



UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
CENTRO UNIVERSITARIO UAEM ECATEPEC

“Analista en el Control de Punto de
Compromiso en Administración de Fraude en
una Institución Financiera”

MEMORIA LABORAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN ADMINISTRACIÓN

P R E S E N T A :

JUAN CARLOS CARRANZA RAMOS

ASESORA: M. EN A. MARIA ANGELICA REYNOSO CASTILLO

ECATEPEC DE MORELOS, ESTADO DE MÉXICO

MAYO 2013



Universidad Autónoma del Estado de México
Centro Universitario UAEM Ecatepec

ASUNTO: VOTO APROBATORIO DE ASESOR.

Ecatepec de Morelos a 17 de Mayo del 2013

LIC. DANIELA GONZÁLEZ RODRÍGUEZ
JEFA DE TITULACIÓN DEL C.U. UAEM ECATEPEC
P R E S E N T E.

Por este conducto me permito informarle que el pasante: **JUAN CARLOS CARRANZA RAMOS** con numero de cuenta **0523526** de la **LICENCIATURA EN ADMINISTRACIÓN** ha concluido el desarrollo de su **MEMORIA**, con el titulo:

“ANALISTA DEL CONTROL DE PUNTO DE COMPROMISO EN ADMINISTRACIÓN DE FRAUDE EN UNA INSTITUCIÓN FINANCIERA”

Manifiesto que el borrador del trabajo escrito reúne las características necesarias para ser revisado por la Comisión especial nombrada para tal efecto.

ATENTAMENTE

MTRA. MARÍA ANGÉLICA REYNOSO CASTILLO
NO. DE CEDULA PROFESIONAL: 1155864





Universidad Autónoma del Estado de México
Centro Universitario UAEM Ecatepec

ASUNTO: VOTO APROBATORIO DE REVISORES.

Ecatepec de Morelos; a 17 de Mayo del 2013.

LIC. DANIELA GONZÁLEZ RODRÍGUEZ
JEFA DE TITULACIÓN DEL C.U. UAEM ECATEPEC
PRESENTE.

Me es grato comunicarle que el trabajo de **MEMORIA** titulada:

**“ANALISTA DEL CONTROL DE PUNTO DE COMPROMISO EN LA
ADMINISTRACIÓN DE FRAUDE EN UNA INSTITUCIÓN FINANCIERA”**

Que para obtener el Título de: **LICENCIADO EN ADMINISTRACIÓN**

Presenta el pasante: **JUAN CARLOS CARRANZA RAMOS**

Con número de cuenta: **0523526**

*Cumple con los requisitos teóricos – metodológicos suficientes para ser aprobado,
así puede continuar con los trámites correspondientes para su impresión.*

R E V I S O R

MTRA. LAURA EDITH ALVITER ROJAS
NO. CEDULA PROFESIONAL: 6822937

R E V I S O R

MTRA. MARÍA MONTSERRAT LUNA SIERRA
NO. CEDULA PROFESIONAL: 7871827





Universidad Autónoma del Estado de México
Centro Universitario UAEM Ecatepec

ASUNTO: IMPRESIÓN DE TRABAJO ESCRITO.

Ecatepec de Morelos; a 21 de Mayo del 2013.

C. JUAN CARLOS CARRANZA RAMOS
PASANTE DE LA LICENCIATURA EN ADMINISTRACIÓN
PRESENTE.

Por este medio le comunico a usted, que al haber cubierto los trámites correspondientes al desarrollo del trabajo escrito bajo la modalidad **MEMORIA** con el fin de obtener su Título Profesional, se le aprueba la **IMPRESIÓN DE SU TRABAJO** con el título:

“ANALISTA DEL CONTROL DE PUNTO DE COMPROMISO EN LA ADMINISTRACIÓN DE FRAUDE EN UNA INSTITUCIÓN FINANCIERA”

Con el Objetivo de establecer la fecha de Evaluación Profesional, le recuerdo que la presentación final del trabajo escrito es de su completa responsabilidad.

Sin más por el momento, reciba un cordial saludo.

ATENTAMENTE
“PATRIA, CIENCIA Y TRABAJO”
“2013, 50 Aniversario Luctuoso de Poeta Heriberto Enríquez”

LIC. DANIELA GONZÁLEZ RODRÍGUEZ
JEFA DE TITULACIÓN DEL C.U. UAEM ECATEPEC



CENTRO UNIVERSITARIO U.A.E.M
ECATEPEC
TITULACION



AGRADECIMIENTOS

A mis Padres...

Quienes me han heredado el tesoro mas valioso que puede dársele a un hijo que sin escatimar esfuerzo alguno para formarme y educarme, porque la ilusión de su vida ha sido convertirme en una persona de provecho y hoy con este éxito demuestro que lo han logrado. Por todo y por mucho más GRACIAS.

A mis Profesores...

Por el tiempo, dedicación y apoyo que recibí de su parte para que hoy en día sea la persona que soy, aplicando los conocimientos recibidos de su parte en mi desarrollo profesional.

DEDICATORIAS

En especial a Dios, porque fue quien coloco todos los mejores momentos, personas y lugares para que me acompañaran en el camino de mi vida profesional y personal.

A mis Padres, porque son parte fundamental de mi vida, asi como lo fueron y seran para mi formacion academica. Gracias por su apoyo incondicional y por el gran conocimiento que me transmitieron para mi crecimiento personal y profesional. Gracias por todo el esfuerzo que utilizaron para que yo sea una persona de bien.

A Janeth Rivera mi Esposa, por que se convirtio en el pilar de la realizacion de esta memoria laboral, ya que con su ayuda se puedo completar. Ademas de ser la inspiracion para mi crecimiento personal y familiar. Gracias por todo el amor y apoyo que me brindas siempre.

A mis Hermanos como un testimonio de gratitud y correspondiendo al esfuerzo y apoyo recibido, con cariño.

INDICE

Introducción

Capítulo I.

Marco referencia1

| | |
|---|----|
| 1.1 Analista de control del punto de compromiso..... | 1 |
| 1.2 Historia de la empresa..... | 1 |
| 1.3 Misión..... | 5 |
| 1.4 Principios de la empresa..... | 6 |
| 1.4.1 Objetivo común..... | 6 |
| 1.4.2 Ingenio..... | 6 |
| 1.4.3 Finanzas responsables..... | 6 |
| 1.4.4 Liderazgo..... | 6 |
| 1.5 Ubicación del puesto..... | 6 |
| 1.6 Organigrama..... | 7 |
| 1.7 Tipos de analistas y ejecutivos en la administración de prevención de fraude..... | 8 |
| 1.7.1 Analistas de monitoreo en tiempo real..... | 8 |
| 1.7.1.1 Analista de crédito..... | 8 |
| 1.7.1.2 Analista de débito..... | 8 |
| 1.7.2 Analistas de avisos de viajes..... | 9 |
| 1.7.3 Ejecutivos de contacto que colaboran directamente con el analista de PCC..... | 9 |
| 1.7.3.1 Definición de llamadas de entrada para prevención de fraude..... | 10 |
| 1.7.3.2 Definición de llamadas de salida para prevención de fraudes..... | 10 |

| | |
|---|----|
| 1.8 Definición de cuentas comprometidas..... | 11 |
| 1.9 Definición de patrón de consumo o de viaje..... | 12 |
| 1.10 Medios de acceso de fraude..... | 13 |

Capítulo II.

Marco teórico

| | |
|---|----|
| 2.1 Definición de prevención..... | 14 |
| 2.2 Definición de fraude..... | 15 |
| 2.3 Tipos de fraudes..... | 17 |
| 2.4 Herramientas que utilizan los defraudadores para el compromiso de las tarjetas de crédito y débito..... | 19 |
| 2.4.1 Nuevas técnicas de clonación de tarjetas de crédito y débito..... | 23 |
| 2.5 Formas de detectar el fraude..... | 24 |
| 2.6 Mención de fraude en el código penal federal de México..... | 25 |
| 2.7 Definición de administración..... | 26 |
| 2.8 Proceso administrativo..... | 26 |
| 2.9 Definición de control..... | 27 |
| 2.9.1 Elementos del control..... | 27 |
| 2.9.1.1 Relación con lo planeado..... | 27 |
| 2.9.1.2 Medición..... | 28 |
| 2.9.1.3 Detectar desviaciones..... | 28 |
| 2.9.1.4 Establecer medidas correctivas..... | 28 |
| 2.9.2 Importancia del control para la administración de fraudes..... | 28 |

Capítulo III.

Núcleo argumental

| | |
|--|----|
| 3.1 Misión de la administración de fraude..... | 29 |
| 3.1.1 Misión del puesto en particular..... | 30 |

| | |
|---|----|
| 3.2 Herramientas del puesto..... | 30 |
| 3.3 Importancia del puesto..... | 30 |
| 3.4 Funciones del puesto..... | 31 |
| 3.5 Aportaciones al puesto..... | 34 |
| 3.6 Diagrama de flujo para casos de validación..... | 39 |
| | |
| Conclusiones y Sugerencias..... | 40 |
| Referencias..... | 44 |

Introducción

El principal objetivo de realizar esta memoria laboral es obtener el título de licenciado en administración y mostrar parte de los conocimientos y experiencia adquiridos en el puesto que desempeño.

Es importante dar a conocer, como un administrador puede desenvolverse en el puesto de control del punto de compromiso para el área de prevención de fraudes y como es que los conocimientos y habilidades obtenidos en la carrera pueden hacer una mayor capacidad de desempeño en el área y puesto a laborar.

Empezaremos a tomar noción sobre el tema resaltando que la creciente liberación e integración de los mercados financieros mundiales, el libre movimiento de capitales, así como la rapidez y la eficacia de la transferencia de dinero por vías alternas y electrónicas, han consolidado el sistema financiero global, pero también lo han hecho más vulnerable a diversos actos delictivos.

Muchos acontecimientos históricos en la administración de riesgos financieros se han desarrollado a nivel mundial como innovaciones regulatorias debido a los cambios realizados por los organismos de control, estos toman importancia cuando los fracasos corporativos y en especial aquellos problemas vinculados con la quiebra de entidades o hechos de gran magnitud por el volumen de pérdidas ocasionadas dan pie a la elaboración de procesos internos que ayudan a mitigar el fraude.

Todo esto también ha derivado una mayor preocupación por la gestión del riesgo operativo.

De acuerdo a los noticieros, revistas financieras y algunos periódicos se ha podido ver como los fraudes se han intensificado en la última década siendo el sector financiero el más perjudicado; aproximadamente entre 150 a 200 denuncias mensuales por eventos de fraude en tarjetas de crédito y débito se registran en la Policía Judicial.

Se desarrolla la memoria laboral con el objetivo específico de proporcionar las funciones en base al control de fraudes en tarjetas de crédito y débito aplicadas en al área de administración de prevención de fraudes.

También se explican algunas de las actividades que dan una implementación de indicadores claves de riesgo así como un conjunto de herramientas y estrategias de gestión de riesgos financieros basados en tecnologías analíticas, que integran toda información corporativa de fraudes con el objetivo de hacer análisis comparativos, identificar patrones de comportamiento sobre las anomalías detectadas, y explicar algunos de los modelos predictivos que puedan ser fácilmente adoptados por las entidades financieras a nivel nacional e internacional y que se desempeñan en el área.

Capítulo I

Marco referencial

Por principio en este primer capítulo se comenzará por describir algunos conceptos y definiciones que se utilizan de forma cotidiana en la institución financiera, con el fin de que el lector pueda identificar el entorno y componentes que integran la función del Analista en el Control de Punto de Compromiso en la Administración de prevención de fraude.

1.1 Analista de control del punto de compromiso

El analista de control del punto de compromiso o Analista PCC, se define como aquella persona encargada de aplicar sus conocimientos a través del uso de las herramientas y tecnologías, utilizadas para la prevención y reducción de fraudes en tarjetas de crédito y débito, basados en los objetivos y parámetros del área misma.

1.2 Historia de la empresa

El puesto arriba descrito pertenece a un área considerada como el pilar del banco, por lo tanto, se desarrolla desde los inicios y fundación de la empresa. Para poder entenderlo se deben conocer los antecedentes y la historia de esta institución en donde se ubica y desarrolla el puesto.

Para efecto de conocimiento sobre el objeto de estudio, se hace la descripción de la institución financiera en la que se prestan los servicios, desde este momento se denominará BMX, se comenta que parte de lo publicado en esta memoria laboral es de conocimiento interno de la empresa únicamente, ya que por razones éticas se evita plasmar en estas

líneas las estrategias que se utilizan para combatir el fraude dentro de la empresa.

BMX fue fundada el 2 de junio de 1884, producto de la fusión de dos bancos, el Banco Nacional Mexicano y el Banco Mercantil Mexicano. Estos se unieron como alianza estratégica para aprovechar fortalezas y oportunidades de ambas, dando en ese momento, lugar a una nueva institución, para responder a las necesidades económicas que planteaba el país. El apoyo gubernamental se hizo evidente al ser el mismo Presidente de la República Manuel González, quien en su momento impulsará la constitución de este nuevo banco.

El 15 de mayo de 1884 se suscribió el contrato que creó el Banco Nacional de México. Firmando el Ejecutivo Federal el Gral. Miguel de la Peña, y el señor Eduardo Noetzlin como apoderado y representante de los accionistas.

El 31 del mismo mes de mayo, el Congreso de la Unión decretó la aprobación del contrato y el Presidente de la República, personalmente autorizó los estatutos por conducto del Secretario de Hacienda y que habían sido previamente aprobados por la Junta General de Accionistas.

Finalmente, el 2 de junio de 1884 se reunieron en el edificio colonial sede desde esa fecha, los consejeros de los bancos fusionados, encabezados, los del Nacional Mexicano por Antonio de Mier y Celis, Félix Cuevas y León Stein, y los del Mercantil Mexicano por Nicolás de Teresa, Manuel Ibáñez y Rafael Ortiz de la Huerta, y declararon, que quedaba consumada la unión de los dos bancos que desde entonces funciona con el nombre de Banco Nacional de México.

Las actividades de la institución se iniciaron bajo la dirección del señor José V. del Collado, auxiliado por don Ramón Usandizaga en la

caja, y por dos docenas de empleados más que formaban toda la plantilla del personal en la Ciudad de México.

El Banco tenía sucursales en Mérida, Veracruz, Puebla, Guanajuato y San Luis Potosí, meses después, otra en Guadalajara. En la actualidad tiene más de 1,260 oficinas en la República y 2,808 cajeros automáticos.

A pesar de lo difícil de la situación económica del País, a BMX le permitió obtener resultados positivos desde el primer momento, se impulsó la emisión de billetes, el cobro de obligaciones fiscales y el manejo de una cuenta especial en el Banco Nacional de México para este tipo de operaciones.

El Banco manejaba operaciones de deuda pública interna y externa desde sus inicios como hasta la actualidad, como ejemplo son las inversiones y créditos para clientes nacionales y las cuentas de negocios para extranjeros como inversiones y títulos.

BMX, en sus primeros años, impulsaba los negocios privados en el país mediante una concesión de privilegio, lo que le permitía, a la vez que lo obligaba, a participar en la resolución de los problemas de la Hacienda Pública.

En la segunda guerra mundial el banco participó activamente en dotar al país de una infraestructura industrial en forma decidida, a través de créditos y diversas asesorías, al nacimiento y consolidación de innumerables empresas.

El banco inició la implementación de cuentas de ahorro al mercado mexicano en 1929, los servicios fiduciarios en 1935, el servicio de auto-banco en 1947, los préstamos personales en 1958, los préstamos para la adquisición de bienes de consumo duradero en 1961, la tarjeta de crédito en 1968, los ejecutivos de cuenta en 1971, las cajas permanentes en

1972, la exitosa Cuenta Maestra en 1986, Banco en el Súper en 1992, Mi Cuenta y Cuenta Básica BMX, para niños y jóvenes en 1994 y recientemente Bancanet.

Su infraestructura tecnológica, informática, electrónica y de telecomunicaciones, le han permitido mantenerse a la vanguardia en la creación y lanzamiento de nuevos productos y servicios bancarios y garantizar la operatividad de los mismos.

En febrero de 1977 se integraron al Banco Nacional de México la Financiera BMX, Financiadora de Ventas BMX y la Hipotecaria BMX para constituirse y participar como banca múltiple, que concentra y proporciona los servicios especializados de depósito, ahorro, financieros, fiduciarios e hipotecarios.

En el nivel internacional, Se tienen oficinas en Nueva York, Los Ángeles, Madrid, Londres, Tokio, Nassau y Singapur, ha participado con un Comité en París desde 1929, con el establecimiento en Nueva York de la primera agencia de un banco latinoamericano en EUA. BMX siempre ha participado en el desarrollo social y cultural, aportando su esfuerzo al conocimiento y difusión de nuestros valores culturales. Ha venido otorgando estímulos a la educación y a la investigación principalmente en materia de economía, ciencia, tecnología, finanzas y banca.

En 1951 instituyó el Premio Anual de Economía, en 1968 el de Ciencia y Tecnología, en 1985 el de Historia Regional y desde 1925 se publica de forma ininterrumpida la revista Examen de la Situación Económica de México. A partir de marzo de 1991 se creó el Archivo Histórico BMX, único en su tipo en el país, que incluye una Biblioteca de Banca y Finanzas.

En los últimos años, ha enfocado su atención al apoyo de poblaciones y personas que pasan por situaciones económicas difíciles, a

través de Fomento Social BMX y se ha distinguido también por su labor en el rescate y restauración de edificaciones coloniales.

De 1982 a 1990 BMX funcionó como Sociedad Nacional de Crédito, y en 1991 se reprivatizó y formó el Grupo Financiero BMX-Accival, que tiene como propósito la excelencia, mediante la dedicación para lograr la más alta calidad en los servicios, es decir, el cambio de nombre fue para hacer énfasis en la privatización y reestructura del banco para dar servicio a los clientes de calidad.

El 6 de agosto de 2001 se integró formalmente el Grupo Financiero BMX a Citigroup, la institución financiera más importante a nivel mundial, con el objetivo de conformar el grupo financiero más sólido, global y competitivo en México.

A continuación se describe la Misión de Citigroup ya que por esta se rige BMX.

1.3 Misión

“En Citi, se reitera el compromiso que tenemos con nuestros clientes y con la compañía. La misión y los principios fundamentales que se describirán más adelante han sostenido al banco por generaciones.”

“Hacer posible el progreso Citi, trabajar incansablemente para prestar servicios a personas, comunidades, instituciones y naciones. Con una experiencia de 200 años enfrentado retos y aprovechando oportunidades a nivel global, nos esforzamos para obtener los mejores resultados para nuestros clientes y con soluciones financieras simples, creativas y responsables, nuestra institución conecta a más de 1000 ciudades, 160 países y millones de personas, por ello somos un banco global; somos Citi.”

De forma escrita la misión se entrega en copia a los participantes en los cursos de inducción.

1.4 Principios de la empresa

Los cuatro principios clave que nos guían para cumplir la misión son:

1.4.1 Objetivo común

Un solo equipo, con un solo objetivo; servir a nuestros clientes y a nuestras contrapartes.

1.4.2 Ingenio

Mejorar la vida de nuestros clientes a través de innovaciones que aprovechen el alcance y la profundidad que caracteriza a nuestra información, red global y productos de nivel mundial.

1.4.3 Finanzas responsables

Una conducta transparente, prudente y confiable.

1.4.4 Liderazgo

Personas talentosas y altamente capacitadas, quienes tienen una cultura en la que se respeta la diversidad y que exige excelencia e iniciativa.

1.5 Ubicación del puesto

El analista de control de punto de compromiso se ubica en el área de PCC (Punto de Control de Compromiso) que está conformada por elementos dependientes del área de estrategias que se encuentra dentro de la dirección de la administración de fraudes, dichos elementos son los siguientes:

- a) Monitoreo débito (se refiere al proceso de monitorear transacciones de los clientes en tarjetas de débito.)

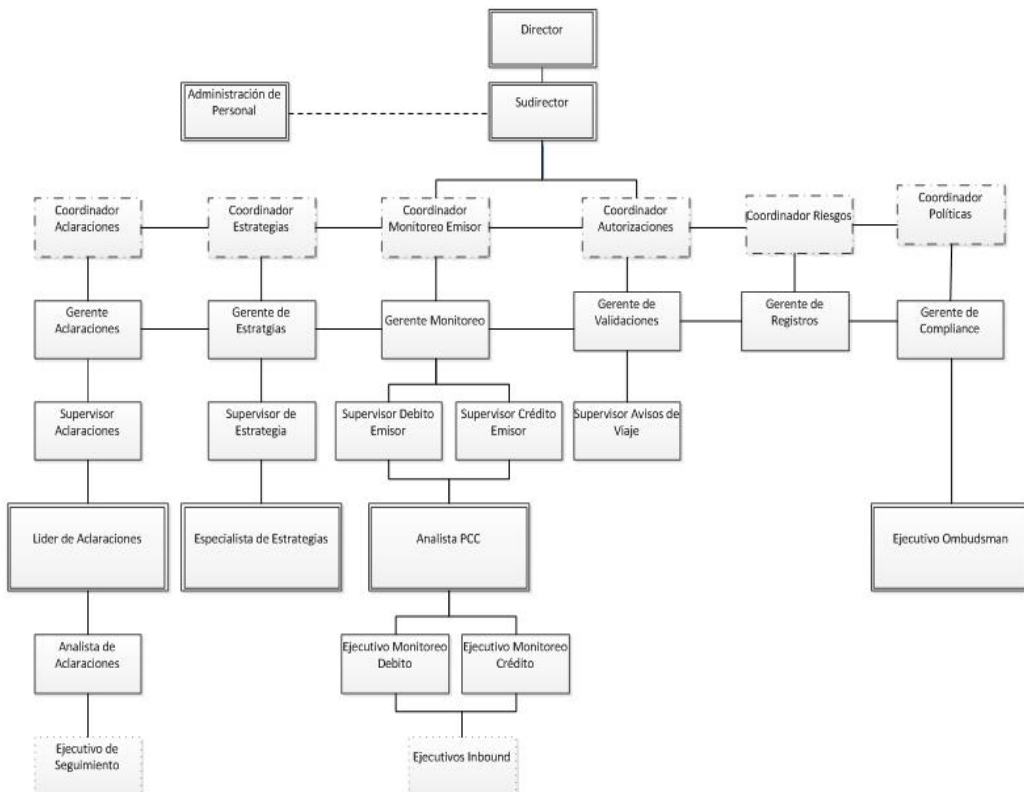
- b) Monitoreo de crédito. (se refiere al proceso de monitorean transacciones de los clientes en tarjetas de crédito.)

1.6 Organigrama

En el área de prevención de fraudes, los puestos están divididos en 7 niveles, estos son distribuidos al obtener cierta puntuación según la importancia del mismo puesto y el impacto que las funciones desempeñadas tienen al negocio en general.

En el caso de la dirección y subdirección están colocadas en el nivel uno por ser los puesto de mayor importancia en el área. El analista de PCC se localiza en el nivel 5. (Ver figura 1)

Figura 1. Organigrama del área de prevención de fraudes.



(ELABORACIÓN PROPIA)

1.7 Tipos de analistas y ejecutivos en la administración de prevención de fraude

Hay diferentes tipos de analistas y ejecutivos de administración de fraudes, entre los más relevantes como apoyo directo del Puesto que explico en esta memoria son:

1.7.1 Analista de monitoreo en tiempo real

Este tipo de analista, su labor consiste en verificar las transacciones efectuadas en el banco con ayuda de sistemas institucionales y se puede ver las transacciones que efectúan los clientes en tiempo real, lo que permite analizarlos en el mismo momento en que se efectúan.

El analista debe aprender las reglas de detección que el banco ha establecido, porque su trabajo consiste en monitorear las alertas que surgen por las transacciones de los clientes que se salen del patrón normal de consumo. Los analistas de monitoreo en tiempo real se dividen en “analistas de crédito” y “analistas de débito”, mismos que a continuación se describen:

1.7.1.1 Analista de crédito

Es la persona que monitorea las transacciones de los clientes en tarjetas de crédito.

1.7.1.2 Analista de débito

Es la persona que monitorea las transacciones de los clientes en tarjetas de débito.

1.7.2 Analista de avisos de viajes

Este otro tipo de analista se encarga de verificar las transacciones, de la misma manera que los analistas de crédito y débito, aunque no siempre pueden ser transacciones en tiempo real; estos usan reglas de detección que el banco ha establecido y poder analizar transacciones antiguas en bases de datos, además son los encargados de monitorear las alertas que surgen por las transacciones de los clientes, que se salen del área de consumo, es decir, no es usual que los clientes de forma rutinaria hagan transacciones en otra entidad, estado o país sin dar algún aviso del viaje por realizar, aquí se resalta la importancia en la detección que hacen los sistemas en tiempos y distancias de los clientes, un ejemplo para comprender estas últimas reglas es que no es lógico que un cliente con su tarjeta este comprando un producto en un establecimiento en particular a las 13:30 horas en México y a las 14:00 horas, este haciendo disposiciones de efectivo en Estados Unidos.

1.7.3 Ejecutivos de contacto que colaboran directamente con el analista de PCC

Los ejecutivos de prevención de fraudes más cercanos y que cooperan directamente con el analista de control del punto de compromiso, son los que se encargan del contacto directo con el cliente, estos ejecutivos tienen dos funciones primordiales que se dividen en: llamadas de entrada y llamadas de salida.

A continuación se describirá en forma breve en qué consisten este tipo de llamadas.

1.7.3.1 Definición de llamadas de entrada para prevención de fraude

Las llamadas de entrada son las que los clientes efectúan directamente hacia el banco por iniciativa propia o por que con anterioridad han recibido mensajes del área de prevención de fraudes solicitando que se comuniquen.

Los encargados de atender esas llamadas son ejecutivos de prevención de fraudes que dan seguimiento a solicitudes que el cliente requiere en el momento de la llamada o dan seguimiento a una solicitud del banco. Estos ejecutivos se rigen bajo las normas y políticas del área, las cuales son de conocimiento interno únicamente.

1.7.3.2 Definición de llamadas de salida para prevención de fraudes

Las llamadas de salida son las que en base a un análisis de una cuenta y las transacciones que conlleva, requieren contacto con el cliente, esto por no tener la seguridad sólo con el análisis de que la tarjeta que utiliza el cliente para transaccionar no está comprometida y hay la evidencia de que algunas operaciones que se estén llevando a cabo se presentan como sospechosas o tienen patrón de fraude, en base a esto para el contacto con el cliente es necesario validar información que el analista requiera para descartar el posible compromiso de la información de las tarjetas que están transaccionando.

Cualquier empleado dentro del área de prevención de fraudes tiene la facultad para realizar llamadas de salida ya que el área siempre está al servicio de protección y seguridad de las tarjetas, así que si es necesario o conveniente se pueden efectuar este tipo de llamadas.

Las llamadas de salida se basan en protocolos de comunicación que ha establecido la institución financiera, para mantener la calidad y profesionalismo con el cliente, además de que se respetan horarios y palabras establecidas por educación y las leyes impuestas por el país. Un claro ejemplo es que en una llamada de salida no se pueden usar palabras irrespetuosas, tecnicismos, alterantes y fuera de horarios (11 pm a 6 am).

1.8 Definición de cuentas comprometidas

Para entender un poco más de las cuentas que se deben de administrar en este puesto, hay que saber porque se utiliza el término “cuentas comprometidas”, estas se refieren a la cuentas o tarjetas que ya están clonadas total o parcialmente y que con anterioridad el área de estrategias mediante el uso de sus procesos y sistemas determina que una cuenta y/o la información de seguridad de las tarjetas, la puedan tener terceras personas que no son el cliente únicamente, esto puede tener en un futuro un posible fraude y por consiguiente una afectación para el banco, los negocios a los que se han hecho transacciones con la tarjeta y por último el cliente.

El análisis de cuentas comprometidas son parte de las funciones que se desempeñan en el puesto de control de punto de compromiso, ya que los fraudes se detectan en base a monitoreo de transacciones, estas pueden ser en tiempo real y son detectadas por el analista en base a un seguimiento y análisis a través de sistemas institucionales, u otra forma es poder detectarlo en la base de datos que concentra información detallada de todas las transacciones que solicitamos para analizar el hecho de contener un patrón de fraude.

A las cuentas comprometidas ya detectadas también se les conoce como “insumo” ya que es el principal objetivo de acción para un analista en el área de prevención de fraudes y es la base del trabajo diario.

Una vez teniendo el insumo, se tiene que determinar qué plan de acción se debe tomar con cada cuenta, estas decisiones se toman por los procesos ya establecidos por el banco en los cuales aplican conforme el tipo de compromiso que adquirió la tarjeta o la cuenta y en el cómo se puede atacar o detener el fraude.

1.9 Definición de patrón de consumo o de viaje

Un patrón de consumo o de viaje es aquella secuencia de transacciones que realiza un cliente y se puede dar por entendido que son legítimos del cliente, es decir, que en realidad el cliente está utilizando la tarjeta y no terceras personas con los datos del cliente, por otra parte están los que llevan una secuencia de viaje.

Las transacciones tienen características especiales que los analistas pueden detectar como lo es una disposición de efectivo moderada, estas disposiciones se efectúan en horas particulares del día, que no son de riesgo y en “zona”, para familiarizarse con este último término se puede decir que están cerca de su domicilio o que están cerca de un destino.

Con el análisis adecuado, se puede dar por entendido que el cliente se está desplazando, consumiendo de manera legítima o que está de viaje, cuando por ejemplo, se presenta reservación de hotel con montos moderados, pago de servicio de transporte, casetas, etcétera, a esto se le denomina patrón de viaje y con patrones de consumo que los

analistas de débito y crédito deben tener en cuenta para un buen control y prevención de los fraudes.

1.10 Medios de acceso de fraude

Con el fin de mostrar los puntos de protección que abarcan el trabajo y estudio de los analistas de prevención de fraudes, se mostraran los medios de acceso al fraude, es decir, las maneras que existen para poder comprometer la información confidencial de los clientes para el uso ilícito.

Los medios de acceso de fraude que pueden tener las tarjetas son:

- ✓ Voz, cargos
- ✓ Terminal punto de venta (TPV)
- ✓ Interred
- ✓ Banca electrónica
- ✓ Cajero permanente
- ✓ Internet
- ✓ Adquirente doméstico
- ✓ Adquirente internacional
- ✓ Cajero red nacional
- ✓ Cajero red internacional
- ✓ Audio respuesta
- ✓ Voz emisor internacional Visa
- ✓ Voz emisor internacional Mcard
- ✓ Manual
- ✓ Lectura de banda
- ✓ Circuito integrado
- ✓ Lectura y envío de banda completa

Los términos antes mencionados son tipificados por el banco y observados en reglas internas, las cuales contienen significados específicos para uso propio y exclusivo de la institución financiera.

Capítulo II

Marco Teórico

En este capítulo se presentan las principales funciones que desempeña el analista de control de punto de compromiso, para esto hay que comprender y ubicar las mismas dentro de la administración, que permitirá conocer y describir el nombre del puesto y el área donde se monitorea, detecta y se resuelve la problemática.

2.1 Definición de prevención

De acuerdo a la Procuraduría General de Justicia, la palabra prevención significa: medidas y acciones dispuestas emitidas con anticipación con el fin de evitar o impedir que se presente un fenómeno peligroso que servirá para reducir sus efectos sobre la población.

Esto aunado a la definición jurídica de la palabra delito que se precisa como: una conducta, acción u omisión típica (tipificada por la ley), antijurídica (contraria a Derecho), culpable y punible. Supone una conducta infraccional del Derecho penal, es decir, una acción u omisión tipificada y penada por la ley.

La prevención encierra dos aspectos importantes:

- Prevenir que el individuo realice conductas delictivas o ilícitas.
- Evitar que las personas sean sujetas o víctimas de algún delito.

2.2 Definición de fraude

Se conceptualizará el término de Fraude de acuerdo a diferentes autores, para dar a conocer como se percibe en diferentes contextos:

Cifuentes (1986) dice que la noción de fraude implica una inmediata referencial al engaño, al acto contrario a la verdad, al recto proceder. Esta referencia general nos permite una aproximación al concepto de frustración de los fines de la ley o de los derechos de un tercero. El fraude supone, en este sentido, una conducta tendiente a eludir los efectos de una norma imperativa o de origen convencional, abstrayéndose del cumplimiento de ellas con auxilio de otra vía negocial, receptada a su vez por la ley. Se configura el fraude por medio de actos reales, serios y no aparentes (no simulados); no diverge de la voluntad declarada. Es precisamente esta realidad, la que amparada en la norma legal, elude las disposiciones de otra o perjudica a un tercero. Generalmente el fraude se estructura a través de acciones, no de omisiones, que en el caso de reflejar la pasividad del deudor en el ejercicio de sus derechos, caerán en el ámbito de la Acción Subrogatoria. El fraude puede penetrar en el campo de la invalidez negocial y sancionarse con la correspondiente nulidad, o alejarse de ese ámbito para constituir un supuesto de ineficacia parcial por la vía de su oponibilidad al acreedor legitimado que triunfa.

Para Torres (2001) el vocablo fraude viene de la locuciones latinas *fraus*, *fraudis*, que significan falsedad, engaño, malicia, abuso de confianza que produce un daño, por lo que es indicativo de mala fe, de conducta ilícita. Este significado aplicado a las relaciones jurídicas de naturaleza obligacional o creditoria, resulta indesligable de los actos de disposición que realiza el deudor con los que se reduce a la insolvencia o,

por lo menos, opone dificultad para que su acreedor o acreedores puedan hacer efectivo su derecho a ser pagados.

De acuerdo al Código Penal Federal (art 386) señala que el que comete el delito de fraude es el que engañando a uno o aprovechándose del error en que éste se halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido.

El delito de fraude según el Código Penal Federal se castigará con las penas siguientes:

I.- Con prisión de tres días a seis meses o de 30 a 180 días de multa, cuando el valor de lo defraudado no exceda de diez veces el salario mínimo vigente;

II.- Con prisión de seis meses a tres años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario mínimo general vigente;

III.- Con prisión de tres a 12 años y multa hasta de 120 veces el salario, si el valor de lo defraudado fuere mayor de 500 veces el salario. Que es una manera muy antigua de conseguir beneficios mediante la utilización de la inteligencia, viveza y creatividad del ser humano, considerado como un delito, cabe destacar que aunque se puede controlar de cierta forma es casi imposible terminar con el fraude por su manera de evolucionar o de crear nuevos fraudes.

Con la detección y prevención del fraude, se pueden ahorrar pérdidas económicas para la institución.

En pocas palabras se concluye que el fraude es el delito creativo para los hampones profesionales, ya que se requiere de mentes ingeniosas y hábiles, con conocimientos en diferentes áreas como son

las tecnologías de información computacionales (Tics) y financieras entre otras, para llevar a cabo este tipo de delito, y se puede decir que es prácticamente imposible de evitar, porque en el momento en que se aplica una estrategia para erradicarlo, alguien aplica algo nuevo para seguir defraudando.

Las normas internas del banco son las que pueden definir el fraude en base a cómo lo perjudica económicamente, las barreras que se perciben y que permiten el crecimiento del fraude radican en la administración, es importante hacer mención en que diversos factores y gente mediante un mal proceso administrativo son afectados y los medios más vulnerables que ponen a prueba los estándares de calidad y seguridad que el banco se ha propuesto, además se inclina a saber y definir mediante la buena administración como podemos conseguir un control y chequeo de la prevención de fraudes para evitar afectaciones de los mismos que pueden ser muy dañinos para los negocios, clientes o la misma institución financiera.

2.3 Tipos de fraudes

Es importante señalar que existen diferentes fraudes, la CONDUCEF los tipifica de la siguiente forma:

- Fraude genérico, específico e informático
- Fraude con el uso de tarjetas de débito o de crédito falsas
- Fraude con el uso de cheques falsos, o de cheques originales obtenidos de forma ilícita

- Fraude en el desvío de fondos destinados al pago de impuestos y los accesos indebidos a los sistemas informáticos de las Instituciones Financieras, con la finalidad de realizar transferencias ilegales de recursos.

La minuciosa imaginación para ejecutar estos delitos es abundante; simplemente, en materia de tarjetas bancarias se encuentra la falsificación integral de las mismas, incluido el copiado total de la banda magnética (conocido como skimming), que permite el traslado de los datos registrados en la original hacia otro plástico, de manera que se tiene un duplicado exacto de la verdadera.

Los fraudes con cheques no se quedan atrás. En muchos de los casos se trata de documentos apócrifos derivados de la falsificación integral de los esqueletos que los componen. El uso de la tecnología de punta para este propósito es algo común, así como para la elaboración de identificaciones falsas para hacer los cheques cobrables.

En base a los comentarios por expertos, el fraude que más se ha popularizado es el perpetrado en contra de los contribuyentes de impuestos. Algunas personas que trabajan en bancos, coludidas con los empleados de las recaudadoras fiscales realizan toda una serie de maniobras para desviar los pagos de personas físicas y morales hacia otras cuentas bancarias.

Una modalidad de fraude que está alcanzando dimensiones preocupantes es el realizado a través de transferencias electrónicas sobre el soporte de la red mundial. El defraudador se hace del Número de Identificación Personal (NIP) del titular de la cuenta y, por medio del servicio de banca por Internet, transfiere los recursos de la cuenta hacia otra para disponer ilícitamente de recursos ajenos.

Dado que es difícil determinar quién ha sido el autor del fraude, la legislación considera a los titulares como partícipes de “lavado de dinero” y, por tanto, culpables de disponer ilícitamente de recursos ajenos.

No obstante que pueden darse situaciones de riesgo en instituciones bancarias, el Usuario debe tener la certeza de que cuenta con el respaldo por parte de la institución y del instituto para la Protección al Ahorro Bancario cuando sea el caso.

El Artículo 91 de la Ley de Instituciones de crédito menciona: Las instituciones de crédito responderán directa e ilimitadamente de los actos realizados por sus funcionarios y empleados en el cumplimiento de sus funciones, sin perjuicio de las responsabilidades civiles o penales en que ellos incurran personalmente.

2.4 Herramientas que utilizan los defraudadores para el compromiso de las tarjetas de crédito y débito.

A continuación se muestran ilustraciones de cómo el crimen organizado capta la información de las tarjetas de débito y crédito así como los números de identificación personal (PIN). El crimen organizado usa esta información para crear una tarjeta nueva con la información del propietario y con el PIN puede obtener acceso a las cuentas y vaciarlas, es decir, retirar todo el efectivo.

La imagen 1.1 es proporcionada por el departamento de seguridad de un banco y muestra la apariencia normal de un cajero automático.

Imagen 1.1 cajero automático



En la imagen 1.2 se puede apreciar una de las cavidades indebidas que se pueden colocar al cajero y que contiene un lector de tarjeta adicional para copiar la información de su tarjeta y duplicarla.

Imagen 1.2 Ranura adicional



En la imagen 1.3 se aprecia un monitor y dispensador de folletos, el cual, para cualquier cliente puede parecer normal, el objetivo de presentar esta fotografía es resaltar el riesgo que puede existir en un lugar en condiciones normales.

Imagen 1.3 monitor y dispensador de folletos



En esta toma (imagen 1.4) se puede apreciar una cámara de fotografía y video escondida en un contenedor.

Imagen 1.4 Micro Cámara escondida



La micro cámara colocada en algún punto estratégico del cajero automático (imagen 1.5) puede ver el teclado y también el monitor para enviar una foto inalámbrica a una distancia hasta 20 metros. Esto para fines ilícitos.

Imagen 1.5 La micro cámara



En esta imagen (1.6) se muestran los componentes de las cámaras utilizadas para la transmisión de datos con el fin de interpretar lo fácil que es colocarla en espacios reducidos.

Imagen 1.6 Caja dispensadora de folletos



2.4.1 Nueva técnica de clonación de tarjetas de crédito y débito

En este apartado se darán a conocer una técnica de clonación que servirá para alertar a los usuarios en la utilización de tarjetas, esta es una nueva modalidad de clonación de tarjetas de crédito en cajeros automáticos.

- El dispositivo es colocado expuesto, es decir, no es insertado dentro del cajero automático, simplemente esta sobre o a lado del cajero y puede ser visible.
- Los equipos graban vía remota e inalámbrica, además capturan las claves del usuario.

En la imagen 1.7 se muestran los dispositivos que se utilizan para la clonación de tarjetas.

Imagen 1.7 Clonación de tarjetas



2.5 Formas de detectar el fraude

En este apartado se describen las formas más comunes que se utilizan para la detección de fraudes, para su mayor comprensión se iniciará sobre la definición de las mismas.

Labrada (2010) comenta que una de las formas para detectar un fraude es observar, probar o revisar los riesgos específicos de control, identificar los más importantes, vigilar y revisar constantemente su adecuada administración, así como las transacciones de los clientes. No obstante se deben de llevar a cabo pruebas de cumplimiento de la eficacia de los controles y medidas para impedir que la situación de fraude ocurra, lo que permitirá reducir las oportunidades para cometerlo.

Dentro de los controles de prevención de fraudes se incluye la revisión de referencias en procesos de reclutamiento de personal, establecer políticas, procedimientos y segregación de funciones claramente definida, mantener supervisión constante, entrenamiento en prevención de fraudes y cultura corporativa de gestión de riesgos.

Para una oportuna detección de fraudes se debe tener presente que los sistemas de control pueden ser tarde o temprano evadidos por lo que de forma continua deben revisarse y actualizarse, se deben detectar actividades irregulares tan pronto como sea posible, para ello, la detección aplica controles diseñados para alertar al personal apropiado cuando se presentan circunstancias asociadas con actividades fraudulentas, esto incluye desde mecanismos de auditoria interna hasta procesos directos para reportar fraudes de manera rápida.

Existen herramientas de detección computarizada de uso y conocimiento exclusivo del banco y estos son capaces de revisar grandes

volúmenes de datos, identificando patrones sospechosos además de los casos que requieran de una investigación más detallada también existen metodologías y herramientas informáticas que ayudan a los analistas a identificar posibles situaciones de fraude, siendo el objetivo primordial el obtener evidencia suficiente para sustentar las situaciones irregulares detectadas y realizar sus recomendaciones.

2.6 Mención de fraude en el Código Penal Federal de México

Para mencionar el concepto de fraude que existe en México, se abordará el marco legal del mismo.

Para la ley, el acto central de la estafa y fraude es el engaño que se establece desde una parte hacia la otra (la perjudicada), y la consiguiente obtención de beneficios propios a partir de ese engaño. El daño a la propiedad o patrimonio de una persona puede ser muy variado y no necesariamente material.

Por ejemplo, un típico caso de estafa es aquel en el cual una empresa no legal simula vender servicios a individuos para extraerles dinero (por ejemplo, venta de paquetes turísticos a manos de una organización ilícita).

Sin embargo, un fraude también puede significar el daño moral que el estafador realiza sobre otra persona para obtener beneficios (por ejemplo, presentar a una persona como un criminal para que no pueda obtener un trabajo y así obtener sus beneficios).

2.7 Definición de administración

Hasta este apartado de la memoria laboral se puede tener un panorama de lo que es control y fraude, ahora se procede a expresar definiciones de administración ya que es la faltante para poder relacionar los conceptos que interpreten el significado del puesto de analista de PCC dentro de la administración de prevención de fraudes.

Reyes (1992) comenta que "Es un conjunto de sistemático de reglas para lograr la máxima eficiencia en las formas de estructurar y manejar un organismo social".

Oliveira Da Silva (2002) define la administración como "un conjunto de actividades dirigido a aprovechar los recursos de manera eficiente y eficaz con el propósito de alcanzar uno o varios objetivos o metas de la organización"

Para Chiavenato (2004) la administración es "el proceso de planear, organizar, dirigir y controlar el uso de los recursos para lograr los objetivos organizacionales".

2.8 Proceso administrativo

Para resaltar el concepto de control, se iniciará con la definición del proceso administrativo por ser parte fundamental del mismo, para esto se mencionan la definición de algunos autores.

Describe Múch Galindo (1999) El proceso administrativo como el conjunto de fases o etapas sucesivas a través de las cuales se efectúa la administración mismas que se interrelacionan y forman un proceso integral. Tiene 4 funciones que son: planeación, organización, dirección y control.

Para Idalberto Chiavenato (1987) Establece al proceso administrativo como la secuencia de planear, organizar, dirigir y controlar para alcanzar los objetivos deseados, a través de medios, métodos o manera de ejecutar ciertas actividades. Las diversas funciones del administrador, en conjunto, conforman el proceso administrativo. Por ejemplo, planeación, organización, dirección y control, consideradas por separado, constituyen las funciones administrativas; cuando se toman como una totalidad para conseguir objetivos, conforman el proceso administrativo.

2.9 Definición de control

A continuación se abordará el control que es de vital importancia en cualquier organismo, iniciando con su definición para resaltar la importancia del mismo en esta investigación.

Para Terry (1984) es el proceso para determinar lo que se está llevando a cabo, valorizándolo y si es necesario, aplicando medidas correctivas, de manera que la ejecución se desarrolle de acuerdo a lo planeado.

Fayol (1969) comenta que consiste en verificar que todo ocurra de conformidad con el plan adoptado, con las instrucciones emitidas y con los principios establecidos. Tiene como fin señalar las debilidades y errores para poder rectificarlos e impedir que se produzcan nuevamente.

2.9.1 Elementos del control

2.9.1.1 Relación con lo planeado.

El control siempre existe para verificar el logro de los objetivos que se establecen en la planeación.

2.9.1.2 Medición.

Para controlar es imprescindible medir y cuantificar los resultados.

2.9.1.3 Detectar desviaciones.

Una de las funciones inherentes al control es descubrir las diferencias que se presentan entre la ejecución y la planeación.

2.9.1.4 Establecer medidas correctivas.

El Objeto del control es prever y corregir los errores.

2.9.2 Importancia del control para la administración de fraude

- Es importante para que se alcancen exitosamente los planes ya que el control establece medidas para corregir las actividades.
- El control se aplica en su mayoría de los procesos, personas y a los actos.
- Determina y analiza rápidamente las causas que pueden originar desviaciones o fraude, para que no se vuelvan a presentar en lo futuro.

El control es una de las etapas preponderantes del proceso administrativo, que aunque una empresa cuente con magníficos planes, una estructura organizacional adecuada y una dirección eficiente, el ejecutivo no podrá verificar cuál es la situación real de la organización si no existe un mecanismo que se cerciore e informe si los hechos van de acuerdo con los objetivos. El concepto de control puede ser utilizado en el

contexto organizacional para evaluar el desempeño general frente a un plan estratégico.

Desde el punto de vista de Chiavenato (1987) nos indica que el control es una función administrativa, fase del proceso administrativo que mide y evalúa el desempeño y toma la acción correctiva cuando se necesita. De este modo, el control es un proceso esencialmente regulador.

Capítulo III

Núcleo Argumental

Se iniciará el capítulo dando a conocer la misión de esta área en específico, por ser el tema central de la investigación para resaltar la importancia del puesto, así como la responsabilidad del profesional que funja como analista en ésta área.

3.1 Misión de la administración de fraude

La institución financiera para la que laboro, cuenta con una misión del área en general la cual se da a conocer en sus comunicados internos, la cual es la siguiente:

Administrar las pérdidas por fraude y los gastos relacionados a niveles que se logre:

- La mitad de fraudes que hay en promedio en el país.
- Reforzar la imagen de la institución como un lugar seguro para hacer negocios.

- Reducir el fraude a un nivel que se pueda encontrar un equilibrio óptimo entre la necesidad de los clientes para el uso de las tarjetas de crédito y débito contra el negocio para alcanzar ganancias.

3.1.1 Misión del puesto en particular.

Identificar a nivel cuenta los patrones de uso y poder compararlos con los patrones de fraude para mitigar la exposición.

3.2 Herramientas del puesto

Las herramientas más relevantes que se utilizan para el puesto adquieren su importancia, pues sin una de ellas no se puede desarrollar el trabajo, las cuales son:

- Los sistemas institucionales
- Procesos desarrollados por el banco,
- Software y Hardware internos por los cuales entendemos como equipo físico y programas.
- Conexiones de comunicación como internet y teléfono.

3.3 Importancia del puesto

La importancia de un analista de control del punto de compromiso es fundamentada por ser una de las áreas que dan continuidad a la seguridad de los clientes ante los ataques de defraudadores, esta puede convertirse en un pilar para la imagen y reputación del banco. Aunque se detectaran la cuentas comprometidas por parte de las demás áreas que integran el banco, no habría planes de acción ni administración específica como la que desempeña un analista de punto de control de compromiso, ya que en base a los procesos del puesto se puede dar continuidad a la

seguridad de las cuentas y tarjetas de los clientes e imagen de la institución financiera.

En el área de administración de riesgo de fraude del Grupo Financiero existen puestos que sirven para el funcionamiento del área misma, unas de ellas es en donde se desarrollan mis labores.

3.4 Funciones del puesto

❖ Administración de base de datos: es el trabajo que se realiza en un archivo donde se muestran las acciones que debe tomar el analista para cada cuenta, según el tipo de acceso que tenga el fraude y en este archivo se registran los resultados obtenidos después de tomar las acciones correspondientes.

La base de datos que se administra principalmente contiene 6 elementos que son:

- cuentas de los clientes
- información del negocio donde se comprometió la tarjeta o en su caso cajero donde se comprometió la tarjeta
- nombre del analista
- fecha de trabajo
- acción a seguir para cada cuenta
- resultado

Una de las funciones dentro de la administración de base de datos es colocar candados de seguridad según la acción que se solicite.

Es una medida preventiva de atacar de forma masiva la posible generación de fraudes.

- ❖ Colocar candados de seguridad en tarjetas de crédito y débito: Una vez ya detectado el tipo de acceso, se procede a aplicar candados de seguridad que van a actuar específicamente para frenar el posible medio de fraude para evitar más transacciones que puedan llegar a tener afectación. Esta medida es considerada como un plan de prevención.

- ❖ Contacto con los clientes: Una función adicional es cuando ya se tiene una muestra o base de datos que contengan cuentas previamente analizadas y con características de posible compromiso se procede a contactar al cliente y validar transacciones con él, gracias a la interacción e investigación directa con el cliente sobre las transacciones que aparecen en sus cuentas, se podrá validar si todas las reconoce, en este caso solo se le da información preventiva y de cultura de la prevención, en caso contrario se procede a cancelar tarjeta, levantar aclaraciones de los cargos no reconocidos y elaborar formatos para la generación y envío de un nuevo plástico con el fin de cambiar los datos de seguridad que contienen las tarjetas con la finalidad de que nadie que no sea el cliente tenga la nueva información y así proteger la información confidencial del cliente y de la cuenta.

El contacto con el cliente es una de las partes fundamentales para obtener muestras del posible compromiso de las tarjetas, hay veces que el área de monitoreo y estrategias no tiene las bases necesarias para encontrar un punto de compromiso, es decir, con los datos recabados no se puede asegurar que en un establecimiento en particular, esta comprometiendo los datos de los clientes, por eso es que la comunicación con el cliente es una pieza clave para encontrar ese punto de compromiso que ayudara a efectuar acciones contra el fraude.

Lo anterior se hace bajo un concentrado de las cuentas y base de datos al cual, manualmente y una por una se administra el control al punto de compromiso dependiendo el canal de acceso de cada cuenta.

Cabe resaltar que, cuando un analista de control de punto de compromiso tiene el grado o conocimiento de administrador, puede desarrollar los procesos y elaboración de documentos más rápidamente y con mayor calidad, el cual ayuda al desempeño laboral y personal; esto se basa en los conocimientos adquiridos en la carrera los cuales ayudan a mantener una elevada aceptación profesional , desenvolvimiento con los clientes y equipo de trabajo esto por ser una persona con mayor capacidad de análisis y entendimiento.

❖ Monitoreo de transacciones de clientes en tiempo real: es la acción que se debe tomar para la detección de un posible fraude en el momento que se está cometiendo con apoyo de sistemas institucionales e información previa que se recaba de cada cliente.

Se hace en base a un análisis con patrones de:

- Fraude
- Viaje
- Consumo
- Entre otras

Esta medida puede ser preventiva por qué se puede evitar que el fraude crezca, sin embargo, se cataloga como correctiva porque todas las transacciones analizadas ya fueron realizadas.

❖ Análisis de patrón de fraude en cuentas de crédito y débito: es el resultado del análisis entre negocios comprometidos y cuentas comprometidas y sirve para conocer más acerca del modo de operar de un defraudador.

Se trabaja utilizando como insumo cuentas referidas, cuentas canceladas, alertas de otros bancos y confirmación de negocios comprometidos.

❖ Generación de reportes para la información de mitigación de fraude: corresponde a la acción de generar un archivo concentrado en el que se indique las acciones que se tomaron por parte del analista de punto de control de compromiso y los resultados a los que se llegaron así como el comportamiento y seguimiento de las cuentas después de aplicarles planes de acción y corrección.

3.5 Aportaciones al puesto

En este apartado explico el proceso que implanté dentro del proceso de monitoreo para la detección de fraude, antes es necesario que en base a los análisis que hace un analista PCC ya mencionados en esta memoria laboral, se ha detectado que los defraudadores atreves de los medios de acceso de fraude e información personal de los clientes han logrado evolucionar a un nuevo fraude llamado “solicitudes fraudulentas”.

Esta modalidad de fraude todavía no se puede detectar fácilmente solo con los monitoreos ya sean en línea o en base de datos, esto por la dificultad de identificar si se está validando información de un cliente legítimo o un defraudador. Ya existen procesos de análisis que se llevan a cabo en una área especializada de la institución financiera y por agencias externas para la detección de posibles solicitudes fraudulentas, esta área y agencias elaboran reportes que envían al departamento de PCC para su análisis, es en ese momento cuando los analistas de PCC utilizan sus herramientas para decidir si se les permite a las cuentas seguir transaccionando o ya no.

En la problemática anterior el analista de PCC no solo se tiene que basar en los análisis puestos en una concentración de datos, sino también en los análisis en línea y en tiempo real.

Cuando se analiza una base de datos, estos ya no pueden variar, pues los resultados obtenidos por evaluaciones previas ya sean del banco o de una agencia, ya están plasmados en reportes, esto da una limitante a no poderle dar continuidad a las transacciones que puedan verse sospechosas y tomar una mejor decisión, a estas cuentas que en su mayoría cumplen todas las reglas para definir y determinar que es una solicitud fraudulenta se les coloca un candado de seguridad, esto lo hace el analista de PCC, así mismo se plasma la instrucción para que ejecutivos especializados reciban llamadas de los clientes que ya no pueden transaccionar por dichos candados y validar con ellos para tener la certeza de que están hablando con un cliente legítimo y no el defraudador, esta acción es fácil ya que en su los clientes legítimos en su mayoría tienen la inquietud de saber porque no pueden transaccionar con sus tarjetas lo que los obliga a ponerse en contacto con el banco vía telefónica o acudiendo a una sucursal, en ese momento es la institución financiera la que tiene la autoridad de validar todos los datos del cliente para así poder permitirle transaccionar con sus tarjetas.

En el caso de que se le coloque un candado de seguridad a una cuenta fraudulenta, el defraudador no podrá validar datos originales y exigir al banco que le permita seguir transaccionando, he ahí cuando el banco detiene el fraude.

El punto medular de la problemática es cuando un analista de PCC está haciendo monitoreo en línea y detecta una posible solicitud fraudulenta, en este punto del problema el analista se presenta con varias objeciones que le impiden colocar un candado de seguridad, las cuales son:

- No se tiene la certeza de que se trata de una solicitud fraudulenta.
- Las transacciones validadas son de alta importancia para el flujo de efectivo de la institución financiera
- Un candado de seguridad mal aplicado genera molestia en los clientes, mala reputación y detención de transacciones.

Dado que los puntos anteriores son suficientes para que la colocación de un candado de seguridad no se pueda aplicar solo en base a un análisis así es que se procede a tener contacto con el cliente vía telefónica, para esto se utilizan técnicas ya preestablecidas por el área de PCC que no son suficientes para poder validar de manera correcta la legitimidad del cliente, es cuando yo procedo a elaborar un proceso de validación muy rápido al momento de ya estar en contacto con un cliente vía telefónica, el mismo que se encuentra establecido obteniendo las mejores prácticas de confidencialidad que el banco ya tenía y combinándolo con técnicas de "Call Model" dicho curso aprendido en una certificación que obtuve en la institución financiera HSBC misma que se basa en la capacidad de hablar con clientes vía telefónica para obtener información, esta certificación conlleva un contrato de confidencialidad por ser propiedad única del banco(HSBC), esta es la razón por la que a groso modo se explicara únicamente el proceso terminado para la validación de posible solicitud fraudulenta ya que es de elaboración propia.

Primero se debe tener presente la manera de pensar y actuar de la mayoría de los clientes y establecer lo que no les gusta en una llamada telefónica por parte de una institución financiera, a continuación se enumeran las más relevantes:

1. Llamadas de larga duración con un representante del banco
2. Que un representante solicite información confidencial por mínima que sea.
3. Hablar con un desconocido.
4. No saber con quién están hablando exactamente.
5. Brindar información de cualquier tipo.
6. Llamadas de cobranza, ventas y promociones.
7. Horarios inusuales de las llamadas
8. No obtener un beneficio por recibir o atender la llamada.

La segunda parte que se debe tener en cuenta es que en la mayoría de los casos de validación de la solicitud fraudulenta, cuando un analista de PCC decide tener contacto con el posible cliente, este sea el defraudador y que tome identidad ilícita del cliente legítimo.

Los defraudadores con anterioridad obtuvieron parte de la información importante de los clientes la cual les permite apertura cuentas a su nombre, a continuación se mencionan las más usuales.

- Dirección de la vivienda del cliente
- Nombre completo
- Comprobante de domicilio
- Credencial de elector falsificada con datos del cliente
- Referencias personales o laborales apócrifas
- Comprobantes de ingresos falsificados.
- Números telefónicos falsos

Los anteriores puntos son los necesarios para poder aperturar cuentas en las instituciones financieras, en la experiencia obtenida por el área se puede confirmar que un defraudador puede tener solo parte de la

información del cliente ya que sería imposible saber todo lo relacionado a un cliente legítimo como lo son:

- Nombres de familiares
- Referencias
- Beneficiarios
- Otras cuentas aperturadas en el mismo banco
- Límites de crédito
- Saldos de las cuentas
- Movimientos en cuentas de débito o historial crediticio
- Datos del primer domicilio registrado por cliente
- Entre otros.

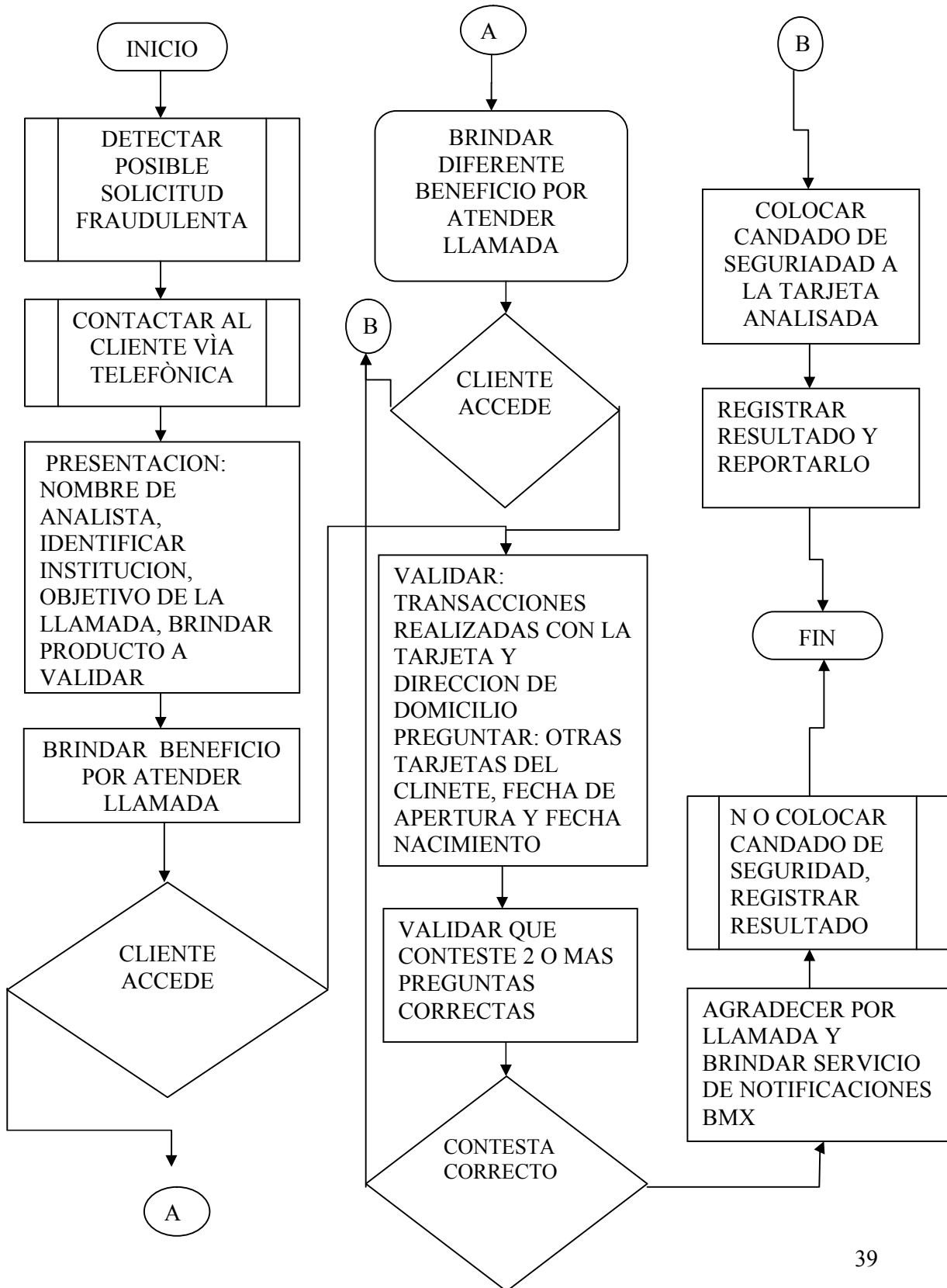
Lo anterior los hace vulnerables a preguntas específicas que los analistas de PCC puedan realizarles.

El tercer punto a tomar en cuenta es que el analista de PCC debe confirmar con quien se está comunicando, ya sea el defraudador o el cliente. En este momento crítico la mayoría de las veces se tiene que lidiar con la astucia de un defraudador y con la desconfianza de un cliente y es así como finaliza el proceso.

A continuación de manera general se explicará a través de un diagrama de flujo el proceso que implemente para los casos de validación la cual combina las técnicas de Call Model para no incurrir en una molestia con el cliente legítimo y con la extracción de información segura con un defraudador.

3.6 Diagrama de flujo para casos de validación

(ELABORACIÓN PROPIA)



Conclusiones y Sugerencias

Por lo arriba mencionado se puede concluir que de las labores que se desarrollan en el área de prevención de fraudes, en particular del control del compromiso, es que, siempre se tiene que estar en constante investigación y análisis de los fraudes para poderse detectar a tiempo de forma preventiva, desde el umbral de los fraudes se puede percibir que están evolucionando cada vez más rápido las formas y métodos que utiliza el hampa al respecto, lo que dificulta su detección con antelación, por lo que se debe contar con personal profesional con mente similar a los defraudadores que sirvan como espías y que se dediquen a la investigación y solución de forma continua por parte de la institución financiera, sin embargo, hay que acrecentar los controles de forma estratégica para ganar la guerra a los defraudadores de manera que se pueda minimizar al máximo el compromiso de las cuentas.

El hablar de procesos que deberían llevar los negocios, sucursales y clientes, es algo en que el banco no puede intervenir directamente, pero es necesario influir mediante comunicados o capacitación acerca de la importancia y cultura de la prevención de fraudes ya que esta sería una de las maneras en que la unión de todas las partes pueden bajar considerablemente la afectación que se tiene actualmente, así poder reducir costos y pérdidas monetarias impactantes tipificadas como el fraude del siglo a través de tarjetas bancarias.

Se debe observar que al contratar personal para el área de administración de fraudes, ésta debe ser confiable e investigada de forma escrupulosa.

Tomando en cuenta la experiencia que se adquiere siendo analista del punto de control de compromiso se pueden dar algunas

recomendaciones eficaces que pueden evitar el compromiso de la información de las tarjetas de los clientes, estas pueden ser:

- ❖ No divulgar claves de acceso como pueden ser NIP y PASSWORD; a ninguna persona, ya sea familiar o conocido porque por mucha confianza que pueda existir con la persona, ésta, tal vez no tome las medidas necesarias de confidencialidad y pueda llegar a manos de alguien más.
- ❖ Tener en mente de que la información de las tarjetas es única e intransferible. Esto ayudará a tener presente que el cliente es el único responsable y dueño de los datos.
- ❖ Al pagar en establecimientos no perder de vista en ningún momento la tarjeta que va a ser utilizada para pagar y que solo sea ingresada en terminales para el mismo fin, así como en lo posible evitar que sean ingresadas en otros dispositivos que sirvan para la copia de datos de la tarjeta.
- ❖ No ingresar la tarjeta en cajeros automáticos que presenten anomalías como dispositivos pegados o insertados en cualquier parte del cajero,
- ❖ Tapar los datos de la tarjeta con la mano cuando se disponga a insertarla en un cajero automático para que nada ni nadie tenga la posibilidad de ver los números de la tarjeta o el NIP que va a ingresar.
- ❖ No acepte ayuda de otras personas para hacer cualquier tipo de transacción, ya sea por cajero automático, internet y telefónica.
- ❖ No ingresar los datos de las tarjetas en páginas de Internet que no sean seguras o que no se pueda comprobar la autenticidad de la página.
- ❖ No mandar claves de acceso o información de las tarjetas a través de mensajes, correos electrónicos, publicaciones en redes sociales y servicio postal.

- ❖ No aceptar tarjetas que no cumplan con datos de seguridad básicos y para esto no es necesario saber acerca de procesos de un banco o de las tarjetas, simplemente basarse a lo lógico como ejemplo podemos decir una tarjeta en blanco que no trae nombres o números e incluso el nombre de alguna institución bancaria o del negocio y que piden que ingresen esa tarjeta a la terminal para hacer el pago, otro ejemplo es que se esté entregando una tarjeta que describe un nombre de persona diferente a la credencial de identificación o que simplemente proporcione una tarjeta alguien del género masculino con nombre de una persona con género femenino, como se puede ver son datos fáciles que al detectarlos y reportarlos a las autoridades competentes o en su caso a el área que está encargada en cada negocio, se puede eliminar que los defraudadores tengan la libertad de transaccionar en cualquier comercio sin limitaciones ni preocupaciones.
- ❖ Evitar aceptar que alguien ajeno haga compras por el cliente, esto no solamente quiere decir que el cliente le de la tarjeta a alguien más para que pague, sino que, hay defraudadores dedicados a ser intermediarios indirectos del negocio y el cliente.
- ❖ Un ejemplo hipotético es que un cliente desee hacer la compra de boletos de avión y un externo le sugiere que le dé el dinero en efectivo a él y que este va a comprar los boletos por el cliente, así evitándole papeleos y ofreciéndole descuentos por que según puede tener convenios con los negocios, el cliente recibe sus boletos sin problema y el defraudador el pago; en este supuesto hay cuatro afectaciones que implican a una institución financiera, la aerolínea y el cliente de los boletos y el auténtico cliente de la tarjeta con la que se compraron los boletos, esto porque los boletos se compraron con tarjeta clonada vía internet . por consiguiente el cliente original que tuvo su información comprometida ingresa una aclaración al banco por cargos no reconocidos, el banco se afecta

económicamente e inicia investigación del cargo, se reporta a la aerolínea y se rechazan los boletos.

- ❖ Todo esto se puede evitar con una cultura de gestión personalizada y siempre tener en mente que las transacciones que se hagan se deben asesorar únicamente con personal autorizado, que se pueda identificar como empleado del negocio y que puede ser intermediario, además verificar cada uno de los productos adquiridos. De esta manera se puede disminuir la forma de actuar de los defraudadores confiados en la buena fe de la gente y clientes.

Referencias

Cifuentes, S. (1986). *Negocio Jurídico* Ed. Astrea, 1ª ed., Buenos Aires, Argentina.

Código Penal Federal Artículo 386.

Chiavenato, I. (1987). *Introducción a la Teoría General de la Administración* Ed. Mc Graw Hill, Bogotá.

Fayol, H. (1969) *Principios de la Administración Científica* Ed. Moderna, México.

Labrada, R. (2010). *Ética en los negocios* Ed. ESIC, México.

Terry, G. (1984). *Principios de Administración* Ed. CECSA, México.

Torres, A. (2001). *Acto Jurídico* Ed. Moreno, 2ª ed., Lima, Perú.

Reyes A (2005). *Administración moderna* Ed. Limusa, México.

Munch, L. (1999) *fundamentos de la administración* Ed. Trillas, México.

Grupo Financiero Banamex (2012). *Curso de actualización: Definición de fraude y riesgos*, México

Grupo Financiero HSBC (2010). *Curso de actualización: Prevención de fraudes, lavado de dinero y riesgo reputacional*, Intranet, México.

Citigroup (2011). *Manual de inducción* México D.F.