Un enfoque para hacer benchmark a los algoritmos para la detección de fraude en la era COVID-19

Revista Latinoamericana de Economía y Sociedad Digital

Issue 2, agosto 2021

Autores: Miroslawa Alunowska Figueroa, Daniel Turner-Szymkiewicz, Juan Sebastián Cárdenas-Rodriguez, Ulf Norinder, Edgar Alonso Lopez-Rojas

DOI: 10.53857/EORG4750

Publicado: 25 agosto, 2021

Recibido: 21 marzo, 2021

Cita sugerida: Alunowska Figueroa, Miroslawa; Turner-Szymkiewicz, Daniel; Alonso Lopez-Rojas, Edgar; Cárdenas-Rodriguez,Juan Sebastián & Norinder, Ulf (2021) "An approach to benchmark fraud detection algorithms in the COVID-19 era" en Revista Latinoamericana de Economía y Sociedad Digital, Issue 2

Tipo: Ensayo

Palabras clave: aprendizaje automático, COVID-19, datos sintéticos para las finanzas, fraude en pagos digitales, simulación de benchmark

---

Resumen

Para afrontar los desafíos en la lucha contra los delitos financieros, especialmente en el contexto de la pandemia del COVID-19, este artículo focaliza en los datos sintéticos financieros y en el uso de una herramienta de benchmark confiable para evaluar los algoritmos de detección de fraude. Los departamentos de control de cumplimiento de las instituciones financieras enfrentan el desafío de reducir el número de personas inocentes a las que se las acusa de fraude por error. Para enfrentar este problema, las instituciones financieras están investigando la aplicación de algoritmos de aprendizaje automático para la detección de fraude y la tecnología de análisis de datos para desarrollar un sistema de detección del fraude más exacto y preciso. Sin embargo, los enfoques para la optimización y la automatización del control bancario y los procesos de testeo son desafiantes ya que no

existe consenso en un benchmark. Investigamos la importancia de medir la aplicación de un benchmark para detectar los delitos financieros ante un sector financiero digital en crecimiento, como es el caso de México. Este estudio cobra especial importancia debido a las serias amenazas que enfrenta un sistema financiero que se está desarrollando rápidamente. (Informe del Banco Central de México 2019) Estos riesgos se han empeorado aún más como resultado de los cambios acelerados hacia los pagos digitales como producto de la pandemia COVID-19.

Abstract

To address the challenges in the fight against financial crime, particularly in the COVID-19 pandemic context, this paper focuses on financial synthetic data and the use of a reliable benchmark tool to test fraud detection algorithms. Compliance departments at financial institutions face the challenge of reducing the number of innocent people erroneously accused of fraud. To cope with this problem financial institutions are exploring the application of machine learning fraud detection algorithms and data analysis technologies to develop a more accurate and precise fraud detection system. However, approaches to streamlining and automating banks' monitoring and testing processes is challenging as there is no consensus on a benchmark. We explore the relevance of measuring the applicability of a financial crime benchmark in the presence of a growing digital financial sector, such as in the case of Mexico. This study is particularly important due to serious threats that are faced by a rapidly developing financial system (2019 Mexican Central Bank Report). These risks have been further exacerbated as a result of the COVID-19 pandemic accelerating the shift towards digital payments.

Resumo

Para enfrentar os desafios na luta contra o crime financeiro, particularmente no contexto da pandemia da COVID-19, este artigo se concentra em dados sintéticos financeiros e no uso de uma ferramenta de referência confiável para testar algoritmos de detecção de fraude. Os departamentos de compliance de instituições financeiras enfrentam o desafio de reduzir o número de pessoas inocentes erroneamente acusadas de fraude. Para lidar com esse problema, as instituições financeiras estão explorando a aplicação de algoritmos de detecção de fraude que envolvem aprendizado de máquina e tecnologias de análise de dados para desenvolver um sistema de detecção de fraude mais preciso. No entanto, as abordagens para agilizar e automatizar os processos de monitoramento e teste dos bancos são desafiadoras, pois não há consenso sobre a referência a ser utilizada. Nós exploramos a relevância de medir a aplicabilidade de uma referência de crime financeiro diante de um crescente setor financeiro digital, como no caso do México. Este estudo é particularmente importante devido às sérias ameaças que um sistema financeiro em rápido desenvolvimento

enfrenta (Relatório do Banco Central do México de 2019). Esses riscos foram ainda mais exacerbados como resultado da pandemia da COVID-19, que acelerou a mudança para pagamentos digitais.

Introducción

La pandemia COVID-19 ha causado un cambio en la sociedad para convencer a las personas que adopten las plataformas de pago digital como la forma primaria de pago (Pandea et al., 2020). Sin embargo, juntamente con el cambio en las actividades del consumidor, vemos una evolución en el fraude que saca ventaja de las vulnerabilidades en los sistemas de pago digital que aparecen en el despertar de cambios tan sustanciales. (Karpoff, 2020). El fraude financiero requiere un amplio conocimiento de los protocolos y sistemas de acceso a las cuentas y los servicios de transferencia; por lo tanto, los bancos han hecho grandes esfuerzos para incrementar la inversión en la seguridad y la protección contra el fraude (van Dril, 2019). Además, estos problemas requieren nuevas formas de sistemas de control para adaptarse rápidamente a las circunstancias contemporáneas. Se ha presentado una solución nueva a este tema como un *benchmark* [1] que puede medir de manera apropiada el funcionamiento de un sistema de control de una transacción. Sin embargo, este desafío presenta uno de los obstáculos más importantes que las instituciones financieras enfrentan hoy.

Las instituciones financieras ponen a punto sus sistemas de control de acuerdo con las normas aplicables, estas pueden estar divididas en dos objetivos claros: detectar y prevenir la actividad delictiva (aumentando los verdaderos positivos) y reducir el número de personas inocentes que son acusadas erróneamente de fraude (reduciendo los falsos positivos) El

esfuerzo de las instituciones financieras para lograr estos objetivos se haya obstaculizado, especialmente por la incapacidad de evaluar de manera correcta la cantidad real de falsos negativos (fraude inadvertido) presente en el conjunto de datos, ya que otorgan indicadores convencionales de detección con poco valor para evaluar el alcance mayor del delito financiero.

El *Deep Learning* (DL) ha sido capaz de desempeñar un papel más efectivo en encontrar la correlación escondida entre el algoritmo de la detección de fraude del aprendizaje automático del usuario, incluso los avances recientes en un aprendizaje profundo y las acciones de fraude. Sin embargo, muchos de estos algoritmos con frecuencia se desarrollan con un input mínimo de un analista y dependen considerablemente de los datos que se otorgan. En sí mismos representan una capa de profundidad adicional en la adopción/ establecimiento de estándares técnicos para crear las mejores prácticas. Todavía es un tema corriente de debate en la industria. Esto es particularmente verdadero dentro de la evaluación del sesgo o evaluación de la imparcialidad de los datos, ya que los modelos de

aprendizaje automático entrenados en un conjunto de datos sesgados causarán sesgo/ discriminación sin intención (Das et al., 2020).

La carrera tecnológica entre el fraude y la seguridad tiene grandes ramificaciones que con frecuencia se reconocen mucho más tarde. Para hacer frente al fraude con rapidez, se introduce con frecuencia un modelo menos sólido, que puede tener tendencia a influenciar a través de las clasificaciones erróneas en los nuevos datos entrantes. Además, para tratar de evitar este enfoque y organizar los datos históricos, las instituciones financieras arriesgan una pérdida de privacidad. Creemos que el uso adecuado de datos sintéticos de referencia puede ayudar a atenuar en gran parte este problema, y por lo tanto reducir la preocupación por el sesgo y la privacidad en la esfera del cumplimiento.

Las normas de confidencialidad restringen muchos datos que pueden usarse para regular el entrenamiento de un modelo adecuado (Zhang et al., 2020) y así se reduce de manera significativa la posibilidad de colaboración entre los diferentes interesados para mejorar las herramientas del control del fraude que pueden prevenir delitos financieros, sesgos y pérdida de privacidad. Una parte fundamental de la solución a estos problemas requerirá una respuesta combinada de la generación de conjunto de datos sintéticos enriquecidos y los indicadores adecuados que pueden hacer un *benchmark* del funcionamiento y la eficacia de los algoritmos de aprendizaje automático que operan como parte de los sistemas de control de las transacciones.

2. Antecedentes y contexto

México es la segunda economía más grande en Latinoamérica y ocupa el lugar 15 entre las economías más grandes del mundo (World Bank, 2020). Tiene un sector financiero muy sólido y un sector bancario bien capitalizado que está compuesto por bancos trasnacionales, bancos nacionales y nuevas empresas especializadas en tecnología financiera (OCDE, 2019). A pesar de ser un trampolín para la internalización de la región, casi la mitad de su población adulta no utiliza el ecosistema bancario. En México, «el efectivo es el rey», aún con la inclusión de soluciones digitales para cooperar con la pandemia, solo 37% de los adultos posee una cuenta bancaria (CNBV, 2020). Esto cobra especial importancia en el sur de México (OCED, 2019) donde algunas áreas han creado su propia moneda alternativa: Tumin (Saldivar and Zavaleta, 2020). Existen diversos factores que han llevado a esta situación, como por ejemplo un alto grado de informalidad económica, bajos ingresos, desconfianza en el sistema bancario, altas comisiones, altas tasas de interés, desprecio por los impuestos y pocos productos para los segmentos de bajos ingresos. Todos los temas mencionados anteriormente sirven como barreras para la inclusión financiera.

A los individuos que son parte de la economía informal les preocupa que parte de sus ganancias vaya a los impuestos, lo que, según su punto de vista, significa menos ingresos. No es inusual que los individuos desconfíen de los bancos y se refieran a ellos como entidades que les «roban» el dinero. Este sentimiento se refuerza aún más al conocer que

los bancos mexicanos son muy rentables (Estañol, 2019) (Juarez, 2015). En promedio, se atribuye 30% del ingreso de los bancos comerciales mexicanos a las comisiones (Condusef, 2017) y las tasas de interés son alrededor del 30 % para las tarjetas, mientras que las pequeñas empresas enfrentan altos costos en los préstamos (OCDE, 2019).

La inclusión financiera le permite a la gente y a los negocios acceder a productos financieros útiles y rentables (World Bank, 2018), lo que ha sido una principal prioridad en México en los últimos 20 años. Para lograr el impacto deseado, se deben establecer marcos y políticas regulatorias (Naghavi, 2020). Uno de los programas más recientes del gobierno que puede ser considerado como un avance en Latinoamérica para la inclusión financiera en la Política de Inclusión Financiera Nacional 2020-2024 (OCDE/CAF, 2020). El programa tiene como objetivo incrementar el número de mexicanos con cuenta bancaria de un 47% en 2020 a un 65% en los próximos cuatro años (SHCP/Ministerio de Educación Pública de la Nación, 2020). Es una colaboración entre el Banco de México (Banxico), el Ministerio de Finanza y Crédito Público (SHCP) y el Ministerio de Educación Pública, construido sobre varias acciones en los últimos 20 años para promover la inclusión financiera. Entre algunas de las acciones relevantes elegidas podemos mencionar:

– El Sistema de Pagos Electrónicos Interbancarios o SPEI® (en 2005), permitir que los negocios (por ejemplo, una popular cadena de tiendas de conveniencia es Oxxo) sean agentes para las instituciones financieras y actúen como intermediarios para el pago de los servicios públicos, retiros o consultas del saldo de la cuenta bancaria (en 2008).

– La creación del Departamento de Inclusión Financiera (en 2009) y sus encuestas (CNBV/INEGI 2012, 2015, 208).

– Política de Inclusión Financiera Nacional 2016

– Ley de Tecnología Financiera (en 2018)

– Plataforma de pago digital o Compra Digital «CoDi» que se basa en los códigos QR y el campo cercano de la tecnología de la comunicación (en 2019)

Del mismo modo que en otros países, la banca digital se ha considerado un componente esencial para lograr la inclusión financiera (Morales Guzman, 2018), (Alonso Fernández de Lis, Hoyo, López-Moctezuma and Tuesta, 2013), (Maina, 2019). El gobierno mexicano se refiere a Alipay como una historia de éxito de tal logro (CNBV, 2020).

Una parte de las soluciones de pago digital son tanto públicas como privadas: Samsung Pay, Apple Pay, CoDi, Rappi Pay, PayPal, MercadoLibre. La figura 1 describe una visión general del ecosistema móvil mexicano; entre los comerciantes y los clientes existen varios actores: instituciones financieras (bancos); autoridades regulatorias (por ejemplo Banxico y SHCP), tecnología de internet (por ejemplo, fibra óptica y tecnología 4G) y su infraestructura, proveedores de servicios móviles (por ejemplo Telcel) modelos de pago Móvil (por ejemplo, Paypal, Apple Pay), dispositivos (por ejemplo, Samsung) y fabricantes de chips, redes de

tarjetas (ej. Visa, Mastercard, American Express), procesadores de pago, proveedor de servicios de pago/plataforma de pago, puntos de venta, fabricantes y redes de pago.

Figura 1: Panorama general del Ecosistema Móvil Mexicano. Entre los comerciantes y los clientes existen varios actores: las Instituciones Financieras (bancos); las autoridades regulatorias (por ejemplo Banxico y SHCP), la tecnología de internet (por ejemplo fibra óptica y tecnología 4G) y su infraestructura, los proveedores de servicios móviles (por ejemplo Telcel), los modelos de pago móvil (por ejemplo, Paypal, Apple Pay), los dispositivos (por ejemplo, Samsung) y los fabricantes de chips, redes de tarjetas (por ejemplo, Visa, Mastercard, American Express), los procesadores de pago, los proveedores de servicios de pago/plataforma de pago, puntos de venta, fabricantes y redes de pago.

El Sistema Financiero Mexicano está estructurado con dos actores principales en juego; las autoridades financieras o los entes reguladores y las instituciones financieras. La figura 2 representa el panorama general del Sistema Financiero. Los dos entes reguladores más importantes son el Banco de México (Banxico), que ha sido autónomo desde 1994 y el Ministerio de Finanza y Crédito Público (SHCP). Es importante destacar que México es observador de la Convención de Budapest en los delitos cibernéticos y que sus regulaciones se alinean con los entes reguladores internacionales como por ejemplo el Comité de Basilea. Además. el sector bancario está regulado por la Comisión Nacional Bancaria y de Valores (CNBV), que es parte de SHCP y cumple con el reglamento de sistema de pagos y

transfer

Figura 2: Panorama general del Sistema Mexicano financiero.

Continuamente se actualiza el marco regulatorio, una de las reformas más significativas ocurrió en el año 2014 para estimular el acceso a los productos y a la inclusión financiera (Avendaño Carbellido, 2016). Por lo tanto, el derecho bancario se ha adaptado a los avances de la tecnología también (Avendaño Carbellido, 2017). Dos instrumentos legales son particularmente relevantes: la Ley de Instituciones de Crédito (DOF, 1990) y la Ley de Tecnología Financiera (DOF, 2018). El artículo 142 de la Ley de Instituciones de Crédito legisla el secreto bancario, mientras que el artículo 115 solicita el restablecimiento de medidas y procesos para prevenir o detectar el delito como esté definido por los artículos 139, 148 o 400 del Código Penal Federal.

La ley fintech, considerada un hito para la legislación en el sector financiero de América Latina, introduce un régimen normativo para las aperturas bancarias y cubre tres tipos de compañías fintech: las instituciones de pago electrónico, las instituciones para la administración de activos en las instituciones de financiamiento colectivo. El artículo 58 de la Ley de Tecnología Financiera regula el establecimiento de medidas y procedimientos para prevenir o detectar el delito. La Unidad de Inteligencia financiera (UIF) es responsable de llevar a cabo estos procedimientos, un organismo institucional centrado en implementar políticas para combatir el lavado de dinero y el terrorismo financiero, originalmente provenía de la participación de México en el Grupo de Acción Financiera (GAFI) El GAFI es una organización intergubernamental fundada por iniciativa del G7 para desarrollar políticas para combatir el lavado de dinero.

De acuerdo con el Informe del Banco Central de México, los riesgos cibernéticos eran una de las amenazas más serias que enfrentaba el sistema financiero mexicano (Banco de México, 2019). Estos riesgos se han empeorado como resultado del cambio acelerado hacia los pagos digitales provocados por la pandemia COVID-19 (Procuraduría Federal del Consumidor, 2020). Los delincuentes han tomado la oportunidad de aprovechar la emergencia sanitaria y se fijaron como meta a los individuos vulnerables a través del fraude cibernético. Por ejemplo, se calcula que se registraron 4 millones de denuncias en el tercer trimestre de 2020 Además, revela una proporción más grande de fraudes desde el 32% en 2016 al 69% en 2020 (Condusef, 2020). Asimismo, en el tercer trimestre de 2020 las

denuncias por fraude en el comercio electrónico alcanzaron 4.1millones y las denuncias por fraudes en las transacciones bancarias alcanzaron 142.000. La suma total del fraude cibernético alcanzó los 8 millones de pesos mexicanos (UDS430.000). 85% de estas quejas se resolvieron a favor del usuario y las instituciones financieras tuvieron que cubrir el costo de la compensación.

Los datos de la Agencia de Protección Financiera al Consumidor (Consudef) muestran que en promedio ocurren por hora 463 transacciones por fraude en el comercio electrónico y la banca móvil como resultado de estafas. La situación es tan grave que el organismo legislativo decidió intervenir (Senado de la República,2020) En marzo del 2021, el Comité Económico del Senado aprobó un proyecto de ley para combatir el fraude cibernético mediante el incremento de protección del usuario y el aumento de las campañas mediáticas (Senado de la República, 2021).

Los bancos utilizan los sistemas de gestión de tesorería (TMS, por sus siglas en inglés) como uno de los sistemas centrales en las áreas de capacidad de cumplimiento (Figura 3). Generalmente existen tres áreas de capacidad de cumplimiento en prevención de lavado de dinero y programas de cumplimiento contra la financiación del terrorismo (AML/CFT, por sus siglas en inglés): Capital Humano, Sistemas de Control y Gestión por Procesos. Un TMS controla las transacciones de los clientes todos los días o en tiempo real, a medida que la cantidad de transacciones asciende, también lo hace la complejidad del control. En consecuencia, esta dificultad se incrementó durante el curso de la pandemia. Un TMS efectivo debería permitir que las instituciones financieras evaluaran si las transacciones de los clientes son legítimas o sospechosas de acuerdo con su propio historial. Sin embargo, la efectividad de estos sistemas no es ideal y puede generar múltiples gastos. Por ejemplo, existe un gasto operativo en el servicio al cliente cuando la transacción se señala como fraudulenta y es legítima. Mientras que cuando el sistema aprueba un fraude, los costos son reintegrados y el valor de la transacción. Asimismo, el cliente puede sentirse disconforme por el servicio otorgado y llevar su capital a otro lugar.

Un TMS debe actualizarse constantemente para adaptarse a los pasos veloces de los avances tecnológicos, la sofisticación de la actividad delictiva y los requisitos normativos de cumplimiento cada vez más estrictos. Las instituciones financieras encuentran dificultades en seguir el rastro del desarrollo y comparar su desempeño de cumplimiento. Por cierto, muchos directores de cumplimiento están cada vez más preocupados por respetar las normas de cumplimiento lo que demuestra a los reguladores que las instituciones están con iniciativa de identificar a las actividades ilícitas. A pesar de que las instituciones financieras hayan invertido mucho en tecnología que apoye el marco del cumplimiento, la automatización de esta tecnología ha demostrado ser difícil de implementar ya que requiere constante atención y actualizaciones que necesitan mucho tiempo para que no se vuelvan obsoletas.

Tradicionalmente, se detecta al fraude mediante sistemas basados en reglas que usan

algoritmos para realizar varias situaciones hipotéticas de detección del fraude. Para aprobar una transacción, un analista de fraude escribe varias reglas una encima de la otra identifica señales como por ejemplo grandes transacciones inusuales a lugares geográficos desconocidos. Por lo tanto, los sistemas basados en reglas necesitan incorporaciones frecuentes de situaciones hipotéticas para detectar de manera coherente las correlaciones entre el comportamiento del usuario y las acciones fraudulentas. Además, estos sistemas son incapaces de procesar el flujo de datos digitales en tiempo real, lo que resulta preocupante dado el cambio reciente hacia las transacciones digitales durante el curso de la pandemia. En la actualidad, la mayoría de las evaluaciones para ajustar las transacciones sospechosas todavía recae en los directores de cumplimiento. Por cierto, el personal debe considerar una parte significativa de los costos del cumplimiento. Por estas razones, las instituciones financieras están interesadas en invertir en el aprendizaje automático y la adaptación de los algoritmos de aprendizaje profundo para la detección de fraude porque pueden ser más efectivos para encontrar las correlaciones. (Aggarwal, Wareman, and Lehman 2020, 140-166), (Jullum, Loland, Huseby, Anonsen, and Lorentzen 2020). A continuación encontraremos un breve panorama del estado actual delos enfoques de la inteligencia artificial.

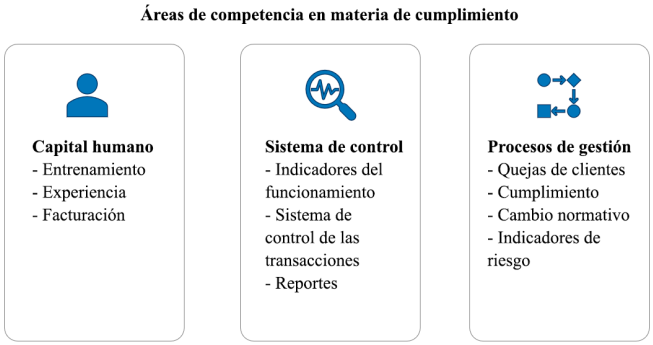

Figura 3: Tipos de áreas de capacidad de cumplimiento. Mapeo del sistema de control de las transacciones dentro del sistema de capacidad de cumplimiento simplificado.

3. Desafíos en el análisis del delito financiero

Esta sección cubre los desafíos actuales en la lucha contra los delitos financieros, especialmente discutiremos el uso y la generación de datos sintéticos financieros y el uso de una herramienta de *benchmark* confiable para evaluar los algoritmos de detección de fraude. Consideraremos la relevancia de medir la efectividad de los controles del delito financiero en el contexto de un creciente mercado de pagos móviles que promociona la inclusión financiera en México.

3.1 Acceso al conjunto de datos financieros

El acceso a los datos del mundo real es un desafío independiente del dominio que está presente en muchos sectores, ya sea el mundo académico, la industria o la gestión. Las transacciones financieras a través de los diferentes canales, como por ejemplo los pagos con tarjetas de crédito, los reclamos de los seguros o los pagos en línea son generadas por las instituciones financieras. Estos conjuntos de datos no están disponibles públicamente debido a las normas de confidencialidad. Asimismo, tener acceso a los conjuntos de datos que tienen fraudes registrados, es decir, las transacciones que demostraron ser fraudulentas, es un esfuerzo más grande. Como tal, si un conjunto de datos anónimos se haya públicamente disponible para la investigación académica, el espacio de tiempo compartido podría no ser suficiente para que el investigador adapte el algoritmo de detección de fraude «para aprender» lo que es un comportamiento del consumidor normal o anormal.

3.2 Conjunto de datos desiguales

Como resultado de la naturaleza desigual de los datos de la transacción en la que los algoritmos de aprendizaje automático están entrenados, su adaptación para la detección de fraude es muy desafiante. Una distribución de clase desigual se refiere a un conjunto de datos en donde el número de transacciones fraudulentas es significativamente más bajo que las transacciones legítimas, es decir acerca del 1% o menos del total de las transacciones. Los algoritmos de la clasificación de aprendizaje automático convencional están diseñados para mejorar el total de la identificación correcta de las transacciones fraudulentas y normales al reducir el rango de error del algoritmo, Sin embargo, el conjunto de datos desiguales puede sesgar en gran medida su funcionamiento. Como resultado, los algoritmos de clasificación pueden ser sesgados o erróneos en la identificación de las clases minoritarias fraudulentas. Sin embargo, para tratar estos temas se utilizan con frecuencia las técnicas de sobre muestreo y submuestreo, como por ejemplo la Técnica de Sobre muestreo de la Minoría Sintética (SMOTE por sus siglas en inglés).

3.3 Datos sintéticos

Los datos sintéticos mostraron ser una propuesta de valor rentable en varios campos (Barr et al., 2020). En finanzas, su uso ha ganado un interés significativo, en particular en las áreas de la detección y cumplimiento del delito financiero (Lopez-Rojas, Axelsson, and Baca, 2018) superando los desafíos planteados mediante el acceso del conjunto de datos financieros debido a las regulaciones de la privacidad (Barse, Kvarnstrom, Jonsson, 2004). Por otra parte, dentro de los datos sintéticos, se pueden simular las condiciones que podrían encontrarse. Por lo tanto, las estrategias potenciales que los delincuentes utilizan pueden tomarse como ventajas para adaptar los sistemas de control actuales a un comportamiento delictivo posible.

Los datos sintéticos se pueden definir como datos completamente nuevos generados para parecerse o mantener las propiedades estadísticas de los conjuntos de datos reales. Una consideración clave es la efectividad de los datos sintéticos cuando se usan. Por ejemplo, un

principio básico para la validación de la utilidad de los datos sintéticos es observar si un modelo de aprendizaje automático construido desde los datos sintéticos funciona tan bien como los modelos construidos desde los datos reales. Por lo tanto, los datos sintéticos deben tener como objetivo simular las propiedades estadísticas de los datos reales, sin embargo el conjunto de datos sintéticos no puede ser la réplica exacta de los datos reales, ya que comprometería a la privacidad que tenemos como objetivo defender.

La calidad de los datos sintéticos depende de dos factores principales; a) el tipo de metodología aplicada a la generación de los datos y b) la solidez, calidad y la profundidad característica de los datos originales. Para comenzar, con solo extrapolar las correlaciones o los patrones entre los atributos del conjunto de datos o variables, no es suficiente para crear datos sintéticos de calidad. Además, es bueno asumir que estamos comenzando con un conjunto de datos reales que es lo suficientemente grande, que tiene tanta información en los atributos como sea posible y que no está sesgado. Aunque no existe un consenso sobre el enfoque para crear datos sintéticos, es importante notar que el método elegido debería explicarse, es decir responder las preguntas sobre el proceso de creación de datos. (Barr et al., 2020). Por cierto, los datos sintéticos enfrentan el desafío de los casos de uso limitado porque la calidad y la confiabilidad de los datos sintéticos no ha sido aceptada por los profesionales. Por consiguiente, se recomienda comparar los datos sintéticos con el conjunto de datos reales para entender completamente su confiabilidad.

En el mundo de las finanzas, los modelos generativos han cobrado interés significativo, ya que pueden preservar la privacidad, es decir, no es posible descubrir el camino de los datos sintéticos hacia los datos originales (Assefa, 2019), aunque un trabajo reciente descubrió que pueden faltar pruebas para respaldar tales reclamos y se requiere una mayor investigación para comprenderlos (Stadler, Oprisanu, and Troncoso, 2020). Sin tener en cuenta esas opiniones, los métodos generativos son considerados mejores que los métodos de desclasificación/ desidentificación, como por ejemplo el enmascaramiento, redistribución, encriptación de datos ya que la desclasificación generada por los datos sintéticos puede volver a seguir el camino trazado hacia el conjunto de datos originales.

3.4 Las limitaciones de los indicadores del aprendizaje automático en el análisis del delito financiero

La implementación del aprendizaje automático o aprendizaje profundo puede asegurar programas de cumplimiento regulatorios eficientes y efectivos y ahorrar dinero para la institución financiera. Se utilizan los indicadores para evaluar el funcionamiento de los algoritmos de detección de fraude. La detección de fraude es a nivel básico un problema de clasificación binaria donde se predice si una transacción es un fraude (positivo) o un no fraude (negativo) Existen cuatro posibles resultados de las clasificaciones, cuando un algoritmo clasifica correctamente una transacción como fraude o no-fraude, es llamada positivo verdadero (PV) y negativo verdadero (NV), respectivamente. Cuando un algoritmo erróneamente identifica una transacción no-fraude como fraude, se llama error tipo I o falso

positivo (FP). Un error tipo II, también llamado falso negativo (FN) existe cuando se identifica a una transacción como no- fraude cuando es un fraude.

La precisión (*precision*), la exhaustividad (*recall*) y la exactitud (*accuracy*) son tradicionalmente indicadores utilizados para evaluar el funcionamiento de la clasificación de los algoritmos, desafortunadamente estos indicadores no son adecuados en la detección de fraude, aunque existe una preferencia para las curvas de precisión-exhaustividad. (Saito & Rehmsmeier, 2015). Las medidas de precisión miden la proporción de las identificaciones de los fraudes que eran correctas. Las medidas de exhaustividad miden la proporción de los fraudes reales que fueron identificados correctamente. F1 *Score* es una función de precisión y exhaustividad. La exactitud describe el «valor cerca de verdadero», sin embargo, en el dominio del fraude financiero no es muy útil ya que los conjuntos de datos sean desiguales, es decir las transacciones fraudulentas son menos de 1%. Si el modelo predice que al menos 99% de todas las transacciones es legítimo, no es una medida muy colaboradora para calcular el funcionamiento del clasificador. Para tratar algunos de estos asuntos hemos visto surgir el coeficiente de correlación kappa de Cohen y el coeficiente de correlación Matthews (MCC por sus siglas en inglés) que tratan de abordar un alcance mayor de las variables para medir el funcionamiento del clasificador. Aunque el uso de K ha sido un área de debate dentro de los dominios del aprendizaje automático (Delgado & Tibau, 2019) y fuera de ellos (Bexkens et al., 2018), observamos una recepción mucho más positiva para MCC (Chicco & Jurman, 2020).

Sin embargo, sentimos que las medidas todavía no son suficientes para formular un *benchmark* adecuado con el aprendizaje automático en el dominio del fraude financiero, y proponemos que el funcionamiento del modelo debería también ser evaluado en término de cantidades financieras de fraudes perdidos y transacciones identificadas erróneamente como normales para determinar los indicadores apropiados, y por lo tanto lograr un clasificador más sólido y discriminatorio.

4. Beneficios de un benchmark financiero

4.1 Detección del fraude en los servicios financieros

Los departamentos de control de cumplimiento de las instituciones financieras enfrentan el desafío de reducir el número de personas inocentes a las que se las acusa. Para enfrentar este problema, las instituciones financieras están estudiando el uso de algoritmos de detección de fraude y la tecnología del análisis de datos para desarrollar un sistema de detección del fraude más exacto. Sin embargo, el enfoque en la optimización y la automatización del monitoreo bancario y los procesos de testeo con frecuencia lleva a preocuparse por el sesgo y la privacidad (Johnson et al., 2019).

Las soluciones que existen dentro de estos dominios están adaptadas para integrarse con TMS Los vendedores los modifican con frecuencia para brindar un nivel más profundo de

análisis y detección de fraude sobre los competidores. Sin embargo, existen soluciones por fuera de TMS que sirven como plataformas para entrenar a los modelos de aprendizaje automático sofisticados para una rápida implementación y clasificación del fraude. Sirven ya sea para expandir el conjunto de datos actuales disponibles agregando más parámetros o expandiendo los existentes para entrenar a los modelos más sólidos. Aunque estas soluciones aumenten la detección de fraude, todavía se hallan bajo la restricción de la privacidad de los datos y están limitadas seriamente en los datos que pueden utilizar.

Como se muestra en la figura 4, las instituciones financieras tienen la tarea concreta de desarrollar y mantener controles para su TMS. Es fundamental para el desarrollo de la detección de fraude tener alertas exactas Las alertas generadas son consideran «buenas» cuando la cantidad de transacciones fraudulentas detectadas es representativa del total del fraude, y el número de personas inocentes que son etiquetadas como fraudulentas sea lo más bajo posible. Por lo tanto, el desafío mayor para los bancos es entender de antemano cuán efectivo es un nuevo control (un algoritmo responsable para la clasificación) en contraste con el control activo existente. Esta ardua tarea regularmente incluye numerosas versiones de ensayo y error, llevando de varios meses hasta años para perfeccionarse. Una vez que se evalúa el nuevo control para estar dentro de un adecuado rango de clasificación, se implementa para tomar decisiones válidas en tiempo real. Sin embargo, con el tiempo, el funcionamiento del control disminuirá y los delincuentes se apartarán de su usual comportamiento para evitar ser detectados. De ese modo, este proceso que requiere mucho tiempo se repite muchas veces, dejando un pequeño vacío para que los delincuentes saquen provecho. Idealmente, con una herramienta de referencia que mida el funcionamiento de estos controles con antelación, las instituciones financieras serán capaces de reducir el tiempo que les lleva para implementar sus controles, y, por lo tanto, utilizar los controles más apropiado para el comportamiento delictivo actual.

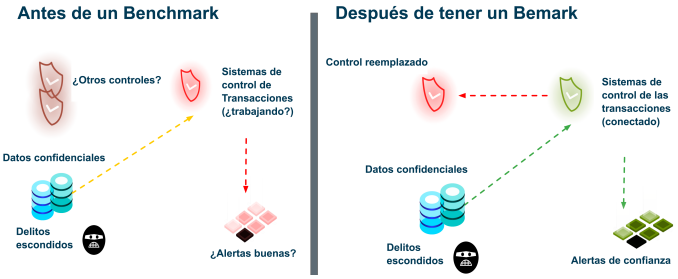

Figura 4: Impacto en la evaluación del delito financiero (*benchmarking*).

4.2 El futuro de la tecnología en los Servicios Financieros Digitales

La pandemia COVID-19 llevó a la población de México a cambiar la forma de hacer las compras y pagar los servicios. Por consiguiente, una gran parte de México ha pasado de utilizar dinero físico a las soluciones digitales, como los teléfonos móviles y los sistemas de pago online. No obstante, el fraude ha seguido esta tendencia y por lo tanto ha incrementado. La transformación digital de muchos sectores, como es el caso del sector

financiero, se ha acelerado como resultado de la pandemia Covid 19. Lo que sugiere que, a medida que la rentabilidad de las entidades financieras aumenta, la inclusión financiera estará jugando un rol más importante en estos ecosistemas.

A pesar de las políticas y las regulaciones puestas en marcha, se han orientado mal los avances tecnológicos en las finanzas. Si se considera a la banca digital como una herramienta para luchar contra la desigualdad y contribuir al empoderamiento económico de la población no bancarizada, es necesario abordar varios desafíos.

En primer lugar, se necesita identificar los factores culturales, prácticos, estructurales y políticos detrás de los cuales algunos mexicanos parecen dudar para adoptar los avances tecnológicos necesarios para ser identificados y abordados. Algunas personas se sorprendieron cuando Sansung Pay decidió no continuar las operaciones en México. Por ende, es importante entender las barreras que contribuyen a la escasa utilización de las apps o servicios financieros como CoDi Samsung Pay. Las altas comisiones son sin duda una de los obstáculos más desalentadores que los consumidores enfrentan cuando consideran la posibilidad de adoptar los pagos digitales Esto se empeora aún más con las poblaciones vulnerables que son más propensas a sufrir dificultades económicas. Además, las poblaciones indígenas o mayores pueden encontrar dificultades en adaptarse a las nuevas tecnologías, por lo tanto, se debe tener más cuidado en evaluar a la accesibilidad de la app para todo tipo de características demográficas. Sin embargo, tal vez un punto clave para abordar sea fomentar la confianza en el sistema: implementar leyes y normas para proteger a los consumidores recorrería un largo camino para establecer la base de todo esto. Aún más, si este tema no se aborda, se perpetuará la sensación de impunidad y por lo tanto la desconfianza en los bancos y sistemas que relacionan estos delicados y complejos sistemas.

En segundo lugar, deberían realizarse otros trabajos para mejorar las leyes y normas vigentes. Como tal, en el reino de los desafíos regulatorios bancarios, observamos un sistema forzado para encajar en un marco rígido que no funciona para las personas que tienen ingresos bajos o credenciales. Razonablemente, deberíamos pensar con una perspectiva diferente para desarrollar servicios financieros inclusivos que sean capaces de ampliar el alcance de la inclusión, mientras sigan siendo rentables y seguros. Las soluciones basadas en el aprendizaje automático tendrán un rol importante en la promoción de la inclusión financiera. Asimismo, se puede debatir el grado de sociedad que permanecerá «sin efectivo». Como tal, vale la pena notar que no debería existir la discriminación contra determinado grupo, por lo tanto, debemos mejorar nuestros sistemas desde cero.

Un *benchmark* sólidamente diseñado que permita la evaluación de la confiabilidad del sistema de detección de fraude es un componente ideal en la creación de un ecosistema digital más seguro que pueda incorporar un amplio rango de datos demográficos que pueden haber sido omitidos con antelación. Por cierto, la confianza de que el delito se reduzca realmente no solo hará que los consumidores se sientan más seguros acerca de dónde guardar su dinero, sino que también hará que el proceso de incorporación se realice

sin problemas, lo cual, con frecuencia, puede disuadir y discriminar contra los potenciales clientes.

El crecimiento de las tecnologías innovadoras es otro paso esencial para construir una sociedad digital económicamente justa; sin embargo, algunas de las áreas de la Ley Fintech deben revisarse para reducir los obstáculos para la entrada de capital para hacer de México un lugar atrayente para las compañías fintech. Otros países, como el Reino Unido, ya empezaron a impulsar políticas para buscar innovación. Un ejemplo es el área de prueba digital para acelerar el desarrollo de las compañías que puedan no tener acceso a los recursos necesarios para su solución. Esta combinación de datos sintéticos y código de espacios abiertos ha tenido éxito en la exploración y cuantificación de tecnologías de inclusión financiera innovadora, por lo tanto, una revista independiente de la industria fintech la ha elogiado (Kalifa, 2021). Como consecuencia, la inclusión de una guía regulatoria para otras innovaciones en servicios financieros, por ejemplo, préstamos de balance, numerosos servicios de inversión o moneda digital del banco central ayudaría a mejorar la inclusión financiera.

En tercer lugar, cuando se tenga en cuenta que los organismos reguladores en sí mismos usarán nuevas tecnologías para modernizarse o mejorar las operaciones y procesos. El crecimiento exponencial de la estrategia de pago móvil para estimular a la inclusión financiera, diversificará a las comunidades que participan en el Sistema Financiero Mexicano. Por lo tanto, los entes reguladores deben estar preparados para abordar un crecimiento sustancial de las diversas situaciones hipotéticas, y adaptarse como corresponde mediante el uso de la tecnología de vanguardia o arriesgarse a sentirse abrumado o incapaz de supervisar al sistema financiero.

En cuarto lugar, se debería crear un enfoque hacia las políticas públicas, las leyes, las normas y la gestión desde cero con una mentalidad nativa digital. Ciertamente, la gestión actual ha evolucionado siguiendo a los avances tecnológicos, pero es innegable que son del pasado. Para un caso en concreto, un clásico TMS puede considerarse como un sistema preexistente arcaico que ha evolucionado para adaptarse a las nuevas reglas, sin embargo, su evolución está limitada por la interacción del usuario. Por lo tanto, se está volviendo mucho más obsoleto en el tiempo, en contraste con un TMS que tiene aprendizaje automático embebido para la toma de decisiones. Existen muchos avances tecnológicos y cambios que provienen del mercado que necesita una rápida adaptación de las soluciones vigentes. Para nombrar algunas, tenemos banca digital, descentralización de la tecnología *blockchain*, moneda digital Todo esto aporta un flujo de nuevos datos con la mayor complejidad que hemos visto; para lo que tanto el marco actual como el anterior definitivamente no están preparados.

En conclusión, existe un gran desafío para crear políticas públicas, leyes, normas y gestión que adhieran al rápido avance de la tecnología. Esto se complica aún más debido a un mercado que se propaga con facilidad y cuyo objetivo es promover un ambiente de

competitividad e innovación, mientras también trata de fomentar la inclusión financiera y proteger a los derechos del consumidor. Por consiguiente, es necesario trabajar con estrategias, por ejemplo, se puede adoptar un diálogo abierto, continuo e inclusivo con los accionistas. Este trabajo se puede complementar con talleres entre los encargados de formular políticas, los académicos y los expertos financieros y tecnológicos para discutir las diferentes formas de beneficiarse con los avances tecnológicos y por lo tanto evitar las dificultades que aparecen con los complejos entornos regulatorios.

Para los delitos financieros y ALD se ha sugerido un modelo de cooperación de triple hélice entre la academia, las instituciones financieras y los organismos encargados de hacer cumplir la ley. para tener beneficios para la lucha contra los delitos financiero. Un mayor desafío lo constituye el hecho de que las instituciones son inflexibles en cambiar de los respectivos dominios; por lo tanto, la falta de entendimiento mutuo y la confianza entre el mundo académico y las instituciones financieras. Por lo tanto, se necesita un gran trabajo para entender las necesidades de los otros, alcanzar un consenso en un entorno colaborativo para la innovación.

5. Conclusión y trabajo futuro

La seguridad es clave para construir y mantener la confianza del consumidor en el uso de la banca digital. Una herramienta de *benchmark* es muy útil para ayudar a las instituciones financieras a gestionar los riesgos regulatorios planteados por el fraude. En este estudio exploramos el particular caso de México y analizamos cómo el *benchmarking* en el control de los delitos financieros puede ayudar a crear un ambiente más seguro que alentará a los mexicanos a utilizar los servicios financieros digitales.

Durante los momentos de inestabilidad, como los vividos con la reciente pandemia, además de hacer proyectos para la era post-COVID, es necesario trabajar en estrategias que fortalezcan al sector financiero digital. Por lo tanto, es esencial crear una infraestructura mucho más dinámica, que aliente la recuperación económica, estimule la inclusión y que aún ayude a crecer y mantenerse como el eje de Latinoamérica. Por cierto, dada la naturaleza multidimensional de los desafíos de la inclusión financiera, el diseño de las estrategias debe incluir el contexto económico y el social. Lo que une a los incentivos e intereses de las partes interesadas (por ej. consumidores, Banxico, el sector público y privado) con la innovación de las tecnologías (por ej., nuevos modelos de negocios, productos).

El punto crucial para abordar este problema es el reconocimiento de que la industria sufre en la actualidad la falta de datos reales de calidad, debido a las restricciones de privacidad o a la falta de almacenamiento optimizado y la depuración de datos. Esto es especialmente un punto crítico cuando se requiere un conjunto de datos identificados, ya que lleva muchos meses reestructurar los niveles organizativos y la infraestructura de datos para hacer uso de los datos históricos reales.

Los datos sintéticos no tienen tal limitación, porque se crean rápidamente y están integrados con etiquetas rápidas para las tareas de aprendizaje automático. Sin embargo, en la actualidad, no existe una medida clara sobre la calidad de los datos sintéticos con los que todos están de acuerdo; además el desarrollo de los datos sintéticos para el delito financiero sofisticado, como por ejemplo el lavado de dinero, todavía se haya en el estado embrionario de su desarrollo.

Aunque se requiere un mayor trabajo para definir tales estrategias dada la evolución de la tecnología y el modo en que finanzas confiables se manejarán, algunas de las áreas clave que impulsarán la innovación son:

A. incremento de la calidad y la confianza en el uso de los datos generados sintéticamente,

B. mayor desarrollo de las herramientas benchmark utilizando datos generados Sintéticamente para los algoritmos de aprendizaje automático.

C. construir las bases para extender el trabajo desde la privacidad hacia los diferentes aspectos de la confianza como la capacidad de explicar todo y solidez para los datos generados.

Estos principios estarán orientados hacia el desarrollo de datos sintéticos de alta fidelidad para informar mejor el aprendizaje basado en los datos y soluciones en el delito financiero para hacer *benchmark* en las áreas de los controles del aprendizaje automático, en consecuencia, preparar el camino para la creación de un ecosistema digital financiero más accesible.

Referencias Bibliográficas

– Aggarwal Nikhil, Wareman Sean, and Lehman Rasmus. 2020. “Applications of machine learning in the identification, measurement and mitigation of money laundering.” Journal of Financial Compliance 4(2), pp. 140-166.

– Alonso Javier, Fernández de Lis Santiago, Hoyo Carmen, López-Moctezuma Carlos and Tuesta David. 2013. “Mobile banking in Mexico as a mechanism for financial inclusion: recent developments and a closer look into the potential market.” BBVA Research Working Papers Number 13/20, June 2013. https://www.rrojasdatabank.info/mobilebanking4.pdf

– Avendaño Carbellido Octavio. 2016. “La reforma financiera y su impacto en el usuario.” Entreciencias: Diálogos en la Sociedad del Conocimiento, vol. 4, núm. 10, 2016 Universidad Nacional Autónoma de México. May 2016, DOI: http://dx.doi.org/10.21933/J:EDSC.2016.10.182 https://www.redalyc.org/jatsRepo/4576/457646537003/html/index.html

– Avendaño Carbellido Octavio. 2018. “The challenges of electronic banking in Mexico.” Revista del Instituto de Ciencias Jurídicas de Puebla. ISSN 1870-2147. New epoch Vol. 12,

No. 41: 87-108

– Banco de Mexico. 2019. “Reporte de Estabilidad Financiera.” Banco de Mexico, December, 2019. https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistemafinanciero/%7B04E197EE-B6FC-7BA1-72A0-32D3E6C9BF28%7D.pdf

– Barr Brian, Xu Ke, Silva Claudio, Bertini Enrico, Reilly Robert, Bruss C. Bayan, Wittenbach Jason D. 2020. “Towards Ground Truth Explainability on Tabular Data” arXiv:2007.10532v1 [cs.LG] 20 Jul 2020

– Barse E.L., Kvarnstrom H., Jonsson E. . 2004, Synthesizing test data for fraud detection systems Conference Paper Conference: Computer Security Applications Conference, 2003. Proceedings. 19th Annual IEEE Xplore DOI: 10.1109/CSAC.2003.1254343

– Bexkens Rens, Claessen Femke MAP, Kodde Izaak F, Oh Luke S, Eygendaal Denise, and van den Bekerom Michel PJ. The kappa paradox. Shoulder & Elbow, 10(4):308–308, October 2018. ISSN 1758-5732. doi: 10.1177/1758573218791813. URL https://doi.org/10.1177/1758573218791813. Publisher: SAGE Publications Ltd.

– Chicco Davide, Jurman Giuseppe. The advantages of the Matthews correlation coefficient(MCC) over F1 score and accuracy in binary classification evaluation. BMC Genomics , 21 (1):6, 2020. ISSN 1471-2164. doi: 10.1186/s12864-019-6413-7. URL https://doi.org/10.1186/s12864-019-6413-7

– CNBV. 2020. “Inclusión Financiera en México.” https://www.gob.mx/cms/uploads/attachment/file/590346/Inclusion_financiera_mexico_difusion.pdf

– Condusef. 2017. “La CONDUSEF informa sobre las comisiones bancarias y sus reclamaciones” https://www.condusef.gob.mx/?p=contenido&idc=379&idcat=1

– Condusef. 2021. “2020 Third trimester report.” https://www.condusef.gob.mx/?p=estadisticas

– CNBV, 2020, p.48 https://www.gob.mx/cms/uploads/attachment/file/590346/Inclusion_financiera_mexico_difusion.pdf

– CNBV, INEGI Encuesta Nacional de Inclusión Financiera https://www.inegi.org.mx/programas/enif/2018/

– Das Sanjiv, Donini Michele, Gelman Jason, Haas Kevin, Hardt Mila, Katzman Jared, Kenthapadi Krishnaram, Larroy Pedro, Yilmaz Pinar, and Zafar Bilal. 2020. “Fairness measures for machine learning in finance.”

– Delgado Rosario and Tibau Xavier-Andoni. 2019. “Why Cohen’s Kappa should be avoided

as performance measure in classification." PLOS ONE , 14(9):e0222916, September 2019. ISSN 1932-6203. doi: 10.1371/journal.pone.0222916. URL https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0222916 . Publisher: Public Library of Science.

– DOF (Diario Oficial de la Federacion). 2018. 9 March. http://www.diputados.gob.mx/LeyesBiblio/ref/lritf/LRITF_orig_09mar18.pdf

– DOF. (Diario Oficial de la Federacion). 1990. Ley de Instituciones de crédito. July 18, 1990. https://www.senado.gob.mx/comisiones/finanzas_publicas/docs/LIC.pdf

– Estanol Eduardo. 2019." Los bancos en México logran mejor desempeño que en sus países de origen." Expansion, February 22, 2019.

– Johnson Kristin, Pasquale Frank, and Chapman Jennifer. Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation. FORDHAM LAW REVIEW, 88:32, 2019.

– Juarez Edgar. 2015. "México, una joya para los bancos extranjeros." El Economista, March 17, 2015 https://www.eleconomista.com.mx/sectorfinanciero/Mexico-una-joya-para-los-bancos-extranjeros-20150317-0182.html

– Jullum Martin, Loland Anders, Huseby Ragnar Bang, Anonsen Geir, and Lorentzen Johannes. 2020. "Detecting money laundering transactions with machine learning" Journal of Money Laundering Control, January 4 2020. ISSN: 1368-5201

– Kalifa, Ron.. 2021. "Kalifa Review of UK Fintech" https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971370/KalifaReviewofUKFintech.pdf

– Karpoff Jonathan M. 2020 "The future of financial fraud." Journal of Corporate Finance , pp. 101694.

– Lopez-Rojas E. A., Axelsson S., and Baca D. 2018. "Analysis of Fraud Controls Using the PaySim Financial Simulator." International Journal of Simulation and Process Modelling. 13 (4), pp. 377-386, ISBN: 1740-2131.

– Lopez-Rojas Edgar Alonso. 2019. "Triple Helix Approach for Anti-Money Laundering (AML) Research Using Synthetic Data Generation Methods." The 10th International Conference on Society and Information Technologies: ICSIT 2019 At: Orlando, USA. ISSN 00401625. doi: 10.1016/j.techfore.2016.04.024.

– Maina Juliet. 2018. "Manual regulatorio y de politicas de dinero móvil" https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/09/GSMA-Mobile-Money-Policy-Handbook_Spanish.pdf

– Morales Guzman, Rafael. 2018. “How Financial Tech Can Aid Financial Inclusion in Mexico.” Cornell Policy Review, November 16, 2018. http://www.cornellpolicyreview.com/fin-techmexico/

– Naghavi Nika. 2020. “State of the Industry Report on Mobile Money” https://www.gsma.com/sotir/wp-content/uploads/2020/03/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2019-Full-Report.pdf

– OECD. 2019. “OECD Economic Surveys Mexico” https://www.oecd.org/economy/surveys/Mexico-2019-OECD-economic-survey-overview.pdf

– OCDE/CAF. 2020. “Estrategias nacionales de inclusión y educación financiera en América Latina y el Caribe: retos de implementación.” http://www.oecd.org/financial/education/Estrategias-nacionales-de-inclusi%C3%B3n-y-educaci%C3%B3n-financiera-en-America-Latina-y-el-Caribe.pdf

– Pandey Neena, Pal Abhipsa, et al. 2020. “Impact of digital surge during COVID-19 pandemic: A viewpoint on research and practice”. International Journal of Information Management , 55:102171.

– Procuraduria Federal del Consumidor. 2020. “Todo a un clic. Compras sin salir de casa (In Spanish).” Mexican Government-Federal Consumer Protection Agency, September 2, 2020. https://www.gob.mx/profeco/articulos/todo-a-un-cliccompras-sin-salir-de-casa?idiom=es

– Saito Takaya and Rehmsmeier Marc. 2015. The Precision-Recall Plot Is More Informative than the ROC Plot When Evaluating Binary Classifiers on Imbalanced Datasets. PLoS ONE, 10(3). ISSN 1932-6203. doi: 10.1371/journal.pone.0118432. URL https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4349800/.

– Saldívar Alejandro, Zavaleta Noé. “Túmin, una moneda que resiste.” Proceso. December 28, 2020 https://www.proceso.com.mx/nacional/estados/2020/12/28/tumin-una-moneda-que-resiste-255250.html

– Senate of the Republic. 2021. “Impulsa Comisión de Economía dictamen para proteger a usuarios; aumentan fraudes cibernéticos”. March, 2021http://comunicacion.senado.gob.mx/index.php/informacion/boletines/50425-impulsa-comision-de-economia-dictamen-para-proteger-a-usuarios-aumentan-fraudes-ciberneticos.html

– Senate of the Republic. 2020. “Urgen legislar en materia de ciberseguridad ante el incremento de delitos digitales.” October 9, 2020 http://comunicacion.senado.gob.mx/index.php/informacion/boletines/49401-urgen-legislar-en-materia-de-ciberseguridad-ante-el-incremento-de-delitos-digitales.html

– SHCP/Ministry of Public Education. 2020. “Politica Nacional de Inclusión Financiera.” https://www.gob.mx/cms/uploads/attachment/file/585234/PNIF_2020.pdf

– Stadler Theresa, Oprisanu Bristena, and Troncoso Carmela. 2020. “Synthetic Data – A Privacy Mirage” arXiv:2011.07018v2 [cs.LG] 11 Dec 2020

– van Driel Hugo. 2019. “Financial fraud, scandals, and regulation: A conceptual framework and literature review”. Business History, 61(8):1259–1299, 2019. doi: 10.1080/00076791.2018.1519026

– World Bank. 2018. “Financial Inclusion.” https://www.worldbank.org/en/topic/financialinclusion/overview

– World Bank. 2020. “Mexico Overview” https://www.worldbank.org/en/country/mexico/overview

– Zhang Wanrong, Ohrimenko Olga, Cummings Rachel. 2020. “Attribute privacy: Framework and mechanisms.” doi: arXiv:2009.04013.

Agradecimientos

Este trabajo fue respaldado por la agencia de innovación del Reino Unido, Innovate UL, con proyectos financiados a EalaX Ltd: FraudSim 82929 y CP-Mark 89039.
Agradecemos a los lectores anónimos y al Dr. Xi Hu (Programa de Becarios de la Facultad de Derecho de Harvard) por sus comentarios útiles.

Notas

↑1 Nota de la traducción: se ha mantenido la palabra “benchmark” en su idioma original, dado su frecuente uso y su significado particular. Refiere a puntos de referencia con fines estratégicos.