PAULO ANDRÉS CADENA CABRERA

MODELO OPERATIVO DE PREVENCIÓN Y CONTROL DE FRAUDE EN UN PROGRAMA DE LEALTAD, QUE PERMITA UNA EXPERIENCIA ACORDE CON EL SEGMENTO DE MERCADO Y HÁBITOS COTIDIANO DE LOS CLIENTES

Bogotá, D.C. – Colombia

2022

MODELO OPERATIVO DE PREVENCIÓN Y CONTROL DE FRAUDE EN UN PROGRAMA DE LEALTAD, QUE PERMITA UNA EXPERIENCIA ACORDE CON EL SEGMENTO DE MERCADO Y HÁBITOS COTIDIANO DE LOS CLIENTES

Paulo Andrés Cadena Cabrera

Mauricio Pérez Salazar

Director

Universidad Externado de Colombia

Facultad de Derecho

Maestría en Gestión Integral del Riesgo

Bogotá D.C. - Colombia

2022

UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE DERECHO

MAESTRIA EN GESTIÓN INTEGRAL DEL RIESGO

Rector:	**Dr. Hernando Parra Nieto**
Secretaría General:	**José Fernando Rubio**
Director Departamento de Riesgos y Seguros:	**Dra. Hilda Esperanza Zornosa Prieto.**
Presidente de Tesis:	**Dra. Hilda Esperanza Zornosa Prieto.**
Director de Tesis:	**Dr. Mauricio Pérez Salazar**
Jurado Examinador:	**Dr. Carlos Restrepo Rivillas**

Nota del Autor

Modelo operativo de prevención y control de fraude en un programa de lealtad, que permita una experiencia acorde con el segmento de mercado y hábitos cotidianos de los clientes.

Maestría en Gestión Integral del Riesgo. Facultad de Derecho. Universidad Externado de Colombia
(Bogotá - Colombia).

La correspondencia con relación a este trabajo debe dirigirse al programa de Posgrado:

Paulo Andrés Cadena Cabrera

Correo Electrónico: paulo.cadena@est.uexternado.edu.co.

Dedicatoria

Este trabajo de grado está dedicado a mi familia, mi esposa Lina Constanza, mi hija María Paz, por su paciencia y apoyo en estos años de sacrificio y esfuerzo, especialmente, por el tiempo que no ha sido posible dedicarles. Su comprensión y amor permitió este gran logro para mi vida personal y académica.

Un reconocimiento especial para mi hijo Juan Diego que desde el cielo siempre me acompaña y nunca ha dejado de estar con nosotros.

Agradecimientos

Ante todo, doy gracias a Dios por permitirme realizar esta Maestría, por concederme salud y tiempo para lograrlo.

Gracias a todas las personas de la Universidad Externado de Colombia, en especial a la Dra. Hilda Esperanza Zornosa Prieto por su profesionalismo en el desarrollo de esta Maestría, y a la Dra. María Alejandra Rodríguez Avellaneda por su apoyo, coordinación y dedicación para sacar adelante este proyecto. Igualmente, gracias a cada uno de los profesores que pusieron a nuestro servicio su conocimiento, agradezco inmensamente su paciencia y entrega durante todo el proceso.

Mil y mil gracias a mis compañeros de Maestría, a todos ellos mis respetos por su profesionalismo y excelente trabajo en equipo. Son grandes personas y me llevaré de cada uno el mejor recuerdo.

Contenido

Lista de figuras

Lista de tablas

Glosario

CONCEPTOS DE GESTIÓN DE FRAUDE

AUTENTICACIÓN BASADA EN RIESGO

La autenticación basada en riesgo proporciona una decisión de acceso en función de una evaluación dinámica del riesgo o el nivel de confidencialidad de una transacción. La autenticación basada en riesgo utiliza analíticas de datos contextuales y de comportamiento para calcular el riesgo.

CIBERSEGURIDAD

Se conoce como la seguridad de la tecnología de la información, puesto que engloba un gran número de técnicas y métodos para proteger el sistema, así como otros dispositivos o las redes.(tecnoredes, blog,dic 2020)

FRAUDE

La palabra fraude viene del latín FRAUDIS, que consiste en una acción que resulta contraria a la verdad y a la rectitud. El fraude se comete en perjuicio de una persona u organización. Consiste, en definitiva, en una conducta deshonesta que busca obtener ventaja injusta sobre otro. (U.Javeriana, s.f Jenith) (ISO Guía CEI 73, 2009)

FRAUDE EXTERNO

Actos fraudulentos cometidos por terceros con los que se relaciona o contrata la organización, en sus diferentes operaciones, en base a los documentos utilizados, los procedimientos establecidos y las obligaciones legales y contractuales asumidas, entre otros elementos, para la identificación de los potenciales delitos cometidos (tipificación), la formulación de la imputación específica (hecho atribuible), la acreditación de la misma (prueba), y la formulación de la estrategia que corresponda seguir, según el contexto en que se encuentre el cliente. (clubensayos, Beida Machuca, 2019)

FRAUDE INTERNO

El uso de la ocupación o empleo de uno para el enriquecimiento personal a través del mal uso deliberado o mala aplicación de los recursos o activos de la organización. (ACFE, recursos contra el fraude,s.f).

En este marco conceptual no podemos dejar atrás autores clásicos como el criminólogo Donald R. Cressey (1961), quien asegura que para que un fraude se materialice deben existir tres elementos:

1º. Motivación (incentivo, presión). Cuando la administración u otros empleados tienen un estímulo o presiones que les aportan

razones justificativas para cometer fraudes. (fraude interno-wordpress,feb 2016)

2º. Poder (Oportunidad). Serían las circunstancias que facilitan las posibilidades de perpetuar fraudes (por ejemplo, la ausencia de controles, controles ineficaces, o la capacidad de la administración para abrogar los controles). (fraude interno-wordpress,feb 2016)

3º. Racionalización, actitud. Cuando las personas son capaces de racionalizar un acto fraudulento en total congruencia con su código de ética personal o que poseen una actitud, carácter o conjunto de valores que les permiten, consciente e intencionalmente, cometer un acto deshonesto. (fraude interno-wordpress,feb 2016)

INGENIERÍA SOCIAL En la ingeniería social los cibercriminales usan las interacciones entre personas para que el usuario comparta información confidencial. Ya que la ingeniería social se basa en la naturaleza humana y las reacciones humanas, hay muchas formas en que los atacantes pueden engañar, en línea o sin conexión. (Norton,s.f)

INTELIGENCIA ARTIFICIAL La inteligencia artificial (IA) hace posible que las máquinas aprendan de la experiencia, se ajusten a nuevas aportaciones y realicen tareas como hacen los humanos. (Universidad nebrija, nov 2019)

MACHINE LEARNING Es un método de análisis de datos que automatiza la construcción de modelos analíticos. Es una rama de la inteligencia artificial basada en la idea de que los sistemas pueden aprender de datos, identificar patrones y tomar decisiones con mínima intervención humana. (SAS, s.f.)

PUNTO COMÚN DE COMPROMISO (PCC) Es un punto en común utilizado por varios usuarios o clientes antes del fraude, el PCC se puede presentar en un establecimiento de comercio (externo) o de forma interna o a través de un proveedor de servicios.

RIESGO Es una valoración del presente con información del pasado, con una dimensión social, de algo que se va a concretar en el futuro. Sólo el futuro nos dirá si la decisión fue acertada o no. (Uexternado, Dra. Hilda Zornosa, 2019)

CONCEPTOS DE GOBIERNO Y ESTRATEGIA

GOBIERNO Gobierno es el conjunto de normas, principios y procedimientos que regulan la estructura y el funcionamiento de los órganos de

gobierno de una empresa o área dentro de una organización. (ISO Guía CEI 73, 2009)

POLÍTICAS Son los lineamientos de actuación de las áreas de gestión de una compañía, asegurando las mejores prácticas con el propósito de buscar el cumplimiento de objetivos de la compañía.

PROCEDIMIENTOS Consiste en seguir ciertos pasos predefinidos para desarrollar una labor de manera eficaz. (definición.de, 2008, actualizado 2021)

CONCEPTOS DE SEGUIMIENTO Y CONTROL

ANALÍTICA La analítica es un campo incluyente y multidimensional que utiliza matemáticas, estadística, modelos predictivos y técnicas de aprendizaje basadas en máquinas para hallar patrones y conocimientos significativos en datos grabados. (SAS, s.f.)

MÉTRICAS Las métricas son aquellos datos expresados numéricamente que sirven para analizar el rendimiento o comportamiento. Ayudan a medir el cumplimiento de objetivos. (ISO Guía CEI 73, 2009)

REGLAS DE ALERTAMIENTO Son reglas de monitoreo que solamente generan alertamiento porque se ha presentado un cambio en el perfil transaccional del cliente, y son analizadas en segunda instancia por un analista quien toma una decisión sobre la misma.

REGLAS DE MONITOREO Son parámetros determinados con base en la analítica y el perfil transaccional del cliente, con el objetivo de identificar cualquier comportamiento inusual en sus consumos dentro del programa de fidelización

REGLAS DE NEGOCIO Son parámetros determinados según la actividad comercial del negocio. Normalmente se miden por valor y cantidad de transaccionales.

REGLAS DURAS Son reglas de monitoreo que bloquean, no permiten la transacción por el alto riesgo de fraude que representa.

CONCEPTO DE NEGOCIO

PROGRAMA DE LEALTAD Un programa de lealtad es una iniciativa de las empresas para estimular que sus clientes actuales hagan nuevas adquisiciones de sus productos y servicios, aumentando su fidelidad hacia la compañía. (rockcontent, blog,junio 2019)

Los programas de lealtad pueden funcionar como poderosos aliados en la tarea de fidelizar clientes en una economía donde

	cada vez es más difícil retener a los usuarios para que regresen a consumir productos y servicios. (rockcontent, blog,junio 2019) Los programas de lealtad pueden definirse como un sistema estructurado de acciones y estrategias de marketing, dirigidas a estimular a los usuarios y clientes de una marca o negocio a que adquieran sus productos con determinada frecuencia. (rockcontent, blog,junio 2019)
RENTABILIDAD FINANCIERA	Por otro lado, la rentabilidad financiera hace referencia al beneficio que se lleva cada uno de los socios de una empresa, es decir, el beneficio de haber hecho el esfuerzo de invertir en esa empresa. (Escuelapce,s.f.)
REPUTACIÓN	Daños a la reputación de la marca que pueden afectar negativamente la confianza de inversores, acreedores y potenciales clientes.

Fuente: ISO Guía CEI 73 (2009)

Resumen

Frente a la necesidad de controlar de forma adecuada el riesgo de fraude transaccional en una compañía de lealtad, se generó la necesidad de investigar y analizar cuál sería el mejor modelo de prevención y control para dicha compañía. Para lo cual se dio inicio a este proyecto que parte de la descripción de los programas de lealtad, teniendo en cuenta que hoy han evolucionado a programas de coalición. Luego veremos quiénes son los grupos de interés en este tipo de programas y cuál es el objetivo de las compañías que hacen parte de este ecosistema.

Dicho esto, nos concentramos en determinar qué tipos de fraudes se pueden presentar en estos programas, sus modalidades aplicadas tanto a la acumulación como a la redención, desde el punto de vista virtual y presencial. Así mismo, nos detendremos en la descripción de tipos de fraudes internos y externos.

A partir de este contexto, definiremos un modelo operativo de prevención y control de fraude transaccional basado en ejes principales, definición del gobierno, gestión, indicadores y aplicación de métricas que permitan conocer los resultados de la implementación propuesta y desarrollada en este modelo.

Por último, entendiendo la necesidad de equilibrar el control del riesgo y la experiencia del cliente, se determinó la importancia de establecer, dentro del modelo, una autenticación basada en riesgo que permita ejercer controles más efectivos, controles que disminuyan fricciones y no afecten la experiencia del cliente. Todo esto bajo dos pilares importantes: la tecnología y la analítica, ya que es a partir de una información adecuada y suficiente como se logran establecer patrones de comportamiento que lleven a mejorar el conocimiento del cliente y propicien la toma de decisiones acertadas y la aplicación adecuada de controles bajo el contexto de una compañía de lealtad.

Palabras Claves: Fraude, Ciberseguridad, Inteligencia artificial, Programa de lealtad; procedimiento, Reputación.

Introducción

Los programas de lealtad o de fidelización iniciaron a principios de los años 80 con las aerolíneas, cuando American Airlines decidió ofrecer beneficios a los viajeros frecuentes. En Colombia tenemos uno de los programas más reconocidos en este sector: Lifemiles, el cual inició en el año 2011 y hoy tiene más de 6 millones de usuarios. (Gestión, mayo 2017)

Estos programas generan acumulación de puntos a través de compras con tarjetas de crédito y con cualquier medio de pago, a través del consumo en establecimientos de comercio que se encuentren afiliados a determinado sistema de fidelización, para lo cual, sólo se requiere un ID como identificación o el número de cédula.

Obtenidos finalmente los puntos, se convierten en un medio de pago (presencial o no presencial) de productos o servicios ofrecidos por los establecimientos aliados al programa, cuyo objetivo principal es el de ofrecer una experiencia al cliente como incentivo para que continúen acumulando a través del consumo en el comercio o de la utilización de la tarjeta.

Sin embargo, la mayoría de los clientes no tienen consciencia de los riesgos de tener gran cantidad de puntos acumulados disponibles, por tal razón, no realizan una buena custodia de sus credenciales utilizadas para la redención o la utilización.

Por otra parte, las compañías que iniciaron con este tipo de programas, sin prever los riesgos implícitos en él, no contaron con un análisis de riesgos, lo que generó que grupos de delincuencia identificarán sus debilidades para atacar y vulnerar, y, en definitiva, obtener información de credenciales o claves que les facilitarán la posterior utilización de los puntos en establecimientos de comercio.

El crimen cibernético no se restringe a los bancos, a los medios electrónicos de pago, a los “brokers” de valores o al comercio electrónico. (Gestión, mayo 2017). Los programas de lealtad se están convirtiendo en un atractivo muy importante para el sector delincuencial.

Hoy en día, las personas se cuidan de las estafas por correo electrónico y teléfono que apuntan a sus datos financieros y personales, pero no piensan que alguien puede querer tener acceso a sus puntos a través del mismo esquema de ingeniería social o a través de un Phishing.(ebizlatam, junio 2017).

Actualmente, y desde hace mucho tiempo, el Phishing se ha convertido en el sistema más eficaz para engañar. En promedio, el 90% de las personas, según datos de Barracuda Networks, ha sido víctima de esta práctica. Los ataques también pueden provenir del uso de equipos compartidos infectados, de un operador de centro de llamadas falso, de una fuga de información en un establecimiento aliado; incluso, de un fraude interno de la compañía del programa de fidelización. .(ebizlatam, junio 2017).

Un programa de lealtad puede perder miles de millones de pesos en un corto lapso de tiempo si no tiene un buen control de sus sistemas de información, de sus canales de servicios, y si no efectúa con frecuencia controles internos o externos con sus aliados. Esta es la razón por la que este trabajo de grado proyecta desarrollar un modelo de prevención y control de fraude para un programa de lealtad, ya que, aunque se han comenzado a realizar esfuerzos por mitigar el fraude transaccional, no han sido suficientes. En vista de esto, consideramos importante intentar dar respuesta al siguiente interrogante: ¿Será conveniente tener un sistema de información transversal entre compañías de lealtad en Colombia, que permitan medir de manera cuantitativa los riesgos de fraude?

Una de las hipótesis frente a esta pregunta es que hoy la lucha contra el fraude no es un problema competitivo. El delincuente no es leal a ninguna marca, busca obtener beneficio personal donde existe una vulnerabilidad. Si se pensara en un sistema de información colectivo que beneficie a todas las compañías que participan en el sector en pro de la prevención y la anticipación del riesgo, ¿se reduciría la pérdida por fraude y mejoraría la experiencia para todos los clientes del ecosistema?

Con una agremiación del sector, lograríamos la unión de varios programas de lealtad con el objetivo de compartir conocimiento, generar una interacción directa con las autoridades competentes, desarrollar modelos frente a fugas de información, modus operandi, y, finalmente,

fortaleceríamos la capacidad de análisis a través de herramientas basadas en inteligencia artificial que nos ayudarían a anticiparnos a situaciones irregulares.

Sin embargo, de implementarse un sistema cooperativo, se debe estudiar muy bien la forma de adaptarlo para que se protejan los tres pilares básicos del modelo: confiabilidad, integralidad y disponibilidad. Esto supone dos retos importantes: cumplir con la ley de protección de datos y proteger el modelo de cualquier riesgo cibernético. Todo lo anterior generaría una revolución en la industrial de lealtad, no sólo por los beneficios desde el punto de vista de riesgo, sino por la oportunidad de concentrar la información del cliente en un sólo repositorio disponible para todo el gremio.

Por otra parte, la metodología utilizada en esta investigación será cualitativa. Describiremos y documentaremos todo el modelo operativo de prevención y gestión de fraude para una compañía de lealtad, revisaremos los métodos utilizamos por compañías de referencia en este tipo de riesgos como COSO y ACFE, y, por último, se entregará un modelo con base en el análisis de sus canales, métodos de autenticación y productos.

Dentro de la etapa de investigación se realizó revisión de documentos referentes en la industria de lealtad, definiendo los ejes del modelo operativo desde el punto de vista de la estrategia y la táctica.

Para terminar, se desarrollará nuestra hipótesis para consolidar una propuesta innovadora, ágil y viable para este tipo de riesgos. Todo esto recopilando información del sector, tanto local como internacional.

Objetivos

Objetivo general

Definir un modelo operativo de prevención y control de fraude transaccional en un ecosistema de lealtad de clientes.

Objetivos específicos

- Identificar cómo está conformado, de una forma general, un programa de lealtad o fidelización.
- Conocer el comportamiento y modalidades de fraude en un programa de lealtad.
- Describir los ejes del modelo operativo de fraude.
- Definir el proceso de gestión del modelo operativo.

Capítulo 1.

Composición de un programa de Lealtad o Fidelización

Es importante conocer, en términos generales, cómo está compuesto un programa de lealtad, quiénes hacen parte de su ecosistema, y toda su estructura, incluidos los roles de cada uno de sus grupos de interés o "stakeholders".

Varias investigaciones, y de diferentes consultoras, han demostrado que en el segmento B2C (Business to Consumer), el costo que representa conseguir un nuevo cliente es mucho más alto que el de mantener a uno ya existente. También concluyeron que los clientes fieles son más valiosos que los nuevos. Esta es una de las razones por las que muchas empresas o marcas han decidido orientar sus esfuerzos en desarrollar programas de fidelización o de lealtad que motiven a sus clientes a seguir comprando y utilizando sus servicios, a cambio de una recompensa.

¿Qué es un programa de lealtad?

Un programa de lealtad es una iniciativa de las empresas que estimula a sus clientes actuales para que hagan nuevas adquisiciones de sus productos y servicios, aumentando así, su fidelidad hacia la compañía. (rockcontent, blog,junio 2019)

Los programas de lealtad pueden funcionar como poderosos aliados en la tarea de fidelizar clientes en una economía donde cada vez es más difícil retener a los usuarios para que regresen a consumir productos y servicios. (rockcontent, blog,junio 2019)

Los programas de lealtad pueden definirse como un sistema estructurado de acciones y estrategias de marketing, dirigidas a estimular a los usuarios y clientes de una marca o negocio a que adquieran sus productos con determinada frecuencia. (rockcontent, blog,junio 2019)

Así mismo, muchas de las estrategias de las empresas también se basan en conseguir, a través de su programa de lealtad, el registro o atracción de nuevos clientes.

Algunas de las recompensas más utilizadas por las empresas en los programas de lealtad pueden ser:

- Puntos que pueden utilizarse o redimirse por productos y/o servicios en la misma compañía.
- Puntos que pueden redimirse por productos y /o servicios de terceros.
- Recompensas en efectivo.
- Recompensas por descuentos especiales en determinados productos o servicios.
- Recompensas en membresías exclusivas.

Los programas de lealtad han venido evolucionando en el tiempo. Hoy en día, la mayoría de compañías buscan no sólo la lealtad de sus clientes a través de programas propios, sino que también intentan participar en programas de fidelización bajo un formato de coalición, donde existe un ecosistema de establecimientos, experiencias, servicios y muchas actividades para que los clientes logren una mayor satisfacción y mejores beneficios.

Este tipo de programas de coalición generan una visión más completa y profunda. Existen beneficios para todo el ecosistema, incentivos para los socios, mayor tráfico para los aliados, cotidianidad para el cliente y mejores ingresos para el programa.

Los programas de fidelización no consisten solamente en gestionar relaciones a largo plazo con los clientes fieles o actuales. También deben hacerse cargo de captar nuevos consumidores que puedan sentirse interesados en la marca. (inloyalty, enero 2018)

Según Inloyalty “Para lograr que el programa funcione adecuadamente tenemos que tener en cuenta los factores y elementos que interfieren en la lealtad de un usuario hacia una empresa, y seguir los siguientes consejos que te mostramos en la siguiente infografía”. .(inloyalty, enero 2018)

Figura 1. ***El éxito en los programas de fidelización en coalición.***

Fuente: Inloyalty (2020). Soluciones de fidelización eficaces y a la medida de tus objetivos. Recuperado de https://inloyalty.es/publicaciones-completo?categoria=11

Esta misma compañía española manifiesta que un programa de lealtad exitoso debe tener cuatro elementos:

Figura 2. ***¿Qué elementos ayudan a que un usuario sea leal a una empresa?***

Fuente: Inloyalty (2020). Soluciones de fidelización eficaces y a la medida de tus objetivos. Recuperado de https://inloyalty.es/publicaciones-completo?categoria=11

Agregaría a este análisis dos elementos que se consideran importante para el cliente. En primer lugar, tenemos la cotidianidad. Un programa de coalición debe tener, dentro de su lista de aliados y socios, una cantidad suficiente de actividades comerciales que le permita al cliente usarlo en su vida cotidiana, por ejemplo: estaciones de servicio, aerolíneas, agencias de viaje, supermercados, establecimiento de ropa y vestuario, comida etc., además de un banco que, como socio fundamental, permita al cliente el aumento de la acumulación de puntos por medio de la utilización de servicios financieros como la tarjeta de crédito. En segundo lugar, tenemos la experiencia. Una compañía debe llegar a sus clientes más por la vía del sentimiento que de la racionalidad; esto mejorará de tal manera la recordación en el cliente, que su experiencia no se limitará a la utilización de puntos o millas.

En la siguiente gráfica resumimos la generación de valor que entrega un programa de coalición para cada uno de sus grupos de interés, socios, aliados y clientes en este caso particular.

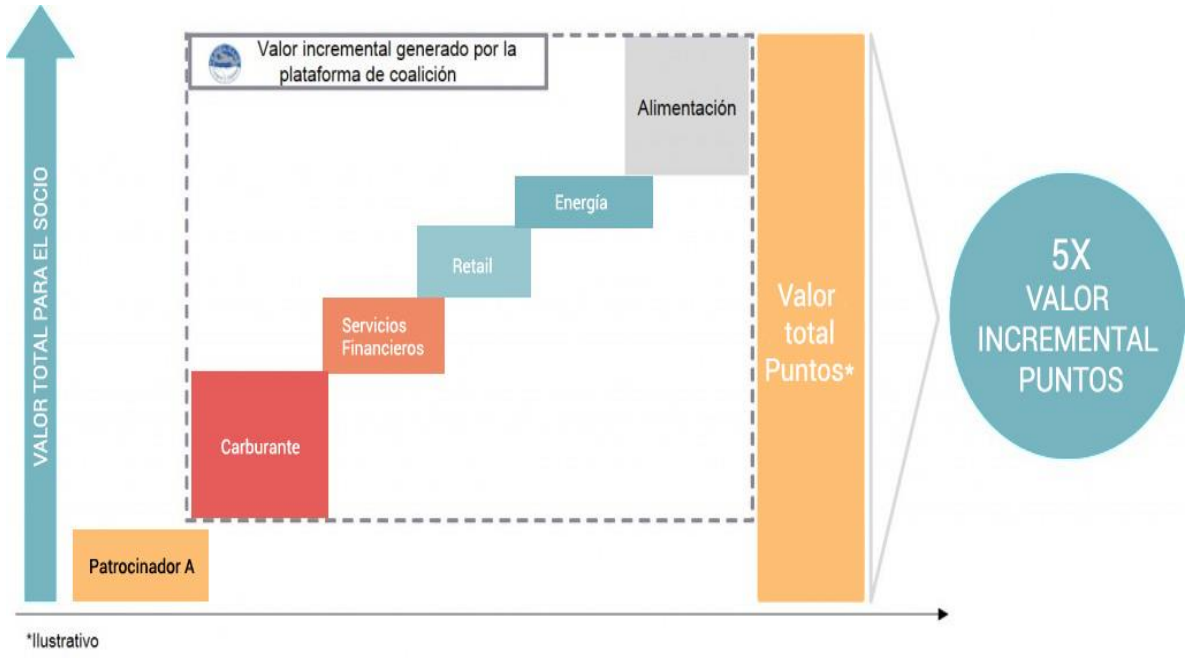

Figura 3. ***Valor incremental generado por la plataforma de coalición***

Fuente: Inloyalty (2020). Soluciones de fidelización eficaces y a la medida de tus objetivos. Recuperado de https://inloyalty.es/publicaciones-completo?categoria=11

¿Quiénes hacen parte de un programa de Coalición?

El primer componente es *la empresa* que ofrece un artículo o servicio y que crea su propio programa de lealtad:

***Empresa*:** "El concepto de empresa refiere a una organización o institución, que se dedica a la producción o prestación de bienes o servicios que son demandados por los consumidores; obteniendo de esta actividad un rédito económico, es decir, una ganancia. Para el correcto desempeño de la producción estas se basan en planificaciones previamente definidas, estrategias determinadas por el equipo de trabajo." (Conceptode, 2019, párr. 8)

En el mercado hay muchas empresas o compañías que tienen su propio programa de fidelización, algunas de ellas son: Starbucks (My Starbucks Rewards), The North Face (VIPeak) y Banco Falabella (Puntos CMR).

La mayoría de ellas ofrecen puntos a través de la utilización de sus servicios o compra de sus productos con el objetivo de ofrecer experiencias a través del conocimiento de los hábitos de sus clientes. Otros ofrecen descuentos especiales dentro del mismo sistema.

Por otro lado, existen programas de lealtad dentro de un ecosistema donde participan varios componentes entre los que podemos nombrar:

Socios: Persona natural o jurídica que hace parte de un contrato. Para el caso particular de los programas de lealtad, los socios se comprometen a aportar un capital a una sociedad, normalmente con una finalidad empresarial, y con el propósito de aumentar dicho capital y de potenciar las marcas que hacen parte de la coalición. Igualmente hacen parte o pueden hacer parte de la junta directiva para la toma de decisiones y control del nuevo activo que están creando.

Aliados: Un aliado estratégico en un programa de coalición es aquel que se dirige a su mismo mercado, pero no es competencia directa. Son otras empresas que también están buscando vender u ofrecer un servicio a la misma persona o empresa ala que usted también quiere venderle. En este caso, a través de puntos, millas o cualquier otro componente de recompensa directo entregado a un cliente. También pueden ser empresas que están en otras industrias pero que coinciden con usted en la persona de contacto, que tiene el perfil que necesita para motivar a los clientes en utilizar una variedad de opciones donde pueda materializar los puntos que obtuvo en el programa

de coalición. El aliado ayuda a lograr la cotidianidad del cliente en el programa y facilita la democratización de los puntos, generando así mayor beneficio al cliente final.

Los aliados también buscan un beneficio con la implementación de los programas de fidelización, ya que con ellos pueden aumentar su flujo de clientes y, por otra parte, mantener a los actuales, esto teniendo en cuenta que ellos también hacen parte del programa.

En un programa de coalición, un aliado tiene la oportunidad de tener dos beneficios, uno de ellos es generar acumulación de puntos a través de las compras que realizan los clientes, esto les permite incentivar a una mayor cantidad de clientes para que utilicen sus productos o servicios. El segundo beneficio está en la redención de puntos, ya que el comercio puede recibir directamente un pago a través de los puntos para la venta de sus productos o servicios.

Clientes: Según foromarketing.com, "se le llama cliente a aquella persona que solicita un bien o servicio a cambio de un pago. Esto quiere decir, que los clientes de una empresa son aquellos que contratan de forma ocasional o frecuente los servicios o productos que esta ofrece."

Es importante tener en cuenta que existen globalmente dos tipos de clientes:

- *Cliente interno.* "Cuando hablamos de cliente interno se refiere a aquellos que intervienen en el desarrollo del producto o servicio. Son los empleados, colaboradores y proveedores."
- *Cliente externo.* "Los clientes externos son aquellos que pagan por obtener los bienes o servicios de la organización. A la hora de clasificarlos podemos dividirlos en distintos perfiles y tipología de clientes externos." (FMK, ForoMarketing, 2016, párr. 3)

Una empresa canadiense especializada en tecnología digital para fidelización y marketing automatizado, identificó una pirámide de fidelización con el objetivo de medir la lealtad de los clientes. (Gómez, 2020)

Figura 4. ***La pirámide de fidelización***

Fuente: Gómez, J. (2020). La pirámide de fidelización: cómo medir la lealtad de los clientes. *Spoonity*. Recuperado de https://www.spoonity.com/es/piramide-de-fidelizacion/

¿Qué es la pirámide de fidelización de clientes?

La pirámide de fidelización mide la lealtad de los clientes de la marca y segmenta la base de compradores en función de sus patrones de consumo del negocio.

Como podemos ver en el ejemplo de arriba, la pirámide de fidelización categoriza a los clientes en los siguientes cinco segmentos: (Spoonity, Gómez, 2020).

a. Clientes más valiosos

En la punta de la pirámide de fidelización se encuentran los clientes más valiosos, aquellos que no podemos perder ya que se genera la mayor ganancia. Son esos clientes que visitan varias veces al mes o, en ciertos negocios como cafeterías, cada día de la semana. Estos clientes generan la mayor parte de los ingresos del negocio. (Spoonity, Gómez, 2020).

b. Clientes con potencial

En el segundo escalón se encuentran los clientes con gran potencial. Son aquellos que están medianamente fidelizados con la marca. Su frecuencia de compra es media-alta y su volumen de compra es importante, llegando a representar hasta una ganancia del 25%. Con estos clientes se trabajará en una estrategia de crecimiento, motivándolos a visitar más frecuentemente el negocio y a comprar más. (Spoonity, Gómez, 2020).

c. Clientes con bajo potencial

En el tercer escalón se encuentran los clientes que visitan poco y consumen poco. Con este grupo de clientes obtenemos una ganancia menor. Sin embargo, este segmento es importante ya que agrupa una cantidad significativa de clientes. Aunque son clientes considerados de "baja inversión", también generan ingresos que no se deben despreciar. (Spoonity, Gómez, 2020).

d. Clientes inactivos

En el cuarto escalón se encuentran los clientes inactivos. Estos son clientes que no han vuelto a visitar o comprar en un determinado plazo de tiempo – normalmente en 6 semanas o más, dependiendo del tipo de negocio–. Lamentablemente, en la mayoría de los negocios, este segmento es el más grande de todos. (Spoonity, Gómez, 2020).

e. Prospectos con potencial

Por último, tenemos el segmento de clientes nuevos, aquellos que acaban de realizar su primera compra con nosotros. A estos clientes los tenemos que captar desde el primer momento, para que su valor con nosotros crezca. (Spoonity, Gómez, 2020).

En un programa de coalición es importante la participación de varias categorías o actividades comerciales, las cuales permitirán una mayor cotidianidad y experiencia para cada uno de los clientes y aliados. Entre las más importante se encuentran:

- Mercado
- Banca
- Entretenimiento
- Gastronomía
- Moda y accesorios
- Viajes
- Hogar
- Tecnología
- Deportes
- Música
- Seguros
- Salud y Belleza
- Vehículos
- Mascotas
- Arte y Cultura.

Estructura general de un programa de Coalición

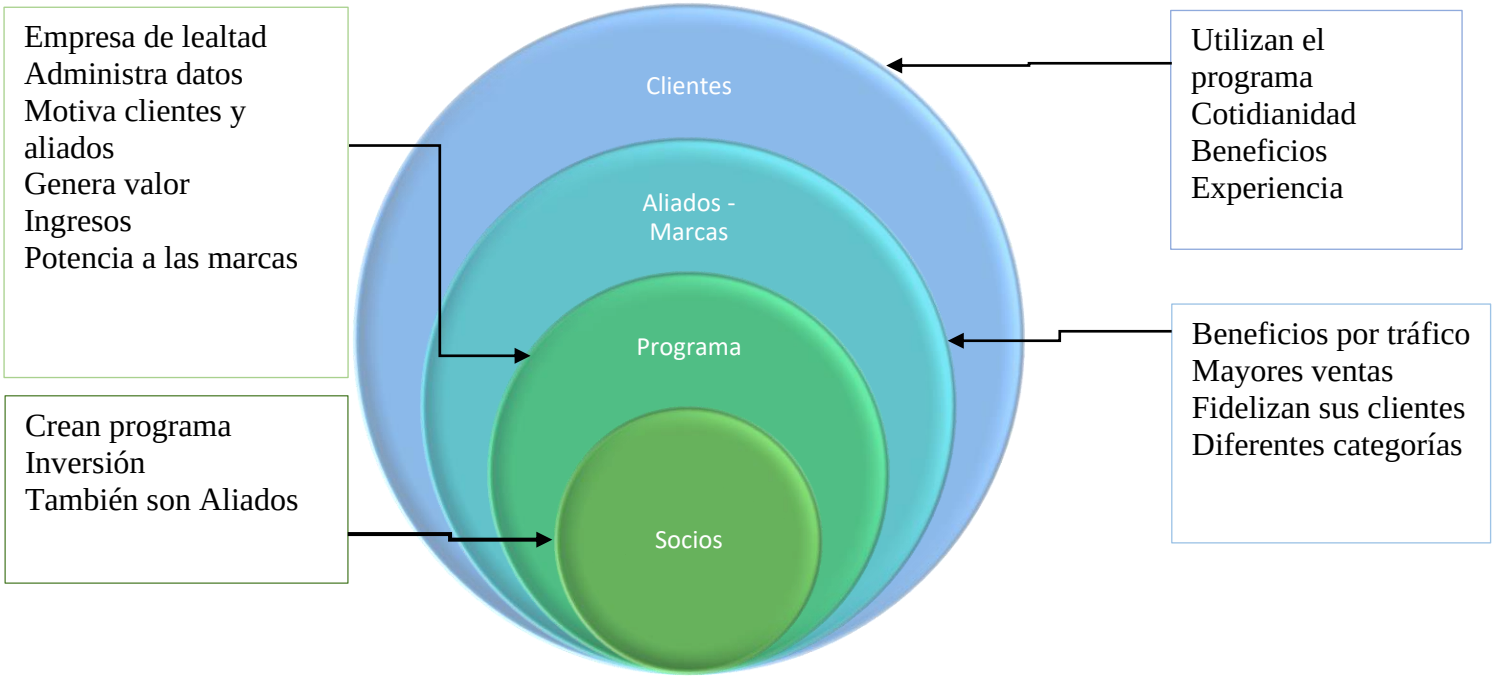

Figura 5. ***Estructura general de un programa de Coalición***

Fuente: Elaboración propia.

Capítulo 2

Valor de un programa de lealtad

Actualmente podemos afirmar que lo más valioso de una compañía son sus clientes, ellos y su información son el activo principal de toda organización, son la pieza fundamental de cualquier negocio, ya sea del sector servicios o del productivo. Muchas empresas hoy en día se enfocan en la consecución de clientes nuevos, a cambio de mantener y cautivar a los que tienen en la actualidad y soportan sus ingresos.

Cuando una compañía se enfoca en mantener los clientes de su ecosistema, debe orientar sus esfuerzos en fidelizarlos y generarles experiencia y recordación, aspectos que se han convertido en los retos para el crecimiento empresarial en los últimos 10 años. Las compañías deben apuntarle a la lealtad del cliente, ya que resulta alrededor de 6 a 7 veces más costoso atraer un cliente nuevo, que mantener a un cliente antiguo. Las empresas que destinan el 5% de sus inversiones para la retención de sus clientes, logran por lo menos un 5% y hasta un 95% el retorno de beneficios (microtech,16 febrero 2021).

Esta reflexión la realizamos sin desconocer que toda compañía también debe hacer esfuerzos en atraer clientes nuevos, sin embargo, de cada 100 clientes nuevos, solamente el 5%, aproximadamente, realiza una segunda o tercera compra o utiliza un nuevo servicio.

En el año 2019, la compañía consultora KPMG realizó una encuesta a 18.520 consumidores alrededor de 20 países para ver la “verdad sobre la lealtad del cliente”. Dicho estudio obtuvo los siguientes datos: (KPMG, 2019, Growjo, s.f.).

- El 86 por ciento recomendará una compañía a amigos y familiares.
- Es probable que el 66 por ciento escriba una crítica positiva después de una buena experiencia.
- El 46 por ciento seguirá siendo leal, incluso después de una mala experiencia.

En esa misma encuesta se registra una estadística del uso de los programas de lealtad por países, observando resultados muy importantes. Para el caso de Australia, por ejemplo, la cifra de las empresas encuestadas llega al 61%, mientras que en Latinoamérica tenemos porcentajes del 39%, como es el caso de México.

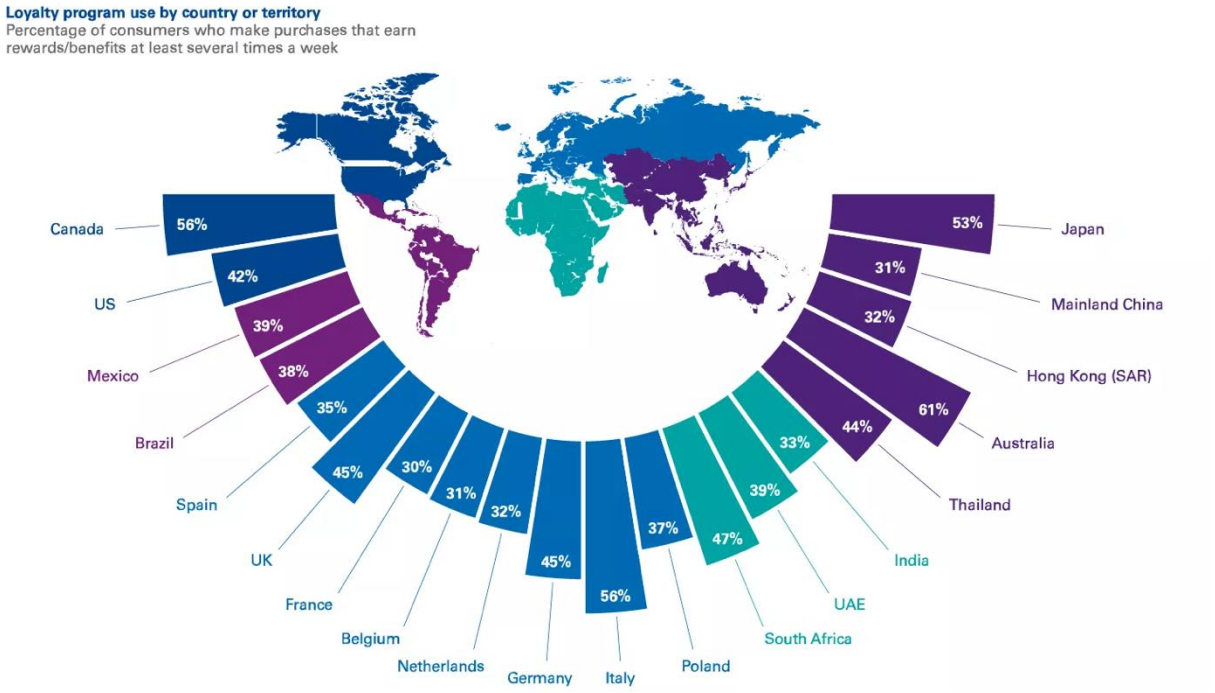

Figura 6. ***Uso del programa de fidelización por país o territorio.***

Fuente: KPMG, 2019, la verdad sobre la fidelidad del cliente, p. 3. home.kpmg/customerloyalty

Dentro de los tres beneficios de la fidelización de un cliente, está *la experiencia de la compra excepcional*, la cual se obtiene con tecnología y un buen análisis de la data para lograr que el cliente tenga una experiencia única y personalizada en el momento de la compra. El segundo beneficio es *el enamoramiento con la marca*, el cual se logra a través de la ruta de fidelización; el marketing persona a persona, por ejemplo, es una de las estrategias potentes para lograr enamorar a los clientes. El tercer beneficio es *el aumento de la rentabilidad de la compañía*. Según lo señala Sohail Khan, conferencista y escritor en Forbes y autor del libro "Guerrilla Marketing and joint ventures" (2021), (Spoonity, Torio J. M. (s.f.)): "Si puedes retener a un cliente por dos años, en lugar de dos meses, tu rentabilidad aumentaba 12 veces sin esfuerzo o costo extra de conversión. Se llama principio de valor del tiempo de vida".

Con base en los beneficios mencionados, existen programas de fidelización que son ya referentes en muchos mercados y actividades comerciales. A nivel mundial tenemos el caso de Nectar: (Growjo, s.f.).

Ubicación: Reino Unido

Fundación: 2002

Socios: Sainsbury´s, BP, eBay, Expedia y Virgin Trains

Valor: Hace uso de big data para realizar ofertas personalizadas

Ingresos: 30 millones de dólares anuales. Fuente: Growjo

Es una compañía de marketing que tiene el programa de coalición más grande del Reino Unido y ha logrado devolver, en 19 años de operación, un aproximado de 16 millardos en recompensas a sus clientes; tiene alrededor de 20 millones de clientes y sobrepasa los 500 aliados que permiten generar acumulaciones y redenciones en el programa.

Un referente en la región es Lifemiles:

Ubicación: Colombia

Fundación: 2011

Valor: Es un programa de lealtad que inició como viajero frecuente de la aerolínea Avianca. Hoy tiene alrededor de 200 comercios aliados.

Lifemiles se encuentra valorada en cerca de US $ 1.115 millones (unos $ 4 billones de pesos Colombianos), y desde el año 2021 se encuentra en la lista de las 491 compañías de todo el mundo consideradas como “unicornios” (The Global Unicorn Club), denominación asignada a las empresas que tiene un valor mayor a US$ 1.000 millones. (Semana, 2020; E&N, 2015).

El 2 de octubre de 2020, el señor JT Genter, periodista especializado en aviación para la revista Forbes, aseguró en la “W Radio” que el programa de pasajero frecuente de Avianca puedo tener más valor que la propia aerolínea. Dijo también: “El programa de millas representa un gran flujo de capital. Es una gran inversión porque es una gran ganancia”, (W Radio, 2020). Así mismo, presentó el ejemplo de American Airlines, empresa valorada en 20.000 millones de dólares. Esta

información coincide con un artículo de la revista “The Economist” en su edición del 20 de noviembre de 2021, donde titulan: “Los esquemas de viajero frecuente proporcionan a las aerolíneas un salvavidas”. Según este escrito, el programa viajero de American Airlines, creado hace 40 años, hoy lo valoran entre 18 mil millones y 30 mil millones de dólares, esto indica que tendría un valor superior que la misma aerolínea, cuya capitalización bursátil es de 12.900 millones de dólares. (The economist, 2020).

Si el programa de Lifemiles es más valioso que el mismo Avianca, es importante conocer cuál es el valor de la aerolínea. Según la lista de las 1000 empresas más grandes de Colombia, Avianca se encuentra en el puesto 30 con las siguientes cifras financieras:

RANKING	NIT	NOMBRE	INGRESOS OPERACIONALES 2020*	GANANCIA (PERDIDA) 2020	TOTAL ACTIVOS 2020	TOTAL PASIVOS 2020	TOTAL PATRIMONIO 2020	INGRESOS OPERACIONALES 2019*	GANANCIA (PERDIDA) 2019	TOTAL ACTIVOS 2019	TOTAL PASIVOS 2019	TOTAL PATRIMONIO 2019
30	890100577	AVIANCA	$ 3.257.801.264	($ 1.818.938.276)	$ 16.502.571.853	$ 17.525.567.652	($ 1.022.995.799)	$ 9.307.045.218	($ 1.694.806.666)	$ 18.498.349.056	$ 18.333.155.655	$ 165.193.401

Nota: Valores en miles y su fuente es Supersociedades.

Dentro de este análisis, también valoramos otra compañía colombiana que hoy por hoy conforma uno de los programas de coalición más importantes del país con aproximadamente 135 aliados y 5 millones de clientes. Estamos hablando de Puntos Colombia, una compañía que con tan solo 3 años y medio de existencia (creación en el año 2018 cuando se unificaron los programas de lealtad de Bancolombia y El Grupo Éxito), ya se ubica en el ranking 634 de las 1000 empresas más grandes de Colombia.

RANKING	NIT	RAZON SOCIAL	INGRESOS OPERACIONALES 2020*	GANANCIA (PERDIDA) 2020	TOTAL ACTIVOS 2020	TOTAL PASIVOS 2020	TOTAL PATRIMONIO 2020	INGRESOS OPERACIONALES 2019*	GANANCIA (PERDIDA) 2019	TOTAL ACTIVOS 2019	TOTAL PASIVOS 2019	TOTAL PATRIMONIO 2019
634	901081311	PUNTOS COLOMBIA S.A.S	$ 238.436.087	$ 12.669.127	$ 150.770.495	$ 135.356.096	$ 15.414.399	$ 191.754.402	($ 6.272.515)	$ 155.423.019	$ 152.677.747	$ 2.745.272

Nota: Valores en miles y su fuente es Supersociedades.

Puntos Colombia es una compañía que realiza aproximadamente 500 mil transacciones de redención mensuales y alrededor de 20 millones de transacciones de acumulación, excelentes flujos de caja que coincide con los grandes programas de lealtad de las aerolíneas.

De acuerdo con lo anterior, podemos concluir que las compañías que hoy ofrecen recompensas y que hacen parte de programas de coalición, son muy bien valoradas, tienen unos

buenos flujos de caja y la facultad de manejar la información de millones de clientes, activo muy valioso para cualquier compañía.

Para tener una referencia, tanto Lifemiles como Puntos Colombia hoy gestionan más clientes que bancos como Banco Falabella con alrededor de 2 millones de clientes, Caja Social con 2.3 millones de clientes, BBVA con unos 1.5 millones de clientes e ITAU que también tiene en Colombia alrededor de 700 mil clientes. Podemos notar cómo estas dos compañías de coalición doblan en cantidad de clientes a dichas entidades financieras.

Teniendo en cuenta esta cantidad de transacciones, ingresos y clientes, vemos que se trata de compañías que gestionan unos riesgos significativos desde el punto de vista de protección de datos, fraude y riesgos cibernéticos, los cuales se pueden materializar, generando pérdidas importantes para sus clientes, socios, aliados y empleados. Es por esta razón que se hace necesario evaluar el impacto que el fraude puede generar en cada una de ellas.

Impacto del fraude

Según Gartner (PaymentsJournal, Daniel Shkedi, 2020), en Estados Unidos, cerca de 140 millardo de dólares, en puntos de lealtad no son redimidos o utilizados por sus clientes, esta situación genera un incentivo para el delincuente que, a través de diferentes modalidades, logra materializar el fraude de los puntos no utilizados por los clientes.

Según datos de la Asociación de Seguridad de Lealtad (LSA), unos 3.1 millardos de dólares en puntos son canjeados de forma fraudulenta en Estados unidos. (PaymentsJournal, Daniel Shkedi, 2020).

Un informe del año 2020 de una empresa llamada Akamai, dedicada a servicios de ciberseguridad en el segmento de lealtad, demuestra que hubo 100 mil millones de ataques de enumeración para obtener y validar las credenciales de los clientes entre el periodo de julio de 2018 y junio de 2020 (Akamai, 20 octubre 2020). Este tipo de ataques se utiliza con frecuencia porque las credenciales de 4 dígitos son fáciles de adivinar y, a su vez, los clientes las utilizan en diferentes plataformas, por ejemplo, la misma clave de la tarjeta débito del banco es la misma del programa de lealtad.

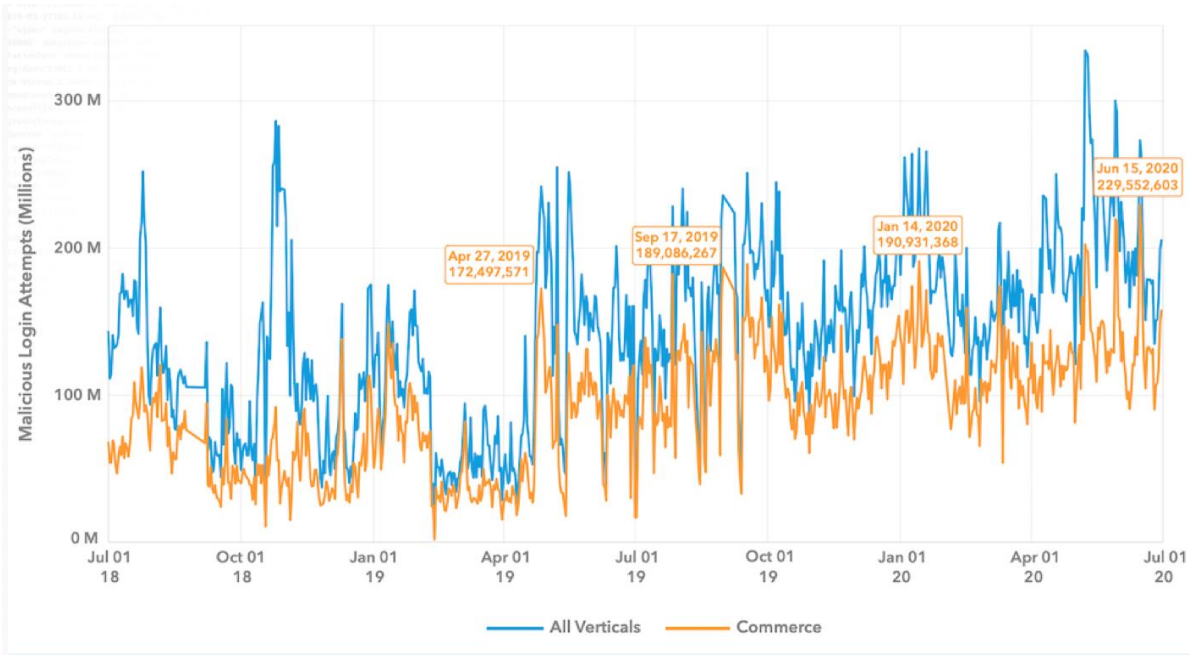

Figura 7. ***Intentos diarios de abuso de credenciales (julio de 2018 - junio de 2020)***

Fuente: Akamai, 20 octubre 2021, fidelidad a la venta – el fraude en los sectores de retail y hotelería, volumen 6, numero 3, p. 3.

En la conferencia de Loyalty Fraud Prevention Asociation (LFPA), realizada en el mes de mayo del 2019 en Londres, se mencionan datos importantes sobre las cifras de fraude, entre ellos los siguientes:

- Casi el 40% del tráfico en sitios web relacionados con viajes provienen de robots imitadores.
- El 80% del fraude de viajero frecuente se descubre por accidente.
- Desde el 2016 – 2017 los ataques a los programas de lealtad se triplicaron con un 48% de ataques de ATO (account takeover o suplantación de cuentas), con un costo de 2.3 billones de dólares en todo el mundo.

Un dato alarmante es el costo de pérdida de un cliente después de una situación irregular o de vulnerabilidad, ya que un 17% de los clientes detendrían o paralizarían cualquier relación comercial y de negocios con una empresa que permitiera una violación de sus datos personales; así mismo, un 26% de los clientes cancelarían la afiliación al programa de recompensas o membresía después de un incidente de fraude de lealtad, y un 33% se quedaría con el programa, pero esperarían una recompensa de puntos o millas por el daño causado (Rodrigo Camacho, 2019).

Según Zia Hayat – CEO and Founder, de Callsing, en la red oscura se venden constantemente datos de clientes con puntos disponibles para que puedan ser utilizados y materializados en redenciones fraude. Se dio un ejemplo de aerolíneas.

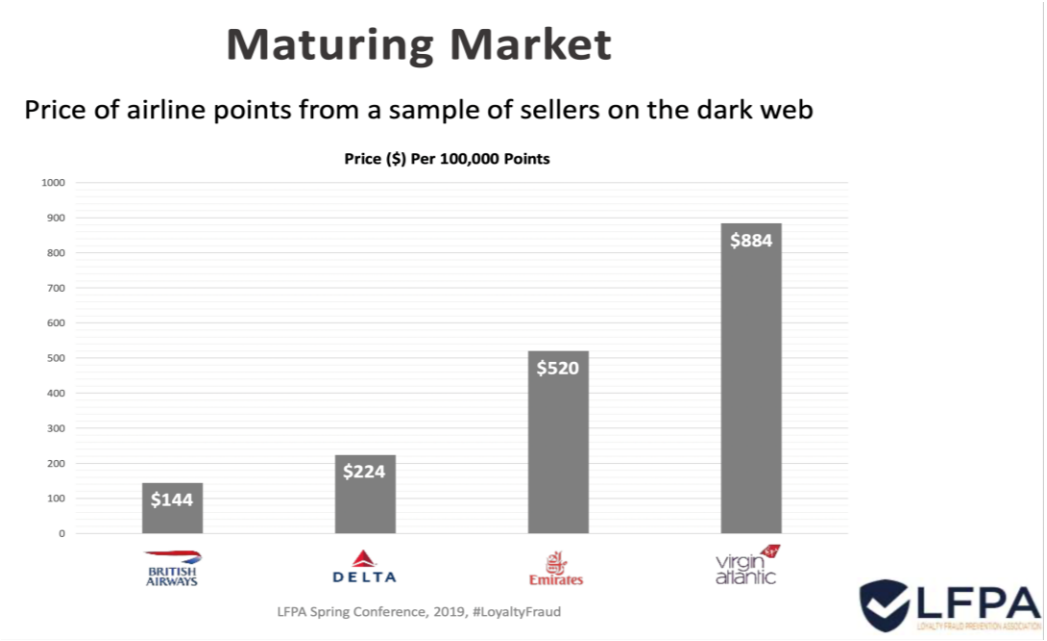

Figura 8. ***Maduración del mercado***

Fuente: Loyalty Fraud Prevention Asociation (LFPA), mayo del 2019. Londres.

En un documento de Comarch llamado "Todo lo que necesitas saber sobre fraude de fidelidad", (Comarch, CMR&Marketing, s.f.), se registran algunos datos importantes, los cuales fueron extraídos de las encuestas que realizaron a 1600 clientes del sector de lealtad:

- El 72% de los gerentes de los programas de lealtad han experimentado situaciones de fraude.
- El 93% de los encuestados dicen que prefieren una compañía de lealtad que tenga un programa de prevención de fraude.
- El 81% de los clientes relacionan las recompensas por puntos=dinero.

En una encuesta realizada a más de 120 instituciones en Norte América (Estados Unidos y Canadá), llamada "Faces of fraud 2021" (Appgate y SMG information Security, 2021),

observamos que frente a la pregunta: "¿Cómo evalúan la situación actual los encuestados de la encuesta faces of fraud 2021?", el 60% la califican por encima del promedio o superior frente a la gestión de identificación y mitigación del fraude, el 55% manifiestan que sus clientes carecen de la conciencia suficiente para protegerse, y el 50% afirma que los estafadores tienen mucha información que les ayuda a la materialización del fraude. En la siguiente gráfica podemos observar los resultados completos:

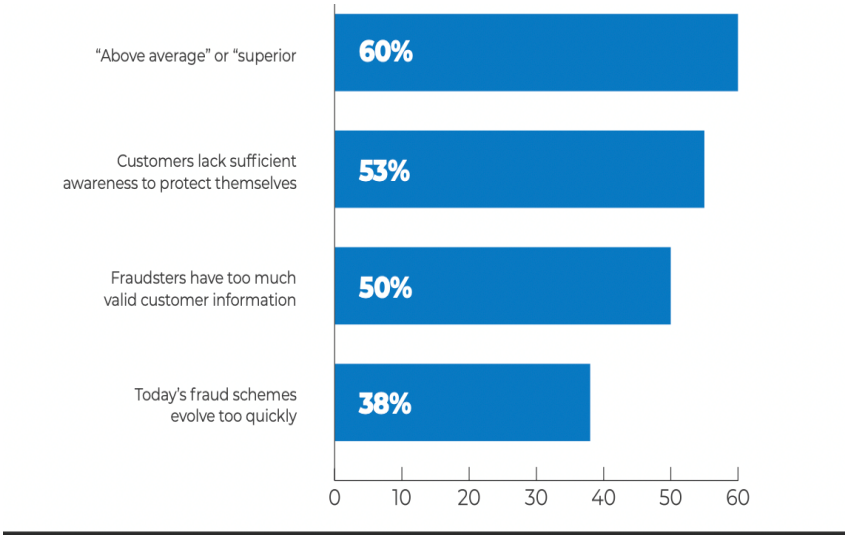

Figura 9. ***Materialización del fraude***

Fuente: AppGate – iSMG Information Security Media Group, 2021, la encuesta faces of fraud 2021, p. 8.

Para un programa de lealtad es fundamental considerar el equilibrio del control y gestión del fraude versus la experiencia del cliente. En este estudio se consideró este tema con la siguiente pregunta: ¿Cuál de estos tiene la mayor prioridad para su institución en las soluciones de cara al cliente: la prevención de fraudes o la experiencia del cliente? Este fue el resultado:

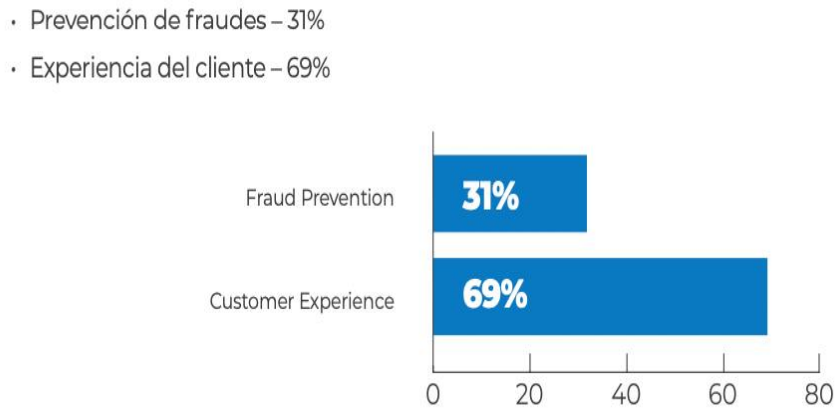

Figura 10. ***Equilibrio de control y gestión***

Fuente: AppGate – iSMG Information Security Media Group, 2021, la encuesta faces of fraud 2021, p. 9.

Esto demuestra que la gran mayoría de compañías encuestadas le dan prioridad a la experiencia del cliente antes que a la prevención de una situación fraudulenta; sin embargo, es muy importante sostener que la experiencia en un caso de fraude debe ser cuidadosa a pesar de lo incomoda que resulte, esto con el fin de recuperar la confianza del usuario, ya que una situación negativa puede generar una acción positiva.

La preocupación de los encuestados está enfocada en la suplantación de cuentas con un 45%, el *phishing* con un 42%, y el compromiso de correos electrónicos empresariales, que también son catalogados como *phishing*, con un 36%. Esto significa que las tres preocupaciones están ligadas a ingeniería social, estrategia utilizada por los delincuentes para obtener información de sus víctimas a través de un engaño.

Dentro de un modelo de prevención de fraude es fundamental el uso de la tecnología, sin ella diríamos que es imposible realizar una buena gestión del riesgo y de la experiencia. En esta encuesta se valora la siguiente pregunta: ¿En cuál de las siguientes tecnologías planea invertir en los próximos 18 meses?, la gran mayoría de las entidades coincidieron en que la inteligencia artificial es importante con un 41%, seguido de la autenticación multifactor con un 27% y de los sistemas de detección y seguimiento con un 27%.

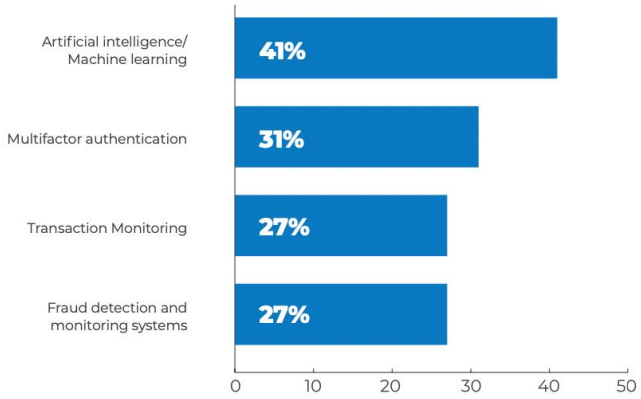

Figura 11. ***Uso de la tecnología para una buena gestión***

Fuente: AppGate – iSMG Information Security Media Group, 2021, la encuesta faces of fraud 2021, p. 10.

En el último año se han presentado dos factores que han generado, en la mayoría de instituciones, un aumento de incidentes de fraude. Uno de ellos es la pandemia Covid19 que incrementó la cantidad de información que se maneja en redes sociales, situación que los delincuentes han sabido aprovechar para obtener información y generar situaciones de fraude. El segundo factor es la transformación digital que llevó a un aumento significativo de transacciones no presenciales, tendencia que se venía dando desde hace varios años, pero que se aceleró de forma exponencial con la llegada de la pandemia, aumentando así el riesgo. No obstante, muchas compañías no estaban lo suficientemente preparadas para asumir este tipo de cambios.

En el contexto colombiano tenemos tres programas de lealtad que operan de forma independiente. Nos referimos a Puntos Colombia, Lifemiles y Leal, los tres son digitales, no tienen puntos físicos de atención, sus clientes se registran y nacen desde lo digital en su página web, adicional a esto tienen Market Place en sus sitios web para ofrecer productos y servicios a sus clientes de forma no presencial.

Por lo anterior, tiene sentido la pregunta que se encuentra en la encuesta ya citada, ¿ha aumentado, disminuido o se ha mantenido estable el número de incidentes de fraude / pérdidas financieras que involucran a su organización durante el último año? El resultado afirma que el 81% de incidentes de fraude se ha mantenido o se ha aumentado y sólo el 10% nota una disminución, así mismo, el 59% manifiesta que las pérdidas han aumentado o se han mantenido estables, y sólo el 22% ve una disminución, como lo observamos en el siguiente gráfico:

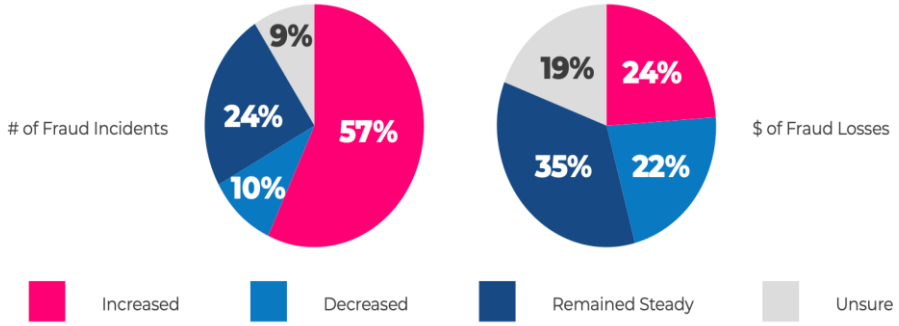

Figura 12. ***Comportamiento número de incidentes de fraude***

Fuente: AppGate – iSMG Information Security Media Group, 2021, la encuesta faces of fraud 2021, p. 17.

Más allá del costo financiero que genera una pérdida por fraude, existen otros riesgos importantes a considerar, y que afectan la productividad de la compañía, generando otros perjuicios dentro y fuera de la organización. Entre ellos tenemos las pérdidas adicionales, producto de una situación fraudulenta, esto considerando que existen unos costos de operación para la redención y la acumulación, ya que las compañías de lealtad pagan peajes por sus transacciones a las redes, y por la utilización de datáfonos. Adicionalmente, un caso mal atendido puede generar una sanción por parte de un ente regulador, sin contar el valor al que puede ascender el mantener la operación de control y fraude.

Por otro lado, en este tipo de situaciones también existen pérdidas por riesgo reputacional. Dentro de este mismo estudio se preguntó: ¿Qué pérdidas no financieras sufrió su organización por los incidentes de fraude? El 55% manifestó que su principal pérdida no financiera es la "pérdida de productividad", en segundo lugar, el impacto reputacional, y tercero, las relacionadas con asuntos de cumplimiento regulatorio, como lo apreciamos en la siguiente gráfica:

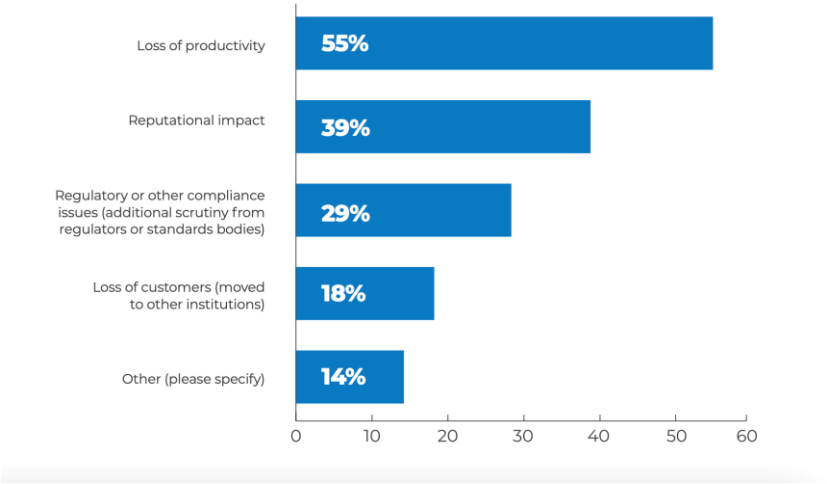

Figura 13. ***Pérdidas financieras por incidentes de fraude***

Fuente: AppGate – iSMG Information Security Media Group, 2021, la encuesta faces of fraud 2021, p. 18.

Una de las motivaciones al realizar este trabajo de investigación, que posteriormente propone un modelo de prevención de fraude para una compañía de lealtad, es la de entregar, de manera organizada y estructurada, una herramienta que le permita a un gestor de incidentes de fraude controlar de forma eficiente este tipo de riesgos. Hemos visto, a partir de las encuetas, que existen tres barreras principales para mejorar la prevención del fraude dentro de una organización. En primer lugar, se encuentran las barreras manuales con un 51%, lo que significa que no existe una metodología para la gestión ni automatización de procesos, tampoco indicadores de seguimiento ni coordinación entre las áreas de la compañía y los entes externos. Por otro lado, tenemos las barreras técnicas con un 46%, relacionadas con la falta de comunicación entre los controles y los esfuerzos duplicados entre las áreas. Por último, encontramos la experiencia del cliente con un 42%. Este es el resultado final que responde al ya mencionado interrogante:

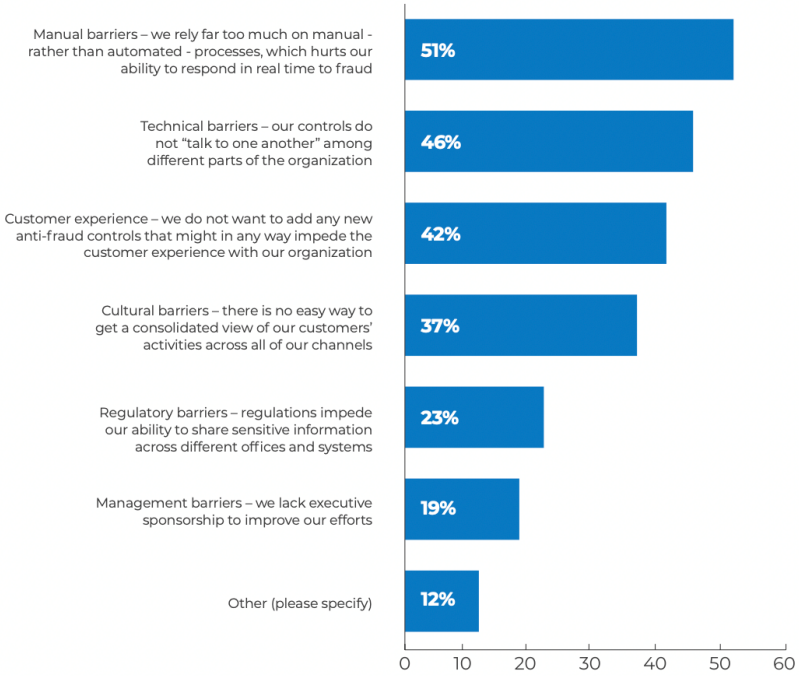

Figura 14. ***Principales barreras para mejorar la prevención de fraude***

Fuente: AppGate – iSMG Information Security Media Group, 2021, la encuesta faces of fraud 2021, p. 22.

En definitiva, con las cifras antes mencionadas, sabemos que existe información suficiente que le permita al sector de lealtad mejorar sus controles y procesos frente al riesgo de fraude transaccional, para lograr, en primera medida, mejorar sus capacidades internas, y, en segundo lugar, organizarse como grupo que tiene un enemigo en común. En la actualidad, este sector de negocio carece de una organización que le permita tener retroalimentación y acompañamiento como agremiación, a diferencia de las entidades financieras que cuentan con Asobancaria, y de las aseguradoras que cuentan con Fasecolda.

Capítulo 3

Modalidades de fraude que se pueden presentar en un programa de lealtad

La lealtad de un cliente en un programa de este tipo es difícil de lograr y de mantener en el tiempo. Empresas que se dedican y se incorporan en programas de coalición ubicadas y dedicadas al sector de los viajes, transporte, ropa y vestuario, combustibles, etc., pasan meses o incluso años buscando la fidelización perfecta para que sus clientes queden satisfechos, proporcionándoles productos o servicios de fácil acceso en diferentes canales. Encontrar el equilibrio perfecto entre la seguridad y la experiencia del cliente no es una tarea fácil para una compañía de lealtad.

Los clientes de este tipo de programas buscan un acceso sin fricciones, sin restricciones a sus recompensas (puntos). Teniendo en cuenta que un punto o milla tiene un valor en pesos, hoy en día se constituyen en un medio de pago adicional en muchos establecimientos de comercio. También buscan que sus puntos o millas sean seguros, pero esta seguridad no debe afectar la experiencia; sin embargo, cuando la seguridad se debilita a favor de la experiencia del usuario, aparecen los estafadores, los ciberdelincuentes.

Todas las organizaciones están sujetas a riesgos de fraude, y las compañías de lealtad no son la excepción, de hecho, un siniestro de fraude en grandes cantidades y de forma continua puede generar el cierre de una organización. Adicionalmente, dentro de un proceso de recuperación y resiliencia por un evento de fraude, sin contar la pérdida económica directa que afecta los estados financieros, genera unos costos legales, un riesgo reputacional incalculable, y la pérdida masiva de clientes cuya experiencia se ha visto afectada por una situación fraudulenta.

Según Harán (2020), se denomina fuga de información “al incidente que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de esta (tanto todos como un grupo reducido). Se trata de un incidente que puede ser tanto interno como externo” (párr. 3)

Internas

Se puede presentar de forma intencionada (dolo) o accidentalmente por funcionarios internos de la compañía o por un proveedor de servicios que trabaja dentro o para la organización.

- *Deliberadas:* Se filtran o revelan datos confidenciales con el propósito de obtener una ventaja económica o causar un daño o perjuicio a las organizaciones: sanciones económicas, la pérdida de una ventaja competitiva, la pérdida de imagen, reputación o materialización de fraudes, etc. (Banco Santander España, 2018)

Los eventos de situaciones deliberadas o con dolo, se presentan también bajo dos circunstancias:

a. Penetración de un empleado: Ocurre cuando un tercero o externo realiza una propuesta de entregar información confidencial y privada de la compañía a cambio de un beneficio económico o en especie.
b. La infiltración de un empleado: Se genera cuando una banda delincuencial, a través de uno de sus integrantes, busca la manera de trabajar directamente en la compañía, con el objetivo de cometer el hecho ilícito, en este caso, extraer información confidencial con el único ánimo de obtener un beneficio.

- *Involuntarias:* Se filtran o revelan datos confidenciales de manera accidental o no intencionada, por ejemplo, por no seguir las buenas prácticas de seguridad de la información. (Banco Santander España, 2018).

Externas

Se genera por entrega de datos sensibles a personas por parte de un aliado, socio o cliente dentro de un programa de coalición.

- Clientes: Una fuga de información es atribuible a un cliente por exceso de confianza en el tema de seguridad, falta de interés en la protección de sus datos y desconocimiento de las políticas de seguridad.

Según Kaspersky (2020), la ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados. (Latam Kaspersky, 2020).

También se presenta la fuga de información cuando el mismo cliente realiza una operación de redención en un establecimiento aliado, y permite que un tercero observe su información personal, en este caso clave personal y documento de identificación.

- *Aliados:* Se materializa cuando, dentro las operaciones normales en un programa de coalición, existen fallas en la infraestructura del aliado que ocasionan la pérdida de datos de los clientes, o porque un funcionario del mismo aliado permite y entrega la información de los clientes después de realizar la operación de redención o acumulación.

- *Socios:* En un programa de coalición pueden existir intercambios de información dentro del proceso de registros al programa, conciliaciones y acumulaciones que en determinando momento se pueden materializar en fugas de información por falta de controles y definiciones dentro de las políticas de seguridad de la información de la compañía.

Algunos datos importantes que se observaron en el año 2020, con relación a fugas de información, dan a conocer el estado de protección en ciberseguridad que hoy tenemos en muchas empresas: (Welivesecurity, Hará, 2020)

- El 56% de los usuarios cree que su información personal no está realmente protegida en línea. (Encuesta de ESET).
- 3 de cada 4 usuarios perdió dinero o información por no contar con un backup. (Encuesta de ESET).
- Durante el primer semestre del 2020 la cantidad de brechas de datos disminuyó en comparación con años anteriores. Sin embargo, el número de registros expuestos (27 mil millones) es cuatro veces mayor que los reportados en cualquier otro reporte previo para el mismo período de tiempo. (Risk Based Security).
- 86 millones de dólares es el costo promedio a nivel global de una brecha de datos para una organización, y el costo por cada registro de información personal identificable es el más alto con un valor promedio de 150 dólares por registro. (IBM).
- Los errores de configuración en servidores en la nube (19%) y el uso de credenciales robadas y/o comprometidas (19%) fueron los principales causantes de brechas de datos, seguidos por

la explotación de vulnerabilidades en software de terceras partes (16%) y el phishing (14%). (IBM).

- El 80% de las brechas de datos incluyó la fuga de información personal identificable de consumidores, mientras que en el 32% de las brechas se comprometió propiedad intelectual. (IBM).
- El 52% de las brechas de datos fueron provocadas por ataques maliciosos, mientras que el 23% fue debido a errores humanos. (IBM).
- Más del 80% de las brechas de datos provocadas por actores maliciosos involucraron ataques de fuerza bruta o el uso de credenciales robadas. (Informe Verizon).
- El 30% de las brechas de datos involucran a actores al interior de la empresa u organización, mientras que el 70% fueron provocadas por externos. (Informe Verizon).

Algunos de los eventos más escuchados por fugas de información tanto en Colombia como el mundo fueron:

a. Facebook

Figura 15. ***Se filtraron más de 500 millones de datos de Facebook.***

Fuente: T y N.

b. **Target**

Figura 16. ***Target condenado a pagar 18,5 millones por una brecha de seguridad.***
Fuente: Inbe-cert

c. **Adidas**

Figura 17. ***Adidas sufrió de información.***
Fuente: Robles

d. **JP Morgan**

Figura 18. ***JP Morgan Chase reconoce violación masiva de datos***

Fuente: MS JP Morgan.

e. Barclays

Figura 19. ***El Barclays Bank ante la fuga de información de 27.000 archivos confidenciales***

Fuente: WeliveSecurity

Las consecuencias que este tipo de riesgos generan para una compañía son altísimas, no sólo por las situaciones de fraudes materializadas, sino también por el riesgo reputacional (incalculable), sumado a las sanciones por parte del regulador de cada país, lo que puede llevar, en muchas ocasiones, a la quiebra de una compañía.

Según ACFE “El fraude es cualquier acto u omisión intencional diseñado para engañar a otros, lo que hace que la víctima sufra una pérdida y / o el perpetrador logre una ganancia”. (párr. 15)

En una empresa de lealtad podemos encontrar fraude tanto interno como externo. Iniciaremos con la contextualización del fraude interno. Según el mismo ACFE (Asociación Certificadores de Fraude) es “El uso de la ocupación o empleo de uno para el enriquecimiento personal a través del mal uso deliberado o mala aplicación de los recursos o activos de la organización" (p. 23)

En este marco conceptual no podemos dejar atrás autores clásicos como el criminólogo Donald R. Cressey (1961), quien menciona que para que un fraude se materialice, deben existir tres elementos:

a. Motivación (incentivo, presión). Cuando la administración u otros empleados tienen un estímulo o presiones que les aportan razones justificativas para cometer fraudes. (fraude interno,febrero 2016)

b. Poder (Oportunidad). Serían las circunstancias que facilitan las posibilidades de perpetuar fraudes (por ejemplo, la ausencia de controles, controles ineficaces, o la capacidad de la administración para abrogar los controles), (fraude interno,febrero 2016).

c. Racionalización, actitud. Cuando las personas son capaces de racionalizar un acto fraudulento en total congruencia con su código de ética personal o que poseen una actitud, carácter o conjunto de valores que les permiten, consciente e intencionalmente, cometer un acto deshonesto. (fraude interno, febrero 2016).

Con base en lo anterior, un fraude interno en un programa de lealtad se puede presentar dentro del proceso de acumulación para después poder materializarlo en una redención ya sea de puntos o millas.

Pero, ¿qué es una acumulación de puntos?, es una transacción de acreditación donde el cliente realiza compras en un establecimiento de un comercio aliado y recibe como beneficio puntos por éstas. También se pueden presentar acumulaciones realizando compras con tarjetas de crédito (asumiendo que el programa tiene dentro de sus aliados un banco).

Ahora aclaremos **¿qué es un fraude por acumulación?** Se presenta en una transacción de acumulación o modificación irregular del saldo de puntos que afecta la cuenta de un cliente vinculado al programa y que no fue realizada por el titular de este, causando una pérdida económica y reputacional cuantificable para el aliado, socio, el programa o el cliente, y cuya causa es una transacción no permitida en el programa.

Se inicia cuando en el comportamiento de un cliente se identifica un incremento inusual o sospechoso de sus acumulaciones (no guardan relación con su conducta habitual y pueden afectar el promedio de facturación normal de un aliado, sin justificación). Este tipo de hallazgos puede ameritar una investigación del comportamiento del cliente, y derivar hacía investigaciones de fraude interno. También se pude determinar su procedencia de malas práctica de los empleados en

los comercios aliados, o errores humanos u operativos en la manipulación de los dispositivos POS donde se registran las acumulaciones tanto en aliado como dentro del mismo programa de lealtad.

Normalmente, este tipo de situaciones se presentan en dos modalidades:

a. Infidelidad de un funcionario de un establecimiento aliado: En los procesos de acumulación de puntos o millas, en la gran mayoría de programas, se realizan con un usuario o a través del número de documento de identidad, el cual sirve como conector entre el cliente, aliado y el programa. En este caso, el funcionario del establecimiento acumula dichos puntos por una recompensa en el pago de un producto o servicio, a un número de documento diferente al del cliente real, esto indica que los acumula a un tercero.

b. Registros de puntos a una cuenta en los procesos operativos y de conciliación: Se presenta cuando un funcionario que hace parte del programa de lealtad o cualquiera de los socios, genera acumulaciones de puntos de forma directa y con dolo, ya sea manual o a través de procesos automáticos, el cargue de puntos a cuentas de terceros sin el debido soporte de su acumulación.

En la siguiente gráfica se ilustra cómo desde las acumulaciones de aliados se observa claramente el aumento de transacciones de acumulación, las cuales deben generar una alerta y un proceso de validación inmediato, ya que se salen de todos los parámetros normales.

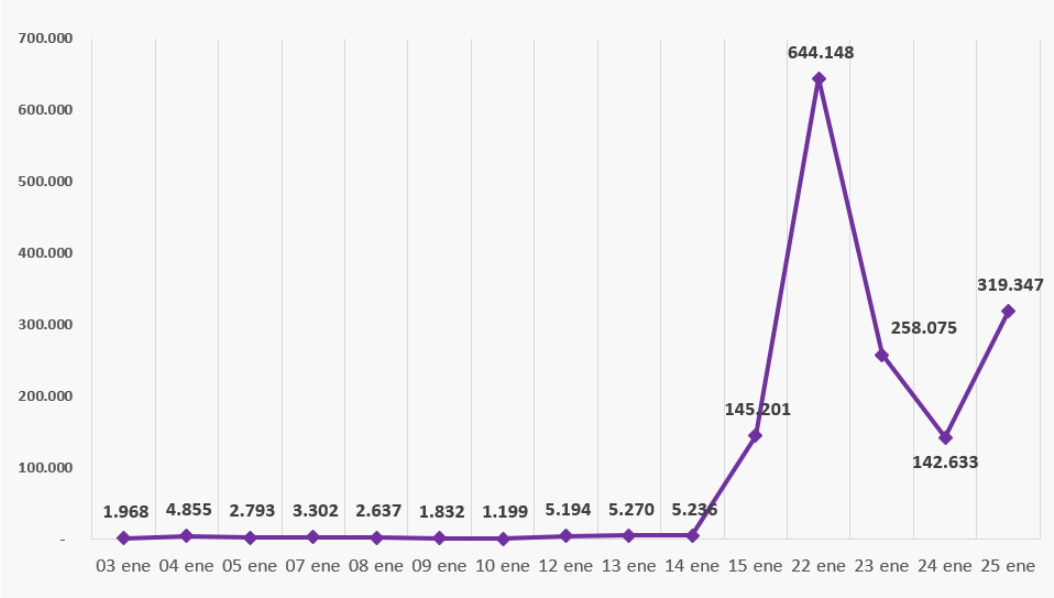

Figura 20. ***Aumento de transacciones de acumulación***

Fuente: Puntos Colombia, 2021

Una vez contextualizado el fraude por acumulación, iniciaremos el camino del entendimiento del fraude por redención en un programa de lealtad, este tipo de fraude está dentro de situaciones externas, enfocadas al riesgo transaccional.

¿Qué es una redención? Es una transacción que permite a un el cliente registrado en el programa la utilización de sus puntos en un comercio aliado, presentando su documento de identificación y adicionando un método de autenticación que en su mayoría es una clave personal.

Desafortunadamente, las cuentas de puntos o millas en un programa de lealtad son elecciones fáciles para la delincuencia, ya que la gran mayoría están protegidas por una combinación de nombre de usuario y/o número de la cédula de ciudadanía y contraseña estática (posiblemente de 4 dígitos), las cuales son olvidadas con mucha facilidad por los clientes. Una vez son obtenidas por un tercero, se canjean los puntos por mercancía, mercado, servicios, vuelos, hoteles, tarjetas de regalo o combustible.

¿Qué es el fraude por redención?

Son aquellas transacciones donde se utilizan los puntos de la cuenta de un cliente, a cambio de un producto o servicio. Dichas operaciones son realizadas en puntos de venta de aliados físicos o través de los canales virtuales que ofrece el programa. En este caso particular, el cliente manifiesta no haber participado en dichas redenciones.

Bajo este concepto, se define el fraude presente y el no presente en un programa de coalición.

Fraude Virtual – no presente

El fraude virtual es el evento delictivo que realizan ciberdelincuentes, afectando clientes (persona natural o jurídica). Aquí realizan acciones que les permitan conocer o acceder a información sensible, de tal manera que, posteriormente, puedan materializar el fraude en los canales virtuales con la obtención de productos o servicios, que para el caso podrían ser tiquetes aéreos, paquetes turísticos, bonos de diferentes aliados, etc.

Fraude presente

El fraude presente es aquel que ocurre cuando en un Aliado que comercializa productos y servicios de manera presencial, se presenta una persona con la información necesaria (identificación o usuario de un cliente y/o número de cédula y clave personal) para realizar una redención sin ser el cliente titular de la cuenta y sin contar con su aprobación. Esto representa una suplantación física del cliente titular para lo cual usan documentación falsificada o se valen de estrategias disuasivas que permitan generar lazos de confianzas en los establecimientos y evitar la presentación del documento de identidad; igualmente, se puede materializar a través de fraude interno en los aliados, al usar la información de clientes previamente conocida.

Adicional al fraude por acumulación y redención, se pueden presentar situaciones fraudulentas desde el registro al programa, llamado **suplantación de registro**: este tipo de fraude inicia cuando un cliente es suplantado al momento de registrarse en el programa. Ocurre cuando el cliente acumula puntos por compras con tarjeta de crédito y un tercero se registra a su nombre para utilizar dicha acumulación.

Capítulo 4

Ejes principales que puede tener un modelo de prevención y control de fraude en un programa de lealtad

Para poder generar una buena gestión de fraude en una compañía de fidelización, es necesario definir una estrategia alineada a los pilares y los objetivos estratégicos de la compañía, así mismo, este modelo permitirá estandarizar los procesos, canales y servicios de un ecosistema general de un programa de fidelización, con un único gobierno y un marco operativo.

El Modelo Operativo permite describir el funcionamiento de una organización y definir las capacidades de negocio requeridas para ejecutar la estrategia de forma eficiente y efectiva, cumpliendo con las expectativas de clientes, empleados, socios y aliados.

El modelo incorpora las interacciones que deben tenerse en cuenta en el marco de gobierno y los diferentes "stakeholders" que hacen parte del ecosistema estratégico y operativo de un programa de fidelización, entregando elementos claves alrededor del mismo para una mayor sinergia en pro de la adecuada administración del riesgo de fraude transaccional.

Figura 21. ***Grupo de interés del modelo operativo.***

Fuente: Fuente propia.

Dentro de la propuesta tendremos en cuenta los 5 principios básico que se analizaron en la guía práctica de ACFE "managing the business risk of fraud"[1], discriminados de la siguiente manera:

Principio 1: Como parte de la estructura de gobierno de una organización, un programa de gestión del riesgo de fraude debe tener incluida una política (o políticas) por escrito para transmitir las expectativas del consejo de administración y la alta dirección con respecto a la gestión del riesgo de fraude. (Acfe, s.f)

Principio 2: "La organización debe evaluar periódicamente la exposición al riesgo de fraude para identificar posibles esquemas y eventos que la organización necesita mitigar". (Acfe, s.f)

Principio 3: "Deben establecerse técnicas de prevención para evitar posibles eventos clave de riesgo de fraude, cuando sea factible, para mitigar posibles impactos en la organización". (Acfe, s.f)

Principio 4: "Deben establecerse técnicas de detección para descubrir eventos de fraude cuando las medidas fallan o se realizan riesgos absolutos". (Acfe, s.f)

Principio 5: "Debe existir un proceso de presentación de informes para solicitar información sobre posibles fraudes, y se debe utilizar un enfoque de investigación y acciones correctivas para ayudar a garantizar que el fraude se aborda de manera adecuada y oportuna". (Acfe, s.f)

Para COSO (Committe of Sponsoring Organizations of the Treadway) llamado "Fraud Risk Management Guide", donde también habla de 5 principios de la gestión de riesgo de Fraude, los cuales resumimos de la siguiente manera:

Principio 1: "Programa de gestión que demuestre las expectativas del consejo de administración y la alta dirección, y su compromiso con integridad y valores éticos con respecto a la gestión del riesgo de fraude". (Coso. S.f)

[1] Sponsored by, the institute of internal Auditors, The American Institute of certified public accountants y asosiation of certified fraud Examines - "managing the business risk of fraud"

Principio 2: “Para identificar esquemas y riesgos de fraude específicos, evaluar su probabilidad e importancia, evaluar las actividades de control de fraude existentes, e implementar acciones para mitigar los riesgos residuales de fraude”. (Coso, s.f)

Principio 3: “La organización selecciona, desarrolla e implementa actividades de control de fraude preventivo y defectivo para mitigar el riesgo de que ocurran o no eventos de fraude detectados de manera oportuna”. (Coso, s.f)

Principio 4: “La organización establece un proceso de comunicación para obtener información sobre posibles fraudes y despliega un enfoque de investigación y acción correctiva para abordar el fraude de manera adecuada y oportuna”. (Coso, s.f)

Principio 5: “La organización selecciona y realiza evaluaciones continuas para determinar si cada uno de los cinco principios de la gestión de riesgo de fraude se está cumpliendo y operando, y comunica, al programa de Gestión de riesgos de fraude, deficiencias de manera oportuna, para que las partes responsables puedan tomar medidas correctivas, incluida la alta dirección y el consejo de administración”. (Coso, s.f)

En la siguiente tabla, observaremos una relación entre los 5 principios de ACFE y COSO, donde tres de ellos son idénticos (Gobernanza, Evaluación e investigación), adicionalmente el principio No. 3 de COSO está orientado a las actividades de prevención y detección, lo que equivale a los principios No.3 y No. 4 de ACFE, y por último el principio No. 5 de COSO, que hace referencia a un seguimiento continuo de todos los principios con el objetivo de obtener información oportuna para la toma de decisiones dentro del modelo y en beneficio de la compañía.

Tabla 1. ***Principio de ACFE y Principios de COSO***

Principios de ACFE	Principios de COSO
1. Gobernanza de riesgo de fraude	1. Gobernanza del riesgo de fraude
2. Evaluación del riesgo de fraudes	2. Evaluación del riesgo de fraude
3. Prevención de fraude	3. Actividad de control de fraude

4. Detección de fraude	4. Investigación de fraude y acción correctiva
5. Investigación de fraude y acción correctiva	5. Actividades de seguimiento de la gestión de riesgo de fraude

Fuente: Elaboración propia. Información tomada de ACFE y COSO.

Estos principios estarán inmersos dentro del modelo de prevención y control de fraude que se presentará en este trabajo. Consideramos importante presentar un modelo por capas para que, de una manera muy sencilla y efectiva, logremos gestionar el riesgo de fraude sin afectar de una forma considerable la experiencia del cliente.

La experiencia del cliente frente a situaciones de fraude es muy importante en un programa de lealtad. Un cliente espera disfrutar de su recompensa y percibirla como un valor agregado en la interacción con el programa. Dicha experiencia la tendremos en dos momentos:

El primero es cuando un cliente presenta una reclamación por fraude, de esta forma se atiende el caso de forma ágil, adecuada y oportuna para que el cliente sienta que es un pilar importante y fundamental para la compañía.

La segunda, y es la ideal, consiste en prevenir y detectar a tiempo una situación de fraude antes de su materialización, de esta forma el cliente no se verá afectado por esta situación y, por el contrario, podemos aprovechar este incidente para generar una experiencia excepcional.

Por lo anterior, este modelo estará desarrollado en tres niveles, el primero de ellos es el de ***Gobierno,*** en él cubriremos el principio No. 1 ACFE/COSO. Segundo, tenemos la ***Gestión*** donde se valoran los riesgos (principio No. 2 ACFE/COSO), se implementarán controles para prevenir la materialización de fraudes (principio No. 3 y No.4 ACFE y No. 3 de COSO), así mismo, se desarrollarán las capacidades para la operación de dichos controles (principio No. 4 ACFE y No. 3 de COSO) y, por supuesto, en caso de la materialización de un evento de fraude, se realizarán los procesos de investigación (principio No.5 ACFE y No. 4 de COSO), con dos objetivos principales: primero, atender la reclamación de un cliente, y segundo, lograr identificar vulnerabilidades que permitan generar controles adicionales y prevenir futuros incidentes. En el

tercer nivel encontramos las métricas, muy importantes para lograr identificar si las acciones que estamos desarrollando están dando resultados, así como para determinar comportamiento y tomar acciones a tiempo.

Este modelo de tres niveles se desarrollará como se observa en el siguiente gráfico:

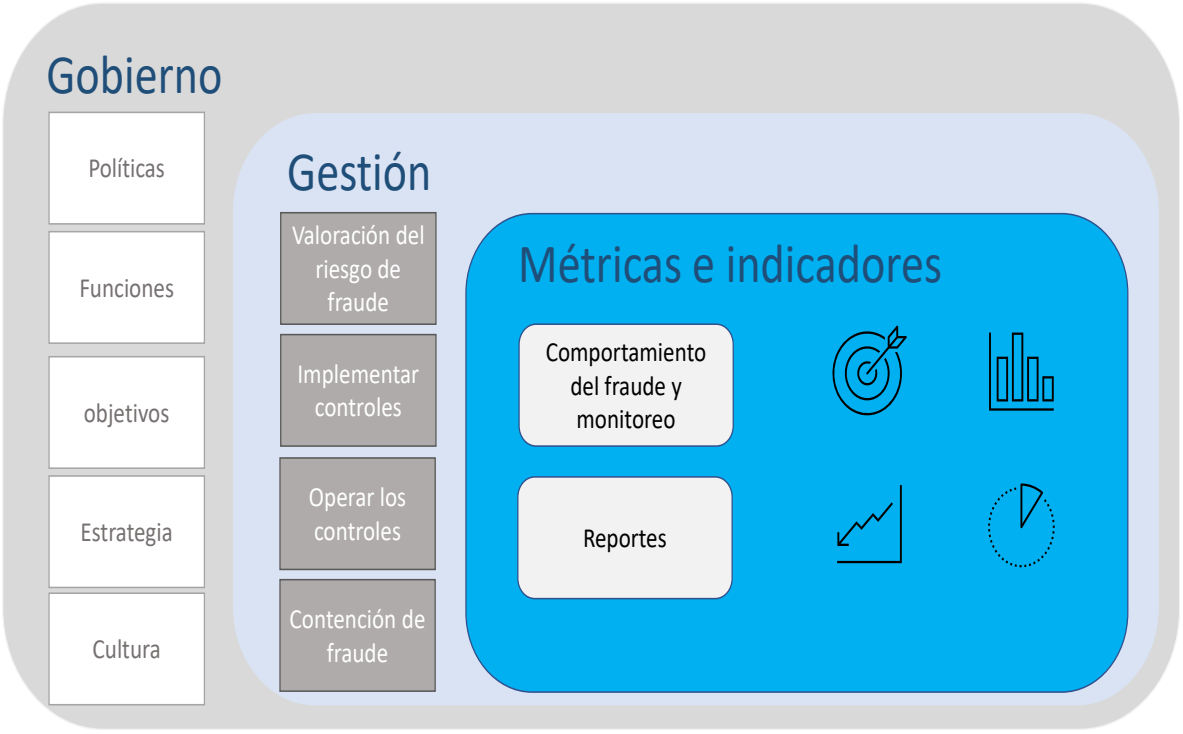

Figura 22. ***Modelo de tres niveles: Gobierno, Gestión y Métrica e indicadores***

Fuente: Cyxtera, 2018.

Dentro de este marco teórico definimos estas tres capas de la siguiente manera:

Gobierno: Responderemos a las preguntas ¿por qué? y ¿para qué? En esta capa definiremos la estrategia transversal para del modelo de prevención y control de fraude, y debe desarrollar los marcos de referencia que permitirán la materialización de la estrategia.

Gestión: Responderemos a las preguntas ¿Qué?, cómo y quién opera y gestiona la prevención de fraude frente a los lineamientos de la estrategia de gobierno?

Métricas: Responderemos la pregunta ¿Qué está pasando? Se realizará seguimiento constante a los indicadores, generando métricas de fraude y de experiencia frente al fraude y gestión de éste.

Gobierno

Es muy importante que exista dentro de la organización un gobierno corporativo, donde se puedan identificar claramente cuáles son los lineamientos que dirigen a la empresa y cómo se controla.

Como se mencionó en la introducción de este capítulo, tanto ACFE como COSO recomiendan, en su primer principio, la importancia de un Gobierno dentro de la Gestión y control de fraudes. El primer principio de la guía práctica de "managing the business risk of fraud" de ACFE (Asociación certificadora de Fraudes), llamado ***Gobernanza del Riesgo de Fraudes*** textualmente menciona: "Como parte de la estructura de gobierno de una organización, un programa de gestión del riesgo de fraude debe estar en su lugar, incluida una política (o políticas) por escrito, para transmitir las expectativas del consejo de administración y alta dirección con respecto a la gestión del riesgo de fraude".

COSO (Committe of Sponsoring Organizations of the Treadway), en la Guía de gestión de riesgo de fraude, en su primer principio denominado ***Gobernanza de Riesgo de fraude,*** menciona lo siguiente: "Programa de gestión que demuestre las expectativas del consejo de administración y alta dirección y su compromiso con alta integridad y valores éticos con respecto a la gestión del riesgo de fraude."

Esto indica que tanto ACFE como COSO coinciden en presentar el Gobierno como primer principio para una buena práctica dentro de la gestión del riesgo de fraude.

Un buen gobierno debe iniciar desde las partes interesadas. En este caso se deben tener en cuenta las expectativas que tienen hoy en día los clientes, socios, aliados, proveedores, accionistas y, por supuesto, los empleados de la compañía.

La junta directiva, seguido del presidente de la compañía y sus directores, debe ser el órgano rector dentro de la organización. Es necesario que desde ahí exista una conciencia sobre el riesgo de fraude que considere la ética empresarial y se definan las políticas que marcarán el camino de la organización.

Este primer nivel de Gobierno lo desarrollaremos tomando como base el siguiente diagrama:

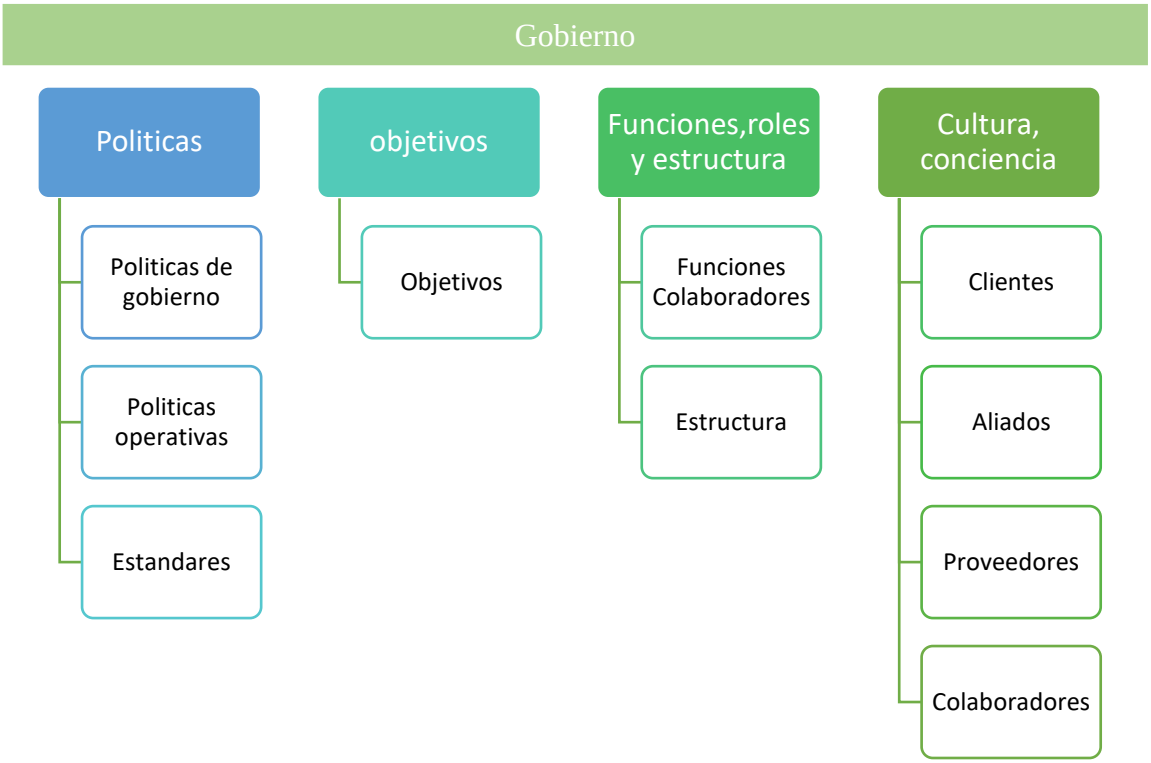

Figura 23. ***Modelo Gobierno***

Fuente: Cyxtera, 2018.

I. Políticas

Políticas de gobierno

Las políticas de Gobierno representan los lineamientos y marcos de actuación de la Prevención y Gestión de Fraude en un programa de lealtad. Son muy importantes para una adecuada toma de decisiones y apoyan a cohesionar la organización de manera asertiva. Básicamente la enfocamos en dos elementos claves:

a). Política de prevención y gestión de fraude

Esta política tiene como objetivo y alcance el establecimiento de mecanismos, controles y gestiones de prevención de fraudes necesarios para mitigar el riesgo de fraude transaccional, así como su gestión de manera adecuada.

Compromisos claves de la prevención de fraude que estarán incluidos en la política:

- Contribuir a controlar y mitigar el riesgo, así como las vulnerabilidades que puedan presentarse en un fraude interno o externo que involucra a clientes, aliados y/o socios.
- Proporcionar planes de conciencia a colaboradores, aliados y proveedores en los riesgos asociados al fraude transaccional, para una adecuada implantación de controles de acuerdo con el rol, responsabilidad y participación dentro de sus funciones.
- Implementar procedimientos de control ajustados al apetito y tolerancia de riesgo del programa de coalición.
- Anticipar escenarios que puedan generar un riesgo de fraude a clientes, aliados y/o socios.
- Gestionar y garantizar el cumplimiento de las políticas de seguridad de la información y ciberseguridad.
- Realizar revisión, evaluación y seguimiento constante al Plan Estratégico de Prevención de Fraude.

b). Comité de prevención y gestión de fraude

Deberá establecerse la conformación de un comité encargado de hacer seguimiento a las actividades estratégicas alineadas al plan estratégico de la compañía. Su función principal es la toma de decisiones y comunicación frente a la priorización y/o cambios que deban definirse en la estrategia de Prevención de Fraude.

El comité debe reunirse de manera periódica y/o extraordinaria en caso de ser requerido (recomendable cada mes), para hacer evaluación de los indicadores estratégicos, métricas de fraude y cumplimiento del plan estratégico que permita tomar decisiones inmediatas o priorizar necesidades requeridas para garantizar una adecuada gestión del fraude al interior del programa de coalición.

Políticas Operativas

Estas políticas las vemos encaminadas a cuatro puntos principalmente: gestión de requerimiento de clientes, políticas de resarcimiento, políticas de monitoreo, políticas de gestión de reglas.

a) Políticas de gestión requerimiento de clientes o reclamaciones por transacciones desconocidas.

Se deben incluir los lineamientos que permitan gestionar de una forma adecuada las reclamaciones por presunto fraude de los clientes. Deben contener lo siguiente:

- Tiempos de respuesta para PQR´s de cara al cliente. Pueden estar establecidos por la segmentación que tenga el programa, por ejemplo, más agilidad para los clientes que representen una mayor participación.
- Establecimiento de eventos críticos de servicio para los casos especiales (Originados por fraude), que permita tomar decisión de cara al cliente y de manera rápida, sobre la respuesta y/o abono de su caso.
- Definir guiones de contacto y/o respuesta a clientes víctimas de fraude.
- Establecer abonos de monto mínimo que pueden ser solucionados durante la llamada (favorables y/o desfavorables). Se debe definir el tope o pérdida de puntos que se puede asumir en esta solución, teniendo en cuenta algunos criterios como: clientes reincidentes (Con más de 2 requerimientos de fraude solucionados durante la llamada en un periodo de tiempo), valor, tipo de reclamación, tipo de cliente y afectación o cambios de datos en la cuenta.
- Establecer criterios claros para bloqueo o desbloqueos de cuentas.
- Lineamientos sobre el aseguramiento de la cuenta, como cambios de claves, restablecimiento de datos originales, cambios de claves en correos personales de los clientes, todo esto con el objetivo de evitar una segunda situación de fraude.

b) Políticas de monitoreo transaccional

Hace referencia a los lineamientos que se deben tener para generar una buena gestión de prevención y detección de fraude transaccional, tanto desde la óptica de una acumulación de puntos, como desde la redención de puntos en todo el ecosistema.

- Lo primero que se debe realizar en este punto es tener una adecuada confidencialidad de las reglas y los modelos utilizados en el motor de riesgo.
- El área debe estar ubicada en un lugar con un adecuado control de ingreso físico, bajo las siguientes recomendaciones:
    - El acceso al área debe ser restringida, sólo pueden ingresar personas que laboren en ella o previamente autorizadas por el personal a cargo del área.
    - Confidencialidad total en el manejo de la información.
    - Las personas a cargo del monitoreo transaccional no deben usar teléfonos celulares al interior del área y/o dispositivos de almacenamiento electromagnético.
    - En lo posible, se debe realizar control de acceso biométrico y con CCTV.

- Se deben tener políticas de bloqueo y desbloqueo de cuentas.
    - Establecer parámetros mínimos para bloqueos luego de gestión de una alerta (confirmada, no confirmada, pendiente). Además de definir seguimiento a través de indicadores de manera constante (Efectividad). Establecer horario de comunicación con los clientes.
    - Definir los tiempos para desbloqueo de una cuenta cuando el cliente no ha confirmado o negado la ocurrencia de un fraude por difícil contacto.
    - Bloqueos masivos (Fugas de Información): Establecer atribuciones del equipo de monitoreo para gestionar bloqueos masivos. Definir marco de actuación para estos eventos.
    - Definir guiones de contacto con clientes.
    - Establecer los canales de comunicación de cara al cliente, SMS, correos electrónicos, WhatsApp, llamadas telefónicas etc.

c) Políticas de diseño e implementación de reglas, modelos de detección y contención de fraude.

- Es fundamental la confidencialidad del diseño e implementación de las reglas tanto de negocio, alertamiento y reglas duras.[2]
- Es clave implementar una matriz RACI[3] que defina y oriente el gobierno para la implementación.
- Definir en qué momento se activa una medida de contención de fraude, establecer el nivel de incremento de fraude y determinar las actividades a desarrollar y sus responsables.

Estándares

Es importante contar con unos estándares mínimos para orientar de forma adecuada la gestión y control del fraude transacción de un programa de Lealtad.

a) Estándares de prevención y control de fraude en la organización

- Requisitos y controles para la implementación de un nuevo canal transaccional o de atención, identificando la autenticación del cliente, parámetros de gestión, observación de log de consultas para futuras investigaciones y una adecuada gestión en el área de monitoreo, accesos, entre otros.
- Disponibilidad de la información transaccional con el objetivo de realizar una buena investigación y gestionar la detección y prevención en las herramientas de monitoreo.
- Información mínima para realizar una adecuada gestión de las reclamaciones de fraude, gestión de los PQR´s y análisis de causa raíz.
- Información mínima para un buen análisis y gestión de puntos de compromiso (fugas de información).

---

[2] Reglas de negocio: se utilizar para controles una situación fraudulenta desde lo catastrófico, se realizan según actividad comercial del aliado o segmentación de clientes.

Reglas de alertamiento: se utilizar para detectar comportamientos inusuales según perfil transaccional del cliente.

Reglas duras: generan un bloqueo de la transacción (no la permiten) y ocurre cuando existe una calificación de riesgo muy alta sobre la misma.

[3] RACI: matriz de asignación de responsabilidades, R (responsable), A (Autoridad), C (consultor) e I (conformado)

b) Estándar de prevención y gestión de fraude con aliados.

- Capacitación para ingreso al programa, guiones y temas bien determinados.
- Cláusulas y responsabilidades frente a situaciones de fraude interno.
- Generación de auditorías de forma periódica.
- Apoyo con información en los procesos de investigación.

II. Objetivos

Objetivo General

Debe estar orientado en dos aspectos, uno de ellos relacionado con la alineación y apoyo a la estrategia corporativa para controlar y mitigar el riesgo reputacional, el riesgo estratégico, de fraude y de cumplimiento, y, segundo, mejorar los indicadores de experiencia frente al fraude. Por tratarse de una compañía de lealtad, es fundamental este aspecto.

Objetivos específicos

- Definir el plan estratégico para la prevención y control de fraude.
- Priorización de requerimientos e iniciativas, enfocados en el análisis y evaluación del riesgo transaccional.
- Atender de manera ágil, asertiva y oportuna los requerimientos de fraude de clientes.
- Detectar y gestionar de manera oportuna y ágil los eventos de fraude a través de los diferentes canales de servicio.
- Realizar un seguimiento continuo a los indicadores estratégicos y gestión de Prevención y Gestión de Fraude.
- Mantener el índice de tolerancia al fraude por debajo de lo estimado en presupuesto y plan estratégico.

III. Funciones, roles y estructura

Describir claramente las funciones y roles que cada puesto de la estructura organizacional de Prevención y Gestión del Fraude debe cumplir para administrar el riesgo de manera adecuada.

a) Estructura

A continuación, se enmarca la estructura propuesta para la operación del Modelo de Prevención y Gestión del Fraude dentro de este marco investigativo. Está orientada a garantizar una administración *end to end* de las diferentes capas que dan dinamismo y fortalecimiento del riesgo de fraude transaccional.

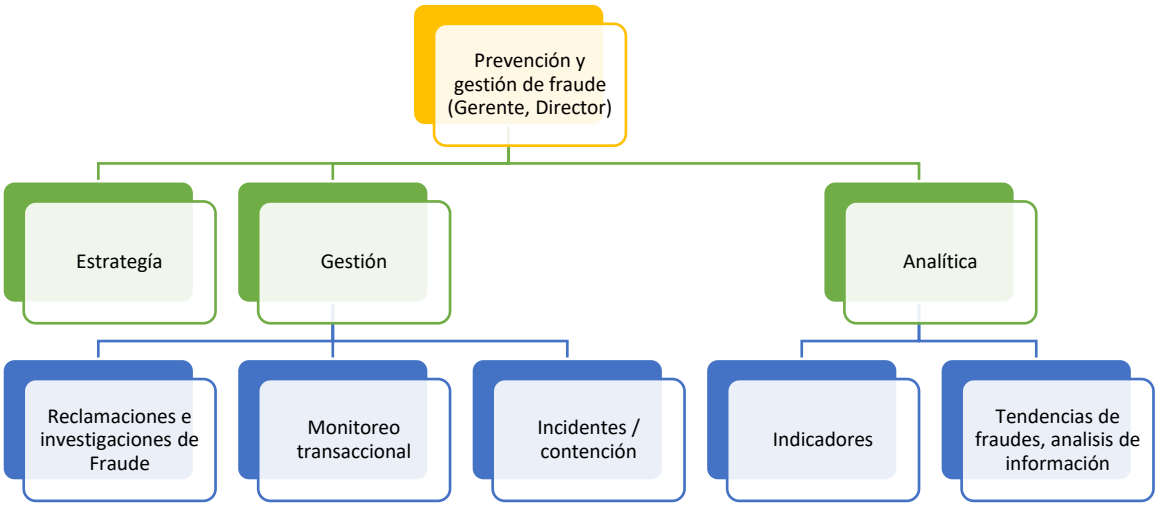

Figura 24. ***Prevención y gestión de fraude (Gerente - Director)***

Fuente: Cyxtera.

Funciones y Roles

Para lograr una buena estrategia dentro del modelo de gestión y prevención de fraude en una empresa de lealtad, se deben identificar las funciones y roles de cada uno de los colaboradores del equipo de trabajo.

Tabla 2. ***Área, funciones y rol***

Área	Funciones	Rol
Prevención y control del fraude	• Definir la estrategia que utilizará para la puesta en marcha del modelo Prevención y gestión de fraude. • Implementar y gestionar el modelo de prevención y control de fraude • Desarrollar, difundir y aplicar las estrategias para la detección y prevención de fraude. • Liderar y gestionar una cultura centrada en el cliente, pensar en la experiencia. • Asegurar la identificación de vulnerabilidades asociadas a eventos de fraude. • Velar por el cumplimiento de los estándares de calidad en la atención de reclamos de fraude. • Coordinar y colaborar con los *stakeholders* en la definición y ejecución de las estrategias que mitiguen los riesgos de fraudes.	Director o Gerente

	• Definir la tolerancia al riesgo.	
Estrategia	• Definir las políticas que alineen el modelo de Gestión y Prevención de Fraude a la visión corporativa • Definir los procesos que den cumplimiento a las políticas definidas • Definir las métricas que permitan validar la alineación del modelo operativo al negocio. • Debe contemplar los cuatro pilares fundamentales de la administración de riesgo: Prevenir, Detectar, Reaccionar y Responder.	Analista o Especialista
Gestión	• Administrar la atención de PQR´s relacionadas con temas de fraude (analizar, evaluar, responder). • Administrar la gestión de monitoreo, así como las herramientas de monitoreo transaccional. • Proponer reglas y parámetros que permitan	Jefe

	mitigar y/o disminuir focos de fraudes. • Proponer reglas y parámetros que permitan mitigar y/o disminuir focos de fraudes. • Definir los KPI´sde los procesos de gestión de modelo. • Implementar y operar la metodología de gestión de incidentes de fraude. • Analizar la causa raíz de los eventos de fraude de manera permanente, teniendo visión holística de los mismos.	
Analítica	• Analizar e interpretar datos que apoyen la estrategia y gestión de fraude. • Capacidad para diseñar modelos que permitan determinar y predecir patrones de fraude. • Generar métricas, KPIs, reportes periódicos. • Identificar tendencia de fraude.	Especialista

	• Analizar datos para mejorar la gestión de monitoreo, falsos positivos.

Fuente: Elaboración propia, Cyxtera

IV. Cultura y Conciencia

Un programa de conciencia es fundamental en un modelo de prevención y control de fraude. Debe ser un habilitador importante para comunicar las expectativas de la gestión de riesgo de fraude, así como es un eje muy clave para la prevención.

Debe ser transversal a todos los participantes del ecosistema de lealtad (Clientes, Aliados, Proveedores y Empleados). En una cultura de Prevención de Fraude, se debe definir un plan de educación constante que haga parte de las políticas de Prevención que enmarcan el gobierno del modelo.

La educación y la sensibilización son un elemento fundamental en la prevención, esto garantiza el uso adecuado de los canales y los servicios del programa. Es un trabajo que debe hacerse desde el individuo de tal manera que permee en el colectivo, y así garantice su evolución en el tiempo y al mismo ritmo de los cambios tecnológicos que se vayan dando en los procesos y el ecosistema.

Se debe definir un objetivo general y varios objetivos específicos orientados a lo siguiente:

- Generar e incrementar el nivel de conciencia de los grupos de interés.
- Enfocarse en los cambios de comportamiento para prevenir situaciones de fraude.
- Mejorar el nivel de conciencia de los actores.
- Debe estar alineado con la necesidad del negocio.
- Orientado a cumplimiento de requerimientos legales y normativos.

Así mismo, es importante realizar un diagnóstico del inicio del programa con escalas y matrices del nivel de riesgos de cada individuo evaluado.

Gestión

Una vez definido el Gobierno y los lineamientos para poder conocer la ruta del modelo, se debe generar y encontrar el camino para una buena gestión de actividades tanto preventivas como correctivas y de contención.

a) Valoración del riesgo de fraude

Como lo menciona la guía de gestión de riesgo empresarial de ACFE, en su principio No. 2, toda organización debe evaluar el riesgo de forma constante para identificar posibles eventos que se necesitan mitigar.

Según ACFE "El fraude, por definición, implica una mala conducta intencional, diseñada para evadir la detección". Por esta razón, dentro de la valoración del riesgo de fraude, se debe participar con un equipo que permita razonar estratégicamente para anticipar al comportamiento de un posible estafador, ya sea interno o externo.

Para evaluar el riesgo de fraude se define como "efecto de la incertidumbre en los objetivos" (ISO Guía 73, 2009), dichos objetivos se enfocan desde el punto de vista estratégico de la compañía. Ahora, la incertidumbre la podemos catalogar como la deficiencia de información, sea parcial o total, en función de los siguientes tres elementos:

$$\text{Riesgo (E)} = \text{Probabilidad}^{4}\text{ (E)} * \text{Consecuencia}^{5}\text{ (E)}$$

(E), se refiere al evento es "ocurrencia o cambio de un conjunto de circunstancias en particular". (ISO Guía 73, 2009)

De otra parte, la incertidumbre la podemos ver desde el punto de vista cuantitativo y cualitativo. Estos dos conceptos son muy importantes porque, al momento de valorar los riesgos, los podemos analizar a través de una distribución de probabilidad (cuantitativa) o a través de una matriz de riesgos y un mapa de calor (cualitativa), aunque lo más recomendable, para la evaluación del riesgo de fraude, es realizar el análisis desde las dos formas.

[4] Probabilidad: con qué frecuencia se presenta o se materializa un evento

[5] Consecuencia: ¿cuáles son los impactos en caso de materializarse el evento?

- Distribución de probabilidad (cuantitativa)

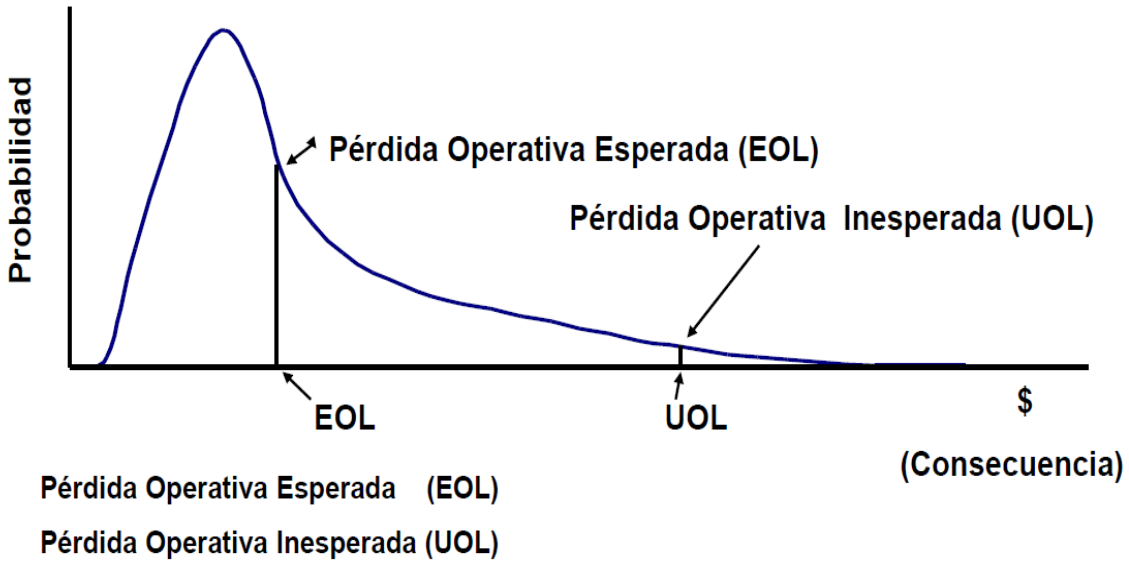

Figura 25. ***Distribución de probabilidad (cuántica)***
Fuente: Alaris. Fundación Latinoamérica de Administración de Riesgo.

Para calcular este valor dentro de un programa de lealtad, podemos tener en cuenta los siguientes aspectos:

- Proyección de clientes.
- Valoración de los impactos y la frecuencia de los fraudes presentados en un periodo de tiempo.
- Distribución de los puntos que tienen las cuentas de los clientes (saldos disponibles en sus cuentas), según percentiles.

A través de esta distribución de probabilidad, podemos definir cuál será la tolerancia al riesgo [6]desde el punto de vista cuantitativo, recordando que, para llegar a esta definición, la organización debe tomar los riesgos inherentes[7] basados en el apetito de riesgo[8] que se tenga.

- **Mapa de Riesgo (Cuantitativo – Cualitativo)**

Rango Consecuencia Y	**Criticidad Individual (1-Y)**	**Criticidad Individual (2-Y)**	**Criticidad Individual (X-Y)**
Rango Consecuencia 2	**Criticidad Individual (1-2)**	**(Criticidad Individual (2-2)**	**Criticidad Individual (X-2)**
Rango Consecuencia 1	**Criticidad Individual (1-1)**	**Criticidad Individual (2-1)**	**Criticidad Individual (X-1)**
	Rango Probabilidad 1	**Rango Probabilidad 2**	**Rango Probabilidad X**

Figura 26. ***Mapa de Riesgo (cuantitativo – Cualitativo)***

Fuente: Alaris. Fundación Latinoamérica de Administración de Riesgo.

[6] Es el nivel de riesgo que quiero asumir una vez han sido tratados, mitigados o controlados. También es la capacidad máxima financiera que quiero asumir dentro de un presupuesto.

[7] Son todos los riesgos en una organización sin controles de forma virgen.

[8] Es el tipo de cantidad de riesgos que está dispuesto a asumir una organización para el cumplimiento de los objetivos.

- **Mapa de Calor**

Rango Consecuencia C (Catastrófica)	Criticidad Individual (1-C)	Criticidad Individual (2-C)	Criticidad Individual (3-C)
Rango Consecuencia B (Considerable)	Criticidad Individual (1-B)	(Criticidad Individual (2-B)	Criticidad Individual (3-C)
Rango Consecuencia A (Insignificante)	Criticidad Individual (1-A)	Criticidad Individual (2-A)	Criticidad Individual (3-A)
	Rango Probabilidad 1 (Baja)	Rango Probabilidad 2 (media)	Rango Probabilidad 3 (Alta)

Figura 27. Mapa de Calor

Fuente: Alaris. Fundación Latinoamérica de Administración de Riesgo.

Para poder realizar una evaluación del riesgo de fraude en una compañía de lealtad, se menciona que dichos riesgos están catalogados por su naturaleza como riesgos Operativos[9], y de ellos se desprenden los siguientes tipos de riesgos frente a situaciones de fraude:

- Fugas de información de bases de datos interna.
- Fugas de información externas en aliados y socios o clientes.
- PQR’s mal gestionados.
- Suplantación de clientes en los canales de atención (sitios Web, Aplicaciones, Call Center, WhatsApp).
- Suplantación de clientes en puntos de ventas de los aliados.
- Fraudes no identificados por falta de controles de monitoreo y procesos de gestión de incidentes.
- Posibilidad de fraude interno por uso indebido de los sistemas de información.
- Suplantación de clientes en e-commerce o ventas virtuales.

[9] Son riesgos controlables tener acceso a la fuente.

- Insuficiente conciencia por parte de los grupos de interés.
- Posibilidad de suplantación en trasmisión de información de acumulación de aliados.
- Acumulación irregular por parte de cajeros en los puntos de venta de los aliados.
- Insuficiencia en gestión del gobierno de riesgos.

b) Implementar los controles

Es muy difícil, por no decir que imposible, que una organización pueda eliminar por completo el riesgo de fraude. Siempre existirán personas motivadas para comprometerse o materializarlo, y, desafortunadamente, por falta o deficiencia en los controles, puede surgir una oportunidad para que en cualquier organización alguien anule un control o se una con otros para ejecutarlo.

Por lo anterior, es fundamental la implementación de soluciones de prevención de fraude, además del diseño y ejecución de procesos de gestión, a partir de los criterios, políticas y necesidades identificadas dentro de la estrategia.

Las organizaciones son susceptibles al fraude, para muchas de ellas no es rentable intentar eliminar todos los riesgos de fraude generados. Una compañía de lealtad debe diseñar sus controles para poder detectar, en lugar de prevenir, algunos riesgos de fraude externo. Por la misma naturaleza del negocio (el cliente espera una recompensa por la fidelidad), la compañía define cuáles riesgos debe tratar y gestionar, ya que eliminar un riesgo puede resultar más costoso que controlarlo y monitorearlo.

También ocurre lo contrario si los costos estimados de diseño, implementación y monitoreo de los controles contra el fraude –como herramientas, personal o capacitación–, excede el impacto estimado del riesgo. Es posible que su implementación no sea rentable, como dice el dicho popular: “Es más costoso el remedio que la enfermedad”.

La implementación de controles debe tener una análisis cuantitativo y cualitativo frente al impacto que esto puede generar para la generación de valor a los clientes, aliados, socios y empleados del programa, ya que los mismos, por el contrario, podrían generar una mala experiencia, una pérdida en las ventas o clientes insatisfechos, afectando directamente la utilización del programa y el futuro de la organización.

c) Operar los controles

Antes de iniciar con la operación de cada uno de los controles para la prevención del fraude, es posible que se puedan eliminar o adicionar algunos de ellos. Por esta razón, mencionaremos algunos, los cuales pueden ser diferentes, según la compañía y la evolución.

- ***Registro al programa***

Es fundamental que los controles se apliquen desde el registro de un cliente al programa, procurando que se realice en el menor tiempo posible y con todos los parámetros de seguridad para lograr una plena identificación. Un proceso ágil se puede generar solicitando información básica y confrontándola con alguna base legal de un estamento de control, o a través de una compañía de tratamiento de datos que gestione este tipo de riesgos.

- Nombre y apellidos
- Fechas de expedición de cédulas
- Lugar de expedición
- Ciudad de expedición
- Tipo de documento
- Número de documento
- Correo electrónico
- Número de celular.

Otra forma más avanzada para controlar este tipo de registros es por medio de la validación de una identidad digital, que se puede realizar de la siguiente manera:

- Datos básicos del cliente.
- Registro biométrico, puede ser facial, dactilar, voz etc.
- Validación documental, originalidad de los documentos.
- Confrontación de información frente al registro.

Una tercera forma de realizar este control, que muchas veces resulta más efectiva, es a partir de la combinación de varias capas de seguridad al momento del registro al programa, discriminadas de la siguiente manera:

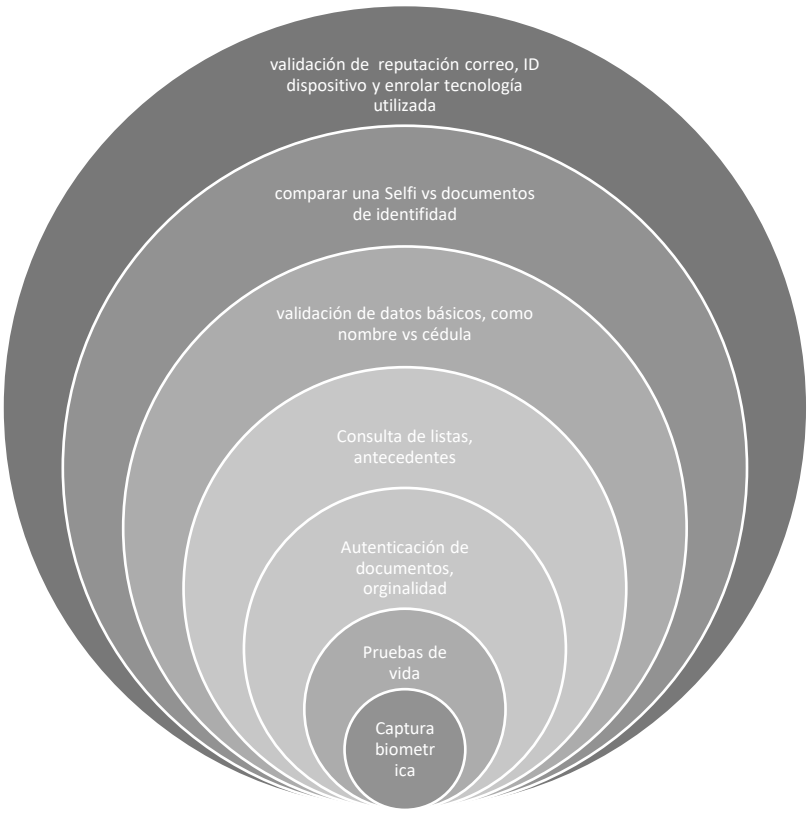

Figura 28. ***Capas de Seguridad – Registro de programa***

Fuente: Elaboración propia.

- ***Atención de reclamaciones por fraude***

En un programa de lealtad, los requerimientos de fraude requieren estar alineados al modelo de experiencia de la organización. La gestión dentro de este proceso debe garantizar un flujo ágil, veraz, oportuno y soportado en una política de resarcimiento definida con anterioridad, con el fin de darle el dinamismo requerido y ofrecerle al cliente una excelente experiencia, aunque ella se encuentre en un contexto de fraude.

Este proceso tiene un flujo de 6 actividades, relacionadas en la siguiente figura:

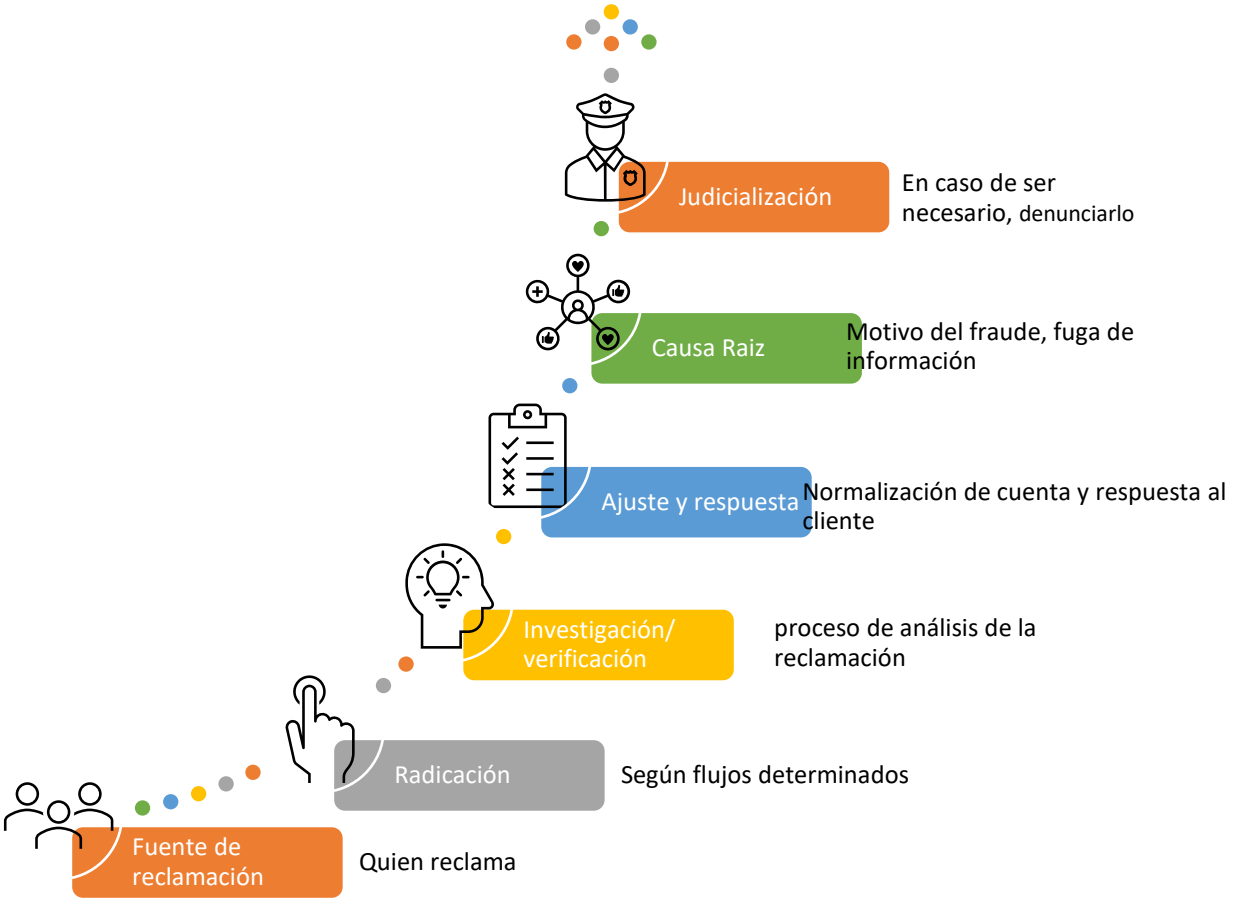

Figura 29. ***Proceso reclamación por fraude.***

Fuente: Elaboración propia. Apoyo Cyxtera.

I. Fuente de reclamación

La reclamación por un fraude se puede presentar desde tres puntos de vista:

- Cliente: Puede realizar la reclamación por cualquiera de los canales destinados para tal fin, (Call center, WhatsApp, Chat o Web).
- Otros grupos de interés como socios, aliados o funcionarios de la organización.
- Monitoreo: El área de monitoreo transaccional de la organización puede detectar este tipo de situaciones e iniciar el proceso de reclamación.

II. **Radicación**

En este proceso se deben tener en cuenta varias actividades para poder orientar al cliente y atender el caso en los flujos determinados. Dichas actividades son:

- Identificar tipo de evento de fraude.
- Validar estado de cuenta, cliente y/o Factor de Autenticación, realizar el bloqueo temporal o permanente de alguno de ellos o todos según el evento.
- Realizar preguntas de validación del caso (Guión de radicación).
- Determinar tipo de caso y aplicar políticas:
  - Monto Inferior
  - Solución en Primer Contacto
  - Clientes Vip
- Entregar respuesta con promesa y recomendaciones. Deben existir guiones establecidos para unificar la experiencia y facilitar la labor del funcionario que atiende el caso.
- Radicar el caso en bases de datos con el detalle de las transacciones de fraude reclamadas por el cliente.
- Generación de informes propios e indicadores de gestión periódicos.

Es recomendable que el equipo que integra el área tenga un alto conocimiento sobre fraude (sus modalidades y la forma de mitigación). Por tanto, se debe garantizar un proceso de capacitación y actualización de forma constante.

III. **Investigación / Verificación**

En esta etapa del proceso se debe realizar un buen análisis de la reclamación con el objetivo de entregar una respuesta, a favor o contra del cliente, que esté acorde a las políticas de resarcimiento. Algunas de las actividades más importantes en este punto son:

- Identificar transacciones de redención y/o acumulaciones reclamadas vs las transacciones que normalmente realizaba el cliente antes de la reclamación.
- Entender los cambios de su cuenta antes de la reclamación, como cambios de clave, cambios de datos personales e intentos de ingresos a su cuenta.

- Identificar promedios de transacción, horarios de uso, actividades comerciales que frecuenta.
- Identificar el buen uso de sus credenciales o claves personales.
- Se debe elaborar un informe claro y conciso sobre el análisis realizado y sus conclusiones, con el fin de justificar la devolución o no de los puntos.

IV. **Ajuste y Respuesta**

Este proceso no lo debe realizar el área de prevención y control de fraude, es recomendable que se ejecute en el área de operaciones, y tiene las siguientes actividades:

- En este punto se debe normalizar la cuenta[10], generar desbloqueo de la cuenta y confirmar los cambios de credenciales para evitar una nueva situación de fraude.
- Realizar el ajuste a la cuenta conforme a las conclusiones de la investigación y las políticas de resarcimiento.
- Respuesta al cliente.
- Documentar el caso y cerrarlo en las aplicaciones utilizadas para este tipo de controles y dejar la trazabilidad de éste.

V. **Causa Raíz**

Es importante identificar vectores de ataque, vulnerabilidades y causas del fraude presentado, partiendo de las investigaciones realizadas en el punto III. (Investigación y verificación). Al final de este proceso se suministra información estratégica para definir controles y acciones que mitiguen el fraude. Dentro de las actividades más importante de este punto tenemos las siguiente:

- Realizar análisis periódicos a los casos radicados por fraude, de acuerdo a la modalidad que éste tenga. Para ello se analizarán aspectos como actividades comerciales, aliados involucrados, tipos o segmentación de clientes, ubicación de los clientes etc.

[10] Es realizar el ajuste o devolución de los puntos

- Seguimiento a las métricas de manera diaria para identificar picos de manera inmediata.
- Integrar información de los casos desde aliados, canales y áreas transversales de la organización.
- Evaluar convergencias (Transaccional, consultas, logs, IPs utilizadas, entre otros).
- Evaluar fallas en controles o ejecución de procesos alrededor del ecosistema.
- Determinar clientes en riesgo y definir acciones según políticas de Prevención de Fraude (Eventos masivos en caso de aplicar).
- Diseñar informe con resultados, hallazgos y recomendaciones.
- Presentación del informe al interior de la Gerencia y/o Dirección.

VI. **Judicialización**

Para algunos eventos e investigaciones determinadas se deben generar los canales y mecanismos de denuncia penal de los procesos de investigación realizados dentro de la organización, ya sea que, por su monto, cantidad de transacciones y afectación a los aliados, se determine la necesidad de colocar en conocimiento de las autoridades competentes el caso para su investigación y juzgamiento.

Este proceso se debe realizar en conjunto con el área jurídica o tener dentro de la compañía una empresa externa experta en este tipo de denuncias para que apoyen el trámite legal.

- ***Monitoreo transaccional – motor de riesgo***

Para una compañía de lealtad, el riesgo de fraude está ligado, en un porcentaje muy alto, a lo transaccional. Es decir que la pérdida por situaciones irregulares se presenta en las operaciones de redención y/o acumulación. Es por este motivo que desarrollar un modelo de monitoreo transaccional es primordial dentro de la estratégica de prevención y control de fraude. Aquí un ejemplo:

Figura 30. ***Modelo de monitoreo transaccional***

Fuente: Elaboración propia. Apoyado Cyxtera.

El objetivo de este modelo es el de gestionar, de una forma adecuada, el alertamiento de transacciones riesgosas.

i. Análisis de información: Para realizar cualquier cambio en una regla determinada, es importante analizar el impacto que dicho cambio generaría en el programa en aspectos como falsos positivos, cantidad de fraude que podría llegar a detectarse, potencial de detección, número de puntos, cantidad de clientes que se afectarían, combinaciones que podrían utilizarse para ser más efectivos (montos, ciudades, calificaciones de riesgo, perfil transaccional del cliente, etc.).

   Adicionalmente, sería necesaria la implementación de herramientas de monitoreo transaccional de fraude que cuenten con capacidades de Machine Learning con el fin de propiciar un aprendizaje continuo y asegurar un buen perfilamiento del cliente, lo

que llevaría a minimizar las cargas operativas de análisis de información y mejoraría la experiencia del cliente.

ii. Diseño de reglas: Deben estar basadas en la analítica y los objetivos del programa para lograr un equilibrio entre la detección y la experiencia. Así mismo, se debe aprovechar la información disponible, orientada por un equipo especializado con la mayor confidencialidad posible.

iii. Prueba de la regla: Las nuevas reglas que apoyarán la gestión deberán ser probadas antes de su puesta a producción, determinando su efectividad (Falso positivo) e impactos en niveles de servicio y/u operativos. Es importante modelar estos cambios en la misma herramienta y con datos reales.

iv. Implementación: Luego de cumplir con las condiciones y políticas definidas como marco de gobierno de operación en la Prevención de Fraude, las reglas serán puestas en producción, garantizando una gestión adecuada de las mismas.

v. Gestión de alertas: La gestión de alertas deberá tener capacidad de gestión 7x24, según las condiciones del programa. La capacidad del equipo deberá estar ajustada a los volúmenes de alertamiento generados, reglas de negocio y/o reglas de cliente, de acuerdo con la solución que se defina como parte de apoyo a la gestión. El bloqueo y contacto con el cliente debe estar acorde a las políticas de operación de fraude definidas como marco de gobierno en Prevención de fraude.

vi. Seguimiento y ajuste de reglas: Deberá realizarse de manera constante. A partir de los indicadores de gestión, es indispensable priorizar ajustes (Cambios, eliminación o implementación de reglas), garantizando el objetivo de control a través de la detección oportuna de transacciones de fraude.

- ***Capacidades analíticas***

La información y los datos son un pilar fundamental para un modelo de prevención de fraude, sin ellos sería imposible lograr una buena gestión de prevención, detección, recuperación y experiencia para los clientes. Este modelo está orientado en el riesgo de fraude transaccional de

tal forma que la información que se entregue en los procesos deberá proyectar el resultado y el futuro de la organización.

- ***Modelos de puntos de compromiso***

Cuando se presenta un fraude, debe existir de forma obligatoria una fuga de información que permitió la materialización de la pérdida. Pueden existir varios focos de fuga de datos entre ellos:

- Internos: Dentro de la misma organización o un proveedor que trabaje para ella.
- Externos: En establecimientos aliados y con los mismos socios.
- Cliente: El cliente es una fuente de fuga de información. Hoy en día es muy frecuente por la ingeniería social de la que es susceptible. El más conocido es el Phishing[11].

Elaborar una iniciativa donde se puedan identificar de una forma ágil las fugas de información, es una acción clave para un modelo de prevención y control de fraude. Esto permitiría ubicar e identificar a los clientes que podrían estar comprometidos o en situación de riesgo. A partir de esto, se podrían programar medidas de prevención de fraude como cambios de claves, monitoreos constantes, utilización de dobles factores de autenticación etc.

En un modelo de puntos de compromiso se debe tener en cuenta toda la información posible del cliente y la interacción con el programa, socios y aliados en un periodo anterior al fraude, con el objetivo de identificar un punto en común entre todos los casos de fraude presentados en un determinado periodo.

d) Contención de fraude

Hace referencia a un equipo de trabajo o área encargada de la respuesta frente a incidencias de fraude transaccional. Debe participar el personal experto en la definición de medidas preventivas y reactivas ante eventos graves.

[11] Phishing: es un proceso fraudulento de la rama de la ingeniería social cuyo objetivo es adquirir información sensible como nombres de usuario, claves o datos de cuentas o tarjetas de crédito a través de una comunicación electrónica.

Las funciones principales de este grupo de trabajo son:

- Atender y gestionar la mitigación y prevención de incidentes de fraude.
- Gestionar la protección de canales, servicios y/o clientes impactados o en riesgo.
- Coordinar de manera centralizada la atención del incidente, con las demás áreas de la organización, midiendo el impacto de las actividades a realizar.
- Determinar y analizar la causa del incidente.
- Guardar evidencias para un posible proceso de judicialización, y entregarlas al área de fraude encargada de gestionarlos.

Métricas e Indicadores

En esta tercera y última capa del modelo de prevención y control de fraude se definen las medidas y KPI´s que nos garanticen una adecuada vigilancia y evaluación de los controles que se han implementado, con el objetivo de anticiparnos a comportamientos, y tomar decisiones acertadas y oportunas. También para determinar los cambios a realizar para mejorar el comportamiento del fraude, y cumplir así con la tolerancia definida por parte de la organización en su plan estratégico.

En los siguientes cuadros identificaremos algunos de las métricas, indicadores y reportes que se deben establecer para una buena gestión del modelo:

a) Métricas

Tabla 3. ***Métricas***

Nombre de la métrica	Descripción
Fraudes por número de casos – ocurrencia	Evolución del fraude materializado (pérdida confirmada) en el tiempo (Horas-Diario-Mensual) por número de eventos.
Fraudes por número de casos – reclamados no materializados	Evolución del fraude reclamado (no hay pérdida), se presentó un intento y fue detectado a tiempo, (hora-días-mes) por número de eventos registrados.
Fraude por cliente afectado	Evolución del fraude ocurrido por cliente afectado, evolución en el tiempo (hora-día-mensual).
Valor del fraude reclamado	Hace referencia a la reclamación de puntos dentro del proceso de reclamación (hora-día-mes).
Valor fraude asumido o pagado al cliente	Evolución del fraude asumido por la compañía a los clientes según políticas de resarcimiento. Reclamación en el tiempo (día-mes-año).
Fraude por tipología o modalidad	Evolución del fraude por modalidad a través del tiempo (día-mes-año).
Fraude por canal	Evolución del fraude por canal (presencial-virtual), a través del tiempo (horas-día-mes-año).
Fraude por aliado	Evolución del fraude por aliado inscrito en el programa de fidelización, se mide el valor, punto de venta y ciudad, a través del tiempo (día-mes-año).

Fuente: Elaboración propia. Apoyado Cyxtera

b) Indicadores

Podemos gestionar dos tipos de indicadores, unos desde el punto de vista estratégico, los cuales deben estar alineados con el plan estratégico de la compañía y otros de gestión internos del área de prevención y control del fraude.

Tabla 4. ***Indicadores Estratégicos***

Objetivo Estratégico de la compañía	Nombre	Descripción	Fórmula
Objetivo A	Siniestralidad	Determinar los niveles de pérdida frente a las ventas de todo el programa	(Valor fraude asumido / los ingresos de la compañía) *100 (redención y/o acumulación)
Objetivo B	Impacto de Fraude	Determinar el impacto real vs la pérdida esperada de forma mensual (Apetito al riesgo)	(Pérdida real / pérdida esperada) *100
Objetivo C	Experiencia / Servicio (bloqueos)	Determinar la eficiencia de los bloqueos generados por el área de monitoreo transaccional	# de bloqueos realizados (fraude) / total de bloqueos realizados
Objetivo D	Atención de PQR´s	Determinar la oportunidad de respuesta hacia las reclamaciones de los clientes	# de casos solucionados a tiempo / total de casos gestionados

Fuente: Elaboración propia. Apoyado Cyxtera

Tabla 5. ***Indicadores de Gestión***

Área	Tipo	Nombre	Descripción	Fórmula
Monitoreo	Operativo / Experiencia	Falso positivo	Determinar la efectividad de las reglas de gestión, de negocio o duras.	Alertas de fraude confirmas / total de alertas generadas.
Monitoreo	Operativo / Experiencia	Contactabilidad	Efectividad en el contacto con el cliente	Clientes con contactos efectivos / total de clientes gestionados
Fraude	Experiencia	Favorabilidad	Los casos con respuesta favorable hacia el cliente	# de casos con favorabilidad / total de casos gestionados
Fraude	Financiero	Pago fraude	Valor asumido con la compañía por reclamaciones de fraude	Valor total asumido por la compañía / el valor total reclamado

Fuente: Elaboración propia. Apoyado Cyxtera

Tabla 6. ***Reportes***

Destinatario	Descripción	Periodicidad	Responsable de entrega
Gerencia General / Comité de fraudes	-Informe evolución de indicadores estratégicos -Proyectos del área y mejoras a los procesos - Seguimiento Planes de acción ya convenidos	Mensual	Gerente / director de área
Director / Gerente de Seguridad	-Informe evolución de indicadores estratégicos y de gestión táctica tanto de fraudes como de monitoreo -Causas de fraude e impacto operativo en el programa -Planes de acción de casos importantes y de impacto para la compañía	Semanal	Jefe de área
Aliados	-Métricas de comportamiento de fraude por puntos de venta. -Evolución de causas raíz. - Planes de acción determinados. - Recuperación realizadas	Mensual	Jefe de área
Jefe de área	-Métricas de Fraude -Indicadores de Gestión -Evaluación de causa raíz -Planes de acción de corto plazo	Diario	Analista de gestión de fraude

Fuente: Elaboración propia. Apoyado Cyxtera

Capítulo 5

Evolución frente a los controles para mejorar la experiencia

Uno de los retos más importantes en un modelo de prevención y control del riesgo transaccional, dentro de un programa de lealtad, es el de poder combinar la experiencia del cliente con la prevención y el control. No se puede llegar a ser tan estricto en los controles porque de esa manera se afectaría la experiencia del cliente. En este capítulo desarrollaremos algunos puntos que nos lleven a determinar la mejor manera de conservar dicho equilibrio.

Evolución en el registro del programa

Hoy en día existen dos tendencias en el mercado, la primera de ellas relacionada con la eliminación de la clave estática para identificación de clientes y autenticación de sus transacciones, y la segunda, relacionada con la migración de los consumos de los clientes a los canales virtuales.

Por lo anterior, se hace necesario realizar un buen registro e identificación del cliente, con el objetivo de controlar el riesgo de fraude por suplantación, y con el fin de gestionar a futuro una autenticación segura de sus transacciones.

a) Soluciones biométricas

Este tipo de soluciones utiliza diferentes tecnologías aplicadas al reconocimiento de personas basadas en sus características fisiológicas e incluso en su comportamiento. Una vez logramos registrar al cliente en el programa a través de la captura de sus datos, extraemos un patrón único para cada uno de ellos. Dichos patrones sirven para identificarlos y compararlos al momento de un proceso transaccional o para el manejo de su cuenta en términos de ingreso, cambio de datos personales, cambios de acreencias y usuario.

Cuando se utiliza un método de registro y posterior autenticación de los clientes con registros biométricos, minimizamos ataques de numeración de login en el sitio Web. Estos ataques son utilizados por hackers para lograr adivinar las claves estáticas que hoy utiliza la gran mayoría de compañías. Posteriormente, materializan el fraude en puntos de venta o de manera virtual.

Algunas de las soluciones más usadas en el mercado son las siguientes:

Facial

En la facial logramos identificar puntos característicos del rostro. Puede evaluar la distancia y la profundidad de los ojos, el color de cabello y la tonalidad de la piel. Así mismo, es importante contar con acciones como una sonrisa para dar fe de vida de los clientes.

De Voz

Con la voz podemos evaluar o identificar el tono, la cadencia, el volumen de cada uno de los clientes. También puede ser utilizado como prueba de vida.

Huella

Una de las más utilizadas en el mercado, es el enrolamiento y reconocimiento del patrón de la huella dactilar de una persona. En este proceso identificamos la profundidad de sus surcos, también es importante desarrollar mecanismos de pruebas de vida como el calor en el dedo.

De la mano

Este proceso es poco usado pero muy práctico. Reconoce los caracteres de los pliegues y la circulación de la mano. También sirve como prueba de vida.

Autenticación basada en riesgo

Un modelo de autenticación basado en riesgo permite a una organización tener una autenticación dinámica, que tiene en cuenta aspectos muy importantes como el perfil del usuario que accede al sistema y el perfil de riesgo asociado a la transacción que se esté realizando, la cual puede ser monetaria[12] o no monetaria[13]. El perfil de riesgo es usado para determinar la complejidad de la autenticación.

[12] Es una forma de pago, representa un valor para el cliente y el programa, en este caso puede ser una transacción de redención de puntos.

[13] Es una transacción que no tiene un valor directo para el cliente, como puede ser un cambio de datos, ingresos al sitio web.

Con el objetivo de mantener los fraudes por debajo del apetito de riesgo establecido por la compañía, se puede implementar la autenticación basada en riesgo. Con ella se lograría identificar al cliente de una forma transparente y sin fricción, utilizando la tecnología que ellos mismos utilizan.

Según Forrester – "La autenticación basada en riesgo (RBA) monitorea silenciosamente las acciones del usuario y el contexto de la transacción para producir un puntaje de riesgo. La RBA frecuentemente lleva a la activación de un método más fuerte de autenticación de usuario". (párr. 6)

La autenticación basada en riesgo tiene como objetivo identificar criterios de riesgo y calificarlos para que, conforme a dicha calificación, se tomen decisiones sobre la viabilidad de la operación. Existen más de 200 criterios que se pueden obtener de un dispositivo sin que ello genere ningún tipo de invasión a la privacidad del cliente, por ejemplo: ubicación geográfica, dirección IP desde donde se está realizando la operación, sistema operativo utilizado, software antivirus, tipo de dispositivo (celular, consola de juegos, PC), etc.

Con esta información podemos determinar si la operación que se está ejecutando representa un riesgo bajo, medio o alto, y sobre dicha calificación podemos tomar acciones como: aprobar la operación, rechazarla, buscar contacto con el cliente con el objetivo de que confirme la transacción, ya sea por medio de llamada telefónica, mensaje de texto, WhatsApp o correo electrónico.

El valor agregado, cuando tenemos una autenticación basada en riesgo, es el de generar la menor fricción posible con el cliente, ya que, al presentarse una situación sospechosa, tenemos la oportunidad de retarlo por medio de validaciones adicionales que permiten comprobar su identidad y la autenticidad de la operación.

Como ya lo hemos mencionado, se trata de un modelo que reduce la fricción con los clientes y ayuda a prevenir el riesgo de fraude transaccional. La autenticación basada en riesgo (RBA) ejecuta y utiliza el nivel necesario de seguridad para cada interacción única del cliente según se perfil transaccional, y al mismo tiempo omite pasos de seguridad innecesarios para transacciones de bajo riesgo, evitando así reprocesos que generarían costos adicionales y un mal servicio al cliente.

En un modelo aplicado con autenticación basada en riesgo, el nivel de riesgo normalmente se da en porcentajes (%). Un nivel de riesgo se crea a partir de una serie de factores relacionados con el perfil de cliente, sus transacciones, movimiento de su cuenta, y ahora, con un cliente virtualizado, se utilizan otras herramientas como la biometría de comportamiento[14] desde los dispositivos, geolocalización y diferentes factores que proporcionan una efectividad mayor.

Una autenticación basada en riesgo la podemos ver como una capa adicional en el modelo de interacción del usuario de un programa de lealtad, como se observa en el siguiente gráfico:

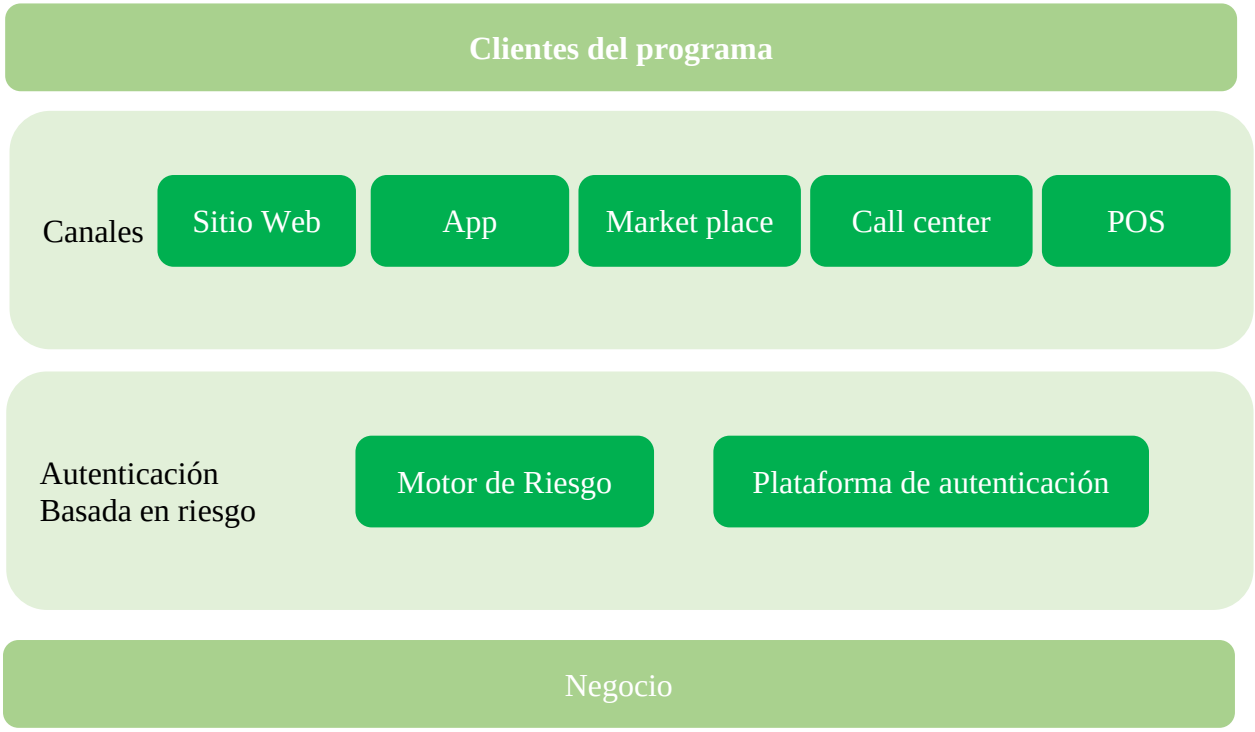

Figura 31. ***Canales para una autenticación basada en riesgo***

Fuente: Cyxtera.

El objetivo de este modelo es evaluar el riesgo transaccional del cliente teniendo en cuenta la información del comportamiento en los diferentes canales, tanto presenciales como virtuales.

[14] Biometría de comportamiento: según Excle.com, "se basa en la idea de que la manera de escribir, usar el mouse y hasta sostener el teléfono son elementos para la creación de una identidad digital que no puede ser suplantada por alguien más".

Con base en la calificación del riesgo, se definirá si se habilita un esquema de autenticación adicional al primer factor.

Componentes de la autenticación basada en riesgo

a) Clientes del programa o perfil del cliente

Hace referencia al perfil que tiene el cliente con base en el uso del programa, sus canales transaccionales, los puntos de redención y acumulación, la información que tiene registrada. Según el modelo, puede existir tres tipos de contextos:

Navegación. En este contexto se debe informar al motor de riesgos bajo qué canal se realizó la transacción objetivo de análisis (Sitio Web, Aplicación, Call Center, WhatsApp etc). Adicionalmente, debe entregar los perfiles de la información en la red, la información de la geolocalización (País, región, IP), la información del dispositivo que está utilizando como medio de navegación y el sistema operativo utilizado.

Aplicación (APP). Siendo un servicio muy similar a la navegación en la red, también se debe entregar información de su geolocalización, tipo de dispositivo, IP, aplicación, región, modelo y sistema operativo.

Transacción. En este caso se debe identificar el punto de origen (presencial o virtual), el tipo de transacción (acumulación o redención), si es una transacción no monetaria como por ejemplo cambio de datos de la cuenta del cliente; el tipo de canal utilizado, la fecha, el valor y la hora de la transacción. En caso de que la transacción se realice desde la aplicación, como por ejemplo una transferencia de puntos, debe enviar la cuenta de origen y la cuenta de destino.

b) Motor de Riesgo

El motor de riesgo hace parte de una herramienta de monitoreo transaccional. Debe trabajar bajo modelos de machine learning, así mismo debe tener los siguientes componentes:

Consola y gestión de casos. Unifica los procesos de investigación de fraudes para gestionar las alertas de monitoreo transaccional y genera reportes detallados. Es importante para el control operativo de las alertas, y facilita la distribución de casos para los analistas de monitoreo.

Integrador de datos. Recibe la información de todas las tramas transaccionales y del Core del negocio, las cuales han sido previamente definidas según las necesidades del programa.

Análisis de comportamiento. Habilita la evaluación de atributos específicos a través de machine learning y decide qué tanta importancia tendrá cada uno. Especifica los tipos de actividad que serán evaluados por los analistas de seguridad. En este caso somos más efectivos, tenemos menos falsos positivos y evaluamos el riesgo de acuerdo con un aprendizaje continuo y no solamente basado en reglas.

Definición de reglas. Se tienen tres tipos de reglas. *Reglas de negocio*, que se define según su actividad comercial, los topes y la cantidad de transacciones. También tenemos *reglas duras*, que se definen según el apetito de riesgo, el comportamiento de los clientes y el nivel de riesgo. Por último, tenemos las *reglas de alertamiento*, que hacen referencia a las reglas generales que pueden tener un nivel de riesgo importante y necesitan un segundo análisis por parte de un funcionario del área de monitoreo.

c) Plataforma de autenticación

Debe estar basada en una autenticación multifactorial. Esta plataforma permite habilitar diferentes esquemas de autenticación para ser utilizados por medio de los canales del programa de fidelización, teniendo como principal insumo de decisión la matriz de autenticación y el riesgo transaccional.

A través de la herramienta de monitoreo, se gestiona el riesgo transaccional. Ahí, la matriz de autenticación permite determinar cuál sería el esquema a utilizar según la calificación del riesgo y conforme a las políticas internas preestablecidas.

Para poder definir una matriz de autenticación es fundamental tener en cuenta tres puntos vitales:

- Realizar una segmentación de clientes, según comportamiento, importancia para el programa y utilización de éste.
- Esquemas de autenticación, basados en la segmentación, canales y la experiencia que necesitamos dar al cliente bajo una integración deseada y sin fricción.

Capítulo 6.

Recomendaciones y Conclusiones

Este capítulo se abordará a partir de dos frentes. El primero de ellos desde el punto de vista interno de la compañía: ¿Cuál es el papel de los funcionarios en cada uno de los procesos? ¿Cómo medir los resultados? El segundo frente estará relacionado con lo externo: ¿Cómo se pueden generar esfuerzos entre compañías del sector para lograr sinergias? ¿Cómo, desde la capacitación y la analítica de datos, se podrían predecir en conjunto situaciones que generen valor para un ecosistema de empresas? Todo lo anterior partiendo del hecho de que el delincuente nunca es selectivo, él solamente aprovecha vulnerabilidades, sin importar de cuál empresa provengan.

Qué podemos realizar desde lo interno.

Experiencia

Esta propuesta define un modelo práctico y aplicable a la prevención y control de fraude transaccional en una empresa de lealtad o de fidelización. Una de las principales premisas de este modelo es que su planificación, definición y elaboración deben estar enfocados en el cliente, en propiciarle una excelente experiencia, en facilitarle los procesos, en entender su cotidianidad, su comportamiento. Es importante anticiparnos, a través de analítica avanzada, a cualquier riesgo transaccional, con el fin de generar un beneficio mutuo frente a situaciones de riesgo que se deben gestionar con base en la experiencia y el servicio que queremos llevar al cliente desde dos puntos de vista:

El primero, anticiparnos a los hechos para evitar el fraude. No puede haber una mejor experiencia. Para lograr esto, recomendamos el siguiente indicador:

- Cantidad de clientes con redención/cantidad de clientes con fraude *100. Este indicador permitirá retarnos y tener los menores casos posibles de fraude, además presenta una

relación directa frente a los clientes que están utilizando el programa. Lo ideal es que esté por debajo de los 0.05%.

El segundo, atender de forma rápida y eficiente, en los posible en menos de 24 horas, las situaciones de riesgo o reclamación que se presenten. Para esto deberá contarse con personas especializadas en el proceso, que manejen comunicaciones amigables y efectivas. Dichas personas deberán tener a su disposición y de manera permanente, todas las aplicaciones. Para lograr la permanencia del cliente en el programa, en muchos casos se hace necesario exonerar al cliente de su responsabilidad. Para tomar este tipo de decisiones se recomienda tener en cuenta dos indicadores:

- Porcentajes de favorabilidad en la respuesta (cantidad de casos reclamados con fraude/cantidad de casos con respuesta a favor del cliente * 100). Recomendable estar por encima del 96%.
- Cantidad de casos abiertos con incumplimiento de ANS (niveles de servicio). Se mide de acuerdo al tiempo prometido al cliente versus el tiempo real de respuesta.

Estrategia

El área de prevención y control de fraude transaccional debe realizar una buena planificación de sus objetivos frente al apetito de riesgo, la experiencia, la pérdida esperada y los indicadores de siniestralidad. Por tal razón, dichos objetivos tácticos deben estar alineados a la estrategia de la compañía, se deben definir las acciones tácticas que permitan ayudar al cumplimiento de los objetivos de la compañía y del área.

A medio y largo plazo, se debe planear la estrategia frente a la prevención del fraude transaccional, y plantarse cuáles serían los objetivos para evolucionar, aplicar tendencias, innovar y aportar de forma positiva al programa, buscando una sostenibilidad a largo plazo para beneficio de todos los grupos de interés.

Dentro de la estrategia de un programa de lealtad, cuyo propósito es el de mantenerse y permanecer en el tiempo, se deben eliminar las claves estáticas para autenticar o identificar al cliente. Es importante utilizar la tecnología y la inteligencia artificial a través de una analítica avanzada y una estructura de datos confiable.

Sinergia

Trabajar en equipo con diferentes áreas de la compañía y el apoyo de los grupos de interés, es indispensable para el logro de los objetivos.

Con Seguridad de la información y ciberseguridad. Esta es un área que genera un valor inmenso al área de prevención y control de fraude. El trabajo en equipo busca minimizar riesgos, identificar vulnerabilidades, fuga de información y garantizar la seguridad en el desarrollo de productos, proyectos, comunicaciones y canales seguros que disminuyan el riesgo transaccional. “Si no hay fuga de información no hay materialización de fraude”.

Con el área de experiencia debe existir una comunicación constante, buscando estar alineados en los indicadores y modelos de experiencia, en los niveles de servicio del cliente, aliados y socios.

Con los aliados, se deben generar estrategias de prevención, autenticación e identificación de clientes en las transacciones de redención y acumulación. Así mismo, es muy importante desarrollar acuerdos de recuperación de puntos cuando se presentan fraudes. Existe una responsabilidad y un beneficio mutuo en este tipo de riesgos.

Riesgos

Constantemente se debe mantener un flujo frente a la identificación, evaluación y control de los riesgos transaccionales. La materialización de los riesgos de fraude deriva a otros riesgos como el reputacional, el cual implica consecuencias negativas incalculables para un programa de fidelización.

Por los compromisos que se tienen con aliados y socios, este tipo riesgos vienen acompañadas de otros como los legales o contractuales.

Por otra parte, es fundamental determinar qué tipo de pólizas necesita el programa para compartir o trasladar parte del riesgo a una aseguradora. Entre las que se pueden considerar: pólizas de manejo, pólizas de infidelidad y riesgo financiero, y pólizas de riesgo cibernético.

Automatización

Es fundamental diseñar un modelo de atención de reclamos automatizado que permita entregar una solución a favor o en contra de la reclamación, con el solo hecho de suministrar al modelo los datos del cliente y los datos transacciones de su reclamación. Esto genera un valor importante porque podemos minimizar tiempos de respuesta, incluso, se puede lograr una respuesta inmediata desde el primer nivel. Este tipo de cambios generan eficiencias internas, al propiciar una buena experiencia que se traduzca en fidelización de los clientes.

También podemos mejorar los procesos de mensajes transaccionales con una comunicación rápida, concreta, directa y en doble vía, que mejorará no solo la experiencia, sino que también ayudará a prevenir una cantidad mayor en pérdidas, situación que beneficiaría la sostenibilidad del programa. A partir de estos mensajes, se toman acciones de forma inmediata y automatizada sobre la transacción y sobre la cuenta del cliente afectado.

Tecnología

La autenticación basada en riesgo permite tener un mejor control del fraude transaccional, mejorando considerablemente la fricción que puede generarse con el cliente. Es la empresa de lealtad quien toma la responsabilidad del análisis y asume las decisiones frente a la operación objeto de verificación.

De igual forma, permitirá tener una contingencia amplia para retar a un cliente en caso de existir una transacción riesgosa, sin la necesidad de negar dicha operación y ocasionar un mal servicio. Esto es posible gracias al envío de un doble factor de autenticación por medio de correo electrónico, vía voz, código QR, Push al celular o mensaje de WhatsApp. Estas acciones también permiten identificar a los clientes y segmentarlos.

Otra de las ventajas, es unir la información que suministra el dispositivo con la información de la transacción para definir una sola matriz y valorar el nivel de riesgo. Con esta acción, prácticamente unimos el mundo digital con el presencial, y lo monetario con lo no monetario. La disposición y manejo de la información, la tecnología y la metodología, llevan a mejorar la experiencia del cliente, que al final es lo más importante.

Qué podemos realizar desde lo externo.

Una vez fortalecidos los controles internos frente el riesgo transaccional, reputacional y de estrategia frente al fraude, –bajo un modelo que le permita de una manera ágil, fácil y eficiente gestionar el riesgo transaccional–, debemos fortalecer todo el ecosistema de compañías de lealtad, para que, a través una mutua colaboración, podamos anticiparnos de forma rápida a situaciones de riesgo que puedan generar una pérdida.

Así como un cliente tiene relaciones con varias entidades financieras y diversos establecimientos de comercio de manera paralela, también puede hacer parte de diferentes compañías de lealtad. Por ejemplo, una persona en Colombia puede estar afiliada al programa de lealtad de CMR puntos Falabella y al mismo tiempo pertenecer a los programas Lifemiles o Tuplus del grupo Aval.

Todas las compañías del sector de lealtad hacen esfuerzos importantes para proporcionar a sus clientes una buena educación en el manejo de sus productos, siendo la concientización el arma principal en la prevención de riesgos. Hoy en día, muchas personas realizan un manejo inadecuado de sus usuarios y claves personales, asignando las mismas a diferentes servicios. Esta situación puede generar riesgos mayores, por ejemplo, un fraude en cadena. El hecho de que haya una vulneración a las claves a través de la ingeniería social que se le practica a un cliente, afecta a todas las compañías en conjunto.

De la misma manera que un ciberdelincuente detecta vulnerabilidades en una persona, puede hacerlo a nivel de compañía. Esos hallazgos son explotados para materializar sus fraudes y, posteriormente, utilizarlos de modus operandi en otras compañías. Esto nos lleva a reflexionar sobre la siguiente hipótesis: ¿Sería conveniente tener un sistema de información transversal entre

compañías de lealtad en Colombia, que permita valorar de manera cuantitativa los riesgos de fraude?

Frente a esta hipótesis encontramos que a nivel mundial existen empresas que se han constituido para generar apoyos mutuos en el sector. En Europa, por ejemplo, encontramos asociaciones como la Loyalty Fraud Prevention Association (LFPA) – Asociación de prevención del fraude de lealtad–, empresa que nación en el año 2016 en Glasgow, Escocia, con el objetivo de apoyar a la industria de lealtad en su lucha contra el fraude transaccional, entre ellos el robo de sus puntos y millas de los programas de fidelización en todo el mundo. (Loyalty Fraud, s.f.).

Desde el punto de vista local, observamos asociaciones que nacieron con el propósito de unificar esfuerzos no sólo desde la lucha contra el fraude sino desde otro tipo de frentes. Estamos hablando de Asobancaria, gremio que representa el sector financiero en Colombia, fundada en el año 1936. Una de las funciones de esta asociación es la prevención del fraude, facilitando un intercambio de información entre las entidades financieras, realizando diferentes comités enfocados en trasmitir experiencias en la prevención del fraude financiero. Así mismo, existe una cooperación muy importante en temas educativos hacia sus clientes y el sector. Constantemente se están desarrollando seminarios para la prevención y control del fraude.

También existen gremios en el sector asegurador, como la Federación de Aseguradores Colombianos (Fasecolda), fundada en 1976. Empresa que también tiene dentro de sus objetivos la prevención y control del fraude. Para ese fin, en el año 2016 se creó la Dirección de Gestión Institucional contra el Fraude, cuyo objetivo era el de “unir al sector a través del conocimiento del fenómeno, la interacción con las autoridades y la construcción de herramientas para el análisis conjunto del fenómeno” (Fasecolda, s.f.). Desde su creación, esta dirección ha generado excelentes resultados en el sector asegurador.

Con base en lo anterior, es posible generar una asociación, entre las compañías de lealtad, que esté enfocada en la prevención y control de fraude. Asociación a la que se podrían unir empresas colombianas como Puntos Cencosud, Latam Pass, Lifemiles, Leal, Puntos Colombia, CMR puntos Falabella, Tuplús, Davipuntos, Puntos BBVA y mi Itaú, entre otros, buscando los siguientes objetivos:

1. Diseñar herramientas que nos permitan compartir información cumpliendo con la ley de protección de datos, para que a través de analítica avanzada y machine learning se logren detectar patrones de fraude en todo el ecosistema, que permitan la anticipación y eviten la materialización del fraude.
2. Identificar y gestionar información de otros ecosistemas en el mundo para detectar comportamientos de fraudes emergentes.
3. Incentivar, a través de Hackathones, la identificación de brechas de seguridad y vulnerabilidades en cada uno de los asociados, generando recompensas a los hallazgos, con el fin de solucionarlos antes de su materialización.
4. Consolidar un programa de conciencia con todos los asociados que incluya capacitaciones desde todos los frentes, por ejemplo: comportamientos, tendencias, analítica, riesgos, estratégica, prevención, monitoreo, etc.
5. Desarrollar una plataforma interactiva para el cambio de experiencias, frente a situaciones ya presentadas, y que puedan generar una anticipación para otra compañía, es decir, aprender de lo ya vivido.
6. Desarrollar anualmente congresos, talleres o conferencias entre los funcionarios de cada una de las organizaciones asociadas con el objetivo de discutir y analizar comportamientos y tendencias de fraude.
7. Buscar alianzas con organismo de seguridad del estado, con el propósito de encaminar esfuerzos contra los grupos organizados que están afectando el ecosistema, en este caso, Fiscalía, policía judicial, grupo de delitos informáticos, CTI, etc.

Bibliografía

ACFE - The Institute of Internal Auditors (s.f.). Managing the business. Risk of fraud: A Practical Guide Sponsored by, the institute of internal Auditors, The American Institute of certified public accountants y association of certified fraud Examines. Recuperado de https://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf.

AppGate, SMG Information Security 2021. La encuesta Faces of Fraud 2021, documento de 39 paginas.

Asobancaria (s.f.). Iniciativas, seguridad, por una red segura. Recuperado de https://www.asobancaria.com

Akamai, 20 octubre 2020. Fidelidad a la venta: el fraude en los sectores de retail y hostelería, estado de internet / seguridad, volumen 6, número 3. Recuperado de https://www.akamai.com/content/dam/site/es/documents/state-of-the-internet/soti-security-loyalty-for-sale-retail-and-hospitality-fraud-executive-summary-2020.pdf

Banco Santander España (2018). ¿Qué es la fuga de información? Blog. Preguntas frecuentes. Glosario. Recuperado de https://www.bancosantander.es/glosario/fuga-datos

Blog Usetada (s.f.). Las últimas investigaciones sobre la construcción de la lealtad del cliente y las relaciones sólidas con el cliente. Recuperado de https://blog.usetada.com/latest-research-on-building-customer-loyalty-and-strong-customer-relationships

Bondbrandloyalty (2020). El estado de la lealtad: un lago de datos que vale la pena explorar. Recuperado de https://www.bondbrandloyalty.com/stateofloyalty/index.html#download-popup

Concepto.de (2019). Empresas. Recuperado dehttps://concepto.de/empresa/#ixzz6rkxbyR4b

COSO - Committee of Sponsoring Organizations of the Treadway. Llamado “Fraud Risk Management Guide”

Comarch, CRM&MARKETING (s.f). Everything you need to know about Loyalty fraud.

Douglas da Silva (09 de septiembre de 2021). Lealtad de marca: 4 niveles para cultivar en tu empresa. Web Content & SEO Associate, LATAM. Recuperado de https://www.zendesk.com.mx/blog/lealtad-de-marca/

EasySol (s.f.). Webinar – Equilibrio entre seguridad y experiencia de usuario autenticación basada en riesgo, Cyxtera. Recuperado de https://www.easysol.net/images/stories/Products/WebinarAutenticacionBasadaRiesgo.php.

EMIS (2021). Leal Colombia SAS. Recuperado de https://www.emis.com/php/company-profile/CO/Leal_Colombia_S_A_S_es_4937516.html

Estrategias y Negocios – E&N (24 de julio de 2015). Lifemiles cuesta casi lo que vale Avianca en bolsa. Recuperado de https://www.estrategiaynegocios.net/inicio/862199-330/lifemiles-cuesta-casi-lo-que-vale-avianca-en-bolsa

Evadian, 7 métodos de autenticación más utilizados, Recuperado de https://www.evidian.com/pdf/wp-strongauth-es.pdf.

Federación de Aseguradores Colombiano – Fasecolda (2016). Gestión Institucional contra el Fraude. Recuperado de https://fasecolda.com/fasecolda/gestion-contra-el-fraude/ Portafolio (26 de abril de 2018). LifeMiles logra duplicar su crecimiento en Colombia. Recuperado de https://www.portafolio.co/economia/lifemiles-logra-duplicar-su-crecimiento-en-colombia-516611

FMK, ForoMarketing. (03 de mayo de 2016). Tipos de clientes y sus características. ¿Cómo calificarlos? Recuperado de https://www.foromarketing.com/tipos-de-clientes-y-sus-caracteristicas/

Gómez, J. (2020). La pirámide de fidelización: cómo medir la lealtad de los clientes. *Spoonity*. Recuperado de https://www.spoonity.com/es/piramide-de-fidelizacion/

Growjo (s.f.). Competidores y alternativas de fidelización de néctar. Recuperado de https://growjo.com/company/Nectar_Loyalty

Harán, Juan Manuel (2 de diciembre de 2020). 29 datos que deja el 2020 que hablan del estado actual de la ciberseguridad. WeliveSecurity. Recuperado de https://www.welivesecurity.com/la-es/2020/12/22/datos-2020-sobre-estado-actual-ciberseguridad/

Hubspot (s,f.) Pasos para armar el programa de FIDELIDAD PERFECTO. Marketing. Recuperado de https://cdn2.hubspot.net/hubfs/1739765/Sin%20uso/PDF/e-book-Programa-de-fidelidad-perfecto.pdf

Inloyalty (2020). Soluciones de fidelización eficaces y a la medida de tus objetivos. Recuperado de https://inloyalty.es/publicaciones-completo?categoria=11

Inloyalty (23 enero 2018). El éxito ne los programas de fidelización en coalición, https://inloyalty.es/publicaciones/2018/01/23/exito-los-programas-fidelizacion-coalicion

ISO Guía CEI 73(2009) Vocabulario Gestión de Riesgo Vigente. Disponible en https://www.academia.edu/39673881/ISO_Gu%C3%ADa_73_2009_VOCABULARIO_GESTI%C3%93N_RIESGO_VIGENTE

KPMG (2019). La verdad sobre la lealtad del cliente. Recuperado de https://assets.kpmg/content/dam/kpmg/ec/pdf/2019/12/customer-loyalty-report.pdf

La W Radio (02 de septiembre de 2020). ¿Se puede calcular el valor del programa LifeMiles de Avianca? Recuperado de https://www.wradio.com.co/noticias/internacional/se-puede-calcular-el-valor-del-programa-lifemiles-de-avianca/20200902/nota/4067178.aspx

Latam Kaspersky (2020). Ingeniería Social: Definición. Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Loyalty Fraud (s.f.). Se lanza la asociación de prevención de fraudes por lealtad a medida que el fraude por fidelidad sigue creciendo. Recuperado de https://www.rewardco.com.au/loyalty-fraud-prevention-association-launches-as-loyalty-fraud-continues-to-grow/

Loyalty Magazine (08 de junio 2021). El negocio del lujo descubre la importancia de la fidelización de los clientes. Recuperado de https://www.loyaltymagazine.com/all-articles/page/2/

Mayr Ojeda, Franz; Patrone Martirena, Franco; Persitz Cohen, Herman Andrés; Sanguinetti Kinrus, Javier; Visca Zanoni, Ramiro Eugenio. (2017). Autenticación pasiva y continúa basada en el comportamiento. Universidad ORT Uruguay. Facultad de Ingeniería, p. 224. Recuperado de https://dspace.ort.edu.uy/handle/20.500.11968/3930

Microtech (16 febrero 2021). ¿Por qué retener clientes es más importante que obtener nuevos clientes?, recuperado de https://www.microtech.es/blog/por-qué-retener-clientes-es-más-importante-que-obtener-nuevos-clientes.

Oficina de Seguridad del Internauta – OSI. (27 de febrero del 2019). Factor de autenticación doble y múltiple. Actualidad. Recuperado de https://www.osi.es/es/actualidad/blog/2019/02/27/el-factor-de-autenticacion-doble-y-multipler

OneSpan (2020). Autenticación basada en riesgos. Recuperado de https://www.onespan.com/es/topics/autenticacion-basada-en-riesgo-rba

PaymenstJournal (abril 14, 2020), Daniel Shkedi. Loyalty program fraud is a Growing problem. Forter is Here to help. Recuperado de https://www.paymentsjournal.com/loyalty-program-fraud-is-a-growing-problem-forter-is-here-to-help/.

Peña. E. S., Ramírez, R. G. y Osorio, G. J. (2014). Evaluación de una estrategia de fidelización de clientes con dinámica de sistemas. Revista Ingenierías Universidad de Medellín. Recuperado de http://www.scielo.org.co/pdf/rium/v14n26/v14n26a07.pdf

Revista Portafolio (28 de febrero de 2020). Prevenir el fraude sin afectar la experiencia del cliente es posible. Recuperado de https://www.portafolio.co/opinion/otros-columnistas-1/prevenir-el-fraude-sin-afectar-la-experiencia-del-cliente-es-posible-538578.

Rewards, B. (15 de octubre de 2019). Más allá de las recompensas: elevar el listón de la lealtad del cliente. Recuperado de https://hbr.org/sponsored/2019/10/beyond-rewards-raising-the-bar-on-customer-loyalty

Rodrigo Camacho, 2019. Nothone, LFPA Spring conference, Loyalty fraud.

Sanson, Miguel (2009). ISO Guía 73:2009 VOCABULARIO GESTIÓN RIESGO VIGENTE. Recuperado de https://www.academia.edu/39673881/ISO_Gu%C3%ADa_73_2009_VOCABULARIO_GESTI%C3%93N_RIESGO_VIGENTE

Sebastián Bortnik (13 de abril de 2010). ¿Qué es la fuga de información?WeliveSecurity. Recuperado de https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

Semana (29 de septiembre de 2020). Rappi y LifeMiles, entre los "unicornios" más grandes del mundo. Recuperado de https://www.semana.com/empresas/articulo/rappi-y-lifemiles-entraron-a-la-lista-de-los-unicornios-mas-grandes-del-mundo/301172/

Semana. (08 de abril de 2019). Sumando puntos de fidelización, la ‘startup’ Leal atrae US$3 millones. Recuperado de https://www.semana.com/emprendimiento/articulo/historia-de-leal-startup-de-programa-de-fidelizacion/269443/

Spoonity, Torio J. M. (s.f.). Cómo aumentar la rentabilidad de tu negocio con un programa de lealtad. Spoonity. Recuperado de https://www.spoonity.com/es/aumentar-rentabilidad-negocio-programa-lealtad/

TransUnión (s.f.). Autenticaciones basadas en dispositivo Clearkey Recuperado de https://www.iovation.com/authentication/clearkey.

Valora Analitik (31 de julio de 2020). Calificación de LifeMiles, programa de viajero frecuente de Avianca. Recuperado de https://www.valoraanalitik.com/2020/07/31/s-p-confirma-calificaci-n-de-lifemiles-programa-de-viajero-frecuente-de-avianca/

Villalobos, Carlos (2021). ¿Qué son los programas de fidelización y por qué debes apostar por ellos? Blog HubsPot. Recuperado de https://blog.hubspot.es/service/que-son-los-programas-de-fidelizacion

Yazztas (S.F.). Los programas de lealtad para los clientes han sido menospreciados por la prensa empresarial por creerlos programas promocionales baratos, modas pasajeras, sin valor real que dan generalmente algo a cambio de nada, en el mejor de los casos. Recuperado de https://yazztas.com/es-verdad-que-los-programas-de-lealtad-generan-mas-valor-para-los-negocios.

Tecnoredes, blog (02 diciembre 2020). Ciberseguridad tecnológica, servicio completo, https://www.tecnoredes.net.co/ciberseguridad-tecnologica-servicio-completo/.

Universidad Javieriana, Jenith E. Linares, (s.f.), Control interno en la prevención y detección de fraude corporativo, https://www.javeriana.edu.co/personales/hbermude/Audire/jelg2.pdf.

Clubensayo, Beida Naomi Machuza, (02 diciebre 2019), Control internos de las organizaciones, pagina 1, https://www.clubensayos.com/Negocios/EL-FRAUDE/4911112.html.

ACFE, recursos contra el fraude, (s.f.), https://acfe-spain.com/recursos-contra-fraude/que-es-el-fraude.

Fraude interno, wordpress, (09 febrero 2016), prevención y detección del fraude interno para cualquier tipo de empresa, el triangulo del fraude, https://fraudeinterno.wordpress.com/2016/02/09/el-triangulo-del-fraude/.

Norton, centro de seguridad, amenazas emergentes, (s.f), https://cl.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html.

Universidad Nebrija, salón de actos, (14 noviembre 2019), inteligencia artificial, https://actos.nebrija.es/42454/detail/la-inteligencia-artificial-entra-en-el-aula.html

SAS, aprendizaje automático, (s.f.), https://www.sas.com/es_co/insights/analytics/machine-learning.html

Definición.de, Julián Pérez y Ana Gardey, (2008, actualizado 2021), https://definicion.de/procedimiento/

SAS, análisis, (s.f.), que es la analítica, https://www.sas.com/es_co/insights/analytics/what-is-analytics.html

Rockcontent, blog, programas de lealtad, (21 junio 2019), https://rockcontent.com/es/blog/programas-de-lealtad/

Escualapce, exámenes, examen resultado de economía de la empresa pce, (s.f), https://escuelapce.com/economia/

Gestión, tecnología, (mayo, 2017) ¿cómo se realiza el fraude relacionado con la fidelidad de las aerolíneas?, https://gestion.pe/tecnologia/realiza-fraude-relacionado-fidelidad-aerolineas-134513-noticia/

Ebizlatam, Ernesto Haikewitsch, (01 junio 2017), el fraude relacionado con los puntos de fidelidad de las aerolíneas a menudo vuela bajo el radar, http://www.ebizlatam.com/fraude-relacionado-los-puntos-fidelidad-las-aerolineas-menudo-vuela-radar/