Comportamiento de los sistemas de pagos en México: una perspectiva de detección de fraudes

Álvaro Mendoza Candia

Resumen

Actualmente, con el crecimiento de la tecnología y de los sistemas electrónicos de transferencia de información se ha revolucionado la forma en que se utiliza el dinero; esto ha llevado a que las empresas, gobiernos y sociedad en general, migren de los sistemas tradicionales de pago hacia los electrónicos donde la seguridad es parte indispensable para que las transacciones de dinero puedan efectuarse de la manera más ágil y correcta.

Uno de los principales riesgos para las instituciones bancarias y financieras es el fraude, ya que ocasiona pérdidas económicas y compromete los datos y la privacidad de los usuarios siendo uno de los delitos más frecuentes y que más profundamente daña a las empresas y a los individuos.

Se describe cómo se han venido comportando los principales sistemas de pagos a cargo del Banco de México: SPEI, SIAC, DALI y CoDi, así como los fraudes más comunes que existen y los diferentes métodos y técnicas utilizados para su detección.

Palabras clave:
Clasificación JEL:

Introducción

El dinero es una palabra que suele referirse a muchas cosas. La podemos emplear como sinónimos de renta y riqueza. Sin embargo, el dinero es un activo financiero que puede utilizarse directamente para comprar bienes y generalmente es aceptado como medio de pago por los agentes económicos para sus intercambios.

El dinero se clasifica de acuerdo con las funciones que tiene en la economía, las cuales son:

- Reserva de valor, esto indica que las personas pueden ahorrarlo y usarlo más adelante, diversificando sus compras a través del tiempo.
- Unidad de cuenta, sirviendo como una base común para los precios.
- Medio de pago, algo que las personas pueden usar para comprar y vender entre sí.

La última función, ha dado al dinero facilidad en muchas de las transacciones hechas por los agentes económicos, ya que como medio de pago sustituyó, en primera instancia al trueque (como forma de intercambio), y después, a los metales como el oro y plata, que fueron acuñándose como monedas (dinero-mercancía). Sin embargo, el utilizar el oro como dinero, tenía algunas dificultades, por ejemplo resultaba muy incómodo y delicado llevarlo consigo, ya que era molesto transportar cientos de onzas de oro, además de que resultaba muy costoso. Sumado a ello, el creciente número de personas dedicados a la acuñación y sin la experiencia debida, tuvo como consecuencia un aumento en el número de falsificaciones, incidiendo en la seguridad del comercio y en la propia credibilidad de la moneda (Guerra, 1997). Como resultado, fueron creándose leyes que suponían una reestructuración de todos los aspectos relacionados con la moneda y su fabricación al tiempo que aportó un endurecimiento de la política general en esta materia.

Existió otro problema al momento de determinar el valor de una moneda, ya que a mayor valor, más rentable resulta falsificarlo. Un ejemplo es cuando una persona cuenta con dos monedas de igual valor, ambos son indistinguibles. Pero por alguna razón, la persona sabe

que uno de ellos es falso. Esto llevaba a considerar que la gente prefería pagar con la moneda mala y ahorrar la buena (Ley de Gresham), lo que desencadenó una inflación inminente y una devaluación constante.

Al paso de tiempo, fueron apareciendo otros problemas relacionados con la falsificación del dinero, uno de ellos era el relacionado a la creación de dinero, ya que a través del surgimiento de los primeros bancos comerciales, donde se realizaban operaciones de cambio y crédito, poco a poco también fueron depositantes de dinero, creando nuevas funciones como el girar cheques para que los comerciantes pudieran pagar sus compras. Sin embargo, la emisión de cheques falsos, provocaba también inflación.

Ante la necesidad de controlar y vigilar la emisión de dinero en la economía, fueron apareciendo los primeros bancos centrales, instituciones que además de contar con dicha función, actuaron como prestamistas de última instancia, cámara de compensación, custodio de reservas, generador de políticas anticíclicas y encargado de los tipos de cambio (Vera, 1995). Más adelante profundizaremos en sus principales funciones, la cual nos centraremos en la supervisión de los sistemas de pago.

Con el crecimiento de la tecnología y de los sistemas electrónicos de transferencia de información se ha revolucionado la forma en que actualmente se utiliza el dinero. La idea del dinero electrónico no es particularmente nueva. Durante décadas, millones de dólares en comercio y transacciones bancarias se han movido electrónicamente. Las tarjetas de crédito y los cajeros automáticos han sido parte importante de la vida diaria de las personas (Levy, 1995). Esto ha llevado a que las empresas, gobiernos y sociedad en general, migren de los sistemas tradicionales de pago hacia los electrónicos. Además de que los agentes económicos buscan alcanzar altos niveles de eficiencia y competitividad, reduciendo sus costos y aumentando sus utilidades, la seguridad también es parte indispensable para que las transacciones de dinero puedan efectuarse de la manera más ágil y correcta.

Ante una marcada digitalización y automatización de las operaciones digitales, existen riesgos que pueden debilitar la estabilidad de las instituciones financieras y de los mercados. Los sistemas de pagos pueden evaluarse según sus riesgos, fiabilidad y costos de transacción (Baliño & Sundarajan, 1996). Uno de los principales riesgos para las instituciones bancarias y financieras es el fraude, ya que ocasiona pérdidas económicas, de imagen y una desconfianza creciente de los clientes, causando un mal funcionamiento de los sistemas de pagos, además de que son comprometidos los datos y la privacidad de los usuarios, que pueden tardar hasta 100 días en saber si fueron víctimas de fraude (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, 2018). Otro estudio señala que, en 2016 más de la mitad de los fraudes tomaron 15 meses en ser detectados (KPMG, 2020).

De todo lo anterior, podemos decir que, el fraude sigue siendo uno de los delitos más frecuentes y que más profundamente daña a las empresas y a los individuos. Asegurar la eficiencia y confianza de los sistemas de pagos, garantizará una estabilidad financiera. Por ello, es importante proveer de vehículos e instrumentos a los usuarios para que realicen sus transacciones de manera fácil y segura.

Como marco teórico analizaremos el modelo de balance de datos que se clasifica como una técnica de preprocesamiento de datos en la detección de fraudes, ya que equilibra la distribución de clases en los conjuntos de datos desequilibrados, lo que puede mejorar la precisión del modelo y reducir el sesgo hacia la clase mayoritaria.

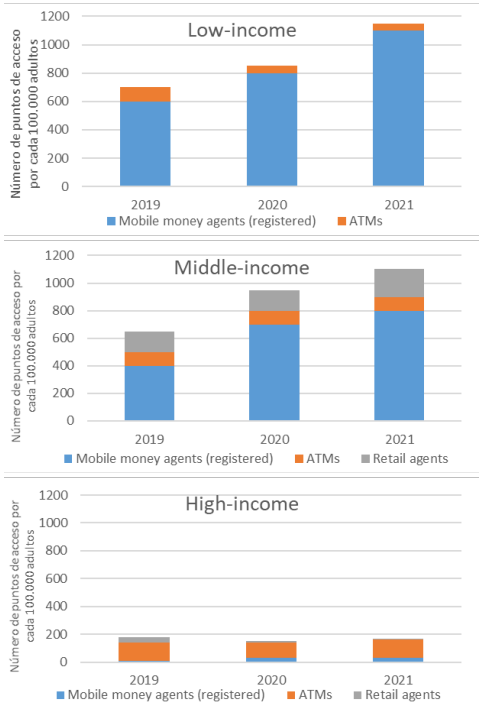
Este ensayo se divide en cinco partes, en el primer capítulo abordaremos el marco teórico que da sustento al funcionamiento de los sistemas de pagos. En el segundo definiremos el marco legal y operacional del banco central, que es el órgano que tiene por mandato regular dar supervisión al sistema de pagos. En el capítulo tres describiremos como se han venido comportando los principales sistemas de pagos a cargo del Banco de México: SPEI, SIAC, DALI y CoDi, para después, abordar en el último capítulo los fraudes más comunes que existen, así como los diferentes métodos y técnicas que actualmente se utilizan para su

detección, aplicando una aproximación de un caso teórico-práctico de un sistema de detección de fraudes. Al final, daremos las conclusiones a las que llegamos en este trabajo para poder tener un mejor enfoque en el que se pueda contar con una estrategia para prevenir, detectar y dar respuesta a los delitos financieros, específicamente, a los cibernéticos.

1. Los Sistemas de Pagos

Derivado de la pandemia mundial causado por el virus COVID-19, los medios de pago electrónicos han cobrado una mayor relevancia. Según datos de la Financial Access Survey 2022 del Fondo Monetario Internacional, el número de puntos de acceso tradicionales, como sucursales bancarias, ha disminuido, mientras que los modos digitales no tradicionales de acceso financiero, particularmente dinero electrónico en economías en desarrollo, han crecido significativamente desde el inicio de la pandemia (Fondo Monetario Internacional, 2022).

Gráfica 1. Nuevas formas de acceso a la financiación



Fuente: Elaboración propia con datos del Fondo Monetario Internacional, 2022.

En la anterior gráfica se observa una mayor adopción de las finanzas digitales sobre cuentas de dinero electrónico, especialmente en países de bajos ingresos donde la aceptación del dinero vía móvil es mayor. En estos países, el número de cuentas de dinero electrónico por cada 1,000 adultos ha crecido en un 30% entre 2019 y 2021, mientras que el número de cuentas de depósito se mantuvo prácticamente sin cambios. Esto reafirma la importancia del dinero vía móvil durante la pandemia, ya que ha aumentado dado el mínimo físico contacto permitido durante los confinamientos y los altos niveles de penetración de dinero electrónico entre las poblaciones no bancarizadas.

Muchas de las transacciones que se realizaban con dinero físico, se sustituyeron por herramientas como las transferencias, banca electrónica, plataformas de pago por internet o celular y el *e-commerce* (comercio en línea).

El comercio en línea, en su sentido más amplio, realiza operaciones comerciales de bienes y servicios basadas en el uso de sistemas de cómputo y en la tecnología de telecomunicaciones, con el fin de agilizar las transacciones entre los integrantes de una cadena de distribución y así, reducir los costos de transferencia del productor al consumidor final (Tavera, 1998).

Siguiendo esta línea de evolución tecnológica, en la actualidad, se ha desarrollado una industria en la que las empresas brindan servicios financieros de manera eficiente, ágil, cómoda y confiable, un ejemplo son las FINTECH (financieras tecnológicas), que no son más que intermediarios entre los bancos y los clientes, y que, en México, han adquirido relevancia dentro de los siguientes sectores:

Tabla 1. Principales funciones de las FINTECH

Medios de pago y transferencias.	Las plataformas de pagos, comercio electrónico y transferencias internacionales.
Infraestructura para servicios financieros.	Evaluación de clientes y perfiles de riesgo, prevención de fraudes, verificación de identidades, APIs bancarias, agregados de medios de pago, big data & analytics, inteligencia de negocios, ciberseguridad y contratación electrónica.
Originación digital de créditos.	Son empresas que ofrecen productos de crédito a través de plataformas electrónicas.
Soluciones financieras para empresas.	Software para contabilidad e infraestructuras de facturación y gestión financiera.
Finanzas personales y asesoría financiera.	Administración de Finanzas personales, comparadores y distribuidores de productos financieros, educación financiera, asesores automatizados y planeación financiera.
Mercados financieros.	Servicios digitales de intermediación de valores, instrumentos financieros y divisas.
Crowdfunding.	Modelo de formación de capital y participación de mercado, en donde las necesidades de financiamiento de proyectos se transmite a una comunidad a través de una plataforma digital y se obtiene apoyo a inversionistas, fondeadores y donantes.
InsurTech.	Tecnología aplicada a la prestación de servicios en el sector asegurador.
Criptomonedas y blockchain.	Desarrolladores de soluciones basadas en el blockchain, intermediarios y mercados de activos digitales.
Entidades financieras disruptivas.	Bancos u otras entidades financieras 100% digitales.

Fuente: Elaboración propia con información de fintechmexico, 2022.

En conclusión, podemos decir que con el uso de la tecnología se traduce un ahorro de costos ya que se cuentan con funciones más automatizadas, permitiendo tener una plantilla reducida. Otra de las entidades financieras que ofrecen servicios de intermediación bancaria de manera 100% digital son los llamados “neobancos”, que se han podido extender rápidamente gracias a sus bajos costos de estructura y su capacidad para crecer con la ayuda de la tecnología. Brindan información actualizada y precisa en tiempo real, atienden vía “online” y están entre los principales interesados en el desarrollo de la inteligencia artificial.

Ante este rápido incremento e incorporación de los intermediarios financieros digitales a la red de sistemas de pagos, es necesario que, no solamente la eficiencia, sino la seguridad de las transacciones que realicen los usuarios a través de estos medios de pago electrónicos, genere confianza y credibilidad en las instituciones encargadas de supervisar y realizar dichas operaciones, estamos hablando de los bancos centrales.

Los sistemas de pagos seguros y eficientes son vitales para que el sistema financiero funcione con efectividad, estos son los medios a través de los cuales se transfieren los fondos entre los bancos. Además, los sistemas de pago son fundamentales para mantener y promover la estabilidad financiera (Banco de Pagos Internacionales, 1998). Podemos decir que, mientras el dinero es la sangre de la economía, los sistemas de pagos son el sistema vascular.

En términos generales, un sistema de pagos es una serie de instrumentos, procedimientos bancarios y sistemas interbancarios de transferencia de fondos que aseguran la circulación del dinero (Banco de México, 2022). Los sistemas de pago se clasifican por el monto de las operaciones que liquidan, las cuales se dividen en dos grupos: los de alto valor (de importancia sistémica) y los de bajo valor (al menudeo). También pueden clasificarse de acuerdo al tipo de liquidación que realizan o a la prontitud con la que la llevan a cabo (pago rápido).

En el 2002, se publica en México la Ley del Sistema de Pagos de México, que tiene por objeto propiciar el buen funcionamiento de los sistemas de pagos que la propia Ley señala, al establecer, para los efectos previstos en este ordenamiento, el carácter definitivo e irrevocable de las órdenes de transferencia y de la compensación y liquidación derivados de éstas, que se procesen a través de dichos sistemas, incluyendo los relacionados con operaciones con valores. Según el artículo 3° de la Ley de Sistemas de Pagos, existen dos requisitos para que sean considerados como sistemas:

1. Que participen, directa o indirectamente, al menos tres sociedades autorizadas para actuar como instituciones financieras conforme a las leyes aplicables, y
2. Que el monto promedio mensual de las obligaciones de pago que acepte el acuerdo o procedimiento de que se trate para su compensación o liquidación en un año calendario, sea igual o mayor al equivalente a cien mil millones de unidades de inversión.

En México, la Ley de Sistemas de Pagos da una base legal firme a los sistemas de pago sistémicamente importantes, y le da facultades más específicas al banco central para regular estos sistemas. Esta ley establece las características para que un sistema de pagos sea reconocido como sistémicamente importante y, por ende, sujeto a dicha ley. Por otra parte, existe una ley complementaria que le da facultades al banco central para regular los servicios y medios de pago que proporcionan los bancos a su clientela y las tarifas que los bancos se cobran entre sí, la cual es la Ley para la Transparencia y el Ordenamiento de los Servicios Financieros.

Es importante recalcar que, para cualquier Sistema de Pagos, su funcionamiento deberá estar sujeto principalmente a su eficiencia y seguridad, así como al desarrollo competitivo de los servicios que se presten. Sin embargo, no todos los medios y canales son igualmente eficientes, si se tienen en cuenta los recursos humanos y materiales involucrados.

1.1 Principios de los Sistemas de Pago

Los sistemas de pagos de importancia sistémica son los más importantes, ya que a través de ellos se pueden transmitir los impactos entre los sistemas y mercados financieros internacionales y nacionales. Los sistemas diseñados deficientemente pueden contribuir a crisis sistémicas si los riesgos no se contienen adecuadamente, con la consecuencia de que los impactos financieros se transmitan de un participante a otro. Los efectos de tales interrupciones podrían extenderse más allá del sistema y sus participantes, amenazando la estabilidad de los mercados de dinero y de otros mercados financieros nacionales e internacionales. Es por ello, que los sistemas de pago sistémicamente importantes son en consecuencia cruciales para la economía, y la política pública debe tomar como objetivos su seguridad y eficiencia.

En 2001, se adoptaron los “Principios Básicos para los Sistemas de Pago Sistemáticamente Importantes” del Comité de Sistemas de Pago y Liquidación de los Gobernadores de los

Bancos Centrales del G-10 (Banco de Pagos Internacionales, 1998), el cual tuvo el objeto de considerar qué principios deberían regir el diseño y funcionamiento de los sistemas de pago en todos los países. Estos principios funcionan como pautas universales para la operación de los sistemas de pago sistemáticamente importantes, dando énfasis en la seguridad y eficiencia en todo el mundo. Todos los sistemas de pagos sistemáticamente importantes deben cumplir con 10 principios, los cuales extienden las Normas Lamfalussy[1] agregándoles varios principios nuevos que se aplican ampliamente a todo tipo de sistemas importantes a nivel sistémico.

Esquema 1. Cronología de los principios universales para la operación de los SPSI

Fuente: Elaboración propia con información de Principios Básicos para los Sistemas de Pago Sistemáticamente Importantes del BIS 2001 y Diario Oficial de la Federación 2002.

Los Sistemas de Pago Sistemáticamente Importantes se refiere a los sistemas que podrían producir o transmitir interrupciones sistémicas en el área financiera debido al tamaño o naturaleza de los pagos procesados. Un sistema sistemáticamente importante no necesariamente maneja sólo pagos de grandes volúmenes; el término puede incluir a un sistema que administre pagos de varios v7olúmenes, pero que tenga la capacidad de producir o transmitir interrupciones por virtud de ciertos segmentos de su tráfico. Los sistemas de pago sistemáticamente importantes pueden estar en manos y ser operados por los bancos centrales o por instituciones del sector privado. También hay casos donde los mismos son propiedad o son operados conjuntamente por organismos públicos y privados.

[1] El nombre del informe se deriva del economista de origen húngaro Alexandre Lamfalussy, el cual analizó temas que afectaban a los esquemas de neteo de monedas múltiples e internacionales, dejando plasmado en el informe, normas mínimas y metas más generales para el diseño y operación de los sistemas de liquidación, compensación y pago.

Los principios básicos pretenden ser de relevancia para todas las estructuras de titularidad e institucionalidad. Dichos principios se dirigen al diseño y operaciones de los sistemas de pago, pero también tienden a influir sobre las acciones de los participantes y los organismos que supervisan a dichos participantes. A continuación, abordaremos los Principios básicos establecidos por el Banco de Pagos Internacionales:

Tabla 2. Principios básicos

Principio	Descripción
I	El sistema deberá contar con una base legal bien fundada en todas las jurisdicciones relevantes.
II	Las normas y procedimientos del sistema deben permitir a los participantes comprender claramente el impacto en el sistema de cada uno de los riesgos financieros en los que incurren a través de su participación.
III	El sistema debe contar con procedimientos claramente definidos sobre la administración de riesgos crediticios y riesgos de liquidez, los cuales especifican las respectivas responsabilidades del operador del sistema y de los participantes, y brindan los incentivos apropiados para administrar y contener los riesgos.
IV	El sistema deberá ofrecer una liquidación final puntual en la fecha de valor, preferentemente durante el día y como mínimo al final de la jornada.
V	Aquel sistema donde se produzcan neteos multilaterales deberá, por lo menos, ser capaz de asegurar la finalización puntual de las liquidaciones diarias en el caso de que un participante con la obligación de liquidación más grande no pueda cumplirla.
VI	Los activos utilizados para la liquidación deberán preferentemente constituir un pasivo del banco central; donde se utilicen otros activos, los mismos no deberán implicar ningún riesgo de crédito, o uno muy pequeño.
VII	El sistema deberá asegurar un alto grado de seguridad y confiabilidad operativa y deberá contar con convenios de contingencia para completar puntualmente el procesamiento diario.
VIII	El sistema deberá ofrecer un medio para efectuar los pagos, que sea práctico para sus usuarios y eficiente para la economía.
IX	El sistema deberá tener criterios objetivos y de conocimiento público para la participación, que permitan un acceso justo y abierto.
X	Los acuerdos acerca de la forma de gobierno del sistema deben ser efectivos, responsables y transparentes.

Fuente: Elaboración propia con información de Principios Básicos para los Sistemas de Pago Sistemáticamente Importantes del BIS 2001.

Aunque los principios se expresan en términos de los sistemas de pago en un solo país, los mismos son igualmente aplicables en los casos en que los arreglos del sistema de pago se extiendan sobre un área económica más amplia, tal es el caso en un único sistema de pago o conjunto de sistemas de pago interconectados cubren una región mayor que un país. Los principios también se aplican a sistemas de pago de moneda múltiple o interfronteriza.

1.2 Sistemas de Pago de Alto Valor

En México, los principales sistemas de pagos que administra Banxico, liquidan cada día un importe promedio cerca de los 4 billones de pesos. Esta cifra equivale a procesar en 4 días un importe similar al PIB anual del país. Para dimensionar la importancia de los sistemas de pagos de alto valor, al cuarto trimestre del 2021, Banxico registro un importe de operaciones 12.80 veces mayor al PIB, mientras que el efectivo en circulación solo representó 8.9% del PIB.

Tabla 3. Evolución del efectivo y de los Sistemas de Pago de Alto Valor vs PIB (Millones de pesos)

Año	Periodo	Billetes y monedas en circulación	Sistemas de Pago de Alto Valor	PIB
2017	1T	1,369,315	266,547,449	21,323,240
	2T	1,371,217	295,405,077	21,808,276
	3T	1,352,869	285,844,986	21,725,415
	4T	1,542,611	270,866,685	22,879,740
2018	1T	1,519,655	283,304,260	22,674,466
	2T	1,532,412	283,783,822	23,651,787
	3T	1,506,101	299,623,102	23,391,884
	4T	1,673,205	282,562,573	24,379,423
2019	1T	1,559,572	304,773,658	23,944,429
	2T	1,573,605	322,415,539	24,388,407
	3T	1,552,833	328,549,433	24,382,570
	4T	1,740,934	318,969,797	25,067,534
2020	1T	1,742,862	304,150,329	24,699,548
	2T	1,856,210	315,939,528	20,196,991
	3T	1,897,192	315,089,629	23,486,676
	4T	2,117,034	308,179,900	25,279,130
2021	1T	2,177,189	317,041,598	25,131,928
	2T	2,152,385	329,507,825	26,275,655
	3T	2,198,221	352,889,692	26,133,175
	4T	2,439,805	352,814,573	27,553,392

Fuente: Elaboración propia con datos de Banxico y CNBV, 2022.

Es indispensable contar con una infraestructura lo bastante robusta para llevar a cabo dichas operaciones, donde las reglas estén bien definidas y, además, que los participantes y medios utilizados aseguren la circulación del dinero.

Los sistemas de pago de alto valor catalogados por Banxico son:

Tabla 4. Sistemas de pago de alto valor

SPEI	Es el principal medio por el cual los bancos liquidan transacciones entre ellos y entre sus clientes.
DALI	Es el sistema de depósito, administración y liquidación de valores, donde se liquidan todas las operaciones con títulos del mercado de valores.
SIAC	Opera en las cuentas corrientes que los bancos tienen en el Banco Central. Es más bien el medio por el cual el Banco de México provee de liquidez a los bancos, pero todavía funciona como un sistema de pagos.
CoDi	Es una plataforma desarrollada por Banco de México que permite realizar ágiles transferencias electrónicas entre cuentas de depósitos de personas físicas y morales utilizando la actual infraestructura de pagos (rieles SPEI).

Fuente: Elaboración propia con datos de Banxico, 2022.

El Banco de México opera el SIAC, SPEI y CoDi, mientras que Indeval S.A. opera el DALI.

Recientemente, con la incorporación de la tecnología en los sistemas de información y comunicación, las Fintech han adquirido relevancia, buscando ofrecer servicios de manera eficiente, ágil y cómoda mediante plataformas como páginas web, aplicaciones móviles y redes sociales. A continuación, describiremos las dos figuras más importantes de las Fintech:

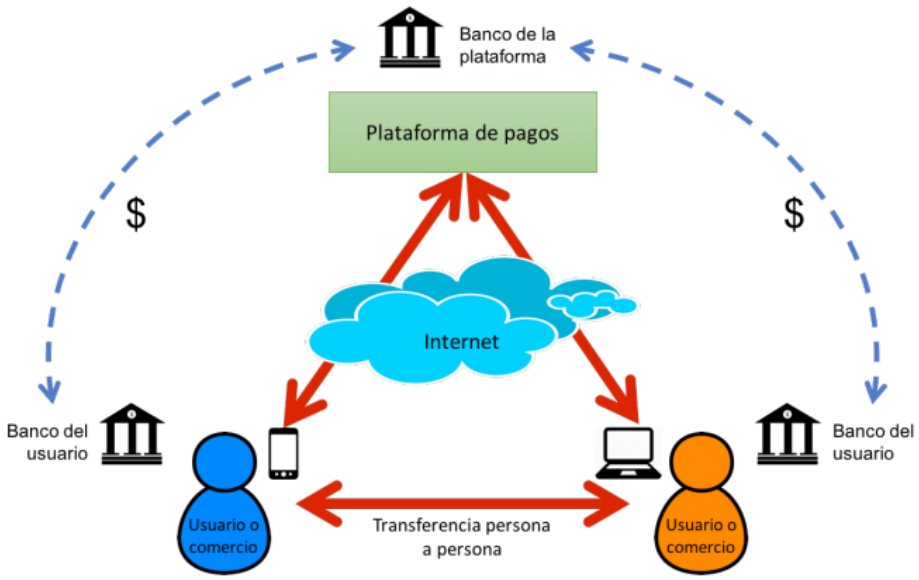
Tabla 5. Figuras de las Fintech

Instituciones de Financiamiento Colectivo (IFC) o Crowdfunding	Instituciones de Fondos de Pago Electrónico (IFPE)
Plataformas que permiten que muchas personas invierten o prestan dinero a cambio de una participación accionaria en la empresa (capital), de un rendimiento (deuda), o en las ganancias y pérdidas de un proyecto (copropiedad o regalías).	Monederos virtuales en los que el cliente puede acumular recursos (en dinero o en activos virtuales) para realizar pagos y transferencias electrónicas. Un ejemplo son las criptomonedas, que son un tipo de moneda digital que no requieren de un banco central, gobierno o alguna entidad central para su emisión y transmisión; pueden ser utilizados como medio de pago.

Fuente: https://www.gob.mx/shcp/articulos/el-sector-fintech-y-su-regulacion-en-mexico.

Este tipo de plataformas ofrecen al usuario una cuenta (no bancaria), llamada cartera digital, accesible a través de una plataforma en línea o una aplicación móvil. Esta refleja el saldo del usuario y le permite hacer depósitos, retiros, envíos directos a otros usuarios sin necesidad de un intermediario financiero tradicional:

Esquema 2. Plataforma de pagos electrónicos



Fuente: Oficina de Información Científica y Tecnológica para el Congreso de la Unión, noviembre 2017

El envío de remesas es una de las aplicaciones de este tipo de plataformas, con mayor potencial de tener un impacto en la economía de países en vías de desarrollo. Esto se debe a la reducción de costos en los envíos internacionales de dinero, lo que puede beneficiar directamente a las familias de millones de trabajadores migrantes (Digital Finance Institute, 2016).

En 2021, se calculó que hay 512 empresas Fintech en México, las cuales consiguieron inversiones por más de 89 millones de dólares entre diciembre de 2015 y enero de 2017 (Banco Interamericano de Desarrollo, 2017). Por su parte, las principales billeteras digitales usadas en México son lideradas por PayPal, BBVA Wallet y Mercado Pago.

1.3 Sistemas de Pago de Bajo Valor

Los sistemas de pago al menudeo procesan muchos pagos de montos bajos, y son utilizados por la población general, por lo que, si su diseño no es adecuado o no operan bien, pueden afectar a gran parte de la población. Los sistemas de pago de bajo valor en México están constituidos por cheques, transferencias electrónicas de fondos, domiciliaciones y tarjetas bancarias.

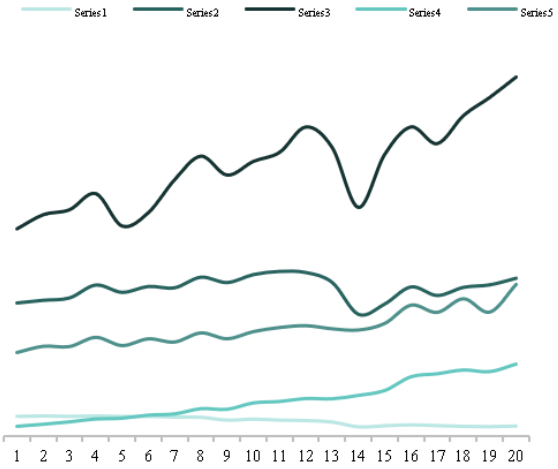
Tabla 6. Sistemas de pago de bajo valor

La Cámara de Compensación Electrónica	Realiza la compensación de los mencionados con excepción de las tarjetas de crédito. Cecoban S.A. de C.V. opera el sistema de registro y compensación de cheques, transferencias electrónicas de fondos y domiciliación y el Banco Central los liquida en el SIAC.
Cheques	Compensa los documentos que los bancos le presentan para su cobro. Esto permite a los clientes de los bancos depositar en sus cuentas cheques de otros bancos.
Transferencias Electrónicas de Fondos	Traspasos diferidos de fondos entre cuentahabientes de distintos bancos. Este sistema se usa principalmente para pagar nóminas y facturas a proveedores.
Domiciliación	Cargos diferidos que hacen los bancos a nombre de compañías que tienen clientes que les han dado autorización para cargar sus cuentas en otros bancos.
Tarjetas	Existen de dos tipos, las de crédito y las de débito. En las primeras el cliente tiene una cuenta deudora con el banco emisor, mientras que en las segundas la cuenta del cliente es acreedora, generalmente una cuenta a la vista. En ambos casos, el cliente utiliza su tarjeta como medio de pago en negocios que cuenten con terminales punto de venta, así como para consultar saldos y disponer de efectivo en cajeros automáticos. Existen varios procesadores de operaciones con tarjetas, por ejemplo, PROSA, E-Global, Visa y Mastercard, que están conectados entre sí. La compensación de las operaciones la realiza dichos intermediarios, y la liquidación se lleva a cabo a través de un banco comercial.

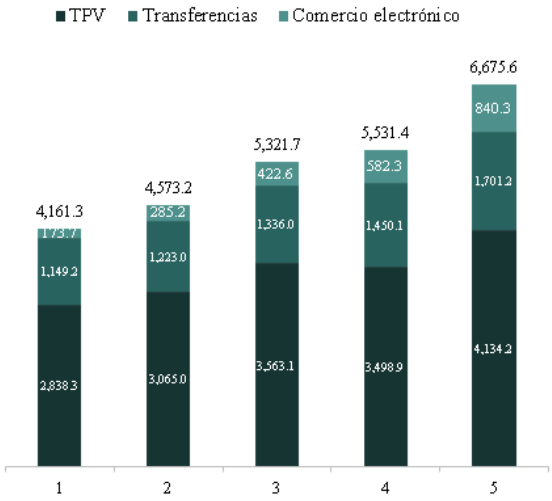
Fuente: Elaboración propia con datos de Banxico, 2022.

El medio de pago distinto al efectivo más usado en México son las tarjetas bancarias, ya que aproximadamente la mitad de los pagos a través de los sistemas de pagos al menudeo son con tarjeta bancaria. Las tarjetas de crédito y débito son emitidas por los bancos comerciales y están asociadas, como ya lo mencionamos anteriormente a un intermediario o marca. Las principales marcas de tarjetas son MasterCard y Visa. Los comercios aceptan en sus Terminales Puntos de Venta (TPV) tarjetas de todos los bancos mexicanos. Para cobrar, contratan los servicios de un banco (adquirente). En la siguiente gráfica podemos ver como las TPV siguen siendo la principal infraestructura para la utilización de las tarjetas bancarias:

Gráfica 2. Evolución de operaciones a través de distintos medios (2017-2021)



Gráfica 3. Evolución anual del total de transacciones y transferencias electrónicas (2017-2021)



Fuente: Cifras del Panorama Anual de Inclusión Financiera, CNBV 2022.

Durante 2021, el importe de transferencias y el efectivo en circulación, ambos como porcentaje del PIB, fue de 165% y de 9%, respectivamente. El mayor importe de las transferencias se efectuó a través de la banca por internet con operaciones interbancarias en su mayoría.

Tabla 7.Transacciones y transferencias en 2021 (% del PIB y Miles de personas)

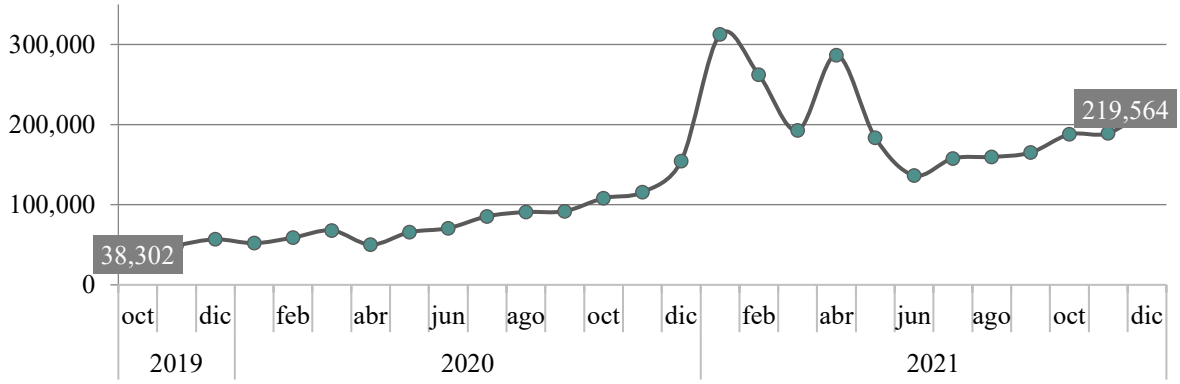
Millones de transacciones y transferencias en 2021	Efectivo en circulación como porcentaje del PIB en 2021	Importe de transferencias como porcentaje del PIB en 2021	Número de transferencias por cada 10 mil personas adultas en 2021	Número de transacciones y transferencias electrónicas per cápita anual en 2021
6,676	8.9%	165.1%	50,287	52.0

Fuente: Cifras del Panorama Anual de Inclusión Financiera, CNBV 2022.

Las TPV registraron 1,132 millones de operaciones, los cajeros 499 millones de operaciones, las transferencias 480 millones de operaciones, el comercio electrónico 228 millones de operaciones y los cheques 34 millones de operaciones.

Durante el periodo de octubre 2019 a diciembre de 2021, las transferencias enviadas por CoDi se incrementaron de 38 mil a 220 mil operaciones (CNBV, 2022).

Gráfica 4. Evolución de las transferencias enviadas por CoDi (2019-2021)



Fuente: Cifras del Panorama Anual de Inclusión Financiera, CNBV 2022.

2. Funciones del Banco Central en el Sistema de Pagos

Los bancos centrales, entre sus principales funciones, tienen la tarea de regular y supervisar un manejo adecuado de los sistemas de pagos, creando una estructura o marco legal y operacional para la administración de los sistemas de pagos. Además, son los únicos encargados de emitir el dinero en circulación, así como de aplicar políticas que regulen ya sea el exceso o escasez del mismo; su calidad de regulador del circulante, lo coloca como el organismo ideal para controlar los caminos o esquemas que recorrerá el circulante, es decir, controlar el sistema de pagos. En este sentido, el Banco de México, es el eje principal en la compensación y liquidación de cheques, así como la regulación, instrumentación, modernización y desarrollo del sistema de pagos en general, y de los sistemas electrónicos en particular. En el caso de estos sistemas de pago electrónicos, el Banco de México ha desarrollado herramientas importantes para una realización adecuadas de los sistemas de pagos, entre las que se encuentran: el sistema de pagos electrónicos interbancarios (SPEI), el sistema de atención a cuentahabientes del Banco de México (SIAC), el sistema de depósito, administración y liquidación de valores (DALI) y el sistema de Cobro Digital (CoDi).

Por otra parte, el Banco de Pagos Internacionales señala que existen cuatro responsabilidades de los bancos centrales que deben aplicar para que el sistema de pagos funciones adecuadamente, las cuales son:

Tabla 8. Responsabilidades de los bancos centrales

1	El banco central tiene que definir claramente los objetivos de su sistema de pago y, además deberá revelar públicamente su papel y sus principales políticas con respecto a los sistemas de pago sistémicamente importantes.
2	El banco central deberá asegurar que los sistemas que opera cumplan con los Principios Básicos para los Sistemas de Pago Sistemáticamente Importantes.
3	El banco central deberá supervisar el cumplimiento con los principios básicos en los sistemas que no opere y deberá tener la capacidad de realizar esta supervisión.
4	El banco central, al promover la seguridad y la eficiencia del sistema de pago a través de los principios básicos, deberá cooperar con otros bancos centrales y con cualquier otra autoridad extranjera o nacional relevante.

Fuente: Elaboración propia con información del Banco de Pagos Internacionales, 1998.

Por su parte, el Banco de México tiene tres papeles frente a los sistemas de pago:

Tabla 9. Papel del sistema de pagos según Banxico

Operador	Tiene bajo su administración el SIAC y el SPEI.
Usuario	Por medio de ellos instrumenta la política monetaria, la política cambiaria, otorga liquidez al sistema financiero, recibe garantías de la banca, participa en servicios de pago al gobierno y usa los sistemas para pagar nómina y facturas a proveedores de las organizaciones.
Supervisor y Regulador	Es el supervisor y regulador de los sistemas de pago de importancia sistémica, así como los medios y sistemas de pago al menudeo.

Fuente: Elaboración propia con información del Banco de México.

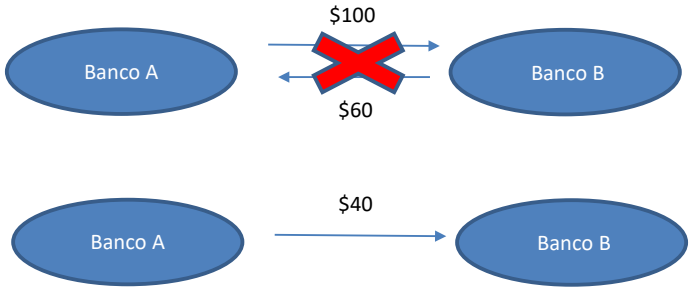
2.1 Liquidación de Operaciones

Para comprender el funcionamiento de los sistemas de pagos es necesario conocer algunos conceptos, como, por ejemplo, la compensación, que es el acto que sustituye muchas obligaciones por un número bastante menor de obligaciones, debido a un acuerdo entre los participantes. El mecanismo por el cual la compensación funciona es:

- Bilateralmente, indica que cada pareja de participantes sustituye los derechos y obligaciones de todas las operaciones entre ellos por una única obligación.

Operar con los citados organismos, con bancos centrales y con otras personas morales extranjeras que ejerzan funciones de autoridad en materia financiera.

Esquema 3. Compensación de los sistemas de pagos

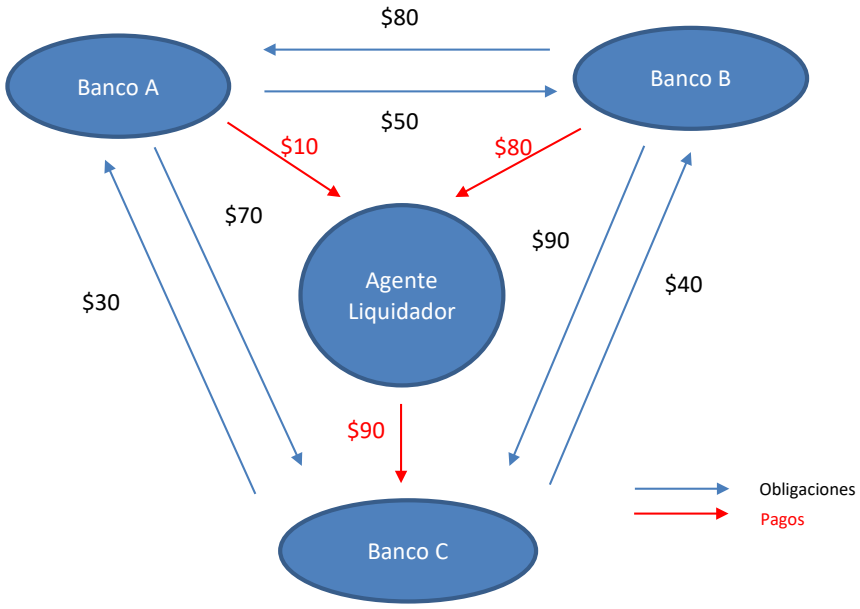


Fuente: Elaboración propia con información del Banco de México, 2022.

Compensando, el Banco A pagará $40 al Banco B, en cambio sin compensación, el Banco A tendría que conseguir $100 y el Banco B $60.

- Multilateralmente, cada participante sustituye todos los derechos y obligaciones con un solo derecho u obligación frente a todo el sistema.

Esquema 4. Liquidación de pagos



Fuente: Elaboración propia con información del Banco de México, 2022.

Tabla 10. Liquidación de pagos

	Banco A	Banco B	Banco C	**Por pagar**
Banco A		50	70	120
Banco B	80		90	170
Banco C	30	40		70
Por recibir	110	90	160	

Fuente: Elaboración propia con información del Banco de México

Es aquí donde la liquidación de pagos permite que la transferencia definitiva de fondos entre dos o más partes salde las obligaciones pactadas. Si el Banco A recibe al final $110 de los bancos B y C y paga $120 para los mismos. La diferencia indica que hay $10 que el agente liquidador mandará al Banco C para que dicha transferencia cuadre.

La liquidación en un sistema de pagos se puede realizar de dos formas:

- Bruta. Las órdenes de pago se liquidan una por una y requiere que el pagador tenga el importe completo del pago.
- Neta. Las órdenes de pago se acumulan y se compensan y liquidan posteriormente en un ciclo de liquidación, usualmente al final del día.

El proceso de liquidación de un sistema también se puede clasificar según la prontitud de la liquidación, es decir, el tiempo en que se liquidan sus operaciones:

- En tiempo real.
- Diferidos.

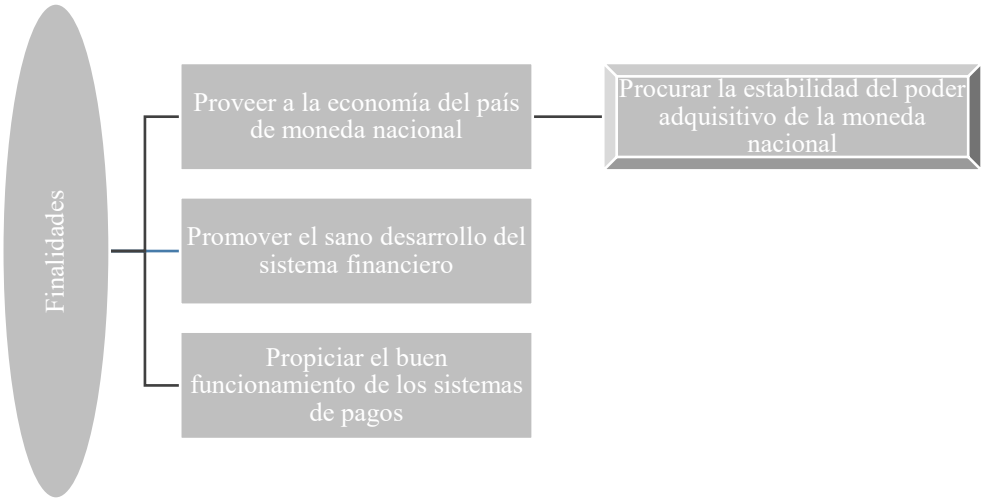
2.2 La Ley del Banco de México

La Ley del Banco de México establece que una de sus finalidades es propiciar el buen funcionamiento de los sistemas de pago. Para hacer esto, la Junta de Gobierno del Banco Central adoptó en enero de 2001 los “Principios Básicos para los Sistemas de Pago Sistémicamente Importantes”, que es un documento del Comité de Sistemas de Pago y Liquidación de los Gobernadores de los Bancos Centrales del G-10 que recopila las mejores

prácticas para el diseño y operación de los sistemas de pago que son importantes para la estabilidad de los mercados financieros (sistémicamente importantes).

De acuerdo con el art. 2º de la Ley, el Banco de México tiene tres finalidades. A continuación, se muestran dichos objetivos, entre ellos, el más importante es la lucha contra la inflación:

Esquema 5. Objetivos del Banco de México



Fuente: Derecho Bancario, Oxford University Press, 2012.

En términos del art 3º de la Ley, el Banco de México desempeñan las funciones siguientes:

1. Regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos.
2. Operar con las instituciones de crédito como banco de reserva y acreditante de última instancia.
3. Prestar el servicio de tesorería al gobierno federal y actuar como agente financiero del mismo.
4. Fungir como asesor del Gobierno Federal en materia económica y particularmente financiera.
5. Participar en el Fondo Monetario Internacional y en otros organismos de cooperación financiera internacional que agrupen bancos centrales.

Además, el Banco de México es una institución que actúa como proveedora de liquidez a otra institución financiera que se ve incapaz de obtener suficiente liquidez en el mercado de préstamos interbancarios y se han agotado otras facilidades o fuentes, es decir, es un banco central que ha sido es un proveedor de servicios de prestamista de última instancia.

3. Evolución del SPEI, DALI y el SIAC

3.1 Sistema de Pagos Electrónicos Interbancarios (SPEI)

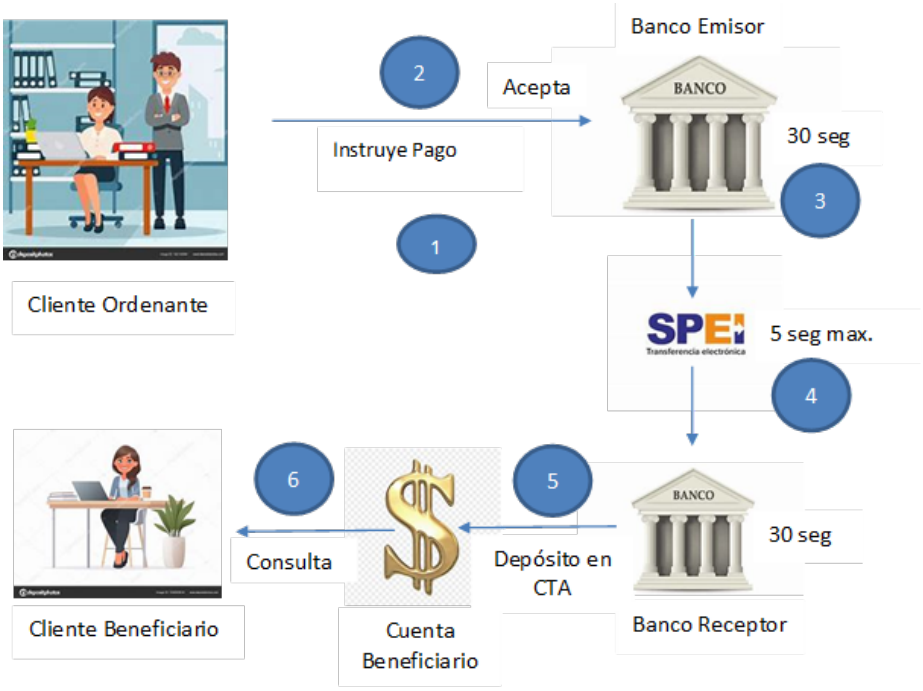
El SPEI empezó a operar el 13 de agosto de 2004, el cual permite realizar transferencias de fondos entre sus participantes. Participan bancos y otras instituciones financieras no bancarias (casas de bolsa, aseguradoras, fondos de inversión, casas de cambio, etc.). Lleva información para indicar si un cliente ordenó el pago y, en su caso, para identificarlo. Asimismo, puede llevar información para instruir al participante receptor para que acredite el pago a uno de sus clientes.

El SPEI ejecuta con frecuencia un proceso que determina que pagos pueden liquidarse con los saldos que los participantes tienen en ese momento. Los participantes deben enviar los pagos que soliciten sus cuentahabientes a más tardar 5 segundos después de aceptar la solicitud. Asimismo, los receptores de un pago deberán acreditar la cuenta de su cliente beneficiario a más tardar 5 segundos después de recibir el aviso de que se ha liquidado el pago.

La seguridad del SPEI está basada en mensajes firmados digitalmente. Para ello, los participantes usarán los certificados digitales y las claves de las personas autorizadas, quienes deberán obtener estos certificados de acuerdo con las normas de la Infraestructura Extendida de Seguridad (IES), del Banco de México.

El SPEI utiliza un protocolo abierto (reglas públicas de comunicación con el sistema) lo que permite a los participantes automatizar sus procesos y brindar más y mejores servicios a sus clientes. Es por ello que, las ventajas a través de este sistema han permitido ofrecer al público en general transferencias en tiempo real a bajos costos. Por ejemplo, antes del SPEI el costo promedio de las transferencias para los clientes de los bancos era de $100 y las transferencias debían ser por un monto de $50,000.

Esquema 6. Funcionamiento del SPEI



Fuente: Elaboración propia con información de Banxico, 2022.

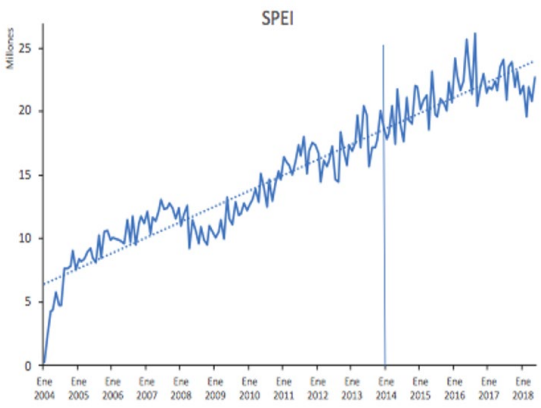
El SPEI es al mismo tiempo un sistema de importancia sistémica y un sistema de menudeo.

A continuación, se presentan algunas características relevantes:

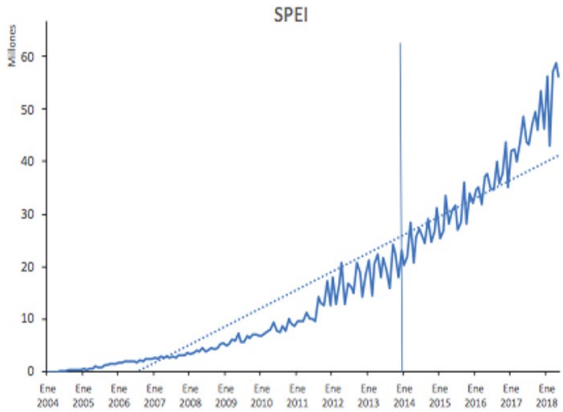
- En él se liquidan los grandes pagos interbancarios y de tesorerías de empresas, así como las obligaciones en pesos del sistema internacional de liquidación de operaciones cambiarias CLS (Continuous Linked Settlement).
- El SPEI liquida cada mes un monto mayor al valor de todo lo que produce México en un año.

A continuación, vamos a describir el comportamiento y la tendencia del SPEI, mostrando su importancia en términos monetarios durante el periodo de agosto de 2004 a diciembre de 2018.

Gráfica 5. Valor monetario (Millones)



Gráfica 6. Número de transacciones (Millones)



Fuente: Elaboración propia con información de Banxico, 2022.

El SPEI es el sistema de pagos más importante del país, liquidando de manera segura y eficiente los grandes pagos de las instituciones financieras y de las tesorerías de empresas, apoyando la estabilidad financiera. Además de que dicho sistema es de importancia sistémica, ya que también liquida las operaciones del público en general. Ante el crecimiento exponencial en la evolución del número de transferencias en el SPEI, se han desarrollado proyectos como el SPEI ampliado, cuyo objetivo es habilitar una nueva instancia del SPEI. Esto permitirá asegurar la continuidad operativa, así como mantener los estándares de servicio y funcionamiento del SPEI ante el continuo incremento de las operaciones. Todo esto permitirá que se incremente la capacidad de procesamiento del SPEI para atender el crecimiento de las operaciones en el futuro.

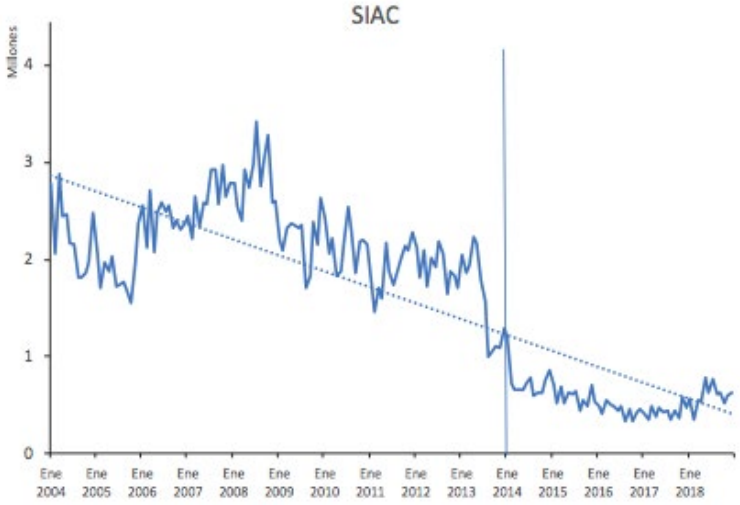
3.2 Sistema de Atención a Cuentahabientes de Banco de México (SIAC)

Es un sistema que administra las cuentas corrientes de los participantes en Banco de México. Si bien permite las transferencias de fondos definitivas entre cuentas de los participantes sin

restricción en el monto, más que un sistema de pagos representa el medio por el cual el Banco Central provee de liquidez a los participantes del sistema de pagos.

Al cierre de los sistemas DALI y SPEI los saldos de sus participantes son transferidos al SIAC y la liquidación del SICAM (Sistema de Cámaras) se realiza también en este sistema. Además, en cualquier momento en que los horarios de operación coinciden, acepta traspasos de fondos de y hacia el DALI y el SPEI. Estas transferencias sólo pueden hacerse entre las cuentas de un mismo participante.

Gráfica 7. Valor monetario (Millones)



Fuente: Elaboración propia con información de Banxico, 2022.

A través del SIAC, el Banco de México provee de liquidez al sistema bancario.

3.3 Sistema de Depósito, Administración y Liquidación de Valores (DALI)

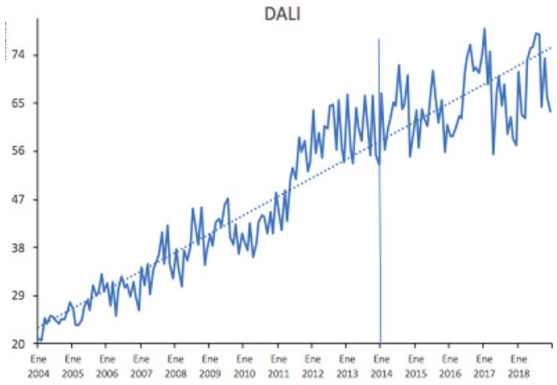
El DALI es un sistema de registro electrónico en cuentas para acciones y títulos de deuda gubernamentales y privados (principalmente bancos y casas de bolsa). El sistema liquida la parte de efectivo de las operaciones mediante un servicio de administración de cuentas de efectivo que el Banco de México proporciona a Indeval, que funge como el depósito central

de valores y es el que lleva registro y guarda de los instrumentos de los mercados de dinero y capitales.

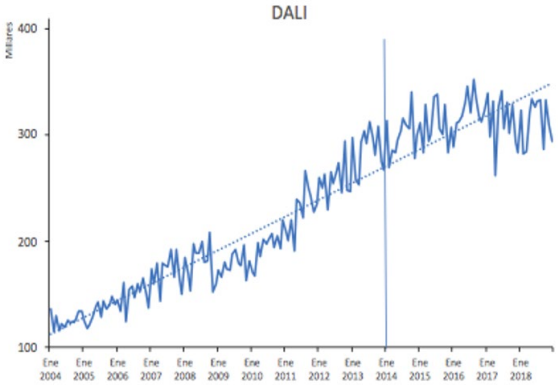
El dinero que se usa para liquidar operaciones se encuentra en el Banco de México y los participantes del DALI pueden transferir fondos de sus cuentas de efectivo a sus cuentas en los sistemas de pago SPEI y SIAC. Al cierre de operaciones, el DALI transfiere los saldos de las cuentas de efectivo de los depositantes a sus cuentas en el SPEI o a la cuenta bancaria que hayan indicado y se comunica con sus participantes por medio de un protocolo basado en el estándar ISO15022. Esto facilita a sus participantes la automatización de sus procesos con valores.

El DALI liquida el mayor monto de los sistemas de pagos en México, alrededor de 60 billones de pesos al mes, ya que incluyen operaciones de los mercados de dinero y capitales.

Gráfica 8. Valor monetario (Millones)



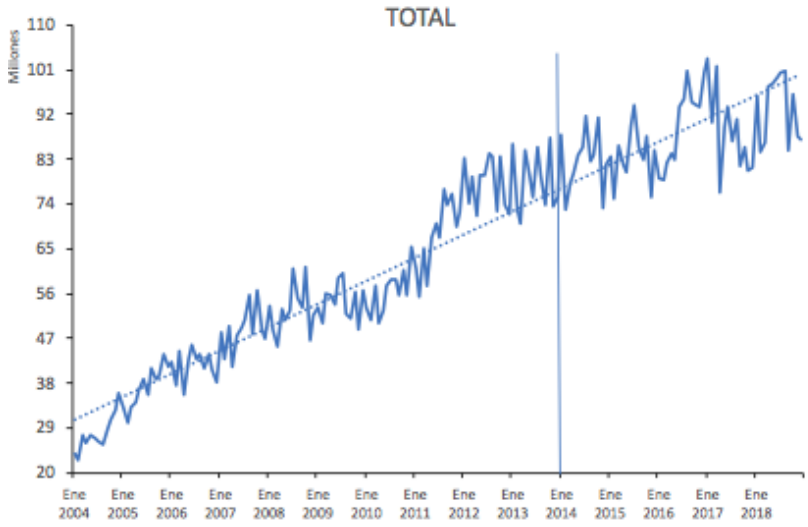
Gráfica 9. Número de transacciones (Millones)



Fuente: Elaboración propia con información de Banxico, 2022.

Por otra parte, en el DALI se liquidan todas aquellas transacciones que son operadas en el mercado de valores, por ello también es un sistema de importancia sistémica ya que a través de él se liquida más del 70% del volumen total de operaciones que son procesadas por los sistemas de pago y de liquidación y de compensación en México.

Gráfica 10. Valor monetario (Millones)



Fuente: Elaboración propia con información de Banxico, 2022.

En conclusión, podemos señalar que el flujo de dinero que circula por el SPEI y el DALI han mostrado una tendencia creciente. Como puede observarse, del total de pagos de alto valor, el sistema DALI es el que tiene mayor peso y en menor medida el SPEI y el SIAC, en ese orden.

Es importante mencionar que, actualmente el SPEI ha adquirido un mayor uso, por lo que dicho sistema permite ser un instrumento híbrido que incide sobre la magnitud del flujo de dinero que circula a través del mismo, ya que los usuarios pueden liquidar en tiempo real o al final del periodo diferido, lo cual flexibiliza su operación. Es por ello que, en virtud de que el SPEI es un sistema híbrido, sus usuarios pueden realizar pagos de alto y bajo valor.

Por otra parte, el número de operaciones en el SPEI se estima que tenga un crecimiento de 63% de 2020 a 2021, y de 52% de 2021 a 2022. Además, las operaciones tercero a tercero menores a $8,000 pesos, las cuales representan aproximadamente el 80% de las operaciones totales, se estima crezcan 80% y 50%, para 2021 y 2022, respectivamente.

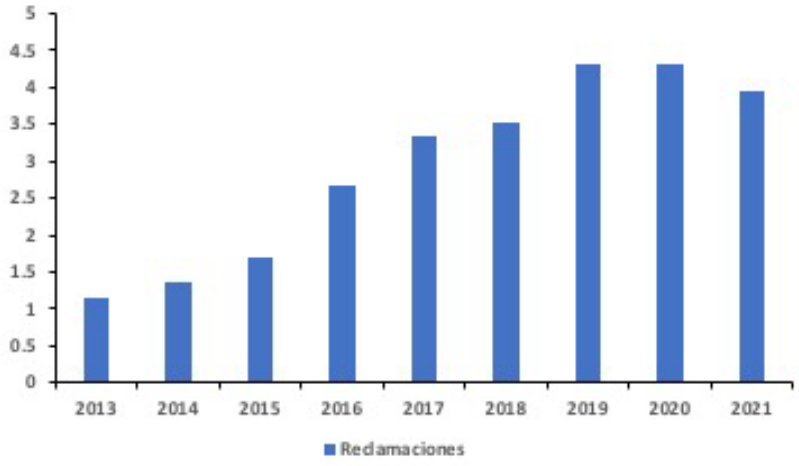
4. Tipos de Fraudes Financieros y Sistemas de Detección

El "fraude" es un riesgo que enfrentan las autoridades monetarias y financieras, porque ocasiona grandes pérdidas económicas a empresas, inversores y empleados. Hacer un depósito, cobrar un cheque, retirar dinero de un cajero automático, solicitar un crédito, pagar con la tarjeta de crédito, realizar compras en línea, son acciones que realiza de manera cotidiana un usuario de servicios financieros, y puede correr el riesgo también de ser víctima de un fraude.

Según un estudio, el crimen cibernético genera 1.5 billones de dólares al año; si fuera un país, su PIB sería el número 13 a nivel global (Bromium, 2018). En términos generales, el fraude es un acto intencional o deliberado de privar a otro de una propiedad o dinero por la astucia, el engaño, u otros actos desleales (ACFE, s.f.). En México, el año 2021 cerró con un incremento del 52% en las denuncias de fraudes bancarios por internet con respecto a 2020 al situarse en 24,215 reclamaciones, según informó la Condusef (Los Angeles Times, 2022).

Del 2013 al cierre del primer semestre del 2021, la tasa media de crecimiento anual de las reclamaciones por fraude en México fue de 16.8%, por lo que en 2019 se registró el mayor número con 4.3 millones, como se muestra en la gráfica siguiente:

Gráfica 11. Número de Tarjetahabientes que reclamaron Fraude en México, 2013-2021 (Millones de personas)



*Cifras al cierre del primer semestre de 2021.
Fuente: Elaboración propia con datos de la Condusef.

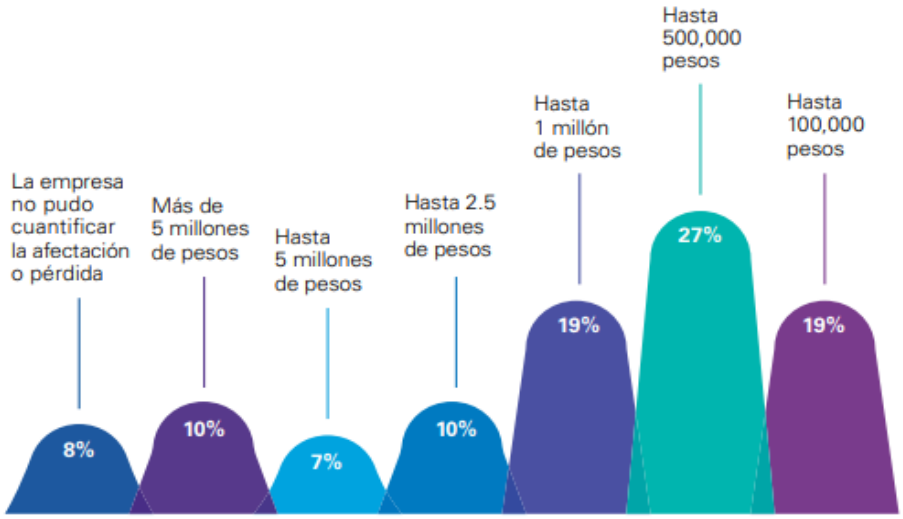
En el sector financiero, el 100% de las entidades e instituciones financieras en México manifiestan que identificaron algún tipo de evento (ataques exitosos y no exitosos) de seguridad digital en su contra. Los eventos de seguridad digital más comúnmente identificados, por ejemplo, durante el año 2018 fueron:

a) El código malicioso o malware (56% del total de las entidades)
b) El phishing dirigido para tener acceso a sistemas de la entidad (47% del total de las entidades), y
c) La violación de políticas de escritorio limpio (31% de las entidades)

Se puede destacar que un 19% de las entidades e instituciones financieras identifican ocurrencia de eventos de malware diariamente (OEA y CNBV, 2019)

Por otro lado, las organizaciones en promedio, han tenido pérdidas que se ubican en 1.4 millones pesos por fraude, cifra que representa 1% del promedio total de ventas anuales; sin embargo, debemos considerar que 8% de las empresas no pudieron cuantificar dicha pérdida (KPMG, 2020).

Gráfica 12. Estimación de la afectación económica



*Información con cifras al 2020.
Fuente: El impacto de los delitos financieros, KPMG.

Por último, Banxico sufrió un ciberataque en 2018, cuando se registraron a cinco participantes en el SPEI con vulneraciones de ciberseguridad, y donde dichos ataques fueron dirigidos hacia los bancos, casas de bolsa y otros participantes del sistema de pagos (Banco de México, 2018)

Una vez explicado el comportamiento actual de los sistemas de pagos en México, en este capítulo trataremos de abordar mediante la incorporación de mecanismos automatizados, el desarrollo de un sistema de balanceo de datos para la detección de fraudes.

La desregulación y la globalización de los servicios financieros, junto con la creciente sofisticación de las tecnologías financieras, hacen más complejas las actividades de las instituciones financieras y, por ende, aumentan sus perfiles de riesgo (es decir, el nivel de riesgo de las actividades y/o categorías de riesgo de una empresa). De acuerdo con la Teoría de la Utilidad Esperada (TUE) de Bernoulli, el riesgo es el producto de la probabilidad de un cierto resultado y su consecuencia. Este concepto aún perdura, como puede verse en la definición de la Financial Stability Board's, la cual señala que el riesgo cibernético es la combinación de la probabilidad de que ocurran incidentes cibernéticos y su impacto (European Systemic Risk Board, 2020)

Dentro del campo de la TUE, se utilizan muchos métodos para la evaluación de riesgos; estos pueden ser ampliamente clasificados como "activos únicos y "sistemas de activos". La diferencia radica en que mientras una evaluación de riesgos de un solo activo implica solo un objetivo, el segundo involucra muchos activos conectados entre sí para formar un sistema. En el caso de la detección de fraudes en los sistemas de pagos, el método de evaluación de riesgos por sistema de activos es el más eficiente y compatible para poder capturar la probabilidad de que ocurra un ciberataque.

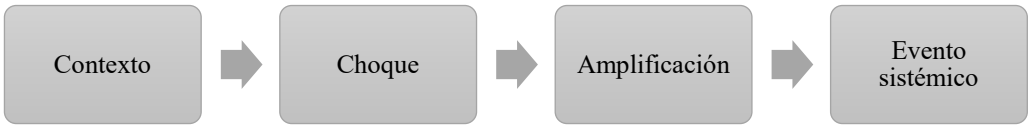
En general, las evaluaciones de riesgo incluyen amenazas, vulnerabilidades, análisis de probabilidad de ocurrencia, determinación de impacto y análisis de controles. La combinación de estos factores le permite asignar una calificación de exposición al riesgo, la

cual se basa en la fórmula de evaluación probabilística de riesgos ideadas por Norman Rasmussen en 1975:

$$cyber\ risk = \frac{ciberamenazas\ x\ vulnerabilidades\ x\ activos\ x\ impacto\ del\ incidente}{contramedidas}$$

Para poder detectar un incidente cibernético, actualmente hay cuatro fases de análisis que el Financial Stability Board ha desarrollado para determinar las implicaciones macrofinancieras del riesgo cibernético y operativo, las cuales son:

Esquema 7. Modelo de riesgo sistémico conceptual



Fuente: Systemic cyber risk, February 2020.

La fase de contexto será útil para el diseño de escenarios, sin embargo, no es esencial para evaluar el impacto sistémico, vulnerabilidades o mitigantes relevantes. Por su parte, la fase de choque describe los impactos técnicos y comerciales inmediatos experimentados en el punto donde el incidente cibernético tiene su impacto inicial. La fase de amplificación explora las interacciones entre las instituciones afectadas que utilizan, y los factores que influyen en cómo se propagan los choques a través de estos sistemas. Por último, la fase evento sistémico examina el punto en el que el sistema ya no es capaz de absorber el choque.

Existe una extensa literatura macroeconómica sobre las diversas formas de contagio financiero donde el sistema puede quedar expuesto. En un artículo elaborado por Eisenberg y Noe, se expone el marco analítico por la cual, los sistemas financieros se encuentran interconectados y como una pérdida en una institución financiera puede conducir rápidamente a pérdidas para otras instituciones (Eisenberg & Noe, 1999). En particular, este contagio se da través de choques de crédito interbancarios, donde las pérdidas crediticias están relacionadas con el riesgo de contraparte y son incurridas por los bancos prestamistas

cuando sus bancos prestatarios incumplan con sus obligaciones. Estas pérdidas pueden entonces conducir al incumplimiento de los prestamistas, lo que resulta en otra ola de choques crediticios.

Por otra parte, a nivel micro, el triángulo del fraude, desarrollado por el criminalista Donald Cressey, describe tres condiciones que comúnmente aparecen cuando se comete fraude. Aquellos que cometen el delito experimentan cierto Incentivo o Presión que los lleva a cometer el acto deshonesto, debe existir una Oportunidad para cometer fraude; y los defraudadores generalmente son capaces de Racionalizar o Justificar sus acciones. La recesión económica es una problemática que influye en estos tres factores (PriceWaterHouseCoopers, 2009).

Esquema 8. Triángulo del fraude

Fuente: Fraude en tiempos de crisis, PwC 2009.

Para actos en los que esté involucrado el factor humano, la categorización de amenazas cibernéticas debe ser mejorado para tener en cuenta los factores antes descritos, ya que, por ejemplo, en tiempos económicos difíciles se incrementa la capacidad de la gente de racionalizar el fraude y la corrupción.

Con la evolución de las prácticas bancarias, los bancos se ven expuestos a nuevos riesgos cada vez mayores, aparte de los riesgos de crédito, de tipos de interés y de mercado, cómo lo que pasa con el crecimiento del comercio electrónico que, conlleva ciertos riesgos (por ejemplo, fraude interno y externo y problemas relacionados con la seguridad del sistema) que todavía no se comprenden completamente.

Por su parte, el Comité de Supervisión Bancaria de Basilea, en colaboración con la banca, ha identificado como posibles fuentes de perdidas sustanciales:

- Fraude interno: errores intencionados en la información sobre posiciones, robos por parte de empleados, utilización de información confidencial en beneficio de la cuenta del empleado, etc.
- Fraude externo: atraco, falsificación, circulación de cheques en descubierto, daños por intrusión en los sistemas informáticos, etc (Banco de Pagos Internacionales, 2003).

Con la explotación de datos se hace posible generar redes más complejas de inteligencia para el análisis de nuevas amenazas, a fin de evitar que se materialicen. Los esquemas de automatización robótica de procesos, el aprendizaje de computadoras y la inteligencia artificial son solo algunos ejemplos de lo que la Cuarta Revolución Industrial nos ofrece.

En el caso de los sistemas de Machine Learning o Aprendizaje Automatizado, se ha recibido mucha aceptación en los últimos años, cambiando de sistemas basados en reglas a soluciones basadas en aprendizaje de máquina. En los sistemas basado en reglas las actividades fraudulentas pueden ser detectadas al revisar algunas señales evidentes, por ejemplo, un gran número de transacciones inusuales o aquellas que ocurren en ubicaciones atípicas, por lo que este tipo de transacciones requiere de una validación adicional. En cambio, los sistemas basados en Machine Learning son más sensibles para detectar eventos ocultos en el comportamiento de los usuarios que podrían no ser muy evidentes pero que son señales de posibles fraudes. Las técnicas de Machine Learning, además de crear algoritmos, ayudan a encontrar posibles correlaciones ocultas entre el comportamiento de los usuarios y la probabilidad de que esas acciones sean fraudulentas.

Otra fortaleza de este tipo de sistemas es que pueden procesar más rápido los datos y requieren un menor trabajo manual, además de que ayudan a reducir el número de aplicaciones en los sistemas basados en reglas. Más delante describiremos detalladamente los tipos y métodos más usados para la detección de fraudes. Además, nos aproximaremos a una evaluación por medio de un modelo de clasificación o balanceo de datos.

4.1 Fraudes Cibernéticos

Se refiere a aquellas estafas que utilizan la red para realizar transacciones ilícitas. Muchas veces, las personas que realizan este tipo de fraudes, se aprovechan del desconocimiento o poco cuidado que las personas tienen al utilizar los servicios financieros en línea, convirtiéndose en un blanco fácil para los estafadores.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros señala los siguientes Fraudes Cibernéticos:

Tabla 11. Fraudes cibernéticos

Correo Basura o Spam.	Se trata de un mensaje enviado a varios destinatarios que usualmente no lo solicitaron, con fines publicitarios o comerciales. La información de dicho correo invita al usuario a visitar una página o descargar algún archivo que, por lo general, es un virus que roba la información de tu dispositivo.
Smishing.	Se envía un mensaje SMS al teléfono móvil, con la finalidad de que se visite una página web fraudulenta, para así obtener tu información bancaria y realizar transacciones en nombre del usuario.
Pishing.	También conocido como suplantación de identidad, en este tipo de fraude, se hacen pasar por una institución financiera y se envía un mensaje indicando un error en la cuenta bancaria del usuario, al ingresar los datos, obtienen información confidencial como: números de tarjetas de crédito, claves, datos de cuentas bancarias, contraseñas, etc.
Vishing o pishing telefónico.	Los delincuentes simulan ser empleados de alguna institución financiera y generalmente convencen al decir que las cuentas del usuario están registrando cargos irregulares o que requieren alguna información.
Pharming.	Consiste en redirigir a una página de internet falsa mediante ventanas emergentes, para robar información. Suelen mostrar leyendas como: "ERROR EN EL SISTEMA. Para solucionarlo da clic aquí".
Comercio Electrónico.	El comercio electrónico es la compra-venta de bienes y servicios a través de internet. Estas transacciones se pagan con tarjetas de débito y crédito, es por ello que se debe de poner mucha atención al momento de llevar a cabo compras, ya que no existe un contacto directo con el vendedor y puede convertirse en fraude.
Doxing.	El doxing consiste en obtener y publicar información sensible de una persona, sin su consentimiento.

Fuente: Elaboración propia con información de CONDUSEF, 2022.

Por otro lado, las formas o modalidades más recurrentes de fraudes son: la sustracción de datos personales, contraseñas, nombres de usuario o números de tarjetas de crédito, que pueden prestarse al robo de identidad; o pagar por tu compra y nunca recibirla; además de reclamar ante el vendedor y no recibir respuesta alguna.

Por su parte, los principales incidentes cibernéticos ocurridos durante 2021, publicados por Banxico fueron los siguientes:

Tabla 12. Incidentes cibernéticos durante 2021

Descripción	Servicios Afectados
Ataque a cajeros automáticos	Cajeros automáticos
Ransomware en servidores y terminales	Banca por internet
Ataque al servicio de transferencia de fondos desde sucursales	Transferencia en sucursales
Ataque a aplicativo de transferencias de fondo para retiro de efectivo sin tarjeta en cajero automático	Cajeros automáticos

Fuente: Elaboración propia con información de Banxico

Con respecto a las personas que realizan estos fraudes (tipos de hackers), según la CONDUSEF, se clasifican de la siguiente forma:

Tabla 13. Tipos de hackers

Cracker.	A diferencia del hacker, este no necesariamente debe tener el mismo nivel de conocimientos que el hacker; estos, realizan múltiples intentos de ataque hasta que logran acceder a los sistemas computacionales para posteriormente causar daños al sistema; su motivación para hacerlo puede ser el dinero o el prestigio, así como por venganza o por fines anárquicos.
Hacker.	Cualquier persona con alto dominio de su profesión (no necesariamente programador), capaz de solucionar problemas a través de hacks (segmentos de códigos muy ingeniosos); son verdaderos conocedores de la tecnología de cómputo y telecomunicaciones; su motivación es la búsqueda del conocimiento como fuerza impulsora.
Ingeniería Social.	La ingeniería social basa su comportamiento en la premisa "Es más fácil manejar a las personas que a las máquinas". Usan técnicas de manipulación psicológica para lograr que el usuario revele información beneficiosa para el atacante. Los ataques de ingeniería social son técnicas que utilizan los ciberdelincuentes para engañar, confundir, estafar o ganar la confianza de las personas con el objetivo de robar información personal, financiera y/o claves de acceso.
Spoofing.	A través de ciertas herramientas o metodologías, se puede desplegar un nombre o remitente en un correo que en realidad proviene de alguien más; esto se conoce como Spoofing.
Pishing.	Las campañas de Pishing son engaños, los atacantes fuerzan a las víctimas a acceder a una página web fraudulenta donde roban información confidencial. También pueden aprovecharse del miedo de una persona con respecto a sus relaciones sociales o mediante publicidad engañosa.

Tabla 13 … Continuación

Malware.	Los virus computacionales, nacieron desde los años ochenta, y han evolucionado con el paso de los años, así como los objetivos de estos. Es así que surge el término de malware para denominar a los softwares maliciosos, que al igual que un virus biológico, buscan infectar y propagarse, a través de los archivos del dispositivo. Los malware buscan causar un mal funcionamiento del dispositivo, acceder a los datos del mismo, acceder a la información almacenada, e incluso, prender el micrófono o la cámara web del dispositivo infectado. Los troyanos son un tipo de malware que se hace pasar por un programa de servicio común, pero en realidad este ya se encuentra alterado por el intruso para poder recopilar información. Hay malwares que no necesitan del usuario para propagarse, a estos se les conoce como gusanos. Pueden esparcirse por correo electrónico a través de las listas de contactos del usuario; se aprovechan de las vulnerabilidades del equipo para infectar sin que el usuario tenga que hacer algo para permitirle la entrada.
Ransomware.	El Ransomware es un Malware que impide a los usuarios acceder a su sistema o archivos personales al cifrar su información y que exige el pago de un rescate para poder acceder de nuevo a ellos. Algunos ejemplos de Ransomware, son: CryptoLocker, WannaCry, Bad Rabbit, Cerber, Crysis, CryptoWall, GoldenEye, Jigsaw y Locky. La diferencia entre ellos es la forma de su propagación e infección del sistema, las vulnerabilidades de las que se aprovechan, el tipo de dispositivo al que va dirigido y el rescate que se solicita.

Fuente: Elaboración propia con información de CONDUSEF, 2022.

4.2 Fraudes Tradicionales

Con el uso de las tecnologías de la información, el internet y la ciencia de datos, la banca ha dado un gran paso hacia la era digital. Sin embargo, antes de existir ciertos mecanismos, las operaciones se realizaban de manera presencial o personal entre el banco y el cliente. Los sistemas al no ser tan sofisticados, tecnológicamente hablando, como lo son ahora, desencadenaban ciertos riesgos antes los movimientos que pudiera realizar el usuario del servicio financiero. Por ello, presentaremos algunos ejemplos de ataques y amenazas que los usuarios detectaron, y que actualmente han evolucionado de tal forma que siguen siendo riesgos latentes para el sistema financiero.

Tabla 14. Ataques y amenazas

Tallado de tarjetas.	Se realiza en cajeros y opera en grupos que alteran la ranura donde va el plástico y al tratar de retirar dinero, una persona le comenta al usuario que el cajero está fallando. Después le piden la tarjeta argumentando que se debe tallar o limpiar, pero en este momento se cambia el plástico y el delincuente se retira. Un cómplice entra entonces al ATM y en lo que la afectada trata de realizar una operación con la tarjeta que no es la suya, observa el NIP que se está tecleando.
Créditos Express.	Son estafas en donde empresas falsas se hacen pasar por gestoras de crédito (empresas con suficiencia económica que ofrecen préstamos) y le ofrecen a la víctima préstamos provocativos con requisitos mínimos, con tasas de interés por debajo de las del mercado, y sin consultar su historial crediticio. Usualmente le piden un depósito anticipado a la víctima, argumentando que son gastos de solicitud y comisión por apertura y, una vez que realizado el depósito. Tiempo después la empresa, desaparece o le informa a la víctima que el crédito no fue aprobado, sin devolverle el dinero depositado.
Pirámides.	Se tratan de cadenas de ahorro que ofrecen ganancias elevadas y son promocionadas generalmente por redes sociales. Existen varios tipos de pirámides como: la Flor de la abundancia, Células de Gratitud, Bolas Solidarias, Círculo de la Prosperidad, entre otros. Las cadenas funcionan a través de aportaciones de todos los participantes, cada uno con un turno de estar en la cima o punta de la pirámide, centro de la flor, etc. La finalidad es ir subiendo de nivel, esperar el turno o llegar a la cúspide y así poder recibir dinero. Todos los participantes deben invitar a más personas para unirse al grupo de ahorro. Hasta que llega un momento en que se vuelven insostenibles, ya que es imposible seguir agregando eslabones indefinidamente. Al romperse la cadena, quienes aportaron dinero, ya no lo recuperan. En el peor de los casos, el organizador de la pirámide desaparece sin entregar el recurso.
Ahorro Informal.	La tanda, se trata de un mecanismo de ahorro informal llevado a cabo en oficinas, amigos, familiares, vecinos, etc. Consiste en reclutar al mayor número de participantes, quienes entregaran quienes entregaran una cantidad fija de dinero por un lapso acordado por los integrantes del grupo. Cada integrante tendrá un número y deberán esperar para recibir el pago determinado. El defraudador suele ser el administrador de la tanta que puede dejar en vulnerabilidad al resto en cualquier momento o cualquier participante que, después de recibir el recurso, incumple con el resto de los pagos.
Trashing.	El delincuente trata recaudar información de la víctima buscando información valiosa en la basura, como estados de cuenta, copias de identificaciones oficiales u otro documento que contenga datos importantes, con los cuales se pueda realizar un fraude; por ejemplo, robar su identidad, realizar transacciones bancarias a tu nombre y despojarlo de sus ahorros.
Alteración de cheques.	El delincuente se acerca a la víctima que está en la fila del banco y ofrece comprarlo para que no se pierda tiempo en la sucursal. Una vez que el delincuente tiene el documento, se retira y procede a alterar algunas partes como el nombre al portador, el monto a cobrar y el endoso.

Fuente: Elaboración propia con información de CONDUSEF, 2022.

4.3 Sistemas de Detección de Fraudes

La industria de servicios financieros está sufriendo de pérdidas y daños relacionados con fraudes, por ejemplo, en Estados Unidos durante 2016, 15.4 millones de clientes fueron blanco de fraudes. Además, considerando que el cambio al espacio digital abre nuevos canales para la distribución de estudios financieros, pero también crea nuevas oportunidades para los estafadores (ASIS, 2021).

Cuando ocurre un fraude la lealtad de los clientes se ve afectada tanto en el ámbito digital como en el físico, se estima que para detectar los fraudes toma alrededor de 40 días, por ejemplo, reportes de algunos bancos indican que un 20% de sus clientes cerraron sus cuentas o se cambiaron de banco después de haber sido víctimas de un fraude, así que el reto para la industria es implementar sistemas en tiempo real que mejoren la precisión en la detección de fraudes.

Como ya se mencionó anteriormente, los sistemas de Machine Learning para detección de fraudes, han recibido mucha aceptación en los últimos años y la industria financiera ha cambiado de sistemas basados en reglas a soluciones basadas en aprendizaje de máquina.

En los sistemas basados en reglas las actividades fraudulentas pueden ser detectadas al revisar algunas señales evidentes, por ejemplo, un gran número de transacciones inusuales o aquellas que ocurren en ubicaciones atípicas, este tipo de transacciones requieren una validación adicional.

4.4 Tipos y Métodos de Sistemas de Detección de Fraudes

En general existen dos tipos de sistemas de detección de fraudes, los tradicionales que son basados en reglas y los de Machine Learning.

Los sistemas basados en reglas usan algoritmos que analizan múltiples escenarios de detección de fraudes, donde los escenarios son comúnmente diseñados por los analistas de fraude. Actualmente estos sistemas aplican en promedio más de 300 reglas para aprobar una transacción, además requieren que los escenarios sean agregados o ajustados manualmente y difícilmente podrán detectar correlaciones implícitas.

En cuanto a los sistemas basados en Machine Learning son más sensibles para detectar eventos ocultos en el comportamiento de los usuarios que podrían no ser muy evidentes pero que son señales de posibles fraudes. Las técnicas de Machine Learning permiten crear algoritmos que pueden procesar una gran cantidad de datos con muchas variables y ayudar a encontrar las correlaciones ocultas entre el comportamiento de los usuarios y la probabilidad de que sean acciones fraudulentas. Otra fortaleza de este tipo de sistemas es que pueden procesar más rápido los datos y requiere un menor trabajo manual, también pueden ayudar a reducir el número de aplicaciones en los sistemas basados en reglas.

Las principales instituciones financieras ya están usando tecnologías de Machine Learning para combatir a los estafadores. Por ejemplo, en el 2016, MasterCard integró un sistema de Machine Learning e inteligencia artificial que procesa las transacciones, ubicación, hora, dispositivo y datos de la compra, este sistema evalúa el comportamiento de la cuenta en cada operación y provee una decisión en tiempo real de si la transacción es fraudulenta (Mastercard, 2020). El objetivo de este sistema es reducir el número de declaraciones falsas en los pagos en comercios.

4.5 Escenarios de fraude y técnicas más comunes de detección

La detección de fraudes no solamente ocurre en los servicios financieros de bancos, sino en otro tipo de ambientes como: seguros, sistema de salud, solicitudes de préstamos y lavado de dinero.

En la detección de reclamos falsos se suelen utilizar técnicas de análisis semántico que permiten analizar textos estructurados y no estructurados. Los algoritmos de aprendizaje de máquina analizan los reportes escritos por los agentes de seguros, policías y clientes en búsqueda de inconsistencias en las evidencias que se presentan. Algunos resultados de los análisis que han reportado algunas investigaciones, indican que, los reclamos falsos suelen no reportarse a la policía, los vehículos viejos suelen estar involucrados en fraudes y el 8% de los accidentes automovilísticos que ocurren durante las fechas navideñas involucran un fraude.

En cuanto a los seguros médicos y de salud son un área que suelen presentar fraudes debido a los procesos complejos y burocráticos, los cuales requieren muchas aprobaciones, verificaciones y papeleo. Los fraudes más comunes son el uso de números de seguros falsos, reclamos duplicados, cargos de pruebas médicas innecesarias, diagnósticos falsos, entre otros. Los hospitales y compañías de seguros sufren de estos problemas, las aseguradoras pierden dinero y los hospitales se ponen en riesgo al involucrarse en crímenes serios. Las técnicas de Machine Learning pueden ayudar a validar restricciones legales, a diversificar la secuencia de recetas médicas y encontrar enlaces sospechosos entre doctores y grupos de pacientes que en conjunto superan el límite de algún medicamento.

Las técnicas de reconocimiento de imagen pueden ser usadas en prevención de fraudes para la validación de identidad, ya que la entrega de medicamentos requiere ciertos pasos de verificación, pero los mecanismos actuales no son ideales por lo que el aprendizaje máquina puede ayudar a resolver problema de validación de identidad, mediante reconocimiento facial y huellas dactilares. En cuanto a los bancos y pago de tarjeta de crédito, los pagos son la parte que está más digitalizada en la industria financiera, lo cual la hace particularmente vulnerable a las actividades fraudulentas.

Los sistemas modernos de detección de fraude resuelven un gran rango de problemas, por ejemplo, la validación de datos y transacciones inusuales. En la validación de datos, algunas técnicas permiten identificar valores faltantes en la secuencia de transacciones donde los

algoritmos de Machine Learning pueden conciliar la documentación, esto asegura la credibilidad de los datos al encontrar inconsistencias en ella y verificando los detalles personales mediante fuentes públicas y el historial de las transacciones.

Para detección de transacciones inusuales se suele analizar el comportamiento del usuario durante las transacciones, en este caso la estadística descriptiva como los promedios, desviación estándar, valores altos y mínimos, son de gran ayuda para analizar el comportamiento. Estas métricas permiten comparar las transacciones por separado contra las transacciones más comunes del usuario, pagos con una gran desviación estándar suelen ser sospechosas, así que una buena práctica es enviar solicitudes de verificación a la cuenta del cliente. En cuanto a las solicitudes de préstamos éstas son sensibles a fraudes que abusan de la información personal, ya que hoy en día casi toda la información personal se puede encontrar en las redes sociales tales como fotos, direcciones y números telefónicos. Esto complica las obligaciones de las instituciones financieras, ya que requieren hacer validaciones más rigurosas mientras que los clientes esperan recibir el préstamo lo más pronto posible, en este escenario se presentan la falsificación de datos personales, el cual es un fraude muy común donde los infractores proveen datos que pueden malinterpretar los ingresos o las capacidades crediticias, lo cual hace que la deuda sea más difícil de recuperar, una forma de afrontar este escenario, es mediante la construcción de modelos de calificaciones o que calculen la probabilidad de fraude.

Los modelos de calificaciones calculan la posibilidad de fraude y la comparan contra una escala estándar, esto ayuda a evaluar qué solicitudes son más propensas a ser fraudulentas. El aprendizaje de máquina y el análisis avanzado resuelven el problema de evaluación de la probabilidad de fraude al clasificar las solicitudes en grupos, estas soluciones permiten minimizar los costos al reducir la necesidad de validar cada solicitud y concentrar los esfuerzos en los prestamos menos riesgosos, también ayuda a mejorar la calificación general de crédito al distinguir entre autores de fraude y morosos.

Un caso de estudio en un banco europeo, encontró que los algoritmos de aprendizaje de máquina detectaron un 52% más casos de fraude, además de que demostraron tener un puntaje de calificación nueve veces más alto que el método tradicional (Banco Central Europeo, 2016).

En el escenario de lavado de dinero las agencias reguladoras, bancos y firmas de inversión, usualmente están involucrados en el monitoreo de posibles actividades de lavado de dinero, ellas deben detectar e informar a los demás de actividades sospechosas, por ejemplo, en un estudio se entrenó un modelo de aprendizaje de máquina con un conjunto de datos con transacciones realizadas por criminales, este modelo combinado con un sistema basado en reglas ayudo a descubrir relaciones ocultas entre movimientos de dinero de actividades criminales. Sistemas de este tipo pueden minimizar la carga de trabajo de las agencias involucradas en el monitoreo (ACFCS, 2016).

Técnicas de Machine Learning que son utilizadas y algunas de sus ventajas.

La detección de anomalías es una de las estrategias más comunes en la ciencia de datos, ésta se basa en clasificar los datos en dos grupos: Los que están en la distribución normal y los atípicos.

Los atípicos en este caso son las transacciones que se desvían de las normales y son considerados como potencialmente fraudulentas.

Las variables en los datos que pueden ser usadas para la detección de fraudes son numerosas, estas van desde los detalles de las transacciones, imágenes y textos no estructurados. Al analizar esos parámetros los algoritmos de detección de datos anómalos pueden responder las siguientes preguntas:

- ¿Los clientes acceden a los servicios de la manera esperada?
- ¿Las acciones de los usuarios son normales?
- ¿Las transacciones son comunes?

- ¿Existen inconsistencias en la información entregada por los usuarios?

Las estrategias de detección de anomalías es quizá la más sencilla, ya que provee una respuesta binaria, la cual puede ser útil en algunos casos, por ejemplo, si la transacción luce sospechosa el sistema solicitará al usuario múltiples pasos de verificación.

La detección tradicional de anomalías no permite revelar si la transacción es fraudulenta, pero es un instrumento que apoya a los sistemas basados en reglas. Existen estrategias más avanzadas que combinan algoritmos de Machine Learning para reducir la incertidumbre, estos pueden ser construidos utilizando diversos modelos matemáticos. Hay dos tipos de estrategias del Machine Learning que son las más usadas en sistemas antifraude, los no supervisados y los supervisados, estos pueden ser usados independientemente o combinados.

- El aprendizaje supervisado entrena al algoritmo utilizando datos que han sido históricamente etiquetados, en este caso los datos existentes ya tienen asignada la variable objetivo y el propósito del entrenamiento es hacer que el sistema prediga esas variables en nuevos datos.
- El aprendizaje no supervisado procesa los datos no etiquetados y los clasifica en diferentes grupos detectando relaciones ocultas entre las variables.

Los métodos de Machine Learning más usados en detección de fraudes son: los bosques aleatorios, máquina de soporte vectorial, vecinos cercanos y redes neuronales.

- Los bosques aleatorios es un algoritmo el cual construye un árbol de decisión para clasificar las observaciones, este modelo selecciona una variable que habilita una división de las observaciones, esta división se repite múltiples veces, como resultado si quisiéramos visualizar cómo funciona el algoritmo, este luciría como un árbol. Para hacer predicciones más precisas los científicos de datos entrenan múltiples árboles de decisión con muestras aleatorias. Los bosques aleatorios son relativamente simples por lo que se podría desarrollar rápidamente un sistema antifraude. Algunas de las ventajas es que son rápidos y sencillos de implementar, además son considerados

como un predictores muy precisos y pueden trabajar con datos faltantes. Algunas de sus desventajas pueden caer en sobreajuste y si las clases están muy desbalanceadas entonces la calidad puede disminuir.

- Las máquinas de soporte vectorial usan un clasificador binario no-probabilístico, esto significa que el algoritmo divide los datos en dos categorías. La línea de división está definida por múltiples hiperplanos en un espacio multidimensional, entonces el algoritmo selecciona el hiperplano que separa mejor las observaciones. Dentro de sus ventajas es que son buenas para trabajar con datos multidimensionales y pueden evitar el sobreajuste, en cuanto a sus desventajas es que son computacionalmente lentas.
- Los vecinos cercanos es un algoritmo que clasifica las observaciones por similitud basándose en la distancia en un espacio multidimensional, las observaciones son asignadas a la clase que corresponde con el vecino más cercano. Cada observación es agrupada usando un parámetro de distancia, en sus ventajas tenemos que es insensible a los datos faltantes y al ruido, además son considerados de alta precisión, no requiere mucha ingeniería para ajustar el modelo. Dentro de sus desventajas es que requiere una gran infraestructura y carecen de interpretabilidad de los datos.
- En cuanto a las redes neuronales estos son modelos que permiten determinar relaciones no lineales entre las observaciones, el modelo es entrenado con datos etiquetados haciendo pasar los datos a través de múltiples capas que son funciones matemáticas. Entre sus mayores ventajas es que son buenas para entrenar relaciones no-lineales en grandes cantidades de datos, usualmente proveen una gran precisión, en sus desventajas tenemos que son difíciles de construir y ajustar, y requiere un alto poder de cómputo, además de que carecen de la interpretabilidad de los resultados.

En resumen, escoger el método de Machine Learning correcto depende del tipo de problema, tamaño de los datos y recursos, y un sistema anti fraude debe tener los siguientes estándares:

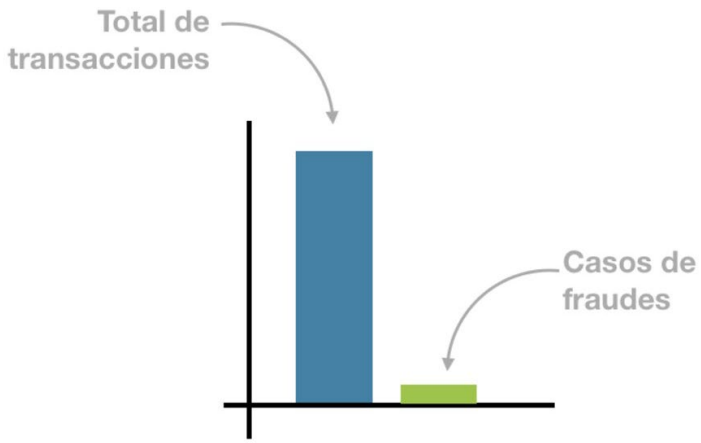
- Detectar los fraudes en tiempo real, mejorar la credibilidad de los datos, y
- Analizar el comportamiento del usuario, y descubrir correlaciones ocultas entre las variables.

4.6 Aproximación a un método para la evaluación de modelos de clasificación

Ante un posible evento de fraude, es necesario elaborar un modelo de clasificación para aproximarnos a su detección, como primer paso validándose a través de la siguiente pregunta: ¿Es el modelo, un modelo realista del problema que estamos direccionando?

El modelo exploratorio a desarrollar en este trabajo es de balanceo de datos, que básicamente consiste en explorar y recopilar un gran conjunto de datos para precisar las mediciones de posibles fraudes (IBM, 2020). Un ejemplo es cuando ocurren casos como la detección de fraudes con tarjetas de crédito, donde puede haber solo 1000 casos de fraude en más de un millón de transacciones, lo que representa el 0.1% del conjunto de datos.

Gráfica 13. Modelo de balance de datos



Fuente: Aprende IA, 2020

Debido a que el problema implica que la información no se encuentre distribuida equitativamente en todas las clases que la componen, generan efectos no deseados en el proceso de clasificación. Esto significa que alguna de las clases del conjunto de datos tiene una cantidad mucho mayor al resto. En este trabajo se considera el caso de conjuntos de datos que solamente tiene dos clases y una de ellas cuenta con una mayor cantidad de ejemplos que la otra, específicamente cuando están altamente desproporcionados. El interés principal es la aplicación de técnicas de balanceo de clases como método de preprocesamiento de datos en

el proceso de entrenamiento, para mejorar, en la medida de lo posible, los resultados de la clasificación.

Nuestro análisis corre con un conjunto de datos teórico de detección de fraudes, que contiene transacciones realizadas por tarjetahabientes, durante septiembre de 2013, en específico en tarjetahabientes europeos. Éste presenta transacciones que ocurrieron en un periodo de dos días, donde 169 fueron fraudes, de un total de 65,366 transacciones.

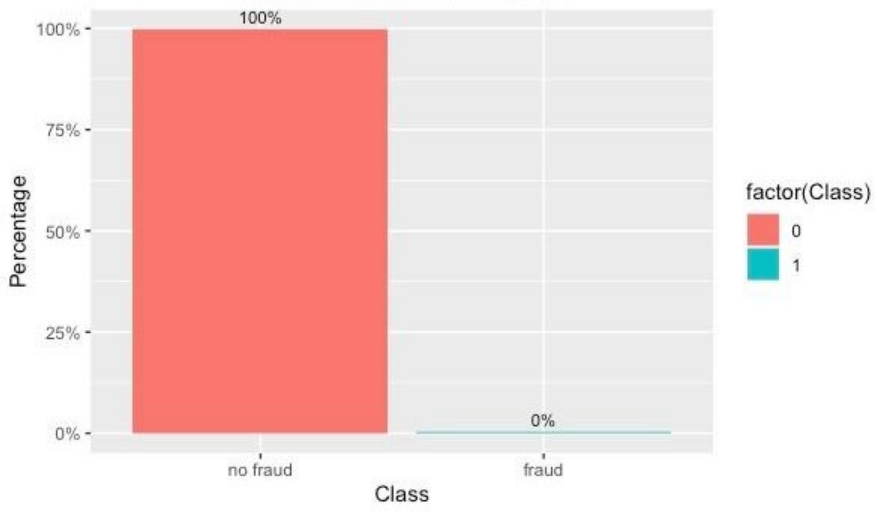
Tabla 15. Transacciones por clase

Transacciones	
Clase 0	Clase 1
65,366	169
99.74%	0.26%

Fuente: Elaboración propia

En la siguiente gráfica, podemos apreciar el volumen del porcentaje de transacciones de fraude contra las de no fraude:

Gráfica 14. Distribución de clases



Fuente: Elaboración propia

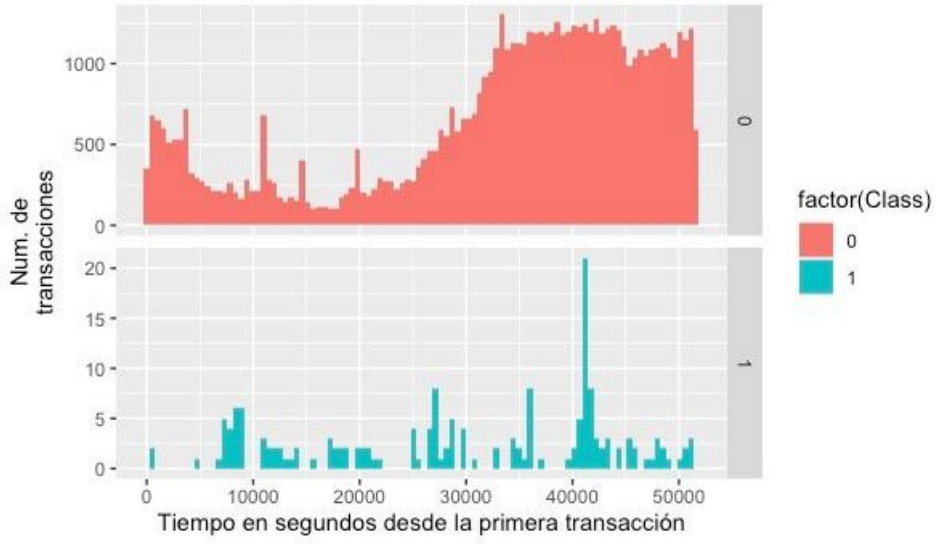
Como se puede notar con estas cifras, el conjunto de datos es altamente desbalanceado, los casos positivos que son fraude representan un 0.26% de todas las transacciones.

Realizaremos una exploración básica, únicamente para observar cómo están los datos y posteriormente realizar un proceso de balanceo de datos.

El conjunto de datos está determinado por 28 variables que son el resultado de una transformación por medio de un Análisis de Componentes Principales (PCA), por lo que las características o información que estén relacionadas con ellas no son las originales. Sin embargo, las únicas variables que no fueron transformadas son las variables "tiempo" y "monto". El "tiempo" contiene los segundos que han transcurrido entre cada transacción y la primera, mientras que la variable "monto" señala el monto de la transacción. Existe otra variable que llamaremos Clase, que es la variable de respuesta y puede tomar el valor de 1 en caso de fraude y 0 en caso contrario. En el apéndice podemos observar un resumen estadístico relacionado con cada variable.

A continuación, vamos a generar unas gráficas exploratorias para determinar cómo se distribuyen las transacciones de fraude y no fraude, esto con el fin de apreciar de forma visual un gran número que no son fraudes contra las que si son.

Gráfica 15. Distribución del tiempo por clase



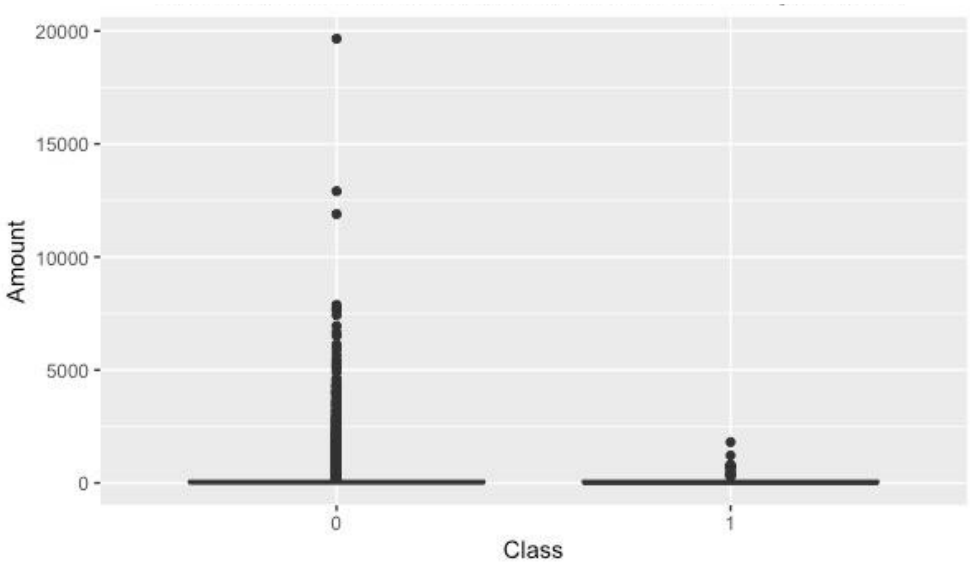
Fuente: Elaboración propia

Como notamos, en la gráfica anterior (color rojo) se muestra la distribución de las transacciones de no fraude durante el tiempo. Podemos ver que tiene una distribución creciente donde suponemos que el menor número de transacciones ocurren durante la noche, mientras que el mayor número en el día.

Por otra parte, el número de transacciones de fraude, sigue una distribución sesgada a la derecha, que es donde se encuentra el pico más alto.

Ahora, vamos a tratar de visualizar el número de montos por cada tipo de transacción:

Gráfica 16. Distribución del monto de las transacciones por clase

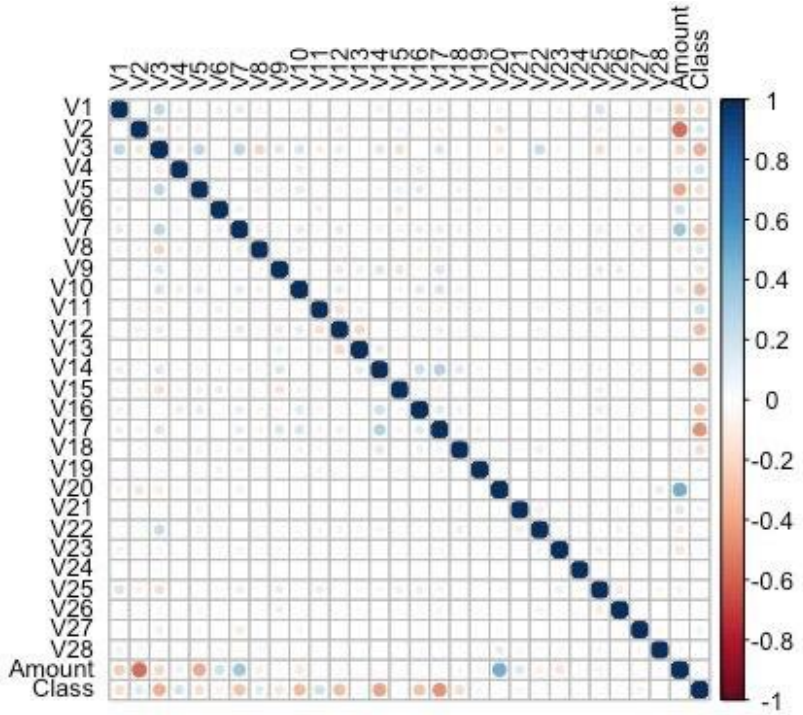


Fuente: Elaboración propia

En el Boxplot anterior, podemos apreciar la variabilidad de las transacciones de no fraude, por lo cual, vemos más puntos del lado izquierdo, mientras que del lado derecho ocurre lo contrario. Además de que las plot de ambas clases son más aplanados.

A continuación, vamos a generar una gráfica de correlación de las variables anonimizadas[2] y el monto:

Gráfica 17. Gráfica de correlación



Fuente: Elaboración propia

Como en el conjunto de datos se realizó un Análisis de Componentes Principales previo y, ya ha sido transformada la información, entonces no existe correlación. Sin embargo, solamente hay información con las variables de monto y clase.

El siguiente paso es generar una pequeña preparación de datos, donde vamos a buscar realizar el balanceo de datos. Por simplicidad, nos enfocaremos con las variables de monto y las transformadas. Cambiaremos la clase a factor y escalamos a variables numéricos, es decir, la clase 0 y 1 pasa a ser fraude y no fraude:

[2] La anonimización es el proceso de convertir los datos en una forma en que no se pueda identificar a individuos.

Tabla 16. Fraudes por clase

Clase	
0	Fraude
1	No Fraude

Fuente: Elaboración propia

Realizando una división de los datos en prueba y entrenamiento para poder calibrar los modelos que se utilizarán, se realiza un Split, que es la división de los datos en diferentes grupos. En este caso será de las transacciones de la clase. Vamos a pedir un 70% de datos de cada tipo de clase y generamos dos datos, que serán los de entrenamiento y prueba.

A continuación, vamos a ver el número de observaciones que quedo en cada conjunto:

Tabla 17. Número de observaciones por entrenamiento

Entrenamiento	
No fraude	Fraude
45,576	118

Fuente: Elaboración propia

Podemos ver que, en este conjunto de entrenamiento tenemos 45,576 que no son fraude y 118 que son fraude.

Tabla 18. Número de observaciones por prueba

Prueba	
No fraude	Fraude
19,610	51

Fuente: Elaboración propia

Por su parte, en el de prueba hay 19,610 que no son fraude y 51 que son fraude.

Podemos decir que, con esta herramienta trataremos de aproximarnos a balancear los datos para determinar los casos posibles de fraude, que ayudarán a las instituciones bancarias a reconocer las transacciones fraudulentas con tarjetas de crédito, con el fin de que a los clientes no se les cobre por artículos que no compraron.

Con lo mencionado anteriormente, únicamente nos aproximamos a explorar las herramientas más importantes que generarán un preprocesamiento de datos, para mejorar, en la medida de lo posible, la detección de fraudes.

Conclusiones

En este trabajo, se ha analizado la relación entre dinero-fraude, visto desde una problemática en un sistema de pagos. Una fuerte presión para adoptar la digitalización ha provocado un aumento del fraude, por ello es importante contar con las herramientas y mecanismos que aseguren las transacciones que los gobiernos, empresas y hogares realizan a nivel local e internacional.

En la detección de fraudes financieros, los conjuntos de datos a menudo tienen una distribución desequilibrada de clases, donde la clase positiva representa un pequeño porcentaje del conjunto de datos en comparación con la clase negativa. Esto puede dificultar el entrenamiento de un modelo de detección de fraudes preciso, ya que el modelo puede sesgarse hacia la clase mayoritaria. El modelo de balance de datos se utiliza para equilibrar la distribución de clases en el conjunto de datos, lo que ayuda a mejorar el rendimiento y la precisión del modelo de detección de fraudes. Como se desarrolló en éste trabajo, esto se logra mediante la aplicación de técnicas de submuestreo o sobre muestreo a la clase mayoritaria o minoritaria, respectivamente, para crear un conjunto de datos balanceado. Una vez que el conjunto de datos está equilibrado, se puede entrenar un modelo de detección de fraudes utilizando algoritmos de aprendizaje supervisado, como árboles de decisión, regresión logística o redes neuronales. El modelo se puede ajustar y evaluar utilizando técnicas como la validación cruzada y la curva ROC para maximizar su precisión en la detección de fraudes.

En específico, pudimos ver que, la mayoría de las transacciones son legítimas, mientras que solo una pequeña fracción es fraudulenta. Esta distribución desequilibrada de clases puede

dificultar el entrenamiento de un modelo de detección de fraudes preciso, ya que el modelo puede sesgarse hacia la clase mayoritaria y no detectar adecuadamente las transacciones fraudulentas.

En resumen, para abordar este problema, el modelo de balance de datos fue una técnica de preprocesamiento útil en la detección de fraudes financieros para equilibrar la distribución de clases en los conjuntos de datos desequilibrados, lo que puede mejorar la precisión del modelo y reducir el sesgo hacia la clase mayoritaria.

La aplicación de estos instrumentos de detección de fraudes nos permite definir un enfoque diferente e innovador en cada una de los procesos de los sistemas de pagos, llegando a una solución a través de diversas técnicas para evaluar, capturar información y conocer aún más a los agentes que intervienen en cada una de las transacciones, proponiendo un diseño basado en el producto o sistema, a fin de tener un diagnóstico eficiente del fraude, identificando los patrones y comportamientos a través de los sistemas de pagos.

Apéndice

```
      Time             V1                 V2                 V3          
 Min.   :    0   Min.   :-56.4075   Min.   :-72.71573   Min.   :-32.9654  
 1st Qu.:27762   1st Qu.: -1.0006   1st Qu.: -0.58593   1st Qu.:  0.1977  
 Median :36958   Median : -0.2432   Median :  0.07481   Median :  0.7739  
 Mean   :33453   Mean   : -0.2404   Mean   : -0.01314   Mean   :  0.6839  
 3rd Qu.:43935   3rd Qu.:  1.1539   3rd Qu.:  0.73049   3rd Qu.:  1.4079  
 Max.   :51630   Max.   :  1.9605   Max.   : 18.18363   Max.   :  4.2261  
       V4                 V5                 V6                 V7          
 Min.   :-5.1726   Min.   :-42.1479   Min.   :-26.1605   Min.   :-31.76495  
 1st Qu.:-0.7240   1st Qu.: -0.8847   1st Qu.: -0.6365   1st Qu.: -0.60300  
 Median : 0.1891   Median : -0.2986   Median : -0.1491   Median : -0.07303  
 Mean   : 0.1714   Mean   : -0.2666   Mean   :  0.1033   Mean   : -0.11335  
 3rd Qu.: 1.0546   3rd Qu.:  0.2729   3rd Qu.:  0.4951   3rd Qu.:  0.42201  
 Max.   :16.7155   Max.   : 34.8017   Max.   : 22.5293   Max.   : 36.67727  
       V8                 V9                 V10                V11          
 Min.   :-73.21672   Min.   :-9.28392   Min.   :-18.27117   Min.   :-4.0499  
 1st Qu.: -0.14252   1st Qu.:-0.66309   1st Qu.: -0.51436   1st Qu.:-0.4823  
 Median :  0.06516   Median :-0.05806   Median : -0.10079   Median : 0.2560  
 Mean   :  0.05943   Mean   : 0.03664   Mean   : -0.04186   Mean   : 0.3136  
 3rd Qu.:  0.34264   3rd Qu.: 0.69501   3rd Qu.:  0.43092   3rd Qu.: 1.1171  
 Max.   : 20.00721   Max.   :10.39289   Max.   : 13.19823   Max.   :12.0189  
      V12                V13                V14                V15          
 Min.   :-17.76914   Min.   :-5.79188   Min.   :-19.2143   Min.   :-4.1525  
 1st Qu.: -0.68112   1st Qu.:-0.63241   1st Qu.: -0.3198   1st Qu.:-0.4083  
 Median :  0.04179   Median : 0.05013   Median :  0.1078   Median : 0.2571  
 Mean   : -0.20988   Mean   : 0.09041   Mean   :  0.1138   Mean   : 0.1482  
 3rd Qu.:  0.58366   3rd Qu.: 0.79038   3rd Qu.:  0.5682   3rd Qu.: 0.8257  
 Max.   :  7.84839   Max.   : 4.46541   Max.   : 10.5268   Max.   : 5.7845  
      V16                V17                V18                V19          
 Min.   :-13.56327   Min.   :-25.16280   Min.   :-9.49875   Min.   :-7.21353  
 1st Qu.: -0.49207   1st Qu.: -0.37942   1st Qu.:-0.56971   1st Qu.:-0.51677  
 Median :  0.05916   Median :  0.03214   Median :-0.08216   Median :-0.02823  
 Mean   : -0.01107   Mean   :  0.08975   Mean   :-0.09405   Mean   :-0.02255  
 3rd Qu.:  0.54605   3rd Qu.:  0.50245   3rd Qu.: 0.39768   3rd Qu.: 0.48509  
 Max.   :  6.09853   Max.   :  9.25353   Max.   : 5.04107   Max.   : 5.22834  
    V20                V21                V22                V23          
 Min.   :-15.80648   Min.   :-34.83038   Min.   :-10.9331   Min.   :-26.75112  
 1st Qu.: -0.16671   1st Qu.: -0.22689   1st Qu.: -0.5267   1st Qu.: -0.17961  
 Median : -0.02303   Median : -0.06201   Median : -0.0815   Median : -0.05189  
 Mean   :  0.04813   Mean   : -0.02849   Mean   : -0.1068   Mean   : -0.03920  
 3rd Qu.:  0.17256   3rd Qu.:  0.11451   3rd Qu.:  0.3085   3rd Qu.:  0.07891  
 Max.   : 39.42090   Max.   : 22.61489   Max.   : 10.5031   Max.   : 17.29784  
      V24                V25                V26                V27          
 Min.   :-2.836627   Min.   :-7.4957   Min.   :-2.53433   Min.   :-8.567638  
 1st Qu.:-0.326128   1st Qu.:-0.1276   1st Qu.:-0.32942   1st Qu.:-0.062834  
 Median : 0.061280   Median : 0.1745   Median :-0.07627   Median : 0.009427  
 Mean   : 0.005713   Mean   : 0.1368   Mean   : 0.01995   Mean   : 0.002271  
 3rd Qu.: 0.402888   3rd Qu.: 0.4231   3rd Qu.: 0.29674   3rd Qu.: 0.082503  
 Max.   : 4.014444   Max.   : 5.5251   Max.   : 3.51735   Max.   :11.135740  
      V28                Amount              Class         
 Min.   :-9.61792   Min.   :    0.00   Min.   :0.000000  
 1st Qu.:-0.00588   1st Qu.:    7.68   1st Qu.:0.000000  
 Median : 0.02274   Median :   26.20   Median :0.000000  
 Mean   : 0.00421   Mean   :   96.24   Mean   :0.002579  
 3rd Qu.: 0.07617   3rd Qu.:   88.13   3rd Qu.:0.000000  
 Max.   :33.84781   Max.   :19656.53   Max.   :1.000000  
```

Bibliografía

Levy, S. (29 de Octubre de 1995). The End of Money? *Newsweek*.

CNBV. (2022). *Panorama Anual de Inclusión Financiera 2021*. Comisión Nacional Bancaria y de Valores.

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (04 de Junio de 2018). Obtenido de http://www.gob.mx/condusef/prensa/usuarios-de-la-banca-pueden-tardar-hasta-100-dias-en-saber-que-fueron-victimas-de-fraude.

Los Angeles Times. (13 de Enero de 2022). La pandemia dispara el número de fraudes bancarios por internet en México. Obtenido de https://www.latimes.com/espanol/mexico/articulo/2022-01-13/la-pandemia-dispara-el-numero-de-fraudes-bancarios-por-internet-en-mexico#:~:text=M%C3%A9xico%20cerr%C3%B3%20el%20a%C3%B1o%202021,de%20Servicios%20Financieros%20(Condusef).

ACFCS. (2016). *Delitos Financieros*. Obtenido de https://www.delitosfinancieros.org/inteligencia-artificial-y-aprendizaje-automatico-para-descubrir-vinculacion-entre-grupos-criminales-y-mejorar-las-alertas/.

ASIS. (2021). *Security Management*. Obtenido de https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/espanol/el-escenario-mundial-del-fraude/.

Baliño, T., & Sundarajan, O. J. (1996). Reforma de los sistemas de pagos y política monetaria. *Finanzas & Desarrollo*, 2-5.

Banco Central Europeo. (2016). Obtenido de https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180926.en.html.

Banco de México. (2018). *Información sobre los Ataques a Participantes del Sistema de Pagos Electrónicos Interbancarios.* Ciudad de México.

Banco de México. (2022). *Introducción a los sistemas de pago*. Obtenido de Banco de México: https://www.banxico.org.mx/sistemas-de-pago/introduccion-sistemas-pago-tr.html.

Banco de México. (2023). Obtenido de Banco de México: https://www.banxico.org.mx/sistemas-de-pago/introduccion-sistemas-pago-tr.html.

Banco de Pagos Internacionales. (1998). *PRINCIPIOS BASICOS PARA LOS SISTEMAS DE PAGO IMPORTANTES A NIVEL SISTEMICO.* Basilea, Suiza: Banco de Pagos Internacionales.

Banco de Pagos Internacionales. (2003). *Buenas prácticas para la gestión y supervisión de riesgo operativo.* Suiza: Comité de Supervisión Bancaria de Basilea.

Banco Interamericano de Desarrollo. (2017). *FinTech: Innovaciones que no sabías que eran de América Latina y el Caribe.* BID.

Bromium. (2018). *Hyperconnected web of profit emerges, as global cybercriminal revenues hit $1.5 trillion annually.* Bromium Inc.

Digital Finance Institute. (2016). *FinTech in Canada.* Canada: British Columbia Edition.

Eisenberg, L., & Noe, T. H. (1999). Systemic Risk in Financial Networks.

European Systemic Risk Board. (2020). *The making of a cyber crash: a conceptual model for systemic risk in the financial sector.* European Systemic Risk Board Occasional Paper Series No 16.

Fondo Monetario Internacional. (2022). *Financial Access Survey 2022 Trends and Developments.* International Monetary Fund, Statistics.

Guerra, J. S. (1997). *Moneda y Delincuencia: Siglos XVI al XVIII.*

IBM. (2020). *IBM Cloud Learn Hub*. Obtenido de https://www.ibm.com/mx-es/cloud/learn/exploratory-data-analysis.

KPMG. (2020). *El impacto de los delitos financieros, Prevención, detección y respuesta.* Ciudad de México: Delinieando Estrategias, Una visión de KPMG.

Mastercard. (2020). *Engagement Bureau*. Obtenido de https://newsroom.mastercard.com/eu/es/press-releases/mastercard-lanza-una-solucion-con-inteligencia-artificial-para-mejorar-la-seguridad-y-conveniencia-de-los-pagos-electronicos/.

OEA y CNBV. (2019). *Estado de la Ciberseguridad del Sistema Financiero Mexicano.* Ciudad de México: Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la OEA.

PriceWaterHouseCoopers. (2009). *Fraude en tiempos de crisis. Un análisis de como el fraude y otros riesgos de integridad afectarán el negocio en el año 2009.* Ciudad de México: PriceWaterHouseCoopers.

Tavera, G. R. (22 de Abril de 1998). Comercio electrónico ¿moda o necesidad? *Expansión*, págs. 85-88.

Vera, S. (1995). *El desarrollo de la Banca Central en Inglaterra y el sistema escocés.* Libretas 23.