# La Esperanza y el Miedo de Banca Abierta

Aplicar para un préstamo puede ser una de las más frustrantes experiencias en la vida. Es una serie de paciencia-agotamiento parar-comenzar, que parece el tráfico de la ciudad de Nueva York un viernes a las 5:00 de la tarde. Vas a un banco por un préstamo. El banco recolecta su información, hacen números, aplican sus fórmulas, luego regresan con un sí o un no. Si la aplicación por poco no reúne los lineamientos de riesgo del banco, piden presentar obligatoriamente un consignatario fiable para el préstamo. No es que el banco no quiere prestar dinero – *es su trabajo*- pero el proceso es el proceso.

La banca es una industria aislada. Todos los registros acumulados para procesar su aplicación para el préstamo, permanecen con el banco en el cual usted aplicó. No se comparte información. Cada y todas las veces que usted aplica para un préstamo debe proveer la información nuevamente. Se convierte en una pesadilla recurrente – Reportes de crédito, explicaciones verbales, historial de empleos, ropa limpia, actitud centrada, esperanza y expectativa — y hay que continuar hasta encontrar una institución financiera que te sirva.

# La Esperanza

La banca abierta podría cambiar todo lo que conocemos sobre fluidez monetaria. Es un modelo conceptual para servicios financieros donde bancos y otras entidades financieras le permiten a los clientes accesar sus datos e información de la cuenta a través de la aplicación interfaz de programación (APls). Esto le permitiría a los clientes de forma segura compartir sus datos con terceras partes, quienes podrían entonces valerse de la información para proveer productos y servicios más personalizados para el usuario final, esto podría sacar al aplicante de préstamo del congestionado tráfico de Nueva York y de alguna manera tele-transportarlo directamente a la institución financiera o proveedor de servicios que conoce sus necesidades, porque esas necesidades han sido ya dirigidas a través de una interface digital. Piense en esto como una aplicación que contacta clientes de préstamos y prestamistas, una en la cual todas las imágenes e información están vinculadas. La banca abierta puede hacer dinero y financiamiento cinético. Puede ir del congestionado tráfico de la ciudad de Nueva York a una autopista alemana en un parpadeo, cambiando el panorama global del financiamiento.

Accesar al capital es el más grande inhibidor en el desarrollo de la economía en los sectores más pobres del globo. Bancos de microcréditos emergieron en India un número de años atrás transformando el panorama de negocios pequeños, ayudando a multitudes de gente a ganar independencia y emprendedurismo con micro préstamos para cosas como equipo de tejer. La banca tradicional en India no se acerca a este sector. La banca abierta puede llenar esta brecha del mercado y muchas otras mucho más eficientemente que los bancos de microcrédito de India y extender el modelo a lo largo del globo si se conecta con instituciones bancarias internacionales. ¿Entonces cuál es la demora? ¿Por qué no hemos entrado aún en el mundo de la banca abierta? En una palabra: seguridad.

# El Miedo

La arquitectura de la banca abierta es construida sobre proveedores de terceros (TPPs). Piense en ellos como corredores de bolsa. Conectan bancos y consumidores. Tienen dos funciones, acceder a información de la cuenta y pagos. Los proveedores de servicios de información de cuentas (AISP) y el proveedor de servicio iniciador de pago (PISP) son la estructura rudimentaria sobre la cual una más completa banca abierta puede ser construida. Sin embargo, la gente puede estar compartiendo su información más personal, su personalmente identificable información (PII) la cual, en manos equivocadas, puede ser ruinoso. Para que la banca abierta emerja necesitamos confianza en la seguridad.

El ecosistema de banca abierta es poblado con aseguradores, fintech, socios de lealtad, proveedores de servicios, herramientas de gestión financiera, servicios contables, minoristas, canales de asesoramiento, proveedores de pensiones, y por supuesto bancos. Todos ellos conectan entre sí con TPPs. Para que este ecosistema exista debe haber una legislación global que lo respalde y el medio que lo ejecute. Medidas como Directiva Dos de Pagos de Servicios Europeos (PSD2) crea una estructura para que TPP exista en su ecosistema. Vino incrementando su fuerza entre enero de 2018 y setiembre de 2019, pero aún se están tomando muchas precauciones. La preocupación número uno es la seguridad de PII. ¿Cómo puede un ecosistema global moviéndose así de rápido, garantizar protección contra la multitud de piratas de datos que operan en el mundo? ¿Cómo podemos ir hacia la banca abierta con todos estos riesgos existentes?

La banca abierta debe hacer frente a estas preocupaciones con autenticación fiable como multi-factor de autenticación (MFA), tecnologías de codificación que protegen datos en tránsito y en reposo y robustos accesos de control que permiten solamente a usuarios y a aplicaciones autorizadas acceder a información sensible. La tecnología que llena este vacío de seguridad está emergiendo rápidamente.

¿pero qué hay de regulación? ¿Cuáles organismos comparables a nivel nacional, regional, hemisférico e internacional podrían proveer las garantías del Depósito Federal de Corporación de Seguros (FDIC) en Estados Unidos o instituciones similares en otros países? El ecosistema de banca abierta será el salvaje oeste o habrá mariscales?  
Todas estas preguntas no han sido contestadas hasta ahora de ninguna manera que pueda mitigar la paranoia del PII. La legislación se está moviendo continuamente y la motivación existe en parlamentos al rededor del mundo, *pero no estamos del todo ahí.*

# AI y ML son la Esperanza

El primer estadio de cualquier tentativa seria de traer la banca abierta a la normalización en el mercado global debe iniciar con limpiar el completamente des-estandarizado mundo de APls que gobierna TPPs. Para que esto de resultados debe haber un nuevo sistema de contabilidad y notación en bancos que los transfiere de sus sistemas y procesos tradicionales hacia un formato de intercambio de datos compatible con infraestructura de la banca abierta.

La industria se encuentra a sí misma detenida entre la estandarización de respaldo de autoridad como en el punto de partida en el mercado TPP y la legislación que ejecuta la estandarización. Hay muy pocas voces activamente hablando de esta brecha de autoridad. Los bancos son internacionalmente gobernados por reglas generalmente escritas por el fondo monetario internacional (IMF), el Banco Mundial o el Banco para acuerdos internacionales (BIS), pero no se hacen oír cómo podrían si fueran fuertes defensores de la banca abierta. El único organismo tangencialmente direccionando el problema es el Comité Basilea III.

Basilea III es un conjunto de regulaciones de banca internacional escritos por el Comité de Basilea en Supervisión de Banca. La tercera iteración de estándares evadidos referencia al sistema de banca abierta, sin embargo, se mueve en esa dirección con estrictas y precisas cláusulas en el manejo de información. —más centrado en gestión de riesgos. Los estándares insisten en que los bancos tienen sistemas de manejo de información compatible o que capturan y reportan datos de una manera específica. Basilea III es un tremendo avance para la banca abierta. Formatos de información consistente garantizan que TPPs utiliza el mismo formato de datos, y el comité ha proporcionado fuerte liderazgo en la aplicación de banca APls abierta, la cual puede ser superada por la banca abierta y TPPs.

¿Entonces donde entra la seguridad en todo esto? La mejor pregunta es dónde no entra. El acuerdo tras el consenso de la ciencia informática del mundo es que las conclusiones de API son las más grandes vulnerabilidades. Esto significa que cuando vas a autenticar en una TPP eres más vulnerable…

Esto puede ser mitigado con inteligencia artificial (AI) o aprendizaje automático (ML) pueden ser usadas para mejorar la comprensión de firmas de amenazas asociadas con tipos específicos de amenazas de seguridad, amenazas de inteligencia en la recolección de información relacionadas con potenciales amenazas de seguridad, tipos de respuestas pueden ser definidos por ML y AI para aumentar significativamente la identificación de potenciales amenazas y ML y AI pueden ser desplegados por huellas digitales como la única identificación de sistemas enfocados en vulnerabilidades y desconfiguraciones. Esto elimina todos los intrusos digitales. Un intruso digital operando al nivel de codificación no será capaz de visualizar lo que el último usuario colocó en el escritorio o en la tableta. Después de que se haya establecido la verificación humana, es absolutamente necesario un proceso de autenticación que consolida la identidad del usuario a través de dos o tres pasos.

Hay un sin fin de posibilidades para MFA. Una contraseña o número personal de identificación (PIN) puede ser usado. Un token de seguridad puede ser pasado a un teléfono inteligente asociado al usuario. Los datos biométricos se están haciendo más comunes con las huellas digitales para abrir computadoras. MFA puede incrementar significativamente la seguridad de un sistema o servicio. En caso de que un intruso sea capaz de burlar un nivel de identificación, este sería detenido por la autenticación multifactorial.

Estos son los pasos correctivos para la seguridad de punta. Pero, ¿Qué hay de los datos en sí mismos, que fluyen libremente por el universo digital? La información es tan voluminosa que darle un sentido sería como diferenciar dos gotas de agua en el Océano Atlántico. Solo AI puede dar significado y agrupar los datos en meta datos que puedan ser posteriormente refinados en grupos de datos que tengan sentido para aglomeradores de datos.La cuartada de las vulnerabilidades de la red son las aplicaciones web y la protección API (WAAP), compartir información sensible de forma segura por autor y autenticación, efectivo manejo del consentimiento del cliente y garantía de conformidad de datos. La mitigación de riesgo humano es tan limitada que no escala. Cualquier operación de transacción de información vista a gran escala va a tener que comprometerse con ML y AI. Es el único camino.