

Situación Economía Digital

ABRIL 2016 | UNIDAD REGULACIÓN DIGITAL



01
El estándar de banca abierta: definiendo el modelo bancario de API

02
Organismos reguladores e inclusión financiera: un panorama cambiante

03
La Directiva de Seguridad de las redes y de la información (NIS)

04
Panorama digital de China: un reino digital gobernado por tres reyes

05
Unicornios: las mayores empresas emergentes

Índice

Resumen	3
1 El estándar de banca abierta: definiendo el modelo bancario de API	4
2 Organismos reguladores e inclusión financiera: un panorama cambiante al que hay que prestar mucha atención	7
3 La Directiva de Seguridad de las redes y de la información (NIS). Parte 1 de 2	10
4 Panorama digital de China: un reino digital gobernado por tres reyes	12
5 Unicornios: las mayores empresas emergentes	15

Resumen

El estándar de banca abierta: definiendo el modelo bancario de API

Las autoridades del Reino Unido encabezan las iniciativas dirigidas a promover una mayor innovación y competencia en los servicios financieros aprovechando la oportunidad digital. La regulación de las API de banca y de intercambio de datos figura actualmente en la agenda de los organismos reguladores debido a los beneficios potenciales que tienen tanto para los consumidores como para las entidades financieras. La definición de un marco sólido para que los bancos puedan intercambiar información y productos colocaría al Reino Unido en una posición destacada para liderar el desarrollo de una normativa internacional

Organismos reguladores globales e inclusión financiera digital: un panorama cambiante al que hay que prestar mucha atención

Cada vez se generaliza más la opinión de que la digitalización de los servicios financieros es un factor decisivo en la promoción de la inclusión financiera. Los riesgos y recompensas de esta evolución, así como las repercusiones que tiene en el trabajo de los grandes organismos que establecen estándares a nivel mundial, se abordan en un nuevo Libro Blanco publicado por la Asociación Mundial para la Inclusión Financiera en marzo de 2016

La Directiva de Seguridad de las Redes y de la Información (NIS). Parte 1 de 2

En 2013, la Comisión presentó una propuesta de Directiva relativa a las medidas para garantizar un elevado nivel común de las redes y la información de seguridad en toda la Unión. Dos años más tarde, el Parlamento y el Consejo acordaron en el texto de la Directiva de red y seguridad de la información (NIS).

Panorama digital de China: un reino digital gobernado por tres reyes

El mercado digital de China opone resistencia a operadores digitales a escala mundial como Google, Amazon y Facebook, pues tres gigantes locales (Alibaba, Tencent y Baidu) dominan el mercado digital a través del control de facto del ecosistema. Ahora también se están introduciendo en los servicios financieros.

Unicornios: las mayores empresas emergentes

Las nuevas empresas tecnológicas están alcanzando en la última década cifras récord de inversión. En el ecosistema de estas empresas destacan las que han alcanzado valoraciones superiores a los 1.000 millones de dólares, que se conocen popularmente como Unicornios. ¿Cómo son estas empresas

1 El estándar de banca abierta

Definiendo el modelo bancario de API

Las autoridades del Reino Unido encabezan las iniciativas dirigidas a promover una mayor innovación y competencia en los servicios financieros aprovechando la oportunidad digital. La regulación de las API de banca y de intercambio de datos figura actualmente en la agenda de los organismos reguladores debido a los beneficios potenciales que tienen tanto para los consumidores como para las entidades financieras. La definición de un marco sólido para que los bancos puedan intercambiar información y productos colocaría al Reino Unido en una posición destacada para liderar el desarrollo de una normativa internacional.

Contexto

En septiembre de 2014, el departamento del Tesoro (HM Treasury) publicó un informe sobre el uso de datos compartidos y datos abiertos en los bancos¹. En dicho informe se exploraban los posibles usos de los datos a través de las API (interfaces de programación de aplicaciones) de forma que se respetaran la protección de datos y la privacidad.

En marzo de 2016, el British Open Banking Working Group (OBWG) publicó un documento sobre el estándar de banca abierta² tras la solicitud que previamente había hecho el departamento del Tesoro en septiembre de 2015. En ese documento se define un marco para establecer el modelo de banca abierta, abordando así la forma en que los propietarios de los datos y aquellos que acceden a ellos deben crear, intercambiar y utilizar dichos datos. La última directiva europea sobre pagos (PSD2), publicada en enero de 2016 y cuya entrada en vigor será efectiva en 2018, obligará a los bancos a proporcionar servicios que permitan a sus clientes recibir ciertos datos a través de Internet y compartirlos de forma fácil y segura con terceros. La inminente regulación general de protección de datos (GDPR) consagrará los derechos de los individuos a la portabilidad de los datos, al consentimiento para compartirlos y a los usos específicos. La implementación del marco del estándar de banca abierta podría acelerar considerablemente la implementación de nuevas regulaciones de la UE sobre los datos bancarios.

La banca de plataformas, donde los desarrolladores externos pueden utilizar las API para crear nuevos servicios y para ampliarlos, tiene el potencial de reconfigurar por completo la cadena de valor y el modelo de negocio de las entidades financieras.

El marco del estándar de banca abierta

La misión del estándar de banca abierta (OBS por sus siglas en inglés) se define como capaz de "liberar el potencial de la banca abierta para mejorar la competencia y la eficacia y estimular la innovación en el sector bancario": El documento del OBS también aborda aspectos clave en torno a la facilidad de uso, la confianza, la seguridad y la gobernanza del estándar.

El documento ofrece una definición clara de los conceptos principales del modelo de API de datos compartidos (figura 1):

- En primer lugar, define los estándares y la taxonomía de datos en las operaciones bancarias, además de aclarar los usos y la propiedad de los datos en cada caso. En las operaciones bancarias pueden generarse datos abiertos, datos compartidos y datos privados (figura 2).

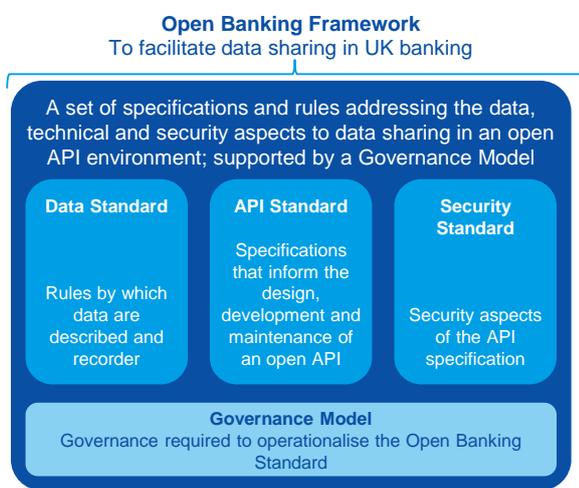
1: Open Data Institute and Fingleton Associates, *Data sharing and Open Data for Banks*, HM Treasury and Cabinet Office, Londres, 2014 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF

2: *The Open Banking Standard*, Open Banking Working Group, Londres, 2016 https://www.scribd.com/document_downloads/298569302

- En segundo lugar, define las API abiertas o los estándares abiertos, en los cuales la tecnología y los datos están abiertos pero a los datos privados solo se puede acceder con permiso de su propietario. En el documento se definen los requisitos de escalabilidad, arquitectura de datos y recursos de los desarrolladores. El foco se centra en la apertura y la facilidad de uso para los desarrolladores, así como en la utilización de recursos existentes que ya son estándar (como OAuth).
- El OBS también define aspectos de la especificación de las API relacionados con la seguridad, lo que incluye la autenticación, la autorización, los niveles y permisos de acceso y el cifrado, así como los estándares de seguridad para proveedores de atributos de datos y terceras partes.
- El modelo de gobierno del ecosistema debe incluir la creación de una autoridad independiente con el fin de garantizar que se mantienen los estándares y obligaciones entre los participantes.

Gráfico 1.1

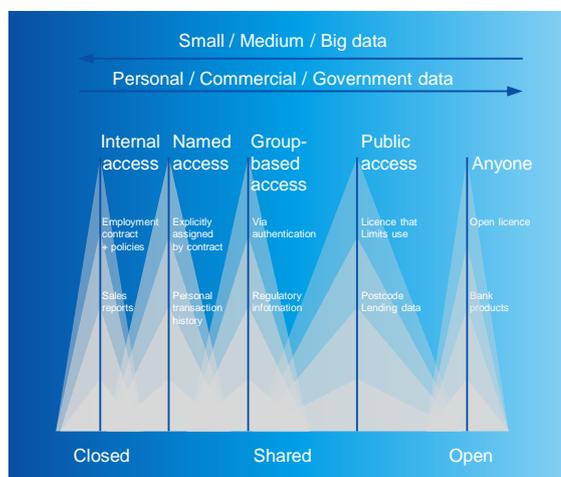
El marco de banca abierta



Fuente: Open Data Institute

Gráfico 1.2

El espectro de datos



Fuente: Open Data Institute

Posibles usos y retos

Al mejorar el acceso a las API y a los datos, se generará un ecosistema de terceros más diversificado. La participación de nuevos actores conducirá a una mayor innovación y selección de productos para los consumidores. El estándar es necesario para eliminar fricciones y permitir economías de escala y alcance.

El intercambio de datos para fines específicos durante el "recorrido del cliente" permite, por ejemplo:

- El desarrollo de nuevos servicios, como los servicios de comparación de cuentas corrientes y herramientas para la gestión financiera personal.
- Mejorar el acceso al crédito tanto para particulares como para PYMES, ya que pueden obtener fácilmente acceso a datos transaccionales históricos con los prestamistas.
- Las PYMES podrían llevar la contabilidad en línea con mayor facilidad, tomando directamente los datos que necesitan para el registro contable en vez de introducirlos manualmente.
- La detección del fraude se puede facilitar con la monitorización de los datos en varias cuentas con el fin de identificar patrones.

Hoy en día, los principales retos en torno al OBS se centran en la seguridad y en el conocimiento de los datos de los clientes para adoptar la propuesta y abordar los futuros marcos legales y regulatorios. Definir el marco es el primer paso para movilizar a los grupos de interés y llevar el OBS adelante.

Hoja de ruta

El plan de implementación propuesto tiene unos plazos ambiciosos, pues aspira a cubrir todo su ámbito a tiempo para cuando la PSD2 entre en vigor. Está previsto poder disponer de un producto mínimo viable para finales de 2016, un producto que pueda ofrecer acceso de lectura básico a los datos.

El modelo de API se ve afectado por varios requisitos legales y regulatorios ya vigentes (como la Ley de Protección de Datos (DPA) en el Reino Unido, el Reglamento General de Protección de Datos (GDPR) en la UE, la ley de competencia, la ley de propiedad intelectual y la Directiva de Servicios de Pago), que deben tenerse en cuenta en la implementación.

Conclusión

El uso de las API para compartir datos bancarios con aplicaciones de software de terceros es obligatorio para cumplir con las regulaciones existentes y con las posibles regulaciones futuras. El uso de las API cada vez es más común en los bancos, pues pueden contribuir a impulsar la velocidad y la rentabilidad en comparación con los antiguos sistemas tradicionales.

Las empresas tecnológicas han utilizado estrategias de API para crear ecosistemas que amplían su oferta de productos de nuevas maneras a bajo coste. El desarrollo de un estándar bancario abierto permitiría a los bancos ampliar sus negocios tradicionales al convertirse en proveedores de API, plataformas de servicios financieros o ambos.

La regulación debe garantizar que el desarrollo de estos modelos de negocio alcanza un gran nivel de seguridad, estabilidad financiera y protección del consumidor. La definición del estándar es un paso necesario en la implementación del modelo, y el gobierno del Reino Unido, al encargarse de este informe, ha tomado el liderazgo de la evolución futura.

2 Organismos reguladores globales e inclusión financiera digital

Un panorama cambiante al que hay que prestar mucha atención

Cada vez se generaliza más la opinión de que la digitalización de los servicios financieros es un factor decisivo en la promoción de la inclusión financiera. Los riesgos y recompensas de esta evolución, así como las repercusiones que tiene en el trabajo de los grandes organismos que establecen estándares a nivel mundial, se abordan en un nuevo Libro Blanco publicado por la Asociación Mundial para la Inclusión Financiera en marzo de 2016

El fuerte compromiso del G20 con la promoción de la inclusión financiera ha provocado la creciente participación de otros organismos que establecen estándares a nivel mundial (los SSB)³, legisladores nacionales y participantes del sector. Al mismo tiempo, tanto instituciones financieras como no financieras han comenzado a ofrecer nuevos servicios financieros digitales con el objetivo de llegar a millones de clientes nuevos. Aunque los organismos reguladores globales valoran el enorme potencial de las funciones que pueden desempeñar estos nuevos servicios financieros digitales en la promoción de la inclusión financiera, también se están dando cuenta de que la naturaleza de los riesgos a los que se enfrentan cambiará a lo largo del proceso.

En marzo de 2016, la Asociación Mundial para la Inclusión Financiera (GPII) publicó un [Libro Blanco](#) tratando de concienciar de este panorama cambiante. El libro es una guía sobre cómo los SSB pueden lograr el equilibrio adecuado entre la promoción de la inclusión financiera digital y los objetivos tradicionales de salvaguardar la estabilidad financiera, garantizando así la protección de los consumidores financieros y el mantenimiento de la integridad financiera. El establecimiento de un marco regulatorio facilitador que sea compatible con los mandatos tradicionales de la regulación financiera es una responsabilidad que recae principalmente a nivel nacional. Aun así, el trabajo de los SSB supone un paso significativo hacia delante y puede guiar tanto a países miembros como no miembros a la hora de abordar el reto de la inclusión financiera.

La inclusión financiera digital: el estado del arte de los organismos reguladores financieros globales

Según la GPII, la inclusión financiera se refiere al uso de los servicios financieros digitales para promover la inclusión financiera. Se caracteriza por el uso de medios digitales para llegar a la población financieramente excluida y desatendida con una diversidad de servicios financieros formales adecuados a sus necesidades y a un coste asequible para los clientes y conveniente para el proveedor.

Hay varios factores que pueden explicar la distinta naturaleza de los riesgos creados por la inclusión financiera digital. Primero, la participación de nuevos proveedores requiere el establecimiento de unos requisitos regulatorios y de supervisión proporcionados de forma que se proteja el marco de igualdad. Segundo, los nuevos servicios y productos, en muchos casos, se ofrecen agrupados. Estos servicios y productos a menudo se basan en tecnología puntera que puede variar en cuanto a calidad, lo que plantea problemas con respecto a la seguridad de los datos. Por último, el perfil de los propios clientes, que muy probablemente carecerán de experiencia con los servicios financieros formales, lo que empeora el reto de

3: El Libro Blanco tiene en cuenta el trabajo de los principales SSB, que incluyen: el Comité de Supervisión Bancaria de Basilea (CSBB), el Consejo de Estabilidad Financiera (FSB), el Comité de Pagos e Infraestructura de Mercado (CPIM), la Organización Internacional de Comisiones de Valores (OICV), la Asociación Internacional de Supervisores de Seguros (AISS), la Asociación Internacional de Aseguradores de Depósitos (AIAD) y el Grupo de Acción Financiera (GAFI).

protección del consumidor. La inclusión financiera digital repercute en varios aspectos transversales relacionados con los mandatos fundamentales de los SSB globales:

- **Protección del consumidor de productos financieros.** La inclusión financiera ya plantea un reto para la protección del consumidor debido a la naturaleza de los propios clientes objetivo, pero los riesgos aumentan cuando se añade a la ecuación la dimensión digital. Por poner un ejemplo, el uso de las plataformas de transacciones digitales (que combinan características de instrumentos de pago y de depósito de valores) y los servicios financieros que pueden ofrecerse a través de estas plataformas plantean varias cuestiones con respecto a la protección de los consumidores que son de interés para organismos como BCBS, CPMI, IADI, IAIS e IOSCO (todos por sus siglas en inglés). La protección de los consumidores también tiene importancia para el FSB y la FATF debido al vínculo con la estabilidad financiera, la mala conducta y la integridad financiera.
- **Interoperabilidad y competencia:** dada la presencia de bancos e instituciones no bancarias (incluidos los operadores de redes móviles), garantizar que los clientes de servicios financieros en competencia pueden funcionar unos con otros es un asunto de máxima importancia. En esta materia, el obstáculo es decidir el tipo y los plazos de la intervención regulatoria. La creciente competencia puede ampliar la oferta de productos y servicios y llevar a unos costes más bajos. Al mismo tiempo, es esencial asegurarse de que la regulación proporcionada para los distintos proveedores sigue un enfoque basado en los riesgos que garantiza un marco de igualdad entre los que participan en actividades similares. Tanto el BCBS⁴ como el CPMI han avanzado el trabajo en este frente.
- **Identidad del cliente y privacidad:** las nuevas tecnologías utilizadas en la inclusión financiera digital (p. ej. las nuevas fuentes de datos y las prácticas de procesamiento de datos) facilitan la implementación de medidas de DD simplificadas (tal como indica el mandato de la FAFT), lo que contribuye a conseguir el equilibrio entre los objetivos de la inclusión financiera y la integridad. Al mismo tiempo, estas prácticas también plantean nuevas cuestiones con respecto a la privacidad de los datos y a la seguridad, pues cada vez hay más instituciones e individuos que manejan datos personales. El incumplimiento de la privacidad de datos y la seguridad aumenta el riesgo de usurpación de identidad y socava la confianza del consumidor, en detrimento de la inclusión financiera.
- **Intermediación financiera no tradicional:** el reto con respecto a la financiación colectiva y otras formas de préstamos P2P es fomentar fuentes de financiación innovadoras que complementen la financiación basada en los bancos garantizando al mismo tiempo la protección eficaz del inversor. Hasta el momento, los regímenes regulatorios de la financiación colectiva están en su infancia y ninguno de los SSB ha publicado aún una guía al respecto, aunque el tema concierne a los mandatos fundamentales de varios SSB.

4: Véase el correspondiente informe BBVA Research Watch: [Guía sobre regulación y supervisión para la inclusión financiera de CSBB](#)

Tabla 1

Temas seleccionados sobre la inclusión financiera digital: relevancia para los SSB globales

	BCBS	FSB	CPMI	IOSCO	IAIS	IADI	FATF
Protección de los consumidores	Dark Blue	Light Blue	Dark Blue	Dark Blue	Dark Blue	Dark Blue	Light Blue
Interoperabilidad y competencia	Dark Blue	Dark Blue	Dark Blue				
Identidad y privacidad	Dark Blue	Light Blue			Dark Blue		Dark Blue
Financiación colectiva	Light Blue	Dark Blue	Light Blue	Dark Blue			Dark Blue

Fuente: BBVA Research basándose en los datos del Libro Blanco de la GPF1 y en la información proporcionada por los SSB.
Azul oscuro: directamente relevantes para el mandato de los SSB. Azul claro: indirectamente relevante

Los supervisores financieros podrían enfrentarse a importantes restricciones operativas y a menudo carecen de la experiencia suficiente para hacerse cargo de esta realidad cada vez más compleja. Por tanto la inclusión financiera digital hace un llamamiento para una mayor cooperación y coordinación entre las autoridades financieras y no financieras para garantizar la uniformidad y la coherencia de las reglas.

3 La Directiva de Seguridad de las Redes y de la Información (NIS). Parte 1 de 2

Regulación para la ciberseguridad

En 2013, la Comisión presentó una propuesta de Directiva relativa a las medidas para garantizar un elevado nivel común de las redes y la información de seguridad en toda la Unión. Dos años más tarde, el Parlamento y el Consejo acordaron en el texto de la Directiva de red y seguridad de la información (NIS).

Contexto

La necesidad de la Directiva de Seguridad de las Redes y de la Información (NIS por sus siglas en inglés) surgió en 2002 tras varios análisis y encuestas en el ámbito de la ciberseguridad en los países de la Unión Europea. Fue entonces cuando se constató la importancia de la seguridad de las redes de información, tanto para el ámbito económico como para la Sociedad misma. Igualmente, se detectó una tendencia alcista de los ciberincidentes. Internet interconecta a los Estados miembros de la Unión Europea de la misma manera que las carreteras enlazan ciudades y países, permitiendo el transporte libre de productos y servicios. Por tanto, se consideró esencial promover la estabilidad y la resiliencia de las redes de información, a fin de asegurar el futuro proyecto del Mercado Único Digital.

Estos estudios hicieron patente la preocupación de muchas empresas y gobiernos europeos por su dependencia de las redes digitales y de sus infraestructuras para ofrecer sus servicios más esenciales. Se consideraba que un incidente NIS podría tener un enorme impacto negativo que comprometería el funcionamiento de los servicios críticos. Del mismo modo, se pensó que dichos incidentes de ciberseguridad afectarían a la confianza del consumidor y de la Sociedad en su conjunto. Dada la disparidad en las capacidades y preparación en el ámbito de NIS de los distintos Estados Miembros, una aplicación voluntaria de NIS no ofrecería la protección suficiente para afrontar los incidentes y riesgos de ciberseguridad. El análisis de los proveedores de infraestructura crítica y de servicios esenciales concluyó que no todos estaban obligados a adoptar las mismas medidas de seguridad, como la gestión del riesgo tecnológico o el intercambio de información con las autoridades. Por lo tanto, quedaba clara la necesidad de tener un enfoque común sobre la seguridad de las redes y la información.

El 18 de diciembre 2015, el Parlamento Europeo llegó a un acuerdo, pendiente de ratificación en 2016, para la aprobación de la Directiva NIS. Esta Directiva tiene como objetivo la mejora de las capacidades de ciberseguridad en los Estados Miembros, para la creación de un ciberespacio más abierto, seguro y resiliente. Con el objetivo de crear una Unión Europea más protegida, pretende también desarrollar recursos tecnológicos e industriales de ciberseguridad e implementar un mercado interno de productos y servicios de ciberseguridad.

Esto generará un espacio donde se contará con una mayor colaboración entre los países y las empresas de la Unión Europea, lo que permitirá reducir el cibercrimen, evitar la fragmentación de planes nacionales de ciberseguridad e incrementar la armonización entre Estados Miembros en la protección frente a incidentes NIS, riesgos y amenazas. Consecuentemente, se mejorará de forma considerable la protección al consumidor, el negocio y el gobierno en el ámbito de la Unión Europea. A tal fin, será preciso que cada país defina los operadores esenciales de servicios de Energía, Transporte, Banca y Salud así como los proveedores claves de servicios digitales tales como buscadores y proveedores de cloud computing. Igualmente, se precisará que estos operadores esenciales tomen las medidas de seguridad necesarias y procedan a informar de incidentes significativos a las Autoridades Nacionales. Por último, será preciso que cada Estado Miembro designe una Autoridad Nacional competente para gestionar el NIS, un Equipo de

Respuesta a Incidentes de Seguridad Informática - CSIRT, acrónimo de la denominación en inglés: Computer Security Incident Response Team - nacional y defina la estrategia nacional y el plan de cooperación de Seguridad de las Redes y de la Información. Resaltar que la Agencia Europea para la Seguridad de las Redes y de la Información (ENISA – acrónimo de su denominación inglesa: EU Agency for Network and Information Security) tendrá un papel fundamental en la coordinación con los distintos CSIRTs. Finalmente, también será fundamental la creación de un plan de cooperación entre los Estados Miembros de información de los posibles riesgos e incidentes de ciberseguridad.

Aspectos a considerar por los negocios online

Los negocios online deberán tener en cuenta cinco aspectos relacionados con el cumplimiento y protección de sus redes de Seguridad e Información (NIS).

En primer lugar, deberán evaluar si su tipo de empresa está sujeta a la directiva NIS. La Directiva afectará a operadores de servicios esenciales y a proveedores de servicios digitales, como los correspondientes a los sectores de Energía, Transporte, Financiero, Hidrológico, Administración Pública y Salud. También se verán afectadas las infraestructuras digitales, los comerciantes online, los buscadores de la red y servicios de Cloud Computing. Sin embargo, no afectará a los proveedores de servicios de pagos, los cuales están sujetos a otras Directivas u obligaciones de seguridad y de declaración de incidentes de ciberseguridad. Tampoco resultarán afectadas las empresas de hardware o software, o las pequeñas y medianas empresas.

En segundo término, la entidad deberá cumplir únicamente con la Ley nacional transpuesta de la Directiva NIS en aquel Estado Miembro donde tenga su sede principal.

En tercer lugar, será crucial que la empresa conozca cuál será la Autoridad nacional a la que deberá informar de incidentes de ciberseguridad, así como la que potencialmente podrá ejercer la sanción por algún incumplimiento de la Ley. A fecha de hoy, no queda claro qué poderes tendrá la Autoridad nacional competente frente al CSIRT nacional. Tampoco queda claro que ocurrirá con posibles duplicidades de notificaciones de incidentes que pudieran solicitar otras regulaciones ya vigentes en algunos países como las de protección de datos o de infraestructura crítica.

En cuarto lugar, el negocio online o la empresa con la necesidad de cumplir con la ley deberá poner en práctica las medidas técnicas y organizativas imprescindibles para proteger su información y sus redes. Estas medidas deberán garantizar la capacidad de gestionar los riesgos y amenazas en la seguridad de las redes y los sistemas de información propios. Para ello se espera que las empresas creen una cultura de la gestión del riesgo tecnológico adoptando medidas apropiadas y proporcionales para garantizar la seguridad de su información y sus redes.

En último lugar, las empresas deberán desarrollar un proceso efectivo, para notificar ciberincidentes bien sea a la Autoridad Nacional competente o al CSIRT nacional.

En un próximo artículo se analizarán los retos que esta regulación plantea para los reguladores de los distintos países.

4 Panorama digital de China

Un reino digital gobernado por tres reyes

El mercado digital de China opone resistencia a operadores digitales a escala mundial como Google, Amazon y Facebook, pues tres gigantes locales (Alibaba, Tencent y Baidu) dominan el mercado digital a través del control de facto del ecosistema. Ahora también se están introduciendo en los servicios financieros.

La economía digital de China

La economía digital de China es enorme. Hay más de 651 millones de usuarios de Internet, lo que constituye la mayor población en línea del mundo (pero con una penetración de apenas el 48%) según datos de febrero de 2016⁵. El 92% de estos usuarios de Internet disponen de su propio teléfono inteligente y cada uno de ellos tiene una media de 4,1 dispositivos conectados a Internet. En 2015, el volumen del comercio electrónico llegó a 589.000 millones de dólares, lo que convierte a China en el mayor mercado de comercio electrónico del mundo, con apenas un 40% de cuota del volumen total⁶.

El mercado digital chino presenta algunas características singulares. Como ejemplo, existe un conjunto de proveedores de servicios en línea completamente diferente al del resto del mundo. Facebook, Twitter, Instagram, YouTube y otros muchos servicios en línea importantes no están accesibles en China. Y pocas personas usan Whatsapp o PayPal. Hay empresas chinas que ofrecen servicios comparables y las empresas de Internet extranjeras hasta ahora han tenido muy poco éxito en China. En su lugar, tres grandes operadores digitales locales, Baidu (motor de búsqueda), Alibaba (plataformas de comercio electrónico Tmall y Taobao) y Tencent (aplicaciones de redes sociales WeChat y QQ), que colectivamente se conocen como los BAT, dominan el mercado. El valor de mercado agregado de las tres empresas alcanza 473.000 millones de dólares y sus ingresos anuales combinados llegan a 20.000 millones de dólares.

Los BAT son tan poderosos en China que su mera existencia a veces impide que surja competencia y se han convertido en participantes vitales en la economía china. Sus negocios centrales son distintos, pero cada vez compiten más entre sí, lo que crea formidables ecosistemas de Internet dentro de China. Otro factor de disrupción digital es el fabricante de teléfonos inteligentes Xiaomi, que con su rápido crecimiento tiene el potencial de crear un cuarto ecosistema importante.

También hay grandes diferencias culturales en lo que se refiere al comportamiento de los consumidores. La sensibilidad de los consumidores chinos a los precios sigue siendo superior a lo que estamos acostumbrados en otros mercados. Este fenómeno a menudo obliga a las empresas a competir únicamente en precios y a veces crea una situación indeseable en que nadie del sector consigue realmente obtener unos beneficios decentes. Otro fenómeno empresarial interesante a tener en cuenta es lo que se llama la "economía de fans" Xiaomi es un maestro en la creación de marca y consigue resultados de ventas asombrosos con el método de conseguir clientes y convertirlos en fans de su marca. Muchas empresas tratan de copiar el éxito de Xiaomi en generar una economía de fans.

El ecosistema de la economía financiera

En los últimos años hay una actividad enorme en la comunidad de capital riesgo. Una explicación parcial de este fenómeno es que varios de los grandes operadores digitales se encuentran ahora en una etapa en que tratan de poner a trabajar el capital excedente a través de inversiones en pequeñas empresas al estilo

5: <http://venturebeat.com/2016/02/12/new-data-shows-the-staggering-growth-of-apps-and-smartphones-in-china/>

6: <https://www.internetretailer.com/2016/01/27/chinas-online-retail-sales-grow-third-589-billion-2015>

del emprendimiento. **En 2015, los BAT gastaron casi 15.000 millones de dólares en fusiones y adquisiciones, una cifra que se prevé que aumente hasta 80.000 millones de dólares en 2016⁷.** Con ello se ha propiciado **el surgimiento de “unicornios” de tecnología financiera** como China Internet Plus Holding (información de descuento sobre restaurantes locales y plataforma de descuento para compras en grupo), Lufax (plataformas de préstamos P2P), Didi Kuaidi (servicio de taxis), DJI Innovations (fabricante de drones) o Zhong An Insurance (seguros en línea).

Los nuevos bancos digitales de China

Los ingresos de la banca minorista de China han crecido un 30% anual desde 2009 y podrían superar los 430.000 millones de dólares en 2020, lo que convierte al país en el mayor mercado de banca minorista de Asia. Por otro lado, **el panorama de la banca minorista ha tenido que enfrentarse a varios retos**, entre otros la liberalización de los tipos de interés, cambios regulatorios importantes y el crecimiento del sistema financiero digital. **Los bancos involucrados están perdiendo su hegemonía en cuota de mercado, mientras que la banca digital se está convirtiendo en algo común.**

El crecimiento de la banca digital está impulsado por dos factores principales: el primero está relacionado con las necesidades de cambio y con el comportamiento del consumidor chino con respecto a lo digital. McKinsey ha comprobado que **más del 70% de los consumidores chinos se plantearían abrir una cuenta en un banco puramente digital**, y hasta considerarían la opción de que fuera su banco principal. El segundo está relacionado con la normativa: con el fin de impulsar la economía y ayudar a las pequeñas y medianas empresas a conseguir financiación con más facilidad, **el gobierno chino anima a entidades no gubernamentales a invertir en instituciones financieras, y hasta permite que empresas privadas abran sus propios bancos.** En 2014, cuando el gobierno anunció que había tomado la decisión de otorgar licencias bancarias para abrir bancos privados, las tres grandes compañías tecnológicas aprovecharon la oportunidad.

Tencent fue la primera. En enero de 2015 lanzó el **WeBank**, el primer banco únicamente en línea del país. WeBank opera principalmente en el negocio de la distribución de productos financieros para otras instituciones, concediendo pequeños créditos personales y préstamos para automóviles. WeBank ha crecido muy rápido tanto en usuarios como en activos (se rumorea que tiene más de 2 millones de usuarios; la empresa no revela ninguna cifra) porque promueve su servicio de préstamos en WeChat y QQ, las aplicaciones de medios sociales dominantes en China, con 800 millones de usuarios. Los productos financieros que vende WeBank tienen una tasa de rendimiento elevada, por lo que con frecuencia se agotan en segundos.

Alibaba lanzó ese mismo mes **MYbank**, que ha estado trabajando en tres tipos de préstamos que están indirectamente vinculados con el negocio central de Alibaba: uno para los residentes de zonas rurales, uno para las nuevas empresas de Internet y uno para los vendedores de Tmall y Taobao. MYbank opera en una plataforma de informática en la nube y la concesión de préstamos se lleva a cabo sin la participación del personal del banco. Para calcular el importe de los préstamos se usan algoritmos de big data que no pueden superar los 5 millones de RMB. La totalidad del proceso es rápida y sencilla y, en el futuro, se prevé que los usuarios solo tendrán que pasar tres minutos en un proceso de dos pasos para conseguir un préstamo de MYbank. Una vez que la solicitud ha sido aprobada, el dinero llegará a la cuenta del usuario de forma instantánea.

Baidu ha seguido otra trayectoria: en vez de solicitar una licencia bancaria, en noviembre de 2015 anunció su decisión de poner en marcha el **Baixin Bank** en colaboración con CITIC Bank, un banco tradicional. El Baixin Bank, establecido por un banco tradicional y un motor de búsqueda gigantesco, tiene como objetivo ofrecer tanto servicios en línea como servicios sin conexión. Además, Baidu ofrece análisis de

7: <http://www.financeasia.com/News/406399,baidu-alibaba-and-tencent-on-deal-trail.aspx>

comportamiento de usuarios, lo que no solo ayuda en la gestión de riesgos sino que también permite que se puedan ofrecer servicios personalizados. En el futuro, el objetivo del Baixin Bank es vender productos financieros y conceder pequeños préstamos a clientes particulares.

Conclusión

Todavía es **demasiado pronto para analizar la evolución de la competencia entre los bancos tradicionales y los BAT**: no hay suficiente información acerca del desarrollo empresarial del WeBank y el MYbank, y aún hay menos información sobre el Baixin Bank. Pero se puede hacer una reflexión interesante desde el punto de vista del mundo occidental: durante años se decía que **la amenaza real para los bancos no era el mundo de la tecnología financiera sino la entrada de los grandes operadores de Internet (como los GAFA: Google, Apple, Facebook, Amazon) en el terrero de los servicios financieros. China es el lugar donde esto ya está sucediendo, por lo que debemos extraer lecciones de su experiencia.**

5 Unicornios: las mayores empresas emergentes

El crecimiento de las nuevas empresas tecnológicas

Las nuevas empresas tecnológicas están alcanzando en la última década cifras récord de inversión. En el ecosistema de estas empresas destacan las que han alcanzado valoraciones superiores a los 1.000 millones de dólares, que se conocen popularmente como Unicornios. ¿Cómo son estas empresas?

El concepto

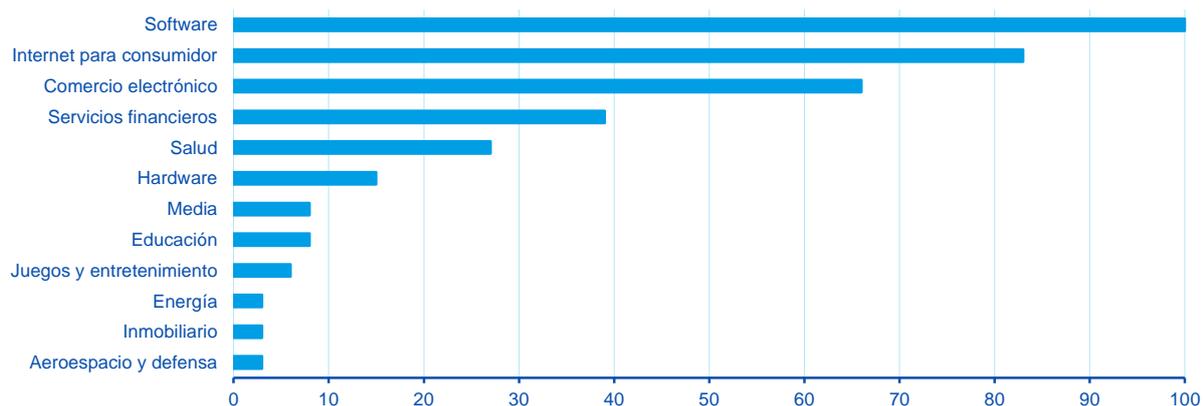
Unicornios es el nombre por el que se denomina a las empresas tecnológicas fundadas a partir de 2003 y valoradas en más de 1.000 millones de dólares (un billón americano). El término fue usado por primera vez en noviembre de 2013 en un artículo de TechCrunch por la inversora de capital riesgo Aileen Lee. Entonces sólo había 39 empresas en este selecto grupo, un 0,7% del total (solo consideraba las empresas de Estados Unidos, incluyendo cotizadas y no cotizadas), y apenas surgían unos cuatro al año: eran tan raras como los unicornios.

Desde entonces no se ha parado de hablar de unicornios entre los analistas del ecosistema de startups, y el concepto se ha redefinido: solo se consideran empresas que aún no cotizan en ningún mercado, entre cuyos inversores hay empresas de capital riesgo no controladas mayoritariamente por inversores institucionales. Este criterio excluye a los gigantes de Internet, que no solo superan las valoraciones de los unicornios, sino que mantienen un crecimiento constante.

Hablamos de empresas de tecnología y las encontramos en todos los sectores que se han visto afectados por la digitalización. Su modelo se basa en la desagregación del negocio de las empresas tradicionales, centrándose solo en una parte de un negocio o detectando nuevos nichos de oportunidad.

Gráfico 5.1

Unicornios por sectores



Fuente: BBVA Research basado en datos de TechCrunch

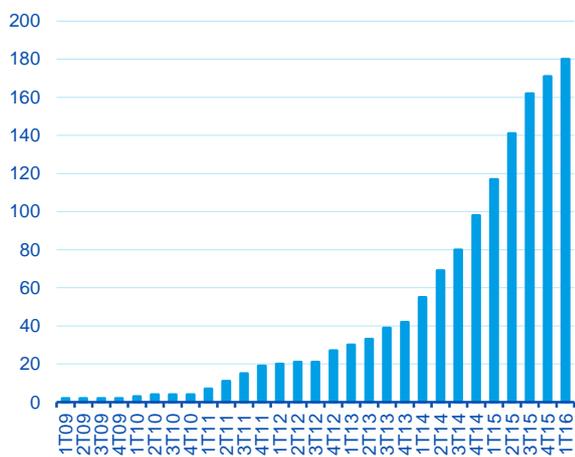
Su propuesta de valor está en muchos casos en nuevos modelos de negocio dentro de la economía digital. Solo en ocasiones estas empresas tienen un fuerte componente de innovación tecnológica, pero en todos los casos aprovechan el valor de los datos como elemento diferencial. Además, muchas de ellas operan como plataformas, definidas como infraestructuras tecnológicas que ofrecen un punto de encuentro entre la demanda de productos y servicios y una oferta de contenidos y aplicaciones.

Algunos datos

En abril de 2016 hay censados cerca de **160 unicornios** en todo el mundo⁸, aunque solo en torno al 1% de las empresas que se crean puede aspirar a convertirse en un unicornio. El tiempo que tarda un empresa en llegar a ser un unicornio se ha ido acortando en los últimos tres años, y 2007 es al año en que se fundaron más empresas de la lista.

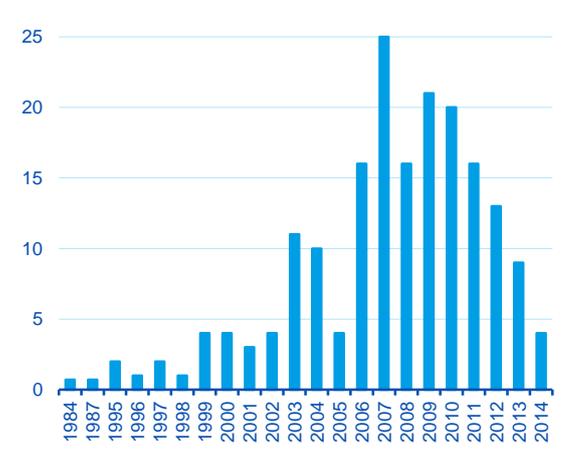
La relación está encabezada por **Uber**, la empresa de transporte que no posee ningún vehículo, valorada en este momento en 51.000 millones de dólares, seguida por la tecnológica china **Xiaomi**, la suma de cuyas valoraciones, 96.000 millones de dólares, es el 17,5% del total de 548.000 millones de dólares en los que se valora el total de los unicornios, de acuerdo a TechCrunch. Los “superunicornios” o “decacornios”, empresas que superan los 10.000 millones, son nada más que 11 en este momento, cuando en 2013 ese umbral sólo lo superaba Facebook.

Gráfico 5.2
Evolución del número de unicornios



Fuente: CrunchBase

Gráfico 5.3
Unicornios por año de fundación



Fuente: CrunchBase

Por ahora estas empresas prefieren no salir a bolsa y obtienen su financiación de inversores que siguen apostando por las empresas emergentes como un activo rentable en entornos de tipos de interés muy bajos, aunque los beneficios que generan por ahora no justifiquen la valoración por sí solos. Los sectores que captan más inversión van evolucionando y, aunque muchas empresas fracasan, el ritmo de nacimiento de los unicornios ha ido incrementándose hasta el momento.

Las valoraciones se basan en las inversiones que realizan los inversores de capital riesgo, por lo que no es posible ver su evolución en tiempo real y pueden revisarse en operaciones posteriores. Al no cotizar en mercados estructurados, las empresas no están obligadas a publicar sus cuentas y su valor se estima en base a perspectivas de negocio con datos como el número de usuarios o el potencial de los mercados en los que operan. Encontramos bastantes casos en los que la valoración ha disminuido de una ronda de financiación a la siguiente, o en la salida a bolsa⁹, creando dudas sobre la realidad de esos valores atribuidos y generando el temor al estallido de una burbuja. Uno de los últimos casos ha sido la oferta

8: A 31 de marzo de 2016, de acuerdo a TechCrunch son 162 (*CrunchBase Unicorn Leaderboard*), mientras CBI Insights contabiliza 159 (*The unicorns list*) y 146 Dow Jones Venture Source (*The billion dollar startup club*).

9: Se puede encontrar información actualizada en la página *The downround tracker* de CBI Insights.

pública de venta (OPV) de Square en noviembre de 2015: de una valoración estimada de 6.000 millones de dólares, el precio de salida en la OPV finalmente se fijó en 2.900 millones de dólares¹⁰.

El **hábitat** natural de los unicornios es Silicon Valley, un lugar que empezó a nombrarse así por vez primera en 1971 y donde se han centrado las principales empresas de la era de internet. En efecto, el mayor número de estas empresas se encuentra en Estados Unidos (88)¹¹, también en la costa Este, seguido de China, con 40. En Europa el número es más pequeño (16), posiblemente debido a la mayor fragmentación del mercado y a las barreras regulatorias que todavía limitan el crecimiento de las startups de este área geográfica. Además, los menores incentivos fiscales a la inversión en este tipo de empresas, unida a los límites que la legislación laboral europea supone para la atracción del talento tampoco ayudan a competir con otras regiones. En Estados Unidos, la JOBS Act de 2012, que tenía como objetivo facilitar la obtención de capital por las pequeñas empresas, permite a las empresas emergentes mantenerse sin salir a bolsa, atrayendo los fondos de los inversores de capital riesgo.

Conclusión

El concepto de unicornio se ha usado para destacar empresas exitosas en su crecimiento exponencial, si bien se mantiene el debate sobre la justificación de algunas valoraciones y su mantenimiento en caso de salidas a bolsa. El miedo a que estemos ante una burbuja similar a la de las empresas .com en los años 90 se mantiene, sin que hasta ahora exista certeza sobre este hecho. Lo que sí es cierto es que su crecimiento está cambiando el panorama en muchos sectores, debido a la novedad de los modelos de negocio que se proponen y a su interpretación de las tendencias de transformación de la economía digital.

10: "Square's disappointing IPO shows the risk of overvaluing tech unicorns", *The Economist*, 19 Nov. 2015

11: De acuerdo a DowJones Venture Source, dato a 9 de abril de 2016 ([The billion dollar startup club](#))

AVISO LEGAL

El presente documento, elaborado por el Departamento de BBVA Research, tiene carácter divulgativo y contiene datos, opiniones o estimaciones referidas a la fecha del mismo, de elaboración propia o procedentes o basadas en fuentes que consideramos fiables, sin que hayan sido objeto de verificación independiente por BBVA. BBVA, por tanto, no ofrece garantía, expresa o implícita, en cuanto a su precisión, integridad o corrección.

Las estimaciones que este documento puede contener han sido realizadas conforme a metodologías generalmente aceptadas y deben tomarse como tales, es decir, como previsiones o proyecciones. La evolución histórica de las variables económicas (positiva o negativa) no garantiza una evolución equivalente en el futuro.

El contenido de este documento está sujeto a cambios sin previo aviso en función, por ejemplo, del contexto económico o las fluctuaciones del mercado. BBVA no asume compromiso alguno de actualizar dicho contenido o comunicar esos cambios.

BBVA no asume responsabilidad alguna por cualquier pérdida, directa o indirecta, que pudiera resultar del uso de este documento o de su contenido.

Ni el presente documento, ni su contenido, constituyen una oferta, invitación o solicitud para adquirir, desinvertir u obtener interés alguno en activos o instrumentos financieros, ni pueden servir de base para ningún contrato, compromiso o decisión de ningún tipo.

Especialmente en lo que se refiere a la inversión en activos financieros que pudieran estar relacionados con las variables económicas que este documento puede desarrollar, los lectores deben ser conscientes de que en ningún caso deben tomar este documento como base para tomar sus decisiones de inversión y que las personas o entidades que potencialmente les puedan ofrecer productos de inversión serán las obligadas legalmente a proporcionarles toda la información que necesiten para esta toma de decisión.

El contenido del presente documento está protegido por la legislación de propiedad intelectual. Queda expresamente prohibida su reproducción, transformación, distribución, comunicación pública, puesta a disposición, extracción, reutilización, reenvío o la utilización de cualquier naturaleza, por cualquier medio o procedimiento, salvo en los casos en que esté legalmente permitido o sea autorizado expresamente por BBVA.

Este informe ha sido elaborado por la unidad de Regulación Digital:

Economista Jefe de Regulación Digital

Álvaro Martín
alvaro.martin@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

Israel Hernanz
israel.hernanz@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Con la colaboración de:

Francisco Borja Larrumbide Martínez
fborja.larrumbide@bbva.com

Lucía Pacheco
lucia.pacheco@bbva.com

BBVA Research

Economista Jefe Grupo BBVA

Jorge Sicilia Serrano

Área de Economías Desarrolladas

Rafael Doménech
r.domenech@bbva.com

España

Miguel Cardoso
miguel.cardoso@bbva.com

Europa

Miguel Jiménez
mjimenezg@bbva.com

Estados Unidos

Nathaniel Karp
Nathaniel.Karp@bbva.com

Área de Economías Emergentes

Análisis Transversal de Economías

Emergentes
Álvaro Ortiz
alvaro.ortiz@bbva.com

Asia

Le Xia
le.xia@bbva.com

México

Carlos Serrano
carlos.serranoh@bbva.com

Turquía

Álvaro Ortiz
alvaro.ortiz@bbva.com

Coordinación LATAM

Juan Manuel Ruiz
juan.ruiz@bbva.com

Argentina

Gloria Sorensen
gsorensen@bbva.com

Chile

Jorge Selaive
jselaive@bbva.com

Colombia

Juana Téllez
juana.tellez@bbva.com

Perú

Hugo Perea
hperea@bbva.com

Venezuela

Julio Pineda
juliocesar.pineda@bbva.com

Área de Sistemas Financieros y Regulación

Santiago Fernández de Lis
sfernandezdelis@bbva.com

Sistemas Financieros

Ana Rubio
arubiog@bbva.com

Inclusión Financiera

David Tuesta
david.tuesta@bbva.com

Regulación y Políticas Públicas

María Abascal
maria.abascal@bbva.com

Regulación Digital

Álvaro Martín
alvaro.martin@bbva.com

Áreas Globales

Escenarios Económicos

Julián Cubero
juan.cubero@bbva.com

Escenarios Financieros

Sonsoles Castillo
s.castillo@bbva.com

Innovación y Procesos

Oscar de las Peñas
oscar.delaspenas@bbva.com

Interesados dirigirse a:

BBVA Research

Calle Azul, 4
Edificio de la Vela - 4ª y 5ª plantas
28050 Madrid (España)
Tel.: +34 91 374 60 00 y +34 91 537 70 00
Fax: +34 91 374 30 25
bbvaresearch@bbva.com
www.bbvaresearch.com