolidar grandes cantidades de información de diferentes fuentes transaccionales, con un reto adicional, que por la naturaleza del proceso de monitoreo para la prevención de fraudes, esta información debe llegar a una base de datos centralizada en línea, para lograr de esta forma mantener procesos mucho más eficientes como por ejemplo el análisis de alertas con información real, antes de su puesta en producción, logrando así una excelencia operativa en el monitoreo para la prevención del fraude.

Según lo analizado, la implementación de un sistema de monitoreo para la prevención del fraude enfocado a Instituciones Financieras, es un proyecto de gran magnitud, por lo que este debe ser divido en fases para mostrar entregables a corto plazo.

Es muy importante el análisis del dimensionamiento de los recursos de hardware, por lo que es recomendable que para esto se tome un tiempo en la definición del alcance del proyecto y cantidad transaccional a alojar en los servidores, así como también la cantidad de procesos a ejecutarse en estos.

La plataforma tecnológica planteada debe convertirse en un aliado estratégico tecnológico que ayude a la preservación de los recursos de los clientes y gracias a la centralización de información poder aplicar métodos de Inteligencia de Negocios para la

mejora continua que den apoyo incluso a estrategias para nuevos servicios financieros a ofrecer a clientes.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Las entidades financieras en sus operaciones diarias, registran millones de transacciones utilizando diferentes canales transaccionales para los diferentes productos que ofrecen instituciones bancarias y conforme aumenta la cantidad transaccional y utilidad de los Bancos, también crece en forma proporcional el fraude para los clientes, ya que individuos no éticos, ven mayores oportunidades de perpetrar una apropiación indebida de fondos; en consecuencia, estos valores por fraudes se están volviendo cada vez más significativos y en muchas ocasiones aunque haya sido un descuido de clientes el origen del fraude, debido a leyes locales, el Banco está obligado a reponer el valor reclamado por el cliente.

Este hecho no solamente afecta a la institución por el valor de reposición del fraude perpetrado, sino también por cada caso que ingresa a observación interna, intervienen muchas áreas (Servicio al Cliente, Legal, Operaciones, Prevención de Fraudes, Seguridad física), lo que trae consigo carga operativa, la cual podría ser utilizada en actividades que realmente generen un valor frente a la prevención de fraude.

CAPÍTULO 1

GENERALIDADES

1.1 Descripción del problema

Como se mencionó inicialmente, las Instituciones Financieras ofrecen varios canales de transaccionalidad (Ventanillas, Banca Web, Cajeros Automáticos, Banca Móvil, Banca telefónica), estos generalmente manejan bases de datos independientes por cada canal, con cierta información registrada únicamente en tablas del servicio al que pertenecen, esto hace que realizar una labor de monitoreo centralizado y relacional se vuelva muy complejo.

Por ejemplo, un cliente transaccionando en ventanillas del Banco, no puede estar físicamente también realizando una consulta de saldos en un cajero automático del exterior; sin embargo al estar la información distribuida no es

posible relacionarla y alertar a personal operativo para que tome acción frente a la cuenta.

Independientemente a este hecho, el Organismos que regula al Sistema Financiero, en el año 2012, expidió una ley en la que se especifica la obligatoriedad de definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones [1].

1.2 Solución propuesta

Debido a la cantidad de canales actuales a disposición de clientes y su descentralización, se propone montar un proyecto por fases, que agrupe la información en un sólo repositorio central, conjuntamente con la implementación de una herramienta especializada en monitoreo para la prevención del fraude.

Dada a la naturaleza cambiante del fraude, es importante que dicha herramienta pueda ajustarse a las variaciones del entorno y permita definir reglas anti-fraude de manera proactiva y sin la dependencia de un área técnica especializada.

Se propone en primera instancia, montar el proyecto para centralización y monitoreo de transacciones para canales electrónicos como Banca por Internet, Banca Telefónica y Banca Móvil. Una vez atacado estos canales que han sido blanco de fraudes en los últimos dos años, la siguiente fase es centralizar la información que realiza el cliente en base a tarjetas de débito y crédito, cabe

mencionar que en el último año el fraude más común en estos canales (Falsificación de tarjetas), ha disminuido por el advenimiento de leyes que obligan a las Instituciones Financieras el uso de Chip integrado, el cual apoya al proceso de autenticación del cliente en caso de falsificaciones de tarjetas.

Es importante recalcar, que existe el reto de carga de la transaccionalidad en línea, sin afectar la operatividad general del core Bancario, así como también que el sistema a implementar para el monitoreo se ajuste a los requerimientos de las Instituciones Bancarias, con respecto al procesamiento de información segundos después de ocurrida.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 Análisis de bondades de una herramienta de monitoreo especializada en la prevención de fraudes.

2.1.1 ¿Por qué una Institución Financiera debe mantener herramientas para la prevención de fraudes?

La cadena de valor de una Institución Financiera gira alrededor de su capacidad de captar clientes para bridarles productos y servicios y así lograr el incremento de sus activos, este tipo de captaciones se convierte en depósitos, los cuales serán el instrumento financiero para realizar inversiones en el mercado bursátil que generen un rendimiento mayor, así como también permite al Banco realizar colocaciones a

clientes para ganar un interés, el mismo que debe estar regulado por entidades de control.

Los clientes depositan su dinero, bajo una premisa principal “La confianza que tienen en su Banco”, generalmente el rendimiento que reciban de sus inversión es secundario.

Frente a esto y a leyes de Organismos de Control, las Instituciones Financieras están obligadas a mantener mecanismos donde el cliente perciba no solamente que su dinero está seguro, sino que también, el Banco mantiene procesos internos que ayudan a precautelar los intereses de los depositantes, generando aún más la preciada confianza que busca el mercado financiero y ganar una buena imagen, que sirva, para aumentar sus captaciones y consolidarse entre los mejores en productos financieros en el país.

Como apoyo a la cadena de valor de las Instituciones Financieras, y debido a la cantidad transaccional es imperativo contar con un sistema de prevención de fraudes que alerte de situaciones no usuales o que no van acorde al perfil transaccional del cliente.

Los casos de fraudes más comunes en una Institución Financiera, las cuales se podrían detectar tempranamente con un sistema

especializado en prevención de fraudes son los que se muestran en la tabla 1[2]:

Tabla 1: Fraudes comunes en Instituciones Financieras

Tipo de Fraudes	Observación
Suplantación de identidad:	Falsificación de cédulas para realizar transacciones a nombre del cliente. Se hacen pasar por clientes legítimos presentándose en Servicio al Cliente, para solicitar transferencias de su propia cuenta a cuentas internas de terceros.
Phishing:	Por medio de mensajes de correo, que hacen referencia a páginas Web falsas, roban todos los datos de autenticación, incluso los datos personales de correo electrónico.
Falsificación de tarjetas de crédito:	Robo de la banda magnética para realizar transacciones con tarjeta presente.

Tipo de Fraudes	Observación
Robo de Información de emboce de tarjetas de crédito y códigos de seguridad	Toman foto del anverso y reverso de la tarjeta y con esto perpetran fraudes con tipo de tarjeta no presente.
Skimming:	Con dispositivos que graban la información de la banda magnética y la visualización de la clave, los malhechores en menos de una hora pueden llegar a obtener gran cantidad de víctimas de estafa financiera. Con la obligatoriedad de tarjetas con Chip, este tipo de fraude tiende a bajar.

2.1.2 ¿Qué aspectos fundamentales debe enfocarse en la elección de una herramienta automatizada para la prevención del fraude?

Para la elección de una herramienta enfocada en la prevención del fraude, para los principales productos que brinda una Institución Financiera, deberían analizarse los siguientes aspectos [4] [5]:

A. Aplicable a diferentes canales transaccionales

Los principales canales transacciones apetecidos para cometer fraudes son:

- Transacciones en cajeros automáticos
- Transacciones utilizando la Banca por Internet.
- Transacciones en ventanilla para realizar transferencias entre cuentas.
- A nivel de tarjetas de crédito:
    - Consumos con tarjetas falsificadas (Está disminuyendo por el uso del Chip), regresando a lo básico que es consumos con tarjetas robadas.
    - Consumos por Internet, robando información de emboce y códigos de seguridad de la tarjeta.

El producto que se elija debe ser lo suficientemente capaz de adaptarse a información que provenga de diferentes canales, considerando que los requerimientos de información para cada canal son distintos, así como también las estructuras de datos son diferentes de una Institución Financiera a otra.

B. Procesamiento en línea

Para que un proceso automático para la prevención de fraudes, sea eficaz y detecte el fraude de forma temprana, la información debe llegar a las estructuras de datos de monitoreo, inmediatamente ocurrida la transacción.

C. Bloqueo de transacciones

La plataforma de prevención de fraudes, en base a un análisis basado en patrones configurados por expertos en esta labor, debe brindar la capacidad de no procesar transacciones que cumplan las características previamente especificadas y poder activar y desactivar estas reglas cuando el usuario experto así lo solicite.

D. Canales para envío de alertas al cliente

Es importante incluir al cliente en la prevención del fraude, no solo para que sea informado de las transacciones que realiza, si no también que este pueda tomar una acción inmediata frente a transacciones no ejecutadas por estos.

Es importante que al momento de la evaluación se considere un medio móvil, que permita al cliente actuar de forma inmediata, tal como una App bajada en el celular que interactúe de forma inmediata entre el Cliente y la Institución Financiera.

E. Facilidad en definición de reglas

Las modalidades de fraudes son muy dinámicas, antes era el auge del Skimming a nivel de transacciones por cajeros automáticos, ahora es el cambiazo (engañan al cliente en los ATMS y cambian la tarjeta original por una falsificada, pero previamente ya han visualizado la clave) o por ejemplo ahora hay bandas organizadas que perpetran fraude, suplantando identidad y con esto ejecutan transferencias a cuentas recién aperturadas. A nivel de tarjetas de crédito muchas veces se realizan fraudes en países específicos y tipos de comercios bien definidos, como gasolineras; en consecuencia, el aplicativo de prevención del fraude, debe permitir al usuario final manipular reglas que se vayan adaptando al entorno cambiante y dinámico del fraude, sin depender del área de Tecnología o teniendo una dependencia muy puntual con ellos, pero en el proceso de definición de nuevas alertas el usuario experto en prevención del fraude debe ser quién manipule las reglas.

F. Pruebas de alerta previo a puesta en producción

El éxito de un proceso de prevención de fraudes, depende mucho que la cantidad de alertas que llegan a los analistas sean los suficientemente aceptables, para poder realizar un análisis óptimo y

rápido, es decir, mantener un nivel bajo de falsos positivos, pero ser óptimos en eficacia de alertas; en consecuencia la herramienta para la prevención del fraude, debe mantener opciones automáticas que permitan, al momento de activar una alerta analizar en base a un histórico la cantidad transaccional que esta generaría e ir afinado la regla hasta llegar a su optimización.

G. Estadístico de uso de transacciones

Posterior al uso del sistema, debería poder evaluarse la efectividad de las alertas configuradas, es decir, cantidad de transacciones que fueron alertas, de estas cuantas han sido descartadas y cuantas fueron realmente fraude, esto servirá finalmente para poder evaluar si la regla está siendo efectiva o definitivamente habrá que depurarla ya que genera muchas alertas y ninguna de las mismas se ha detectado como fraude.

H. Estándares PCI

Debido a que el sistema, debe alojar información de transaccionalidad de tarjetas de crédito, deberá mantener módulos que permitan enmascarar el número de la tarjeta y solamente mostrarlo, por necesidad del negocia a usuarios específicos y evento por evento.

I. Mantenimiento de una funcionalidad que permita realizar análisis predictivo del fraude.

Un punto fundamental al momento de diseñar o adquirir un aplicativo para la prevención del fraude, es que este adquiera conocimiento a través del aprendizaje transaccional de cada cliente.

En la detección de fraude, se debe recolectar información sobre las costumbres transaccionales de clientes, en base a la información histórica de cada una de sus transacciones y si sobre estos datos históricos la Institución tiene la capacidad operacional de diferenciar las transacciones que resultaron ser fraudulentas, también es un insumo importante al momento de predecir nuevas transacciones dolosas.

En tanto los criminales desarrollan nuevas formas de cometer fraude, el aplicativo debe responder rápidamente detectando las variaciones en el comportamiento de los clientes, y adicionalmente aprendiendo los nuevos patrones del fraude.

J. Flexibilidad de acoplamiento a las estructuras de datos propios de cada Institución financiera.

Si se piensa en la adquisición de una herramienta especializada en la prevención del fraude bancario, es importante analizar que no todas las Instituciones funcionan de la misma forma, por lo que sus estructuras de datos jamás serán las mismas, dicha herramienta debe tener la suficiente capacidad de acoplamiento a cualquier tipo de estructuras de datos.

K. Otros aspectos a evaluar al momento de contratación de una herramienta especializada en la prevención del fraude.

En caso de que la Institución decida adquirir una herramienta especializada en la prevención del fraudes, debe tener claro, que la herramientas debe ir acompañada de soporte local y mantenimiento tanto de hardware como de software, con niveles de servicio establecidos, ya que por una hora que deje de operar el sistema de monitoreo, se corre el riesgo de que malhechores incluso en contubernio con personal de la Institución, cometan delitos en contra de clientes y no pueda ser detectado de forma temprana.

2.2 Metodología de análisis a utilizar para dimensionamiento de Hardware a utilizar, que soporte el procesamiento en línea y su capacidad transaccional.

Para el dimensionamiento de hardware, para montar una herramienta de monitoreo en línea de transacciones, es importante tener lineamientos bases a cerca de la cantidad transaccional, sistema operativo a utilizar, motor de base de datos; así como también asesoramiento por parte del proveedor del sistema para que oriente a la Institución cómo su aplicación comparte el procesamiento de sus procesos.

La metodología a usar es la que se detalla a continuación:

- **A nivel de almacenamiento**

  1) Definir qué tipo de productos y servicios se requieren monitorear.
  2) Solicitar información transaccional de cada producto a monitorear para un mes habitual y un mes donde las operaciones sean muy altas.
  3) Estime la cantidad de registros a almacenar, como mínimo por un año.
  4) Considere un gap para tablas de clientes.
  5) Considere los mecanismos de contingencia a discos.

- **A nivel de procesador**

  Para poder dimensionar el procesador a utilizar seguir los siguientes pasos:

  1) Es importante analizar con el fabricante del aplicativo, su diseño al momento de ejecutar procesos de carga de datos hacia los servidores de base de datos del sistema de monitoreo, así como también los procesos de análisis de reglas a nivel del servidor de aplicaciones, esto dará una

pauta importante del diseño a nivel de hilos de procesos a utilizar y en consecuencia de procesador a adquirir para el buen funcionamiento del sistema.

2) Analice el motor de base de datos a utilizar y el sistema operativo sobre el cual correrá el aplicativo de monitoreo e investigue con el fabricante de los mismos la recomendación del procesador a utilizar.
3) Realizar una prueba de carga transaccional, “inyectado” a un servidor de pruebas, transacciones de un día pico, para los productos y servicios seleccionados para el monitoreo. Utilice hasta este momento un equipo con las características según el análisis realizado en los puntos anteriormente detallados.
4) Debido a que la naturaleza del aplicativo de monitoreo es almacenar la mayor cantidad transaccional, de la misma forma como lo hace el servidor de producción de la Institución Financiera, una buena práctica antes de tomar la decisión final, es analizar el recurso usado en producción, ya que podría llegarse a sobreestimar el dimensionamiento.

- **A nivel de memoria**

Cada vez que arrancamos un servidor, se inician una serie de procesos, el valor de la memoria a utilizar dependerá de las aplicaciones que tengamos desplegadas y de la carga del servidor. Así que es importante saber cuántos procesos se utilizan y cuanto ocupa la pila de cada proceso.

Para dimensionar la memoria RAM, se sugiere realizar los siguientes pasos:

1. Definir el sistema operativo a utilizar y basarse en la recomendación del fabricante en el dimensionamiento de la memoria.
2. Investigar con el fabricante del aplicativo de monitoreo la forma que dicho sistema hace uso de la memoria, y si mantiene un estudio de los procesos que utiliza dicho aplicativo y cuanto ocupa cada uno de estos.
3. En caso del servidor de base de batos que deben ejecutarse procesos de carga de datos de forma continua, investigue en ambientes de pruebas y mediante herramienta motorizadas, el uso de la memoria por estos procesos [3].

2.3 Propuesta de fases de implementación alineada a las necesidades del entorno de fraudes en el sistema financiero.

Aspectos básicos a considerar

Dado que generalmente un proyecto de implementación de un aplicativo de monitoreo para la prevención de fraudes es de gran magnitud, debe ser dividido en fases, las cuales sean más manejables y pueda darse entregables en un menor tiempo.

Adicionalmente, el orden de las fases mucho dependerá en la urgencia de cada Institución, sin embargo, la recomendación es iniciar por aquellos

productos/servicios donde se haya tenido mayores experiencias negativas de fraudes.

Es importante mencionar que existen aplicaciones especializadas en monitoreo de fraudes, por lo que es mucho mejor optar por este tipo de herramientas que tienen embebido conocimiento y experiencia para realizar el monitoreo y alertas tempranas para la prevención del fraude.

La propuesta de las fases de implementación son las que se muestran en la Figura 2.1:

Id.	*Nombre de tarea*	*Duración*	*Comienzo*	*Fin*
1	Análisis de datos a utilizar de clientes de la Institución	68d	17/02/2016	20/05/2016
2	Implementación de Sistema de Monitoreo para la Banca por Internet	118d	27/05/2016	08/11/2016
3	Implementación de Sistema de Monitoreo para tarjetas de crédito	110d	07/11/2016	07/04/2017
4	Implementación de Sistema de Monitoreo para tarjetas de débito	110d	07/11/2016	07/04/2017
5	Implementación de Sistema de Monitoreo para transacciones por ventanilla	110d	04/04/2017	04/09/2017
6	Implementación de alertas vía SMS y correo a clientes	109d	11/09/2017	08/02/2018
7	Implementación de modelos predictivos	89d	11/09/2017	11/01/2018
8	Implementación de comunicación bidireccional con el cliente	179d	11/01/2018	18/09/2018
9	Implementación de bloqueo en tiempo real de transacciones inusuales	69d	08/01/2018	12/04/2018

Figura 2.1: Propuesta de fases de implementación.

1. **Análisis de datos a utilizar de clientes de la Institución**

Para un sistema de prevención de fraudes, los datos de la ubicación del cliente es un punto importante para la operación, esta información debe tener una carga inicial y procesos de actualización bien definidos y exactos, ya servirá para que los analistas evalúen con el cliente, aquellas transacciones catalogadas como potenciales fraudes.

2. **Implementación de Sistema de Monitoreo para la Banca por Internet**

Debido a la disponibilidad del servicio transaccional en línea, este es uno de los principales focos de los atacantes, por lo que se recomienda que este sea uno de los primeros entregables.

3. **Implementación de sistema de monitoreo para tarjetas de crédito**

Aunque los emisores del Ecuador están obligados a utilizar tarjetas tipo chip, no todos los comercios y canales que utiliza tarjetas de crédito, están preparados para una transacción segura, por este motivo aún cuando la tarjeta este protegida bajo esta modalidad, el cual graba información única de autenticación del cliente, también se puede procesar transacciones con banda magnética, la cual es muy susceptible a falsificaciones y en este caso el monto del fraude sólo está limitado por el disponible del tarjetahabiente.

4. Implementación de Sistema de Monitoreo para tarjetas de débito

Aunque la obligatoriedad de uso de tarjeta con chip, han ayudado a disminuir el fraude por falsificación de tarjetas, sin embargo las estafas por este canal aún se mantiene, utilizando la modalidad de robo de la tarjeta, cabe mencionar que los Bancos manejan límites de cupos por día, lo cual ayuda detener fraudes a mayor escala.

5. Implementación de Sistema de Monitoreo para transacciones por ventanilla

Las transacciones por ventanilla, exigen controles como presentación de documentos como la cédula de identidad, libreta de ahorros, cheques, si bien es conocido que toda esta documentación es susceptible a falsificación o adulteración, los fraudes en este caso a nivel de volumen son pocos; sin embargo cuando logran obtener todo lo requerido, las pérdidas son significativas.

6. Implementación de alertas vía SMS y correo a clientes

El sistema en base a un enrolamiento previo y con información de su teléfono y correo electrónico, deberá ser capaz de enviar información de la transaccionalidad elegida por el cliente por cualquiera de estos medios.

7. Implementación de modelos predictivos

Una vez que se mantenga información de transaccionalidad, es posible predecir patrones transaccionales de clientes, lo cual permitirá dar pautas al usuario final sobre un posible fraude.

8. Implementación de comunicación bidireccional con el cliente

El discernimiento de una transacción fraudulenta determinada por el cliente y la ejecución de una acción inmediata desde su teléfono inteligente, supera la prevención del fraude incluso del mejor analista de fraudes de la institución. Este módulo es uno de los últimos en implementarse debido a que es importante que la información transaccional esté disponible en el sistema de monitoreo.

9. Implementación de bloqueo en tiempo real de transacciones inusuales

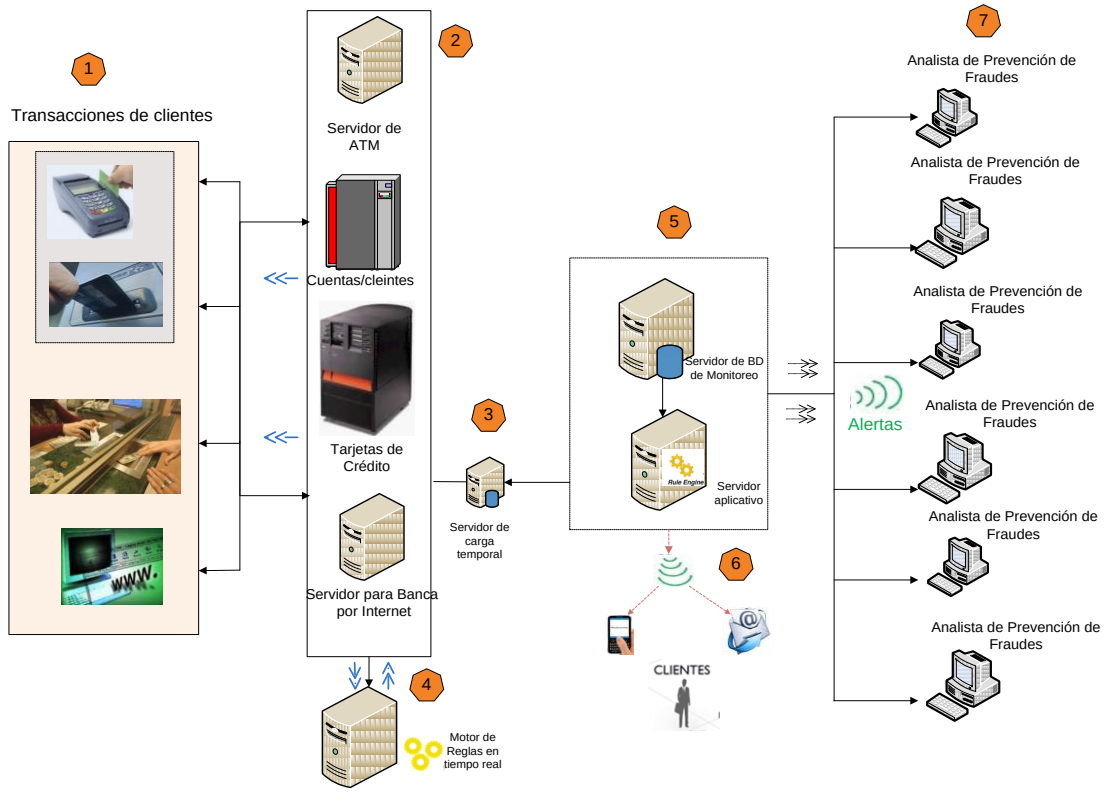
La naturaleza de este módulo, es no permitir transacciones que cumplen con parámetros específicos, por lo que, este es un módulo muy sensitivo y se recomienda que sea instalado una vez que el sistema haya estado en producción un año como mínimo y se conozca con certeza cuales son las alertas que tienen una muy fuerte probabilidad de ser un fraude; de no ser así no es recomendable activar alertas ya que pueden influir negativamente

en la imagen de la Institución Financiera y verse inmerso en una disminución del uso de productos y servicios por parte de clientes.

2.4 Metodología a utilizar para cargar la data desde diferentes ambiente transaccionales hacia un solo repositorio.

El objetivo de un sistema de monitoreo es concentrar la información de distintas productos y servicios de una Institución Financiera, es común que no toda esta información resida en un solo repositorio centralizado, sino más bien, la información necesaria para el monitoreo suele estar distribuida en diferentes servidores e incluso distintas plataformas tecnológicas.

De manera general la arquitectura típica, para implementar el servicio de monitoreo transaccional se muestra a continuación en la Figura 2.2 [4] [5]:



1 Diferentes canales de atención al cliente.

2 Procesamiento de la transacción en los servidores de la Institución Financiera

3 Servidor de carga intermedia, de las transacciones que se requieren para el sistema de monitoreo.

4 Servidor aplicativo, donde se instalará el motor de reglas que se avaluarán en “tiempo real”, cuya función es negar las transacciones que se encuentren bajo los parámetros configurados en dicho motor.

5 Servidor aplicativo y de base de datos que sirve al aplicativo de monitoreo transaccional

6 Servicio de mensajería SMS o correo hacia el cliente.

7 Usuarios finales del sistema de monitoreo.

Figura 2.2: Arquitectura general para el servicio de monitoreo transaccional.

La metodología propuesta para realizar la carga de datos es la siguiente:

- **Realizar un análisis del alcance a abarcar con el sistema de monitoreo para la Prevención de Fraudes.**

Es muy importante definir un alcance de los productos a monitorear y dentro de estos qué tipo de transacciones y alertas claves deberá atender el sistema para la prevención de fraudes, este análisis definirá la información requerida para la implementación del sistema.

- **Definir características del servidor que se usará para carga temporal de la información, que concentrará la data transaccional de los diferentes productos/servicios de la Institución.**

Debido a que generalmente las estructuras de datos son muy diferentes, entre la información propia del core Bancario y lo requerido para un sistema de monitoreo, es necesario que la información en primera instancia sea cargado en un servidor intermedio.

La data que reside aquí es de carácter temporal, ya que una vez transmitida a los servidores finales de la herramienta para la prevención de fraudes, dicha data puede ser borrada, es por esta razón que la capacidad y recursos del servidor intermedio no necesariamente son robustos.

Preferiblemente el servidor intermedio debe contar con un solo motor de base de datos, donde todos los aplicativos guardarán las tablas a utilizar para el monitoreo transaccional, es posible mantener dos, pero esto podría ocasionar latencia en los procesos de carga.

- **Instalación de los procesos de carga hacia las tablas temporales del servidor intermedio.**

  Por buenas prácticas, los procesos que se encargan de extraer la información de transacciones directamente del core, deben ser instalados en el servidor de carga temporal y desde aquí hacer la invocación hacia los diferentes servidores transaccionales, con esto se asegura de no afectar la operativa transaccional debido a un retardo en la carga de información para el sistema de monitoreo.

  Para todas las tablas transaccionales debe ser colocado un número secuencial que identifique cada registro, con el fin de llevar un control al momento de la carga a la base de datos del sistema de monitoreo.

  Todas las tablas cargadas en el servidor intermedio, deben de tener un campo adicional tipo “Bandera”, que ayude a marcar los registros una vez que estos sean transmitidos a la base de datos final del sistema de monitoreo.

- **Realice el mapeo de las estructuras del Core Bancario versus las estructuras del sistema de Prevención de Fraudes.**

  Como se mencionó anteriormente, aunque las Instituciones Bancarias pueden desarrollar un sistema de monitoreo transaccional, existen en el

mercado herramientas especializadas en el tema, estas herramientas cuentas con sus estructuras de datos estándares, la Institución Financiera deberá en gran medida acoplar su información a dichas estructuras, sin embargo como no todas las empresas funcionan de la misma forma, estas estructuras deben tener la capacidad de registrar información única de cada institución.

El acoplamiento de las estructuras de datos de la empresa a las del sistema estándar de monitoreo transaccional, es uno de los puntos más importantes para su funcionamiento adecuado, es aquí donde se debe definir donde se coloca la información que viene de cada estructura/campo del core Bancario hacia el sistema a implementar.

Como buena práctica se considera mapear en las estructuras de datos finales del sistema de monitoreo, solamente los campos necesarios para la operatividad del usuario final, ya que demasiada información podrá llegar a confundir en un proceso que debe ser muy dinámico, en caso de que se quiera mantener campos adicionales como respaldo, es preferible guardar en tablas adicionales en la base de datos; siempre y cuando las tablas no tengan mucho crecimiento en el tiempo.

- **Desarrolle procedimientos de carga para tablas transaccionales, en base al mapeo especificado en el punto anterior.**

Una vez que ya se cuenta con la información transaccional para el monitoreo en tablas intermedias y se sabe exactamente donde colocar cada estructura/campo en el nuevo sistema, se deben desarrollar procedimientos de carga hacia las bases de datos finales del sistema de monitoreo.

La metodología de desarrollo no es estándar, varía dependiendo de cada Institución, para este desarrollo es importante que para las tablas transaccionales se guarde en archivos propios de configuración del nuevo sistema, el último registro cargado, con el fin de mantener un control apropiado en los procesos de réplica.

Como buena práctica se considera para la salida a producción del sistema, tomar la información del repositorio temporal como máximo cada dos minutos, se puede bajar estos tiempos; sin embargo esto debe ser evaluado cuando el sistema ya se encuentre operando por un tiempo y se tenga valores certeros de la cantidad transaccional, ya que las lecturas muy consecutivas pueden afectar el rendimiento de la base de datos y finalmente verse reflejado en una lentitud en las operaciones para el usuario final.

- **Desarrolle procedimientos de carga de datos para tablas maestras y de parámetros, en base al mapeo especificado en el punto anterior.**

Adicionalmente a las tablas transaccionales, deben importarse tablas maestras y de parámetros, se debe de tomar en consideración no cargar de

procesos excesivos a la base de datos, por lo que debido a la naturaleza de datos, es recomendable actualizar esta data en proceso batch.

Estas tablas generalmente se clasifican en las siguientes:

- Tablas de parámetros en general.
- Registros de clientes
- Registros de teléfonos
- Registro de direcciones

Para estas tablas, debido a que no es posible contar con un campo secuencial, ya que no son tablas transaccionales, es importante desarrollar procesos que ayuden a controlar la data cargada en los repositorios finales del sistema de prevención, se recomienda utilizar un campo “Bandera”, que una vez cargada la información en las bases de datos del sistema de monitoreo, se marque este campos como “Cargado”.

Como consideración adicional, cuando se desarrollen los procesos de actualización de la información desde el core hacia las tablas intermedias, dichos programas deben marcar este campo “Bandera”, con un código de estado que indique que el registro se ha modificado, con esto se puede controlar que en la siguiente corrida del proceso batch la información será actualizada.

- **Desarrollar procesos de depuración de tablas intermedias.**

Una vez cargada la data en la base de datos final del sistema de monitoreo, puede ser eliminada de las tablas intermedias, la recomendación es que esta sea depurada en procesos batch diariamente, sin embargo en el momento de la salida a producción, este tiempo puede ser mayor e involucrar varios días para permitir validar la consistencia de datos entre el servidor temporal y la carga final hacia el sistema de monitoreo transaccional. La eliminación, debe basarse en el campo “Bandera”, definido en el párrafo anterior.

2.5 Diseño de la información principal a importar de forma centralizada ya sea en línea y en procesos Batch.

2.5.1 Prevención de Fraudes enfocado a movimientos de cuentas corrientes o ahorros de clientes.

En primer lugar, como se menciona en párrafos anteriores se debe tener bien definido los productos y servicios que se desean monitorear, en caso de que el alcance del proyecto, sea la prevención de fraudes para cuentas de clientes, básicamente se requieren cuatro grupos de información principal:

- Clientes
- Teléfonos y direcciones.
- Datos transaccionales.
- Cuentas Bancarias

- **Clientes, teléfonos y direcciones**

Es básicamente el registro de todos los clientes de la Institución, con su información básica.

Para este caso, estamos presumiendo que tanto la información de teléfonos y direcciones de los clientes, están en la misma estructura de información básica de este.

Esta tabla por su naturaleza debe ser actualizada en procesos batch de forma diaria.

Los campos básicos a importar por parte del sistema de monitoreo son los que se muestran en la Tabla 2:

Tabla 2: Estructura de datos de clientes.

Nombre Campo	Llave	Descripción
Numero_Cliente	X	Código de persona interno
Nombre		Nombre del cliente
Identificacion		Número de identificación personal del cliente
Tipo_Identificacion		Tipo de identificación del cliente
Fecha_Nacimiento		Fecha de nacimiento del cliente
Lugar_Nacimiento		Lugar de nacimiento del cliente
Estado_Civil		Estado civil del cliente
Profesion		Profesión del cliente
Genero		Género del cliente
Id_Nacionalidad		Código identificador de la nacionalidad del cliente
Fecha_Ingreso		Fecha de ingreso del cliente
Direccion		Dirección de localización del cliente
Tel_Oficina		Teléfono de oficina del cliente
Tel_domicilio		Teléfono de domicio cliente
Tel_Movil		Teléfono móvil del cliente
Email		Dirección de correo electrónico del cliente
Tipo_cliente		Identifica si es jurídico o natural
Oficial_cli		Identifica el código de ejecutivo asignado al cliente
Patrono		Nombre del patrono del cliente
Codigo_Sucursal		Código de la sucursal asociada al cliente
Codigo_Estado		Código del estado actual asignado al cliente
Es_empleado		Indica si el cliente es empleado de la entidad bancaria

Nombre Campo	Llave	Descripción
Monto_1		Campo tipo numérico, libre para adaptarse a la necesidad de la institución.
Monto_2		Campo tipo numérico, libre para adaptarse a la necesidad de la institución.
Monto_3		Campo tipo numérico, libre para adaptarse a la necesidad de la institución.
Codigo_1		Campo tipo alfanumérico, libre para adaptarse a la necesidad de la institución.
Codigo_2		Campo tipo alfanumérico, libre para adaptarse a la necesidad de la institución.
Codigo_3		Campo tipo alfanumérico, libre para adaptarse a la necesidad de la institución.
Codigo_4		Campo tipo alfanumérico, libre para adaptarse a la necesidad de la institución.
Codigo_5		Campo tipo alfanumérico, libre para adaptarse a la necesidad de la institución.
Codigo_6		Campo tipo alfanumérico, libre para adaptarse a la necesidad de la institución.
Codigo_7		Campo tipo alfanumérico, libre para adaptarse a la necesidad de la institución.
Codigo_8		Campo tipo alfanumérico, libre para adaptarse a la necesidad de la institución.
Codigo_9		Campo tipo alfanumérico, libre para adaptarse a la necesidad de la institución.
Codigo_10		Campo tipo alfanumérico, libre para adaptarse a la necesidad de la institución.

- **Datos transaccionales.**

Esta es la tabla donde se van a registrar las transacciones que vienen del Core de la Institución Financiera, como la idea es mantener centralizada la información de movimientos del clientes, esta tabla debe ser lo suficientemente adaptable a los diferentes productos y servicios, en consecuencia, deberán mantener campos adicionales “Libres”, para adaptarse a las diferentes tablas que provienen de varios aplicativos.

Esta tabla es muy importante que sea cargada en línea. La información básica de transacciones es la que se muestra en la Tabla 3:

Tabla 3: Estructura de datos de transacciones.

Nombre Campo	Llave	Descripción
Id_Transaccion	X	Identificador de la transacción
Codigo_Transaccion		Código de la transacción
Fecha_Hora		Fecha y hora en que se realiza la transacción
Numero_Cuenta		Cuenta al cual pertenece la transacción
Numero_Cliente		Número identificador del cliente
Numero_Documento		Número de documento que asocia la transacción
Referencia		Referencia complementaria de la transacción
Monto_Dolar		Monto de la transacción en dólares
Codigo_Moneda_Local		Código de moneda del país en el que se origina la transacción
Pais_Originador		País originador de la transacción, para caso de transferencias
Banco_Originador		Banco originador de la transacción, para caso de transferencias.
Banco_Beneficiario		Banco beneficiario de la transacción, para caso de transferencias.
Beneficiario		Persona o cuenta beneficiaria de la transacción
Codigo_Sucursal		Código de la sucursal en la que se realiza la transacción
Detalle_Transaccion		Descripción de la transacción
Id_Cajero		Identificador del Cajero que procesa la transacción
Saldo_Cuenta		Saldo de la cuenta luego de realizada la transacción
Fecha_Ingreso		Fecha y hora en que la transacción se registra en Sentinel
Numero_Cheque		Número del cheque asociado a la transacción.
Canal		Canal por el que ingreso la transacción al banco.
Monto_1		Campo configurable para ingreso de montos adicionales.
Monto_2		Campo configurable para ingreso de montos adicionales.
Monto_3		Campo configurable para ingreso de montos adicionales.
Monto_4		Campo configurable para ingreso de montos adicionales.
Monto_5		Campo configurable para ingreso de montos adicionales.
Monto_6		Campo configurable para ingreso de montos adicionales.
Monto_7		Campo configurable para ingreso de montos adicionales.
Monto_8		Campo configurable para ingreso de montos adicionales.
Monto_9		Campo configurable para ingreso de montos adicionales.
Monto_10		Campo configurable para ingreso de montos adicionales.
Codigo_1		Campo configurable, permite valores alfanuméricos
Codigo_2		Campo configurable, permite valores alfanuméricos
Codigo_3		Campo configurable, permite valores alfanuméricos
Codigo_4		Campo configurable, permite valores alfanuméricos
Codigo_5		Campo configurable, permite valores alfanuméricos
Codigo_6		Campo configurable, permite valores alfanuméricos
Codigo_7		Campo configurable, permite valores alfanuméricos
Codigo_8		Campo configurable, permite valores alfanuméricos
Codigo_9		Campo configurable, permite valores alfanuméricos
Codigo_10		Campo configurable, permite valores alfanuméricos
Codigo_11		Campo configurable, permite valores alfanuméricos
Codigo_12		Campo configurable, permite valores alfanuméricos
Codigo_13		Campo configurable, permite valores alfanuméricos
Codigo_14		Campo configurable, permite valores alfanuméricos
Codigo_15		Campo configurable, permite valores alfanuméricos
Codigo_16		Campo configurable, permite valores alfanuméricos
Codigo_17		Campo configurable, permite valores alfanuméricos
Codigo_18		Campo configurable, permite valores alfanuméricos
Codigo_19		Campo configurable, permite valores alfanuméricos
Codigo_20		Campo configurable, permite valores alfanuméricos
Fecha_1		Campo configurable para ingreso de fechas adicionales.
Fecha_2		Campo configurable para ingreso de fechas adicionales.
Fecha_3		Campo configurable para ingreso de fechas adicionales.
Fecha_4		Campo configurable para ingreso de fechas adicionales.
Fecha_5		Campo configurable para ingreso de fechas adicionales.

- **Cuentas Bancarias**

La tabla de cuenta bancaria, básicamente concentra la información relativa a la apertura de cuentas de clientes, el cual es la base para la operación de la mayor parte de productos y servicios que ofrece cualquier Institución Bancaria.

La información básica de cuentas, puede ser actualizada de manera diaria.

La estructura propuesta es la que se muestra en la Tabla 4:

Tabla 4: Estructura de datos de cuentas bancarias

Nombre Campo	Llave	Descripción
Numero_Cuenta	X	Número identificador del producto
Numero_Cliente	X	Número de identificación del cliente
Nombre_Cuenta		Nombre del producto
Codigo_Sucursal		Código de la sucursal asociada al producto
Codigo_Moneda		Código de la moneda asociada al producto
Codigo_Oficial		Código del oficial de producto encargado
Fecha_Apertura		Fecha de apertura del producto
Fecha_Cierre		Fecha de cierre del producto
Origen_Fondos		Origen de los fondos asociados al producto
Estado		Estado actual del producto
Fecha_Ult_Transaccion		Fecha de la última transacción realizada para el producto
Monto_1		Campo tipo numérico, configurable por el usuario.
Monto_2		Campo tipo numérico, configurable por el usuario.
Monto_3		Campo tipo numérico, configurable por el usuario.
Monto_4		Campo tipo numérico, configurable por el usuario.
Monto_5		Campo tipo numérico, configurable por el usuario.
Monto_6		Campo tipo numérico, configurable por el usuario.
Monto_7		Campo tipo numérico, configurable por el usuario.
Monto_8		Campo tipo numérico, configurable por el usuario.
Monto_9		Campo tipo numérico, configurable por el usuario.
Monto_10		Campo tipo numérico, configurable por el usuario.
Codigo_1		Campo tipo alfanumérico, configurable por el usuario.
Codigo_2		Campo tipo alfanumérico, configurable por el usuario.
Codigo_3		Campo tipo alfanumérico, configurable por el usuario.
Codigo_4		Campo tipo alfanumérico, configurable por el usuario.
Codigo_5		Campo tipo alfanumérico, configurable por el usuario.
Codigo_6		Campo tipo alfanumérico, configurable por el usuario.
Codigo_7		Campo tipo alfanumérico, configurable por el usuario.
Codigo_8		Campo tipo alfanumérico, configurable por el usuario.
Codigo_9		Campo tipo alfanumérico, configurable por el usuario.
Codigo_10		Campo tipo alfanumérico, configurable por el usuario.

2.5.2 Prevención de Fraudes enfocado a tarjetas de débito y crédito.

Un punto muy importante en la prevención del fraude, es mantener monitoreo para las transacciones financiera y no financiera en los productos/servicios que utilizan tarjetas.

La información básica a incluir para este tipo de monitoreo es:

- Tarjetahabiente.
- Teléfonos y direcciones.
- Comercios donde se transacciona.
- Transacciones de débito y crédito.

Debido a la importancia del mantenimiento de forma centralizada de movimientos en una sola tabla, ya que esto ayuda a que el analista de prevención de fraudes pueda identificar movimientos del mismo cliente por diferentes canales y facilitaría la minería de datos en caso de requerirlo, tanto la información de débito como de crédito es mucho mejor que residan en un misma tabla, cabe mencionar que en caso que esta información no se pueda acoplar, técnicamente esto no sería un impedimento para brindar el servicio de prevención de fraudes.

- **Tarjetahabiente, teléfonos y direcciones**

  En esta tabla se registra la información básica del tarjetahabiente y es importante para el seguimiento al cliente.

Por su naturaleza de información, dicha tabla puede ser actualizada en procesos batch de forma diaria.

La estructura básica es la que se propone en Tabla 5.

Tabla 5: Estructura de tarjetahabientes

Nombre Campo	Llave	Descripción
No_Tarjeta	X	Número de tarjeta
Identificacion		Número de identificación del tarjetahabiente
Cuenta		Número de cuenta, asociada a la tarjeta de débito
Nombre		Nombre del dueño de la tarjeta
Cupo		Cupo total del tarjetahabiente
Tipo_Cuenta		Define el tipo de cuenta para el tarjetahabiente (Ahorro o corriente o el tipo de tarjeta de crédito)
Fecha_Emision		Fecha en que emitió la tarjeta
Saldo		Se coloca el saldo en Tarjetas de débito y el Disponible en tarjetas de crédito.
Fecha_Nacimiento		Fecha en que nació el tarjetahabiente
Genero		Indica el género del tarjetahabiente
Extranjero		Indica si el tarjetahabiente es extranjero
Fecha_Ingreso		Fecha en que se ingresó el tarjetahabiente
Extrafinanciamiento		Monto extra aprobado sobre el límite de financiamiento, solo aplica a tarjetas de crédito.
Direccion		Dirección de residencia del tarjetahabiente
Tel_Oficina		Número telefónico de la oficinal del tarjetahabiente
Tel_Domicilio		Número telefónico de residencia del tarjetahabiente
Tel_Movil		Número telefónico móvil del tarjetahabiente
Email		Dirección de correo electrónico al que se puede contactar el tarjetahabiente
Id_Estado		Identifica el estado del tarjetahabiente
Fecha_Estado		Fecha en que se realizó el último cambio sobre el estado del tarjetahabiente
Id_Calificacion		Identificador de la calificación asignada al tarjetahabiente
Codigo_1		Campo de libre uso que puede contener información alfanumérica.
Codigo_2		Campo de libre uso que puede contener información alfanumérica.
Codigo_3		Campo de libre uso que puede contener información alfanumérica.
Codigo_4		Campo de libre uso que puede contener información alfanumérica.
Codigo_5		Campo de libre uso que puede contener información alfanumérica.
Monto_1		Campo de libre uso que puede contener información numérica.
Monto_2		Campo de libre uso que puede contener información numérica.
Monto_3		Campo de libre uso que puede contener información numérica.
Monto_4		Campo de libre uso que puede contener información numérica.
Monto_5		Campo de libre uso que puede contener información numérica.

- **Comercios donde se transacciona**

Esta es una tabla de parámetros muy importante al momento que el operador de la herramienta detecta un fraude, ya que es la base del análisis de los llamados “puntos de compromiso”, que significan, buscar las tarjetas reportadas como fraudes, en el punto en común donde consumieron dichos clientes y detectar en qué comercio pudiere estar el compromiso de datos.

Esta tabla, puede ser actualizada en proceso batch de forma diaria. La estructura básica de comercios es la que se muestra en Tabla 6:

Tabla 6: Estructura de datos de comercios

Nombre Campo	Llave	Descripción
Id_Comercio	X	Identificador del comercio
Id_Grupo		Identifica el grupo o corporación a la pertenece el comercio.
Nombre		Nombre descriptivo del comercio
MCC		Identificador del MCC bajo el cual se clasifica el comercio
Id_Pais		Identificación del país de donde se localiza el comercio
Direccion		Dirección física del comercio
Zona		Código de Área
Telefono1		Número de telefónico del comercio
Telefono2		Número de telefónico del comercio
Fecha_Ingreso		Fecha en que se ingreso el comercio
Estado		Define si un comercio se encuentra activo o no
Representante		Nombre del representante del comercio
Tel_Representante		Número Telefónico del representante
Identificacion		Identificación del representante
Relacion		Define la relación existente entre el comercio y el Representante
Forma_Pago		Forma en que se realizan los pagos al comercio
Ultima_Transaccion		Fecha de la ultima transacción realizada
Id_Calificacion		Identificación de la calificación asignada el comercio
Codigo_1		Campo de libre uso que puede contener información alfanumérica.
Codigo_2		Campo de libre uso que puede contener información alfanumérica relacionada con el comercio.
Codigo_3		Campo de libre uso que puede contener información alfanumérica relacionada con el comercio.
Codigo_4		Campo de libre uso que puede contener información alfanumérica relacionada con el comercio.
Codigo_5		Campo de libre uso que puede contener información alfanumérica relacionada con el comercio.
Monto_1		Campo de libre uso que puede contener montos relacionados con el comercio.
Monto_2		Campo de libre uso que puede contener montos relacionados con el comercio.
Monto_3		Campo de libre uso que puede contener montos relacionados con el comercio.
Monto_4		Campo de libre uso que puede contener montos relacionados con el comercio.
Monto_5		Campo de libre uso que puede contener montos relacionados con el comercio.

- **Transacciones de débito y crédito**

Esta es la tabla que debe de consolidar la información de transacciones tanto de débito como de crédito, para lograr una prevención del fraude efectiva, necesariamente debe ser actualiza lo más en línea posible, cabe mencionar que estos procesos de actualización deben estar programados de tal forma que estas lecturas consecutivas a la base de datos no afecten su rendimiento. La estructura necesaria para el monitoreo para transacciones de tarjetahabiente es la que se muestra en la Tabla 7:

Tabla 7: Estructura de datos transaccional para tarjetas de crédito y débito.

Nombre Campo	Llave	Descripción
Id_Transaccion	X	Este identificador es asignado en el momento en que la autorización se registra en el sistema de monitoreo.
No_Tarjeta		Número de tarjeta al que pertenece la autorización
Monto_Local		Monto en moneda local por el que se realizó la autorización
Tipo_Transaccion		Identificador del tipo de transacción (Retiro, Avance, Consulta)
Codigo_Afiliado		Identificador del comercio afiliado
Nombre_Afiliado		Nombre del afiliado (Utilizado para transacciones en comercios no afiliados a la Institución)
Tipo_Moneda		Indica si la transacción se realizó con moneda local o dólar
Monto_Dolar		Monto de la transacción en moneda dólar
Fecha_Hora_Transaccion		Fecha y hora en que se realizó la transacción
No_Autorizacion		Almacena el número que se le asigna a la transacción cuando se da la autorización
Codigo_Respuesta		Código de la respuesta que se le da a quien solicita la autorización
Disponible		Saldo disponible en la cuenta o tarjeta de crédito
Punto_Entrada		Punto de entrada que se utiliza para ingresar los datos de la transacción
MCC		Identificador del MCC del comercio donde se realiza la transacción
Codigo_Adquirente		Código del adquirente que da trámite a la transacción
Bin		Bin de la tarjeta que se está utilizando para la realización de la transacción
Codigo_Pais		Código del país en el que se realiza la transacción
Terminal_ID		Identificador de la terminal donde se ejecutó la trans.
Archivo_Fuente		Las autorizaciones podrían alimentarse a este sistema desde diversas fuentes, en este campo se almacena la fuente de donde proviene la autorización
Pais_Bin		Identifica el pais al que pertenece el Bin
Pais_Comercio		Identifica el pais al que pertenece el Comercio
Fecha_Ingreso		Fecha en que ingresa la transacción al sistema de monitoreo
Codigo_1		Campo de libre uso que puede contener información alfanumerica.
Codigo_2		Campo de libre uso que puede contener información alfanumerica.
Codigo_3		Campo de libre uso que puede contener información alfanumerica.

Nombre Campo	Llave	Descripción
Codigo_4		Campo de libre uso que puede contener información alfanumerica.
Codigo_5		Campo de libre uso que puede contener información alfanumerica.
Codigo_6		Campo de libre uso que puede contener información alfanumerica.
Codigo_7		Campo de libre uso que puede contener información alfanumerica.
Codigo_8		Campo de libre uso que puede contener información alfanumerica.
Codigo_9		Campo de libre uso que puede contener información alfanumerica.
Codigo_10		Campo de libre uso que puede contener información alfanumerica.
Monto_1		Campo de libre uso que puede contener información númerica.
Monto_2		Campo de libre uso que puede contener información númerica.
Monto_3		Campo de libre uso que puede contener información númerica.
Fecha_1		Campo de libre uso que puede contener información númerica.
Fecha_2		Campo de libre uso que puede contener información númerica.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 Mejoramiento del proceso de análisis de reglas a implementar para análisis de fraudes.

El mundo del fraude es muy cambiante, hoy una regla que funciona a la perfección y evita grandes estafas, mañana puede estar obsoleta, ya que constantemente se están desarrollando mecanismos nuevos de cometer delitos.

Es importante señalar, que por lo general los sistemas de monitoreo, las reglas programadas para la detección del fraude, son basadas en parámetros, los cuales el usuario solamente puede modificar su valor, en caso de que requiera agregar una nueva definición el usuario debe solicitar la modificaciones a los programas a áreas especializadas, ocasionando riesgos por la demora que esto conlleva y dependencia de otra área para lograr un trabajo efectivo al momento de detener los delitos y adicionalmente en muchas ocasiones cuando

se activa la regla, no es lo suficientemente eficaz ya que podría presentar demasiados “falsos positivos”.

Esta propuesta, mejora el proceso de detección, ya que brindarle al usuario final una interfaz amigable, donde pueda generar por sí solo nuevas reglas, en base a cualquier campo de los datos mostrados en las estructuras anteriores y adicionalmente puede evaluar los “falsos positivos” antes de la puesta en producción, ayudando así a la eficiencia en el proceso de prevención y detección del fraude.

A continuación en la Figura 3.1, se muestra una interfaz que se le mostraría al usuario antes de la implementación de una nueva alerta, donde el beneficio principal es la evaluación de la cantidad de alertas que generaría la regla:

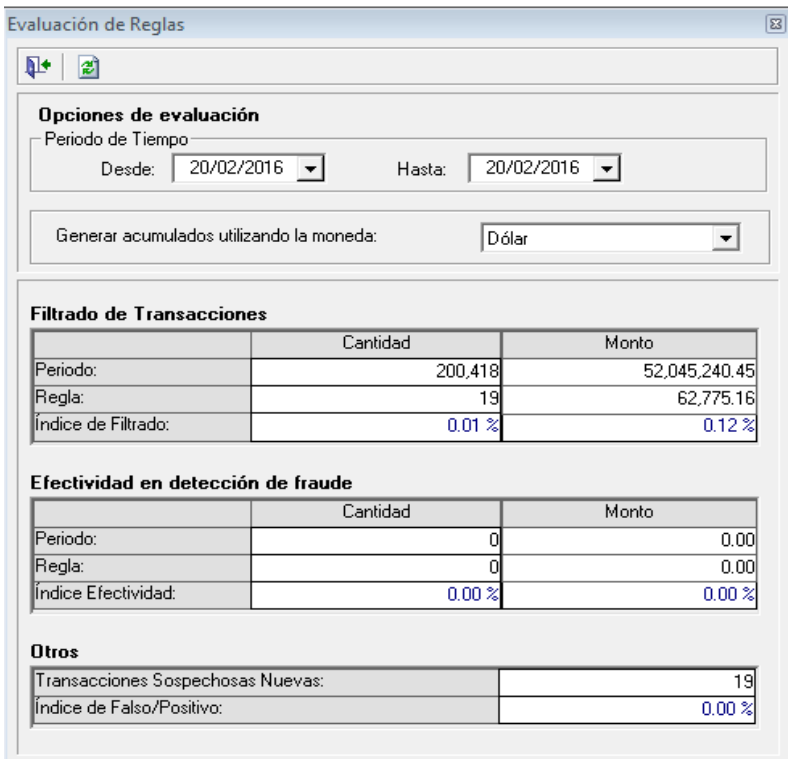


Figura 3.1: Interfaz de usuario para evaluación de reglas

3.2 Centralización de información transaccional para afinamientos de reglas.

Dado que la información de todas las transacciones que se definan en el alcance, residirán en una sola base de datos, el usuario final no tendrá la necesidad de buscar información transaccional en diferentes fuentes, ayudando así al análisis al momento de revisión de casos de fraude.

Adicionalmente, usuarios técnicos pueden acceder de una de forma centralizada, apoyando así al análisis multidimensional y realización de cubos especializados para la prevención, potencializando la toma de decisiones del departamento.

3.3 Mejoramiento en lo que se refiere a adaptabilidad aplicativa al entorno cambiante del fraude e independencia de las áreas técnicas para incorporación de nuevas reglas para la prevención del fraude.

Así como las Instituciones Financieras buscan imponer controles que protejan a sus clientes, los defraudadores también trabajan en descubrimiento de nuevas formas de cometer delitos, es por este concepto que las alertas eficientes de hoy podrán no ser tan efectivas mañana, el sistema provee una interfaz donde se pueda interactuar con toda la información cargada en las estructuras, sin tener que depender de procesos del área de tecnología para poder definir nuevos patrones, mejorando así el proceso de prevención y detección temprana del fraude.

CONCLUSIONES Y RECOMENDACIONES

1. Es muy conocido la evolución del delito financiero, cuando el Banco coloca un control anti-fraude los individuos no éticos inventan un nuevo método de estafa, por ejemplo antes del advenimiento de las tarjetas chip, era muy común el skimming en cajeros, ahora los ladrones apuntan a la ingeniería social para el robo de la tarjeta y visualización de la clave (retrocedieron al anterior método de estafa), o a nivel de cuentas está creciendo la suplantación de identidad para la realización de transferencias muy onerosas a cuentas receptoras que nunca han tenido movimientos mayores a tres cifras o cuentas recién aperturadas. A nivel de tarjeta de crédito se apunta mucho al fraude por internet, antes el auge del fraude era la falsificación de tarjetas producto del robo de información de la banda magnética.

2. La probabilidad de un perjuicio que los defraudadores generen en las Instituciones Financieras será siempre una realidad, porque el negocio es de riesgo, porque la administración de ese riesgo es muy importante en la

intermediación financiera, estudiosos del crimen y que con recursos obtenidos de forma ilegitima, procuran maximizar sus ganancias delictivas. El aplicativo para la Prevención del Fraude debe ser parte del esfuerzo que se realiza para minimizar los efectos negativos de esta realidad.

3. Estamos consientes que una plataforma tecnológica por sí sola no es una “bala de plata” con la cual resolveremos las amenazas del fraude, si no que un aplicativo es un aliado tecnológico que acompaña en la preservación de los recursos de los clientes, que confían en su Institución.

Es por esto que se recomienda lo siguiente:

1. Dentro de las evaluaciones costo/beneficio que pudieren realizar antes de comprar o desarrollar un sistema, se considere la experiencia que tienen las empresas proveedoras de las herramientas que existen en el mercado, las cuales podrían ahorrar mucho tiempo en el análisis, diseño e incluso estas mantienen inmerso lógica para realizar predicciones que alerten en base a un perfil transaccional el nivel de probabilidad que una transacción sea fraudulenta.

2. Finalmente, se confía que la investigación, el análisis de datos, la mejora continua y la innovación son claves en la prevención del fraude; sin embargo se recomienda mantener fuertes medidas de protección de datos y registro de accesos a estos, tanto a nivel aplicativo como de Base de Datos, ya que la

información que servirá al sistema es sensitiva e incluso está regulada bajo leyes de sigilo bancario a nivel de cuentas y estándares de seguridad para mantenimiento de la franquicia para tarjetas de crédito.

BIBLIOGRAFÍA

[1] Normas de Seguridad para canales electrónicos http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf, fecha de consulta Febrero del 2016.

[2] Recomendaciones de Seguridad https://www.bancodelpacifico.com, fecha de consulta Enero del 2016.

[3] Como elegir el mejor procesador para un servidor http://blog.servidoresdeaplicaciones.com/tag/dimensionamiento/, fecha de consulta Febrero del 2016.

[4] Presentación comercial del producto de monitoreo para fraude en cuentas de Instituciones Financieras http://www.smartsoftint.com/esp/images/pdfs/One%20Page%20Cumplimiento%20y%20Riesgo.pdf?lbisphpreq=1, fecha de consulta Febrero 2016.

[5] Presentación comercial del producto de prevención de fraudes en transacciones con tarjetas de crédito, débito http://www.smartsoftint.com/esp/images/pdfs/One%20Page%20Sentinel%20Prevention.pdf?lbisphpreq=1, fecha de consulta Febrero 2016.