Informe sobre la banca abierta (*open banking*) y las interfaces de programación de aplicaciones (*APIs*)

La banca abierta[1] es una tendencia en evolución en muchas jurisdicciones y las autoridades han respondido tomando una amplia gama de acciones en los últimos años. El Comité de Supervisión Bancaria de Basilea ha considerado aspectos de la banca abierta relacionados con el intercambio de datos autorizados por el cliente, en los que el cliente concede inicialmente permiso a un tercero[2] para acceder a sus datos, ya sea directamente o a través del banco del cliente.

Principales conclusiones de los marcos bancarios abiertos

1. La banca tradicional está evolucionando hacia la banca abierta

Si bien el intercambio de datos autorizados de los bancos con terceros se ha estado llevando a cabo durante muchos años, el mayor uso de dispositivos digitales y el rápido avance de las técnicas de agregación de datos están transformando los servicios de banca minorista en todo el mundo. Este intercambio de datos autorizados por los clientes de bancos con terceros se aprovecha para crear aplicaciones y servicios que proporcionen pagos más rápidos y fáciles, mayores opciones de transparencia financiera para los titulares de cuentas, servicios de cuenta nuevos y mejorados, y oportunidades de marketing y venta cruzada. Varias jurisdicciones miembros del Comité han adoptado o están considerando adoptar marcos bancarios abiertos para exigir, facilitar o permitir que los bancos compartan datos del cliente con terceros.

2. Los marcos bancarios abiertos varían según las jurisdicciones en términos de etapa de desarrollo, enfoque y alcance

Las autoridades han tomado o están considerando una serie de acciones relacionadas con la banca abierta en sus respectivas jurisdicciones. Algunas jurisdicciones han adoptado un enfoque prescriptivo, exigiendo a los bancos que compartan datos autorizados por el cliente y exigiendo que terceros que deseen acceder a dichos datos se registren ante determinadas autoridades reguladoras o de supervisión. Algunas otras jurisdicciones han adoptado un enfoque facilitador mediante la publicación de orientaciones y normas recomendadas, y la liberación de normas API y especificaciones técnicas abiertas. Las jurisdicciones restantes siguen un enfoque basado en el mercado, actualmente no tiene reglas u directrices explícitas que requieran o prohíban el intercambio de datos autorizados por el cliente por parte de los bancos con terceros.

- **La banca abierta todavía está en las primeras etapas de desarrollo en una serie de jurisdicciones.** Aproximadamente la mitad de los miembros del Comité no han observado una evolución significativa de la banca abierta en sus jurisdicciones. Dado que los marcos e iniciativas de banca abierta todavía están en las primeras etapas de aplicación en muchas de estas jurisdicciones, aún no se han observado actividades o datos notables sobre las prácticas bancarias y la evolución del mercado.

[1] La banca abierta se define como el levantamiento e intercambio de datos autorizados por el cliente por parte de los bancos con terceros desarrolladores y empresas para crear aplicaciones y servicios, incluidos, por ejemplo, aquellos que proporcionan pagos en tiempo real, mayores opciones de transparencia financiera para los titulares de cuentas, oportunidades de marketing y venta cruzada. Las jurisdicciones individuales pueden definir la banca abierta de manera diferente.

[2] Un "tercero" se define como cualquier entidad jurídica externa que no forme parte de la organización bancaria supervisada. Los terceros pueden ser entidades supervisadas (p. ej. bancos, otras empresas financieras reguladas) o entidades no supervisadas (p. ej. empresas de tecnología financiera, agregadores de datos, socios comerciales, proveedores, otras empresas de pago no financieras).

- **Hay beneficios y desafíos con cada enfoque para abrir la banca a la hora de equilibrar la seguridad y la solidez bancaria, fomentando la innovación y la protección de los consumidores.** Las jurisdicciones que adoptan un enfoque basado en el mercado, con pocos requisitos relacionados con el intercambio de datos autorizados por el cliente; no obstante, se observaron servicios financieros basados en datos con una gama de opciones centradas en el consumidor. Las jurisdicciones con marcos bancarios abiertos más definidos señalaron los beneficios y la eficiencia de tener expectativas claras y consistentes y estándares API. Sin embargo, no está claro si estos marcos bancarios abiertos fueron impulsados por, o impulsarán, la demanda de los consumidores y la evolución del mercado.
- **Los marcos bancarios abiertos también varían en alcance y requisitos.** Algunos marcos, como la Directiva de Servicios de Pago (PSD2) de la UE, se aplican únicamente a tipos específicos de datos, como los datos de tratamiento de pagos, y proporcionan a terceros acceso tanto a "lectura" como a "escritura" de los datos y a la iniciación de pagos. PSD2 no impide que las jurisdicciones miembros adopten un alcance más amplio. Por ejemplo, la iniciativa de banca abierta del Reino Unido requiere además la inclusión de información disponible públicamente sobre sucursales y cajeros automáticos, productos bancarios y comisiones. En cambio, el marco de Australia proporciona derechos de "sólo lectura" con fines de agregación de datos y, finalmente, abarcará a las industrias más allá de la banca, como los sectores de las telecomunicaciones y la energía.

3. Las leyes de privacidad de datos pueden sentar las bases de un marco bancario abierto

Muchas jurisdicciones que han adoptado marcos bancarios abiertos también se actualizaron o planean actualizar sus leyes de protección de datos y/o privacidad. Las leyes de privacidad de datos en algunas jurisdicciones están ancladas en el principio de que el cliente es propietario de sus datos y tiene el derecho de controlarlos. Algunos otros marcos legales ven a los bancos, y a veces a terceros, como el titular de los datos, pero limitan sus derechos para controlar el uso de dichos datos a los límites del consentimiento proporcionado por el cliente. Las reglas de consentimiento de muchas jurisdicciones también establecen restricciones a la incorporación de datos a cuartas partes y a la reventa de datos de clientes para fines más allá del consentimiento inicial del cliente.

4. Las características multidisciplinarias de la banca abierta pueden requerir una mayor coordinación regulatoria

Dentro de cada jurisdicción, varias autoridades pueden tener un papel en abordar cuestiones relacionadas con el intercambio de datos con terceros por parte de los bancos debido a los aspectos multidisciplinarios de la banca abierta. Entre las autoridades pertinentes figuran, por ejemplo, los supervisores bancarios, las autoridades de competencia y las autoridades de protección de los consumidores, entre otros. Dada la variedad de autoridades involucradas y diversos mandatos de estas autoridades, puede ser necesaria una mayor coordinación para abordar posibles incoherencias o lagunas en la reglamentación.

Desafíos identificados para bancos y supervisores

5. La banca abierta aporta beneficios potenciales, pero también riesgos y desafíos a los clientes, los bancos y el sistema bancario

Muchos bancos reconocerían que la banca abierta tiene el potencial de transformar los servicios bancarios y los modelos de negocio bancarios. Sin embargo, los bancos y supervisores bancarios tendrán que prestar mayor atención a los riesgos que convienen con un mayor intercambio de datos con permisos para los clientes y una creciente conectividad entre los bancos y varias partes.

6. Desafíos de adaptación a los posibles cambios en los modelos de negocio

Los bancos pueden enfrentar a desafíos en la adopción de estrategias necesarias para seguir siendo competitivos y rentables en el cambiante entorno digital. Los desafíos relacionados incluyen el aumento de la competencia y la pérdida potencial de ingresos y depósitos debido a los nuevos competidores, fintechs, que ofrecen servicios financieros y otros tipos de servicios (p. ej. contabilidad, impuestos, asesoramiento financiero y marketing).

7. Desafíos de garantizar la seguridad de los datos en un marco bancario abierto

El uso compartido de datos trae muchos beneficios, pero también resulta en una mayor superficie para ataques cibernéticos. Los datos recopilados por terceros, ya sea mediante *screen scraping* (examinar pantalla), ingeniería inversa o métodos de autenticación *tokenizados* a través de API, pueden ser robados o comprometidos. Además, a medida que se comparten más datos con más partes, la posibilidad de una violación de datos aumenta y, por lo tanto, la gestión eficaz de los datos se ha vuelto más crucial.

8. Algunos de los desafíos que obstaculizan el desarrollo de API para compartir datos autorizados por el cliente incluyen el tiempo y el costo para crear y mantener la API y la falta de estándares API comúnmente aceptados

En las jurisdicciones donde el *screen scraping* o la ingeniería inversa sigue prevaleciendo, los bancos se enfrentan al desafío de equilibrar la seguridad contra la facilidad de acceso. Por lo general los bancos prefieren, y en algunas jurisdicciones deben, utilizar métodos más seguros para compartir datos para ciertos tipos de cuentas, como la autenticación simbólica a través de API, en lugar de *screen scraping* o ingeniería inversa. Estos métodos seguros permiten a los bancos ejercer un mayor control sobre el tipo y la extensión de los datos compartidos, y permiten una gestión y supervisión de accesos más seguras. Además, las API proporcionan ventajas para terceros y clientes, incluidas posibles mejoras en la eficiencia, la estandarización de datos, la privacidad del cliente y las protecciones de datos. Sin embargo, persisten algunos desafíos asociados con el uso universal de las API. El tiempo y el costo para construir y mantener las API (particularmente cuando se realizan de manera bilateral con múltiples organizaciones), la falta de normas comúnmente aceptadas acerca de API en algunas jurisdicciones y el costo económico para que los bancos más pequeños desarrollen y adopten API se han citado como desafíos.

9. La supervisión de terceros puede ser limitada, especialmente en los casos en que los bancos no tienen ninguna relación contractual con el tercero, o cuando el propio tercero no tiene autorización reglamentaria

Las jurisdicciones suelen tener normas para la transmisión de datos, el almacenamiento y otros requisitos de seguridad de la información para los bancos, pero la mayoría de estos requisitos de

supervisión se aplican a los bancos y no necesariamente a terceros no bancarios que forman parte de modelos de negocio de banca abierta.

- **Puede haber una amplia gama de acuerdos de terceros en un modelo de banca abierta.** Los terceros pueden incluir empresas fintech que prestan servicios directos a los consumidores, empresas de agregador de datos intermediarios y potencialmente otras partes que pueden no tener relaciones contractuales con los bancos. Los terceros también pueden incluir entidades no contratadas que son autorizadas o tienen cuentan con licencia por autoridades particulares. En las jurisprudencias sin marcos bancarios abiertos definidos, el establecimiento de requisitos específicos para estos terceros puede ser difícil debido a la ausencia de contratos con bancos u otros controles reglamentarios. Además, los terceros pueden ser capaces de asociarse y compartir datos con permisos para el cliente obtenidos de bancos con cuartas partes sin el conocimiento del banco.
- **En ausencia de una relación contractual, los bancos pueden encontrar difícil ejercer el control y el monitoreo sobre terceros.** En muchos casos, el cliente contrata directamente a la empresa de terceros y, por lo tanto, el banco no tiene una relación contractual directa con el tercero.
- **La supervisión de terceros puede depender del marco reglamentario de cada jurisdicción y de las relaciones contractuales entre bancos y terceros.** Muchos supervisores bancarios aplican los requisitos de seguridad y control a través de las expectativas de subcontratación de los bancos, pero pueden tener una supervisión limitada o nula de terceros. Al igual que los desafíos de supervisión de terceros de los bancos, dependiendo de la jurisprudencia, a los supervisores bancarios les resulta igualmente difícil hacer cumplir sus expectativas de supervisión en los casos en que los bancos no tienen contratos en vigor con el tercero o en los casos en que las relaciones no están comprendidas en las expectativas de supervisión existentes.

10. La responsabilidad en caso de pérdida financiera, intercambio erróneo o pérdida de datos sensibles, es más compleja con la banca abierta, ya que hay más partes involucradas

Con más partes e intermediarios involucrados en la prestación de servicios financieros en un modelo de banca abierta, es más difícil asignar responsabilidad y la cantidad de daños al cliente, si los hubiere. El nivel de claridad y detalle de las regulaciones que protegen a los clientes varía según las jurisdicciones y, en algunos casos, puede que no se haya actualizado para tener en cuenta los modelos de negocio de banca abierta.

11. Los bancos pueden enfrentarse a riesgos reputacionales, incluso en jurisdicciones en las que existen normas de responsabilidad establecidas

Muchos bancos se ven a sí mismos como custodios de los datos de sus clientes y los clientes confían mucho en la capacidad de los bancos para salvaguardar sus datos. Además, los clientes a menudo recurren a la entidad regulada (es decir, su banco) primero con quejas y disputas, incluso si el tercero es responsable de la transacción errónea o violación de datos.

1. Introducción

El documento de prácticas sólidas del Comité de Basilea sobre "Implicaciones de la evolución de las tecnologías fintécnicas para los bancos y supervisores bancarios", publicado en febrero de 2018, identificó el impacto de dos escenarios; el "escenario bancario distribuido" (es decir, la fragmentación de los servicios financieros entre las empresas fintech especializadas y los bancos titulares) y el "escenario bancario relegado" (es decir, los bancos titulares que se convierten en proveedores de servicios de materias primas y las relaciones con los clientes que son propiedad de nuevos intermediarios), para ser potencialmente relevantes para los bancos en una economía cada vez más digitalizada. El impacto de estos escenarios es consecuencia de la evolución de los avances tecnológicos que permiten un acceso rápido y ubicuo a la información y a los servicios por parte de los consumidores, que plantean desafíos al modelo tradicional de banca minorista. Los elementos de estos escenarios se están desarrollando actualmente, como lo demuestra la creciente adopción de varios marcos bancarios abiertos y el uso de API, en varias jurisdicciones.

Este informe examina la evolución de la banca abierta en todas las jurisdicciones del Comité con el objetivo de comprender mejor las implicaciones de la banca abierta para los bancos y los supervisores bancarios. El Comité recopiló información de 25 miembros del Comité de 17 jurisdicciones,[3]centrándose en bancos supervisados y datos con permiso según el cliente.

A los efectos de este informe, el Comité se centró en aspectos de la banca abierta en relación con las formas de intercambio de datos con permiso según el cliente, cuando los clientes conceden inicialmente permiso a una empresa externa ("tercero") ya sea directamente o a través del banco del cliente para acceder a sus datos. [4] Este intercambio de datos autorizados por los clientes por parte de los bancos con terceros podría aprovecharse para crear aplicaciones y servicios que proporcionen pagos más rápidos y fáciles, mayores opciones de transparencia financiera para los titulares de cuentas, servicios de cuenta nuevos y mejorados, y oportunidades de marketing y venta cruzada. Estos podrían ser servicios prestados a lo largo de diferentes segmentos de la cadena de prestación de servicios financieros que tradicionalmente han sido proporcionados por los bancos, o nuevos servicios no financieros que crean valor adicional para la cadena de entrega.

2. Base

Con el desarrollo de la banca en línea y móvil, muchos clientes conceden explícitamente a terceras empresas permiso para acceder a sus datos bancarios personales con el fin de obtener otros servicios. El intercambio de datos ha contribuido a nuevos servicios y productos financieros innovadores. Esto incluye, por ejemplo, herramientas de gestión financiera que agregan todas las cuentas financieras de uno en un panel, transmisiones de pagos sin problemas entre cuentas en diferentes bancos, transacciones de pequeño valor, incluidos pagos intradía y comisiones bancarias y herramientas de comparación de hipotecas. La prestación de servicios financieros a los clientes, una vez integrada

[3] Este informe incluye información de las jurisdicciones miembros del Comité de Basilea de Asia: China (CN), Hong Kong (HK), India (IN), Japón (JP), Corea del Sur (KR), Singapur (SG), Tailandia (TH); América: Argentina (AR), Brasil (BR), Canadá (CA), México (MX), Estados Unidos (EE.UU.); la Unión Europea (UE) – Bélgica (BE), Alemania (DE), Francia (FR), Italia (IT), Luxemburgo (LU), Países Bajos (NL), Suecia (SW), España (ES), Reino Unido (Reino Unido); y otras regiones: Australia (UA), Rusia (RU), Turquía (TR), Sudáfrica (ZA).

[4] Como se explica en el informe, los marcos bancarios abiertos difieren entre jurisdicciones. Además de los datos con permiso según el cliente, algunas jurisdicciones incluyen información disponible públicamente en el ámbito de sus marcos. Cuando proceda, se examinan estos aspectos adicionales de la banca abierta.

verticalmente, está siendo ahora desagregada y ofrecida por terceros no bancarios, como las empresas fintech. Al mismo tiempo, estos terceros también pueden crear nuevos servicios que los bancos pueden aprovechar, agregando valor a la cadena de entrega. Estos avances son todos aspectos de la banca abierta.

Para facilitar dicho intercambio de datos y acceder a estos nuevos servicios, muchos clientes bancarios dan permiso a terceras empresas para acceder a su información bancaria, incluidos, por ejemplo, preparadores de impuestos, contadores, asesores financieros y transmisores de fondos de pago. Estos terceros también han contratado los servicios de agregadores de datos, que tradicionalmente emplean técnicas de raspado de pantalla o ingeniería inversa para recopilar datos con permiso según el cliente en poder de los bancos. La práctica del raspado de pantalla, una forma de extraer datos de sitios web, comenzó como copiado y pegado manual y evolucionó hasta convertirse en un proceso automatizado. Para recopilar datos con permiso según el cliente de los bancos, los métodos de raspado de pantalla requieren que un cliente proporcione al tercero sus credenciales de autenticación (por ejemplo, nombre de usuario y contraseña) que el cliente utiliza para iniciar sesión en el sitio web de banca por Internet de su banco. La práctica de la ingeniería inversa, descompila el código de las aplicaciones de banca móvil para averiguar qué información se intercambia entre la aplicación y los servidores de los bancos (a través de la API no pública) y posteriormente construir una versión de ingeniería inversa de la aplicación móvil que sea capaz de explotar directamente la comunicación desde y hacia los servidores de los bancos. Requiere una segunda inscripción de una aplicación móvil (en este caso la versión de ingeniería inversa) al recibir las credenciales de autenticación del cliente y el uso posterior de estas credenciales o incluso la creación de un conjunto propietario de credenciales de autenticación (al tercero). Esta técnica es a menudo favorecida por los agregadores de datos sobre el raspado de pantalla porque es mucho más escalable y robusta, ya que su rendimiento no está influenciado por los cambios realizados por los bancos en su interfaz de cliente. Ambas técnicas no son seguras para el cliente, ya que el tercero mantiene las credenciales que proporcionan acceso completo a la cuenta del cliente, incluyendo por ejemplo, la capacidad de acceder a datos que no han sido autorizados por el cliente, para ejecutar transacciones financieras y para cambiar las credenciales de autenticación de cliente antes mencionadas. En algunas jurisdicciones, también se han desarrollado y utilizado interfaces propietarias y protocolos de comunicación.

Los bancos, terceros y reguladores reconocen los riesgos de seguridad y protección del cliente asociados con el raspado de pantallas y la ingeniería inversa. Los terceros utilizan estos métodos para recopilar y almacenar credenciales de cliente (es decir, nombre de usuario y contraseña), que podrían ser robadas o mal utilizadas, incluso con fines de fraude de pago. El raspado de pantalla o la ingeniería inversa pueden socavar la capacidad de un banco para identificar transacciones fraudulentas, ya que los bancos no siempre pueden distinguir entre el cliente, el agregador de datos y un tercero no autorizado que inicia sesión y extrae datos confidenciales. Además, después de obtener el consentimiento del cliente, terceros (como agregadores de datos) pueden iniciar sesión en la interfaz del cliente del banco y extraer grandes volúmenes de datos a múltiples intervalos, lo que puede poner una tensión en los sistemas informáticos del banco. Sin embargo, los bancos a menudo no niegan el acceso a terceros cuando hay pruebas de que el cliente dio su consentimiento.

Los bancos ahora están descubriendo que los métodos de autorización tokenizados a través de LAS API proporcionan un mayor control sobre el tipo y el alcance de los datos compartidos y son una

forma más segura de interactuar con terceros. Las API permiten que los programas de software se comuniquen entre sí y compartan información sin intervención humana. Las API no son una creación nueva; tienen una larga historia de uso en aplicaciones de software para la comunicación a través de Internet. Sin embargo, la creación y el mantenimiento de API públicas puede llevar mucho tiempo y ser costoso para los bancos (especialmente cuando se implementan de forma bilateral entre bancos individuales y terceros). Esto puede ser particularmente difícil para los bancos más pequeños que carecen de las economías de escala de las instituciones más grandes. La falta de estándares API comúnmente aceptados en algunas jurisdicciones es un desafío adicional.

Los terceros a menudo también prefieren métodos de autenticación tokenizados a través de API públicas en lugar del raspado de pantalla, ya que es más eficiente y no requiere que ajusten sus procesos automatizados cada vez que un banco individual rediseña su interfaz de cliente.

La adopción de API públicas para el intercambio de datos podría dar lugar a oportunidades tanto para los bancos como para terceros para obtener información y estimular la innovación en los servicios financieros. Una economía de intercambio de datos podría cambiar el modelo de negocio bancario tradicional. Sin embargo, a pesar de las oportunidades potenciales, el intercambio de datos ampliado también podría exponer al sector bancario a un conjunto ampliado de riesgos operativos y reputacionales.

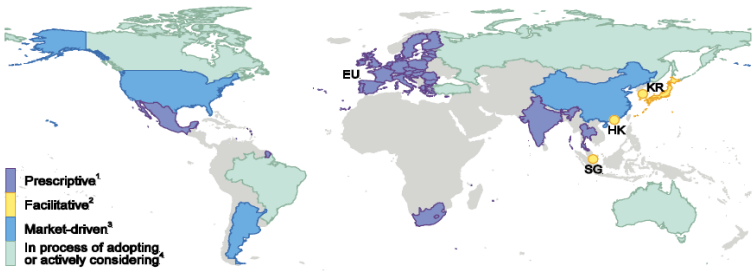
3. Evolución legal y regulatoria de la banca abierta

La adopción de la banca abierta es una tendencia general en todas las jurisdicciones del Comité. El alcance regulatorio y la supervisión de las actividades de banca abierta varían según las jurisdicciones, pero a menudo incluyen el consentimiento fundamental y las expectativas de privacidad, así como los requisitos de seguridad de los datos. Aunque hay un enfoque creciente en el uso de API que se basan en métodos de autenticación tokenizados para compartir datos, la mayoría de las jurisdicciones actualmente no prohíben las prácticas de raspado de pantalla e ingeniería inversa.

Las autoridades han tomado una serie de medidas relacionadas con la banca abierta en sus respectivas jurisdicciones. Algunas jurisdicciones requieren que los bancos compartan datos con permiso satismnito por el cliente y requieren que terceros se registren ante una autoridad reguladora o supervisora en particular. Otras jurisdicciones han emitido orientación y estándares recomendados, y publicado estándares API abiertos y especificaciones técnicas. Las jurisdicciones restantes siguen un enfoque basado en el mercado y actualmente no tienen reglas u directrices explícitas que requieran o prohíban el intercambio de datos con permiso sin cliente por parte de los bancos con terceros (véase la figura 1 a continuación).

Visión global de la evolución de la banca abierta

Figura 1



Los límites mostrados y las designaciones utilizadas en este mapa no implican la aprobación o aceptación oficial por parte del BIS.
UE - Unión Europea, HK - Hong Kong SAR, KR - Corea, SG - Singapur.
[1] Requiere el intercambio de datos, [2] Alienta el intercambio de datos, [3] No hay regla/orientación explícita que requiera el intercambio de datos, [4] En proceso de adopción o considerando activamente la adopción.
Fuente: Sobre la base de la información recopilada de las jurisdicciones del Comité

Entre los miembros del Comité, varios tienen algún tipo de normas bancarias abiertas que requieren que los bancos compartan datos autorizados por el cliente con terceros autorizados. [5] Otros han emitido orientación en lugar de reglas,[6]han comunicado que están en proceso de elaboración de normas, o están considerando activamente la adopción de algún tipo de marco bancario abierto que puede incluir normas.[7] Algunas jurisdicciones se basan en iniciativas impulsadas [8] por el mercado y actualmente no están considerando la adopción de un enfoque basado en normas para la banca abierta. No obstante, cada enfoque tiene beneficios y desafíos a la hora de equilibrar la seguridad y la solidez de los bancos, fomentando la innovación y la protección de los consumidores.

Un marco bancario abierto integral puede incluir normas, normas y/o prácticas de la industria en una serie de cuestiones, así como diferentes autoridades reguladoras. Esto es especialmente cierto en los casos en los que terceros y terceros no regulados obtienen acceso a los datos autorizados por el cliente bancario. Las autoridades involucradas en la banca abierta pueden incluir:

1. Supervisor bancario: autoridad tradicional que establece requisitos y supervisa a los bancos regulados.
2. Cuerpo de Establecimiento de Normas Técnicas o APIs: un organismo que establece normas y certifica entidades que cumplen con dichas normas.
3. Autoridad de la Competencia: autoridad que supervisa, promueve y, cuando es necesario, toma medidas para garantizar el buen funcionamiento de los mercados.
4. Autoridad de Protección del Consumidor: una autoridad que garantiza que los consumidores generalmente no se sintien por las prácticas monopolísticas y oligopolísticas de las organizaciones. En algunas jurisdicciones, sus mandatos pueden incluir garantizar que los consumidores no se desfavorecen por actos o prácticas injustos, engañosos o abusivos.
5. Autoridad de Privacidad de Datos: una autoridad que establece requisitos relacionados con la protección de datos personales y/o de clientes.
6. Mecanismo Alternativo de Controversias: un organismo que proporciona una plataforma o proceso para mediar disputas entre consumidores y organizaciones.

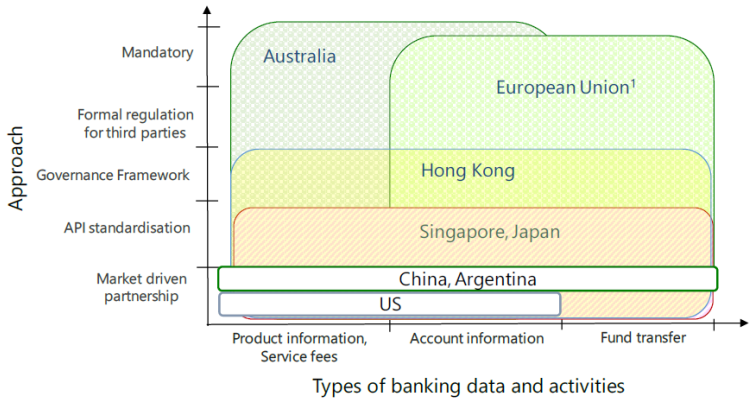
[5] IN, TH, MX, ZA, EU (en el marco de PSD2)
[6] HK, SG, KR
[7] A partir de noviembre de 2018 - En proceso de desarrollo de reglas: AU, BR, RU. Activamente Considerando Adoptar Abierto Banca Marco de referencia: CA, TR.
[8] AR, CN, NOSOTROS

7. Otros: cualquier otro organismo que tenga un mandato sobre las entidades dedicadas a la banca abierta.

En algunas jurisdicciones, como Australia, las autoridades de competencia son responsables de la aplicación de marcos bancarios abiertos para aumentar la competencia en el sector bancario y fomentar la innovación. En otras jurisdicciones, como la UE, la India, Hong Kong y Singapur, el banco central o supervisor bancario supervisa el marco para facilitar los pagos más rápidos y fáciles y fomentar la innovación. El alcance y el grado de prescripción varían según las jurisdicciones. Por ejemplo, en la UE, la atención se ha centrado en los datos de las cuentas de pago. Además, el Reino Unido ha implementado medidas adicionales, como el requisito de que los nueve bancos más grandes y las sociedades de construcción compartan información disponible públicamente sobre sucursales, servicios y tarifas de sucursales y cajeros automáticos. En cambio, Australia tiene previsto proporcionar inicialmente derechos de solo lectura a terceros sin capacidad para transferir fondos, pero los datos de los consumidores de otros sectores, como la energía y las telecomunicaciones, finalmente se cubrirán de manera que los datos puedan ser compartidos entre sectores. Otras jurisdicciones, como Hong Kong y Singapur, emitieron recomendaciones sobre diseños de API abiertos y especificaciones técnicas, con el objetivo de facilitar la adopción de prácticas de banca abierta (véase la figura 2).

Comparación de marcos bancarios abiertos

Figura 2



[1] UE: el perímetro representado en esta figura representa el ámbito de aplicación del PSD2 de la UE, que sólo se aplica a los servicios de pago. Las jurisdicciones individuales dentro de la UE pueden optar por ampliar el alcance de sus marcos bancarios abiertos más allá de los requisitos de PSD2 (por ejemplo, FR y Reino Unido).
Fuentes: Sobre la base de la información recopilada de las jurisdicciones del Comité.

En general, los marcos reglamentarios de banca abierta pueden abarcar permitir el acceso de terceros a los datos con permisos de los clientes, exigir la concesión de licencias o autorizaciones de terceros, imponer restricciones a las prácticas de raspado y ingeniería inversa de la pantalla y aplicar los requisitos de privacidad y divulgación y consentimiento de los datos. Los marcos también pueden contener disposiciones relacionadas con si terceros pueden compartir y/o revender datos a partir de "cuartas partes", utilizar los datos para fines más allá del consentimiento original del cliente y para si los bancos o terceros podrían ser remunerados por compartir datos. Los marcos bancarios

abiertos también pueden contener expectativas o requisitos sobre el almacenamiento de datos y la seguridad. La Figura 2 ayuda a ilustrar cómo los marcos bancarios abiertos se comparan por enfoque y tipo de datos bancarios cubiertos en ciertas jurisdicciones del Comité.

4. Papeles de los bancos, terceros y autoridades reguladoras en un ecosistema financiero digital ampliado

4.1 Licencia y autorización de terceros

La mayoría de las jurisdicciones del Comité no requieren que terceros estén autorizados o autorizados para acceder a los datos autorizados por el cliente del banco (ya sea mediante raspado de pantalla, ingeniería inversa o API). Los supervisores bancarios en estas jurisdicciones generalmente requieren o esperan que los bancos tengan acuerdos bilaterales con terceros que accedan a los datos. Sin embargo, algunas jurisdicciones no requieren ni esperan que los bancos y terceros tengan contratos bilaterales antes de compartir datos.

Para las jurisdicciones que requieren que terceros sean autorizados o autorizados, el alcance de sus normas puede limitar los tipos de terceros que requieren autorización. El ámbito de la autorización puede variar de estrecho a amplio; es decir, de proveedores de pago que acceden a datos relacionados con cuentas de pago a todos los terceros que acceden a diversos tipos de datos con permiso para el cliente. En virtud de los marcos que requieren la concesión de licencias o autorizaciones, las autoridades particulares deben aprobar a estos terceros. No obstante, en función del marco de licencia o autorización, es posible que los terceros cubiertos sigan estando obligados a tener contratos o acuerdos con los bancos antes de acceder a los datos con permiso según el cliente.

En algunas jurisdicciones con regulaciones de banca abierta prescriptivas, como en la UE, se imponen requisitos de intercambio de datos a terceros autorizados que están autorizados o aprobados por los reguladores. Los bancos están obligados a aceptar solicitudes de acceso de estos terceros autorizados, a menos que existan razones objetivas para no hacerlo, como el riesgo de fraude. En particular, el PSD2 de la UE no permite a los agregadores de cuentas no autorizados acceder a los datos de pago autorizados por el cliente. Suponiendo que se concedieran exenciones a los bancos con normas API suficientes, generalmente no se permitiría a terceros autorizados volver a la remediación de pantalla o a la ingeniería inversa de los datos cubiertos por PSD2 (es decir, los datos de la cuenta de pago). Por otro lado, el raspado de pantalla y la ingeniería inversa pueden continuar para[9]los datos de cuentas de no pago, como los datos de la cuenta de valores no cubiertos por PSD2.

4.2 Gestión de riesgos de terceros

Las jurisdicciones suelen tener requisitos de intercambio de datos, almacenamiento y seguridad, pero la mayoría de estos requisitos son para bancos y servicios bancarios subcontratados, no

[9] PSD2 es independiente de la tecnología, pero las Normas Técnicas Regulatorias para una autenticación sólida del cliente y estándares de comunicación abiertos comunes y seguros requieren que el acceso a los datos sea proporcionado por el proveedor de servicios de pago de servicio de la cuenta (Ie el titular de los datos, por lo general el banco) a través de una interfaz segura, ya sea a través de una interfaz dedicada (Ie API) o a través de la interfaz de cliente adaptada. Autorizados y los terceros regulados también deben ser identificados con un eIDAS certificado y las mismas reglas sobre la autenticación segura del cliente se aplican si se utiliza un tercero o no. EBA/GL/2018/07, https://eba.europa.eu/documents/10180/2250578/Final+Report+on+Guidelines+on+the+exemption+to+the+fall+back.pdf/4e3b9449-ecf9-4756-8006-cbbe74db6d03

necesariamente para terceros que contraen directamente con clientes bancarios. En general, los supervisores bancarios tienen una autoridad limitada sobre terceros, especialmente sobre aquellos que no tienen acuerdos contractuales con los bancos que supervisan y sobre aquellos que no están registrados ante una autoridad independiente.

En algunas jurisdicciones, las políticas de externalización responsabilicen a los bancos para garantizar que terceros cumplan con estas normas y, en general, estipulen la documentación como parte de los acuerdos contractuales. En otras jurisdicciones, los supervisores bancarios tienen autoridad de supervisión sobre terceros registrados.

La UE describe sus requisitos de almacenamiento de datos y seguridad para el intercambio de datos en virtud de las Normas Técnicas Regulatorias de PSD2 para una autenticación sólida de los clientes y estándares de comunicación abiertos comunes y seguros. [10] Cuando el tercero esté autorizado o supervisado por una autoridad, no se espera que los bancos de la UE inspeccionen o supervisen los marcos de seguridad de datos puestos en marcha por el tercero autorizado.

Independientemente del tipo de marco vigente, dependiendo de la jurisdicción, podría existir una laguna regulatoria cuando un tercero tenga el consentimiento de un cliente para acceder a sus datos bancarios, pero no tenga obligaciones contractuales con el banco y no esté obligado a ser autorizado por una autoridad determinada (por ejemplo, terceros que practican el raspado de pantalla). En este caso, tanto las autoridades como el banco tendrían una capacidad limitada para estipular requisitos de control de riesgos sobre el tercero no autorizado (y cualquier cuarta parte).

5. Responsabilidad y reparación del cliente

Determinar la responsabilidad final en transacciones fraudulentas o erróneas puede ser un desafío en jurisdicciones donde los marcos de responsabilidad nacionales no se ajustan para tener en cuenta la banca abierta y el intercambio de datos entre varias partes. Los terceros pueden confiar o apoyar los servicios de terceros (es decir, agregadores de datos en algunas jurisdicciones). Cuando se produce una actividad errónea o fraudulenta, no siempre está claro qué parte (banco, tercero o tercero) es responsable. Además, cuando los datos autorizados por el cliente se comparten incorrectamente (por ejemplo, tipo o alcance incorrecto de los datos, o la parte incorrecta), puede no estar claro cómo se deben cuantificar los daños al cliente.

Marco de responsabilidad del cliente. La mitad de las jurisdicciones del Comité tienen leyes o regulaciones existentes o planificadas que abordan la responsabilidad del cliente con respecto al acceso a los datos por parte de terceros. Por ejemplo, PSD2 exige a terceros autorizados que tengan un seguro de indemnización profesional, o una garantía comparable, contra responsabilidades específicas, como transacciones no autorizadas o no ejecución, y ejecución defectuosa o tardía de operaciones de pago. En otras jurisdicciones, la responsabilidad del cliente puede ser abordada por las leyes nacionales de protección de datos personales, las leyes bancarias generales que cubren la protección del cliente contra transacciones fraudulentas, las leyes de protección del consumidor y

[10] Normas de aplicación de PSD2: Reglamento Delegado (UE) 2018/389 de la Unión Europea: las Normas Técnicas De Regulación para una autenticación sólida de los clientes y normas de comunicación abiertas comunes y seguras, https://eur-lex.europa.eu/eli/reg_del/2018/389/oj

los códigos civiles, comerciales y penales. En algunas jurisdicciones, la responsabilidad del cliente se incluye en los contratos o acuerdos bilaterales entre el banco y el proveedor de servicios externo.

Mecanismos alternativos[11] de reclamación o controversia sinfines específicos para la banca abierta. La mitad de las jurisdicciones del Comité tienen mecanismos de tramitación de reclamaciones existentes o planificados o mecanismos alternativos de solución de controversias que abarcan cuestiones relacionadas con la banca abierta.

Entre las jurisdicciones con mecanismos de tramitación de reclamaciones existentes o previstos o mecanismos alternativos de resolución de controversias, la PSD2 de la UE exige que los proveedores de servicios de pago, incluidos terceros autorizados, pongan en marcha procedimientos de resolución de reclamaciones adecuados y eficaces. En Hong Kong, se espera que los términos que abordan los mecanismos de tramitación de reclamaciones se incluyan en contratos con terceros, ya que los clientes no deben ser responsables de ninguna pérdida directa sufrida como resultado de transacciones no autorizadas realizadas a menos que el cliente actúe de forma fraudulenta o con negligencia grave. En Japón, la Asociación de Servicios de Pago Electrónico, un organismo privado, es responsable de gestionar las quejas de los clientes relacionadas con la banca abierta, mientras que en Luxemburgo y Rusia, esa responsabilidad pertenece a las autoridades financieras. En Singapur, la Comisión de Protección de Datos Personales facilita la reclamación entre el cliente y el proveedor. La India tiene un Sistema De Pueblo para las Transacciones Digitales.

Para las jurisdicciones que no tienen orientación regulatoria que requiere mecanismos de quejas o manejo de disputas, los clientes a menudo inicialmente llevan sus quejas y disputas a la entidad regulada (es decir, su banco).

6. Protección de datos del consumidor

Leyes de privacidad de datos. Muchas jurisdicciones que están adoptando o planean adoptar marcos bancarios abiertos tienen leyes generales de privacidad de datos. Estas leyes de privacidad de datos han ayudado a proporcionar una base para el marco bancario abierto de la jurisdicción. Sin embargo, las diferencias en las leyes de privacidad de datos entre jurisdicciones tienen implicaciones para el desarrollo de varios marcos bancarios abiertos. Por ejemplo, el Reglamento General de Protección[12] de Datos (RGPD) de la UE destaca por su principio principal de que los consumidores poseen y controlan sus datos. Por el contrario, las leyes de privacidad de datos de algunas otras jurisdicciones se basan en el principio de que las empresas, incluidos los bancos, son las propietarias de los datos que mantienen. Por ejemplo, en algunas jurisdicciones, se requiere permiso del banco inicial antes de que los datos sean compartidos por el tercero a una cuarta parte. Sin embargo, casi todas las jurisdicciones del Comité restringen a terceros la reventa o el uso de datos para fines fuera del alcance del consentimiento inicial del cliente, y generalmente requieren que los terceros obtengan más consentimiento del cliente antes de revender los datos del cliente.

Divulgación y Consentimiento. La mayoría de las jurisdicciones del Comité tienen, o están en proceso de desarrollar, reglas que requieren divulgación y/ o consentimiento del cliente. De ellos, muchas jurisdicciones requieren el consentimiento del cliente, pero no prescriben el contenido exacto

[11] Definido como un organismo que proporciona una plataforma o proceso para mediar disputas entre consumidores y Organizaciones.
[12] https://eugdpr.org/the-regulation/

del formulario de divulgación. Los requisitos de divulgación y consentimiento se observan principalmente en los acuerdos contractuales entre los bancos y terceros.

***Screen scraping* (Examinar pantalla).** Algunas jurisdicciones han desarrollado, o están desarrollando, limitaciones en el *screen scraping*. Por ejemplo, en la UE, los terceros no pueden examinar los datos de la cuenta de pago a través de la interfaz de cliente estándar de los bancos a partir de septiembre de 2019. [13] En su lugar, los bancos ofrecen API dedicadas o una interfaz de cliente modificada que permite a terceros identificarse mediante certificados de autenticación al acceder a los datos de los clientes. Los terceros utilizan técnicas de raspado de pantalla desde esta interfaz de usuario modificada, pero la interfaz puede limitar o controlar los datos disponibles para el tercero. Esta interfaz de cliente modificada también se utilizaría como mecanismo de contingencia cuando la API del banco no está disponible. En la UE, los bancos pueden quedar exentos de establecer un mecanismo de contingencia si sus autoridades competentes determinan que las interfaces específicas del banco (es decir, las API) cumplen ciertas condiciones. Aunque muchas jurisdicciones no tienen leyes o regulaciones específicas con respecto a la práctica del raspado de pantalla, varias jurisdicciones están emitiendo orientación sobre [14] la autenticación de usuarios basada en marcos de API abiertos que requieren el uso de protocolos simbólicos como las API abiertas de OAuth 2.0, lo que ayudará a la industria a alejarse del *screen scraping*.

7. Futuro potencial del uso de API en la banca abierta

Como parte de sus estrategias de API, los profesionales de la industria están adoptando diferentes combinaciones de API abiertas (interfaces basadas en estándares públicos), API de socios (basadas en estándares diseñados por socios estratégicos) y API cerradas (basadas en el estándar privado del banco). En algunas jurisdicciones, los bancos han adoptado tanto las API de socios como las API abiertas. Mientras que en algunas jurisdicciones de la UE, los bancos han comenzado a adoptar varias estrategias de API, es razonable suponer que más bancos de la UE adoptarán API abiertas en respuesta a PSD2.

Servicios facilitados por API. Casi dos tercios de las jurisdicciones del Comité creen que la banca abierta y el uso ampliado de las API tendrán un impacto en los servicios bancarios. Los principales tipos de servicios bancarios compartidos que se espera que se afecten son los servicios de pago, los servicios de préstamo (por ejemplo, préstamos e hipotecas), los productos y servicios de inversión (incluida la planificación y gestión financiera) y los servicios contable.

Si bien las jurisdicciones del Comité indicaron expectativas de que probablemente habrá un impacto en los servicios bancarios que, en los servicios no bancarios, casi la mitad de las jurisdicciones del Comité creen que los servicios no bancarios se facilitarán mediante el intercambio de datos autorizados por el cliente. Los dos principales servicios mencionados por las jurisdicciones del Comité son aplicaciones de estilo de vida (por ejemplo, servicios de transporte, conserjería, servicios

[13] Las disposiciones de PSD2 sobre la autenticación sólida del cliente y sobre la comunicación segura se especifican directamente en las normas técnicas regulatorias (RTS). Estas incluyen disposiciones sobre el acceso a los datos con permisos para el cliente mediante el uso de "raspado de pantalla".

[14] OAuth 2.0 y sus versiones más recientes proporcionan Autorización flujos para aplicaciones que normalmente se ejecutan en Internet, como API y aplicaciones web. Oauth 2.0 es el ejemplo de implementación de un tokenizado método de autenticación.

inmobiliarios y de ocio) y servicios de negocios (por ejemplo, contabilidad, gestión de gastos, impuestos y servicios de presupuestación).

El impacto de la banca API en los modelos de negocio de los bancos probablemente dependerá de la extensión y la forma de intercambio de datos, el surgimiento de nuevos proveedores de servicios financieros, el cambio en la cuota de mercado y la velocidad del cambio.

8. Usos de terceros de datos con permiso para el cliente

Terceras partes. Los agregadores de datos y los proveedores de servicios de pago son los tipos más comunes de entidades de terceros que acceden a los datos con permiso del cliente. Otros terceros citados en menor medida incluyen asesores financieros, asesores de inversión, aseguradores de seguros, contadores, agentes fiscales, evaluadores de propiedades, agencias de referencia crediticia y procesadores de hipotecas y préstamos. Las jurisdicciones de la UE también hicieron referencia a PSD2 y a las normas técnicas reguladoras complementarias para una autenticación sólida de los clientes y normas de comunicación abiertas comunes y seguras, que contiene disposiciones para que los proveedores de servicios de iniciación de pagos autorizados y los proveedores de servicios de información sobre cuentas (que también pueden ser bancos) accedan a los datos autorizados por el cliente. Las jurisdicciones de la UE observaron un aumento de dichos terceros cuando PSD2 entró en vigor en enero de 2018.

Usos de terceros. Los usos comunes de los datos con permisos para el cliente incluyen el procesamiento de pagos con tarjeta de crédito, servicios de gestión de efectivo y servicios financieros, como robo-advisory y servicios de gestión de finanzas personales proporcionados por empresas fintech. Un tema común identificado entre las jurisdicciones del Comité es que muchos terceros aprovechan los datos para enriquecer la experiencia del usuario al proporcionar vistas agregadas de las finanzas de los usuarios para una mejor planificación financiera. Algunos ejemplos son el reequilibrio de cuentas para habilitar pagos, la supervisión de patrones de gastos, incluidas las alertas y recordatorios de los usuarios, el asesoramiento de inversión basado en los activos financieros de los clientes, los productos de venta cruzada, incluidos los productos de crédito y los programas de fidelización, y los servicios de contabilidad, informes de impuestos y gestión de gastos para clientes corporativos.

Los datos relacionados con los servicios de pago se acceden con mayor frecuencia a través de las API, mientras que los datos con fines informativos (como saldos e historiales de transacciones) se acceden comúnmente a través del raspado de pantalla. Este fenómeno también puede deberse a requisitos reglamentarios en algunas jurisdicciones, como en la UE, donde se espera que los datos relacionados con los pagos se compartan a través de las API.[15]

Remuneración por compartir datos con permiso del cliente. Muchas jurisdicciones del Comité no tienen restricciones reglamentarias sobre la capacidad de los bancos para cobrar tasas a terceros por compartir datos con permisos para el cliente u otros acuerdos de remuneración. Algunas jurisdicciones tienen, o están contemplando activamente, restricciones a la remuneración, o a las tarifas de cobro a terceros destinatarios de datos o a clientes.

[15] Tenga en cuenta que el requisito de utilizar una interfaz específica para acceder a los datos se aplica a partir de septiembre de 2019.

Si bien la mayoría de las jurisdicciones no tienen restricciones a la remuneración, algunas han informado de que hay casos limitados en los que los bancos están siendo remunerados. Estas jurisdicciones no tienen regulaciones para limitar o regir dichas tasas, pero describieron la remuneración como incluida en los acuerdos contractuales entre bancos y terceros. En la UE, aunque el acceso a la información de la cuenta de pago debe proporcionarse "de manera no discriminatoria" en el marco de PSD2 (es decir, sin comisiones y proporcionando el mismo nivel de acceso a todos los terceros autorizados), la remuneración por los servicios adicionales puede estar sujeta a un acuerdo bilateral y normalmente se proporciona sobre una base de comisión con tasas parcialmente fijadas.

Consentimiento del cliente. La mitad de las jurisdicciones del Comité requieren que los bancos obtengan el consentimiento del cliente para compartir los datos de un cliente con terceros, mientras que en la otra mitad de las jurisdicciones, los bancos pueden aceptar el consentimiento del cliente a través de la confirmación proporcionada por el tercero. Esto último es especialmente frecuente en la UE. Una jurisdicción requiere que terceros notifiquen a los bancos el consentimiento del cliente antes de compartir datos con el fin de acomodar protocolos de autenticación seguros. Otras dos jurisdicciones no tienen reglas explícitas con respecto a la autenticación de clientes, por lo que cualquiera de los dos métodos podría utilizarse. Sin embargo, una de esas jurisdicciones tiene expectativas de supervisión para garantizar la validez de los controles de autenticación del consentimiento del cliente y de la autorización digital.

Intercambio de datos con cuartas partes. La mayoría de las jurisdicciones del Comité han indicado que los terceros podrían proporcionar datos a los cuartos, siempre que se especifique en los acuerdos contractuales. Algunas jurisdicciones han implementado leyes o reglamentos que permiten a terceros compartir datos a terceros (por ejemplo, las leyes relacionadas con las agencias de crédito y las regulaciones PSD2 para la UE).

9. Acceso y transmisión de datos

El acceso a los datos y la transmisión por parte de terceros pueden ir desde un proceso básico de copia y pegado de raspado de pantalla hasta la transmisión de elementos de datos estandarizados mediante API. A pesar de la importancia de garantizar la seguridad de los datos con permisos para el cliente, los enfoques para el acceso y la transmisión de datos variaron a través de las jurisdicciones de acuerdo con los respectivos marcos legales y reglamentarios.

En jurisdicciones sin requisitos reglamentarios explícitos, los bancos y terceros tienen más flexibilidad en el acceso a los datos y las prácticas de transmisión. En estas jurisdicciones, el alcance y el proceso de intercambio de datos pueden regirse por un contrato ejecutado entre el banco y el tercero, en particular cuando se accede a los datos mediante API. La protección de la seguridad de los datos, incluida la arquitectura de acceso y transmisión designada, generalmente se establece como un requisito en esos contratos. Incluso en las jurisdicciones que tienen un marco regulatorio establecido, a menudo se requiere un formato de contrato estandarizado, y los bancos generalmente ejercen su juicio para aceptar o rechazar la conexión API solicitada por terceros.

En las jurisdicciones que no prohíben el raspado de pantalla o la ingeniería inversa, existe el riesgo de que terceros se basen en estos métodos para mitigar sus costos (por ejemplo, legal y de TI). Las

preocupaciones con el raspado de pantalla o la ingeniería inversa incluyen el riesgo de que el alcance de los datos recopilados por terceros pueda extenderse más allá del consentimiento original del cliente, el riesgo de restringir los sistemas de TI de un banco no diseñados para consultas automatizadas de gran volumen e inicios de sesión de alta frecuencia por parte de agregadores de datos. Otras preocupaciones incluyen el riesgo de recopilación incorrecta de datos, como resultado de cambios en las interfaces de los clientes de un banco.

Algunos supervisores bancarios supervisan directamente la seguridad de los datos de terceros, mientras que otros lo hacen indirectamente a través de los programas de gestión de riesgos de los bancos supervisados. En cualquier caso, los bancos a menudo tienen un papel principal en garantizar la seguridad de los datos con permisos de los clientes a lo largo de su cadena de servicios de entrega al cliente, garantizando su propia seguridad de los datos o garantizando la seguridad de los datos en terceros a través de contratos.

Transmisión segura. La transmisión segura de datos confidenciales a través de Internet es un control necesario para mitigar el riesgo operativo para los bancos y terceros. Las prácticas comunes que los bancos utilizan para transmitir datos de forma segura a terceros y restringir el acceso a datos confidenciales incluyen el intercambio de certificados y el cifrado de extremo a extremo.

Sistemas *legacy* (heredados). En algunas jurisdicciones, los bancos están implementando directamente API que son compatibles con sistemas *legacy* (por ejemplo, a través de capas de *middleware*) mientras que otros están trabajando directamente con soluciones de infraestructura modernas. Una jurisdicción informó de que los bancos están actualizando sus sistemas e infraestructura debido a las cuestiones de costos y operaciones relacionadas con el mantenimiento y la interconexión con los sistemas *legacy*. Otras autoridades también indicaron que, en algunos casos, los bancos han tenido que mejorar sus mecanismos de resiliencia y recuperación de TI para determinados sistemas *back-end*, como resultado de las mayores expectativas de disponibilidad de las API.

Estándares API locales y regionales. Los estándares API son un conjunto de reglas y especificaciones que podrían ser utilizados por varios bancos y terceros para comunicarse utilizando el mismo conjunto de protocolos de comunicación, perfiles de seguridad y diccionarios de datos. Por lo tanto, los terceros que desean acceder a los datos con permisos de los clientes de los bancos pueden optimizar sus operaciones para aprovechar dichos estándares de API en lugar de diseñar programas individuales que se comuniquen con cada banco.

Una serie de diferentes estándares de API están evolucionando en todo el mundo. La mitad de las jurisdicciones del Comité indicaron que existen normas API comúnmente utilizadas en sus jurisdicciones. El desarrollo de estos estándares a menudo incluye la participación de la industria. Sin embargo, no existe ningún estándar de API adoptado globalmente. A medida que se desarrollan estándares de API regionales y locales en todo el mundo, las empresas de terceros pueden necesitar utilizar diferentes estándares de API para comunicarse con los bancos en diferentes jurisdicciones. Esto podría dar lugar a desafíos potenciales, como ineficiencias para terceros o fragmentación del ecosistema financiero digital.

10. Gestión de riesgos de API

Los miembros del Comité han identificado una variedad de posibles problemas operativos y de seguridad cibernética relacionados con el uso de API, incluidas violaciones de datos, uso indebido, falsificación, ataques de denegación de servicio e inicio de sesión no cifrado. Otros tipos de riesgos identificados incluyen mal funcionamiento de la infraestructura, velocidad de ejecución y operaciones, ataque de hombre en el medio, compromiso de *tokens* y suplantación de direcciones IP. Una puerta de enlace de API también podría ser un único punto de error si no está diseñada para ser resistente.

Los mecanismos utilizados por algunos bancos para mitigar estos riesgos incluyen privilegios de acceso más estrictos, cifrado de extremo a extremo autorizado, mecanismos de autenticación, pruebas de vulnerabilidad, establecimiento de una pista de auditoría, establecimiento de tiempos de expiración de tokens, listas blancas de IP, firewalls y monitoreo de incidentes cibernéticos relacionados con las API como parte del programa general de monitoreo de incidentes cibernéticos.

Muchas jurisdicciones indicaron que sus bancos supervisados aprovechan las políticas de gestión de riesgos existentes, en particular para la seguridad cibernética y el riesgo operativo. Para algunas jurisdicciones del Comité de la UE, se deben realizar evaluaciones separadas para evaluar el cumplimiento de la seguridad de los datos con el RGPD. Esto podría plantear desafíos para los bancos y terceros en el cumplimiento de los requisitos de pago abierto bajo PSD2, garantizando al mismo tiempo el cumplimiento de los requisitos de seguridad de datos personales del RGPD.

11. Conclusión

Muchas jurisdicciones del Comité de Basilea han adoptado, o están considerando adoptar, algún tipo de marco bancario abierto. Los marcos bancarios abiertos varían en alcance y contenido dependiendo de los factores nacionales y regionales, pero comparten muchos riesgos y desafíos comunes. Los marcos reglamentarios y jurídicos de muchas jurisdicciones tienen autoridad limitada sobre algunas de las partes que interactúan con los bancos. La banca abierta tiene el potencial de transformar los servicios bancarios y los modelos de negocio bancarios. Sin embargo, los bancos y los supervisores bancarios deberán prestar mayor atención a los riesgos que acompañan: i) el mayor intercambio de datos con permisos para el cliente; y ii) la creciente conectividad de diversas entidades involucradas en la prestación de servicios financieros.

Anexo: Glosario

a) Banca abierta: el intercambio y el aprovechamiento de los datos con permiso por parte de los bancos con terceros desarrolladores y empresas para crear aplicaciones y servicios, como aquellos que proporcionan pagos en tiempo real, mayores opciones de transparencia financiera para los titulares de cuentas y oportunidades de marketing y venta cruzada. Las jurisdicciones individuales pueden definir la banca abierta de manera diferente.
b) Interfaces de programación de aplicaciones (API): un conjunto de reglas y especificaciones para que los programas de software se comuniquen entre sí, que forma una interfaz entre diferentes programas para facilitar su interacción.
    i. Open API: una interfaz que proporciona un medio de acceso a los datos basados en un estándar público. También conocido como API externa o pública.
    ii. API interna/cerrada: una interfaz que proporciona un medio de acceso a los datos basados en un estándar privado. También conocido como API interna.
    iii. API de socios: una API creada con uno o dos socios estratégicos que crearán aplicaciones, complementos o integraciones con la API.
c) Datos con permiso sano: datos de clientes minoristas en poder de los bancos (por ejemplo, transacciones de clientes, datos de identificación personal e historial financiero del cliente) que están autorizadas por el cliente del banco para ser accedidos por un tercero (y posiblemente compartidos en adelante con cuartas partes).
d) Agregadores de datos: entidades afiliadas y/o de terceros que recopilan datos, incluidos los datos con permiso satisbo del cliente, mediante el uso de API, raspado de pantalla u otros medios. Estas entidades pueden ofrecer servicios directamente al cliente, a otras partes que presten servicios al cliente, o a otras partes (es decir, "cuartas partes").
e) Cuarta parte: un socio o proveedor estratégico al que un tercero subcontrata algún trabajo.
f) Ingeniería inversa: un proceso de análisis de la aplicación compilada para extraer información sobre su código fuente. El objetivo de la ingeniería inversa es entender el código para determinar qué información se intercambia entre una aplicación y un servidor.
g) *Screen scraping (Examinar pantalla)*: el proceso de utilizar *scripts* automatizados para recopilar elementos de datos mostrados de una aplicación para que los datos puedan ser utilizados por otra aplicación. El examinador de plataformas en línea generalmente requiere el uso de credenciales de cliente para iniciar sesión y acceder a los datos como si el examinador de pantalla fuera el cliente.
h) Bancos supervisados: Bancos internacionalmente activos en línea con el alcance del marco BCBS, pero para algunas jurisdicciones del Comité, también se incluyen otros bancos.
i) Tercero: cualquier entidad jurídica externa que no forme parte de la organización bancaria supervisada. Los terceros pueden ser entidades supervisadas (por ejemplo, bancos, otras empresas financieras reguladas) o entidades no supervisadas (por ejemplo, empresas de tecnología financiera, agregadores de datos, socios comerciales, proveedores, otras empresas de pago no financieras).
j) Autenticación *tokenizada*: uso de un *token* basado en software que sustituya las credenciales de seguridad que identifican al usuario y los privilegios del usuario con el fin de acceder a aplicaciones y datos con permiso sin el cliente.