Nueva Directiva de Pagos Europea PSD2 (APIs abiertas)

GARRIGUES

27 de julio de 2018

GARRIGUES

Índice

GARRIGUES

I. PSD2 – ANTECEDENTES

PSD2: origen de la regulación

FinTech en Europa: impulso de reguladores y empresas

FINANZAS & MERCADOS

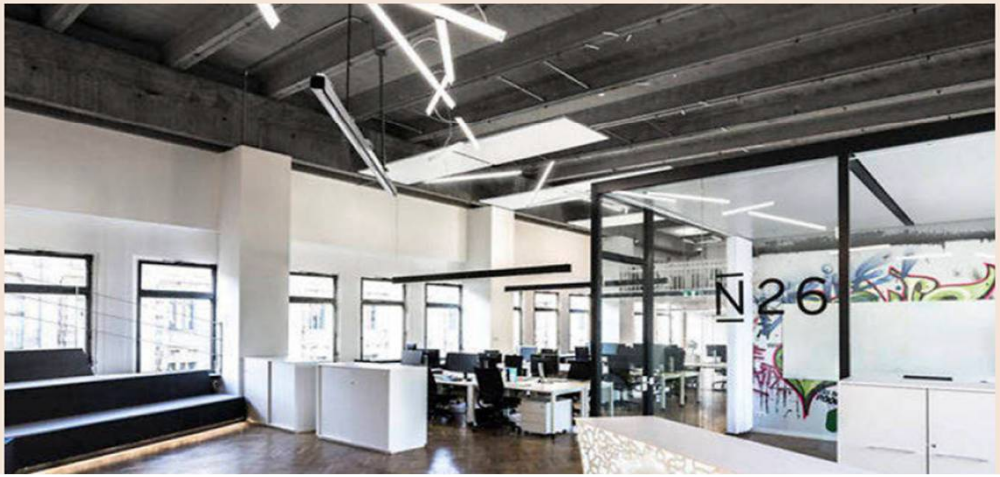
Las 'fintech' crearán 4.500 empleos en España en el próximo año

EL SECTOR SUMA 300 EMPRESAS/ España se sitúa como el sexto país del mundo con más tejido de 'start up' especializadas en servicios financieros. Entre todas facturan cien millones de euros anuales.

R. Lander. Madrid

El emergente ecosistema de las empresas tecnológicas de servicios financieros está dinamizando la contratación en el sector financiero por primera vez en casi diez años, mientras sigue abierto el duro proceso de destrucción de empleo de la banca tradicional.

Las 300 *fintech* y las 90 *insurtech* (especializadas en seguros) que ofrecen sus servicios en España planean contratar en total 4.500 empleados en doce meses, según los datos recabados por Finnovating, consultora estratégica de



La banca tradicional ha eliminado 80.000 puestos de trabajo a consecuencia de las fusiones

La alemana N26 va a contratar cien ingenieros en la oficina que va a abrir en Barcelona

de software, especialistas en márketing digital, fuerza de

PSD2: origen de la regulación
Filosofía

Búsqueda del equilibrio

Impulso del avance tecnológico

- Incrementar la eficiencia en la prestación de los servicios.
- Reducción de los costes (empresas y usuarios).
- Evitar la obsolescencia del sistema financiero.

Protección

- Mantener la protección del consumidor de servicios financieros.
- Proteger la estabilidad financiera y a la integridad en los mercados.
- Evitar la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo.

PSD2: origen de la regulación
PSD1: origen de la norma

PSD1

Hacia un mercado único europeo

- Servicios transfronterizos: ✖ barreras internas.
- Reducción de costes.
- Ventajas para los consumidores.

Disposiciones comunitarias vs. Normas nacionales

- Inseguridad jurídica.
- Desprotección de unos consumidores frente a otros.
- Ineficiencias en la prestación de servicios.
- Desigualdad de condiciones entre los operadores.

Marco jurídico armonizado

- Condiciones de acceso al mercado por parte de los proveedores.
- Requisitos de información.
- Derechos y obligaciones: proveedores y usuarios.

GARRIGUES

PSD2: introducción

La armonización por la seguridad en los pagos

Segunda Directiva de Pagos

Protección al usuario

Aumento de los requisitos que deben cumplir las empresas

Seguridad en los pagos en línea

Reglamento Delegado de Autenticación reforzada de clientes

Nuevos servicios

Iniciación de pagos e información sobre cuentas

FinTech

GARRIGUES

PSD2: introducción
Plazo de transposición

Fecha límite para su transposición: 13 de enero de 2018.

Transposición completa

- Austria
- Bulgaria
- Chipre
- República Checa
- Dinamarca
- Estonia
- Finlandia
- Francia
- Alemania
- Grecia
- Hungría
- Irlanda
- Italia
- Eslovaquia
- Eslovenia
- Suecia
- Reino Unido

Medidas parciales de transposición

- Bélgica
- Lituania
- Malta
- Polonia

No medidas de transposición

- Croacia
- Letonia
- Luxemburgo
- Holanda
- Portugal
- Rumania
- España

Procedimiento sancionador

61%

GARRIGUES

II. NUEVOS SERVICIOS: INICIACIÓN DE PAGOS E INFORMACIÓN SOBRE CUENTAS (AGREGACIÓN)

Iniciación de pagos e información sobre cuentas

Iniciación del pago

1. Servicio que permite ***iniciar*** **una transferencia** por cuenta del usuario.
2. Inicio de la transferencia **desde la banca *online*** con sus claves y credenciales.
3. Proporciona al **beneficiario** (e.g., Comercios *on line*) la **seguridad** de que el **pago** se ha **iniciado**.
4. No mantienen los fondos en ningún momento.

Información sobre cuentas

1. Información agregada sobre varias cuentas *online* de un mismo titular.
2. Cuentas en el mismo o diferentes bancos.
3. **Consentimiento explícito** previo del usuario.

Iniciación del pago e información sobre cuentas
Obligaciones : iniciador/agregador y banco

Iniciadores/Agregadores

- Identificarse ante el banco que mantiene la cuenta.
- **Garantizar la seguridad de las credenciales personalizadas** del usuario.
- No almacenar datos de pago sensibles del usuario.
- **Solicitar** al usuario **exclusivamente** los **datos necesarios** para prestar el servicio.
- No modificar los elementos de la operación: importe, fecha, etc.
- Establecer comunicación segura con el banco.

Bancos

- Con independencia del modelo de negocio que utilicen, **permitir a los terceros usar las claves para acceder a la banca *on-line***.
- **No pueden negarse** a que el usuario utilice un servicio de iniciación/agregación.
- Facilitar inmediatamente la información del usuario.
- Prohibición discriminar órdenes iniciadas por un iniciador frente a las que inicia el usuario desde su banca *online*.

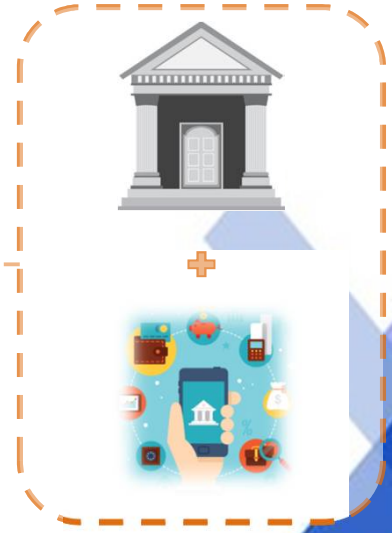
Iniciación del pago e información sobre cuentas
Aspectos comunes

Iniciación y agregación

La prestación de sus servicios depende de la posibilidad de acceder a la información/cuenta en línea que el usuario mantiene en su banco

Requisitos de autorización reducidos

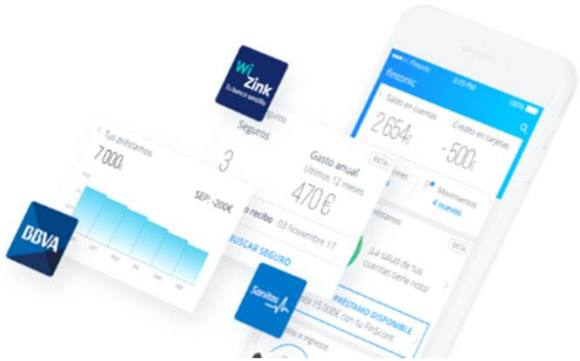
Concurre la presencia de dos proveedores de servicios de pago



GARRIGUES

Qué fácil, qué cómodo

Solo tardas 2 minutos desde que conectas tus entidades hasta que empiezas a sacar partido a tu dinero.



Todos tus productos financieros en una sola app

Todos tus bancos, seguros, tarjetas, préstamos...
organizados automáticamente.
La foto completa de tus finanzas.

VER PRODUCTOS Y SERVICIOS

GARRIGUES

III. APIs ABIERTAS Y SCREEN SCRAPING

APIs abiertas y screen scraping
Concepto

APIs abiertas

Interfaces de programación de aplicaciones que permiten la comunicación e interacción entre módulos de software.

Interfaz específica implementada por los bancos cuyas características y elementos han desarrollado por sí mismos (o encargado a un tercero).

Acceso limitado a los datos que el banco establezca como accesibles a través de esa interfaz.

Screen scraping

Técnica informática automatizada que permite extraer información de una web actuando "como usuario" de la web en cuestión.

Acceso a los datos mediante el acceso a través de la interfaz que habilita el banco al usuario, actuando el tercero "como si fuera él".

Acceso indiscriminado a todos los datos a los que puede acceder el usuario.

PSD2

APIs abiertas y screen scraping
Reglamento Delegado 2018/389: solución a la controversia

Obligación de contar un una interfaz que cumpla los siguientes requisitos

ELEVADO COSTE REGULATORIO

1. Que los terceros puedan identificarse ante el banco.

2. Que los terceros puedan solicitar y recibir información de forma segura: sobre las cuentas y las operaciones.

3. Que los iniciadores puedan iniciar la transferencia de forma segura y recibir información: iniciación y ejecución de la operación.

4. Que permita a los terceros usar el procedimiento de autenticación facilitado al usuario.

Otras obligaciones

Establecer una instalación para pruebas funcionales y de conexión que incluya asistencia a los terceros que la utilicen.

Documentar las especificaciones de la interfaz y ponerlas a disposición de los terceros.

Interfaz: seguir estándares de comunicación de organizaciones de normalización (e.g., ISO).

APIs abiertas y screen scraping
Interfaz obligatoria: neutralidad tecnológica

Bancos pueden decidir facilitar la interfaz

Implementando una **interfaz específica** para el acceso de los terceros

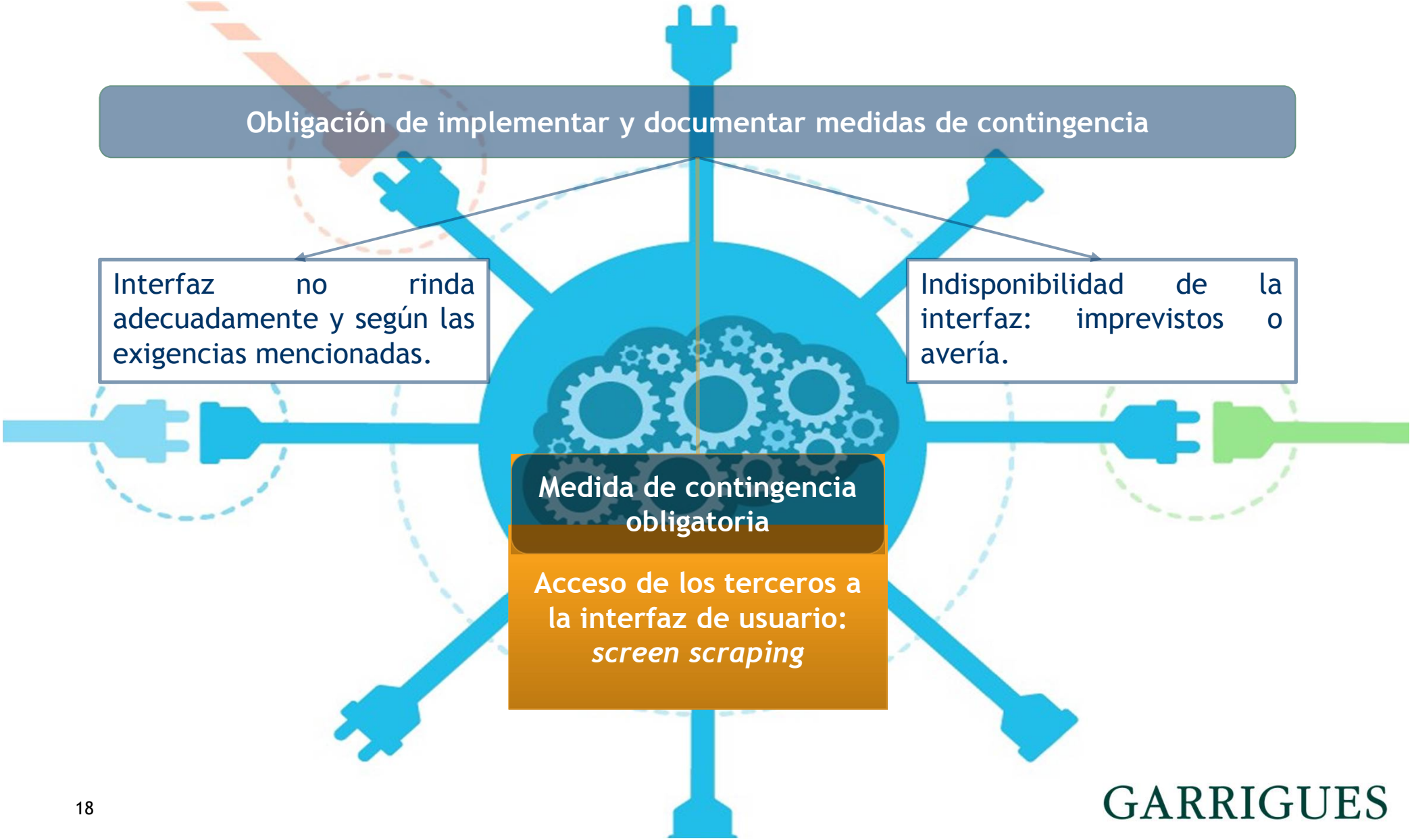
Estándar mínimo: misma disponibilidad y rendimiento que las interfaces de usuarios

Principio de **neutralidad tecnológica** y del modelo de negocio: los bancos deben poder decidir

Permitiendo que los terceros utilicen la **interfaz** que facilitan **a los usuarios**: mediante screen scraping

GARRIGUES

APIs abiertas y screen scraping
Medidas de contingencia para APIs específicas



GARRIGUES

APIs abiertas y screen scraping
Obligaciones de protección de datos de los usuarios

Sujetos obligados al tratamiento

- Bancos
- Terceros

"*Los proveedores de servicios de pago* ***únicamente obtendrán, tratarán y conservarán los datos personales necesarios para la provisión de sus servicios*** *de pago, únicamente con el consentimiento expreso del usuario del servicio de pago*", artículo 94 PSD2.

La iniciación y la agregación se basan en el **consentimiento previo y expreso del usuario** del servicio, lo que incluye el acceso y trato de sus datos.

Principales obligaciones RGPD Europeo

- Elaboración de un Registro de actividades del Tratamiento.
- Designación de un Delegado de Protección de Datos (no obligatorio).
- Redacción de documentación adaptada: cláusulas contractuales, procedimientos, etc.
- Procedimientos internos y análisis de riesgos.
- Formación: personal que trate datos y formación periódica.

Tradicionalmente los bancos se han considerado custodios intachables

GARRIGUES

APIs abiertas y screen scraping
Bancos: evolución progresiva de la tendencia en España

Rechazo a la obligación

PSD2 no dejó lugar a dudas acerca de la obligación aplicable a los bancos de permitir el acceso a sus datos del cliente.

Prohibición del *screen scraping*

La Comisión European mantuvo la posibilidad de utilizar el *screen scraping* como medida de contingencia para evitar eventuales fraudes.

Soluciones actuales

No actuar hasta la transposición

Tendencia actual seguida por un grupo minoritario de operadores que esperan a la completa transposición para cumplir con las exigencias de PSD2

Cumplir PSD2 sin ir más allá

Tendencia actual mayoritaria que consiste en ir adaptándose a los requisitos para estar preparado una vez se produzca la completa transposición.

Cumplir PSD2 aprovechando las oportunidades

Tendencia actual que siguen algunos operadores que implica el uso de las nuevas obligaciones como catapulta al desarrollo de una nueva línea de negocio basada en la digitalización del sector financiero.

GARRIGUES

APIs abiertas y screen scraping
Banca española: principales preocupaciones

PRINCIPAL PREOCUPACIÓN

Level Playing Field

Martes 5 junio 2018 **Expansión** 15

FINANZAS & MERCADOS

La banca pide quitar el tope al bonus de sus directivos tecnológicos

REGULACIÓN/ El sector reclama que la retribución de sus especialistas digitales no esté sujeta a los límites que tienen los banqueros, para que su política de fichajes pueda ser tan atractiva como la de las 'fintech'.

La banca considera que las actuales restricciones limitan su capacidad de captar talento digital

La banca también pide que la inversión en tecnología no penalice las ratios de capital

APIs abiertas y screen scraping
Asociación Española de Banca ("AEB")

ASOCIACIÓN ESPAÑOLA DE BANCA

Identifican como los **dos nuevos operadores** que prestan estos servicios sin ser bancos:

fintonic

FinTech

"Son para las entidades financieras fuentes de innovación con las que colaborar o a las que ayudar en su creación"

+

BigTech

amazon

AliExpress

"Grandes compañías tecnológicas, líderes en otros sectores, que ven oportunidades en algunos segmentos del negocio de los bancos, como en el área de pagos"

eurobits

bizum

GARRIGUES

APIs abiertas y screen scraping
Bancos españoles, modelo BBVA: diferente estrategia

POSTURAS EN EL ENTORNO BANCARIO ESPAÑOL

Postura mayoritaria

Mayoría de entidades

Prácticamente ninguna entidad publicita o facilita detalles sobre su estrategia de APIs abiertas.

La mayoría sólo ofrece acceso a sus APIs a empresas que participan en sus programas de aceleración o que lo solicitan pasando un filtro previo del banco.

La mayoría de las entidades financieras afectadas por PSD2 han optado por comenzar las labores de adaptación para estar preparadas cuando entre en vigor la normativa de transposición.

La tendencia generalizada se centra en reclamar que se les apliquen las mismas *exenciones* que a las *fintech*.

Modelo BBVA

Utilizar las nuevas exigencias normativas para buscar innovadoras soluciones de negocio.

Desarrollo de un sistema de APIs abiertas variado que permite a terceros integrar funcionalidades varias en sus negocios.

APIs abiertas y screen scraping
Modelo BBVA

Interfaz específica

Cada una de las API permite el acceso a un servicio de información diferente.

Algunas de ellas cuentan con condiciones generales que permiten conocer mejor algunas de sus características.

Las APIs se encuentran en un "entorno Sandbox" dentro de la entidad.

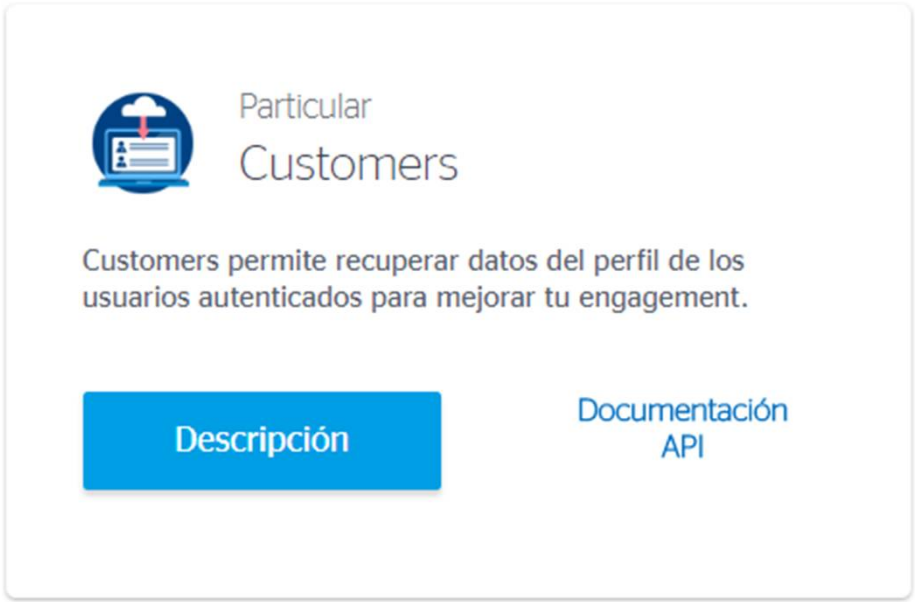
Su uso es gratuito, con la posibilidad de que se comience a cobrar el servicio con preaviso.

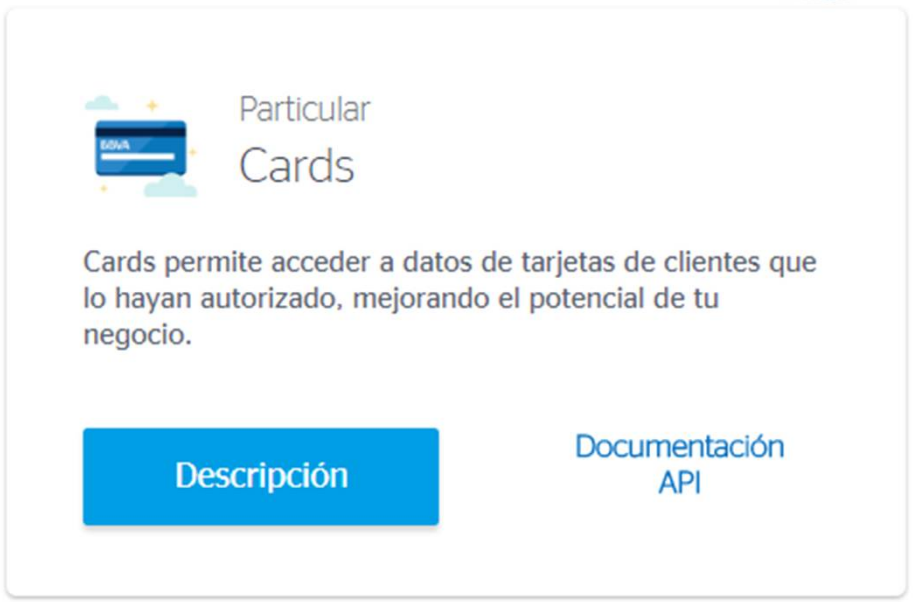
Se destaca la necesidad de que las entidades recaben el consentimiento de sus clientes.

Se menciona específicamente su responsabilidad en el tratamiento de los datos que obtengan "*que él mismo* [cliente] *le proporciona directamente*".

Permiten que el proveedor que utilice el servicio de API **desarrolle un "aplicativo" ("*plugin*") para acceder en nombre del usuario final (cliente de ambos) a la información** concreta a la que permita acceder esa API.

GARRIGUES





Customers permite a los proveedores que la utilicen acceder a los **siguientes datos de los usuarios del banco:**

- Nombre completo del usuario.
- Fecha de nacimiento.
- Sexo.
- Teléfono e E-mail.
- Dirección fiscal.
- DNI, y descarga del mismo.
- Posición global.

Cards permite a los proveedores que la utilicen acceder en nombre del Usuario Final a **la información de sus tarjetas (medios de pago) emitidas por BBVA**, siempre y cuando dicho usuario final solicite y acepte dicho acceso en su aplicación:

- Recuperar PAN, CVV y fecha de caducidad.
- Integra en tu aplicación toda la información relativa a las tarjetas de los usuarios.

GARRIGUES

Agregadores de información sobre cuenteas

Particular

Accounts

Accounts permite a los usuarios preautorizados acceder a los datos principales de su cuenta.

Descripción

Documentación API

Iniciadores de pago

Particular

Payments

Payments permite que apps de terceros ofrezcan transferencias a usuarios pre autorizados.

Descripción

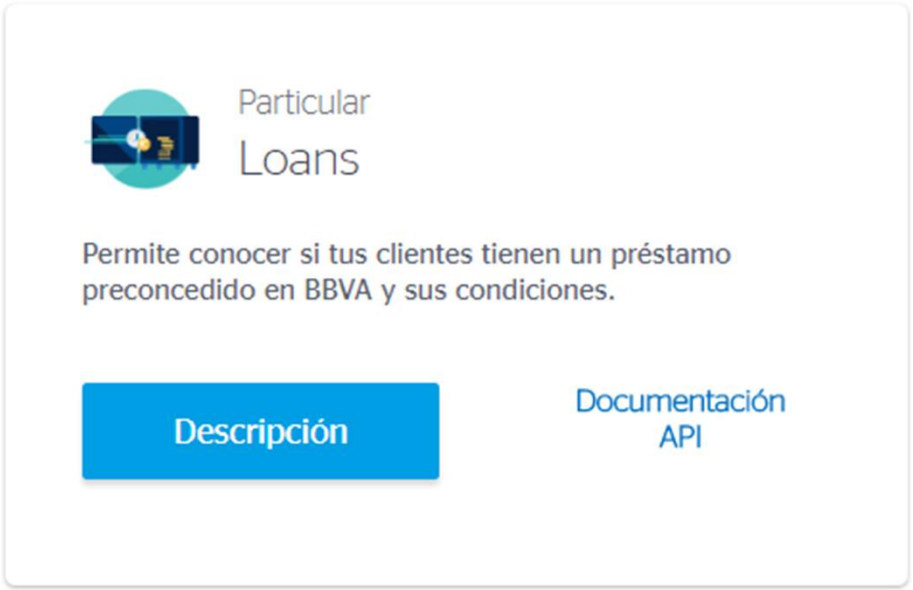
Documentación API

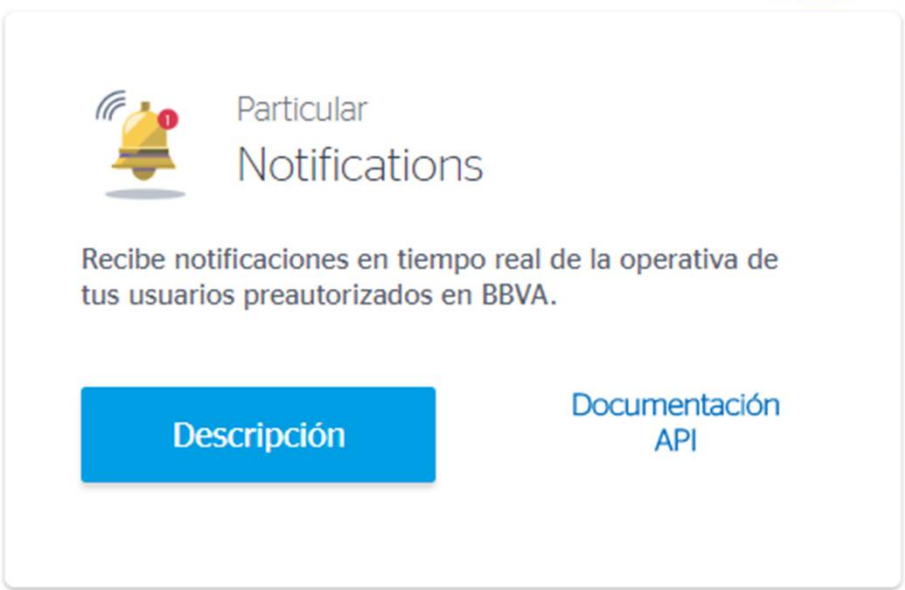
Accounts permite al proveedor acceder en nombre del Usuario Final **a la información de sus cuentas en BBVA**:

- Lista las cuentas, verifica la titularidad, comprueba el saldo y recupera el histórico de movimientos.
- Contextualiza y clasifica los movimientos.
- Histórico de movimientos y consultas de saldo en tiempo real.

Payments permite al proveedor **acceder** en nombre del Usuario Final **a su cuenta en BBVA y desde ella realizar transferencias de dinero con destino a cuentas** en otros bancos.

GARRIGUES





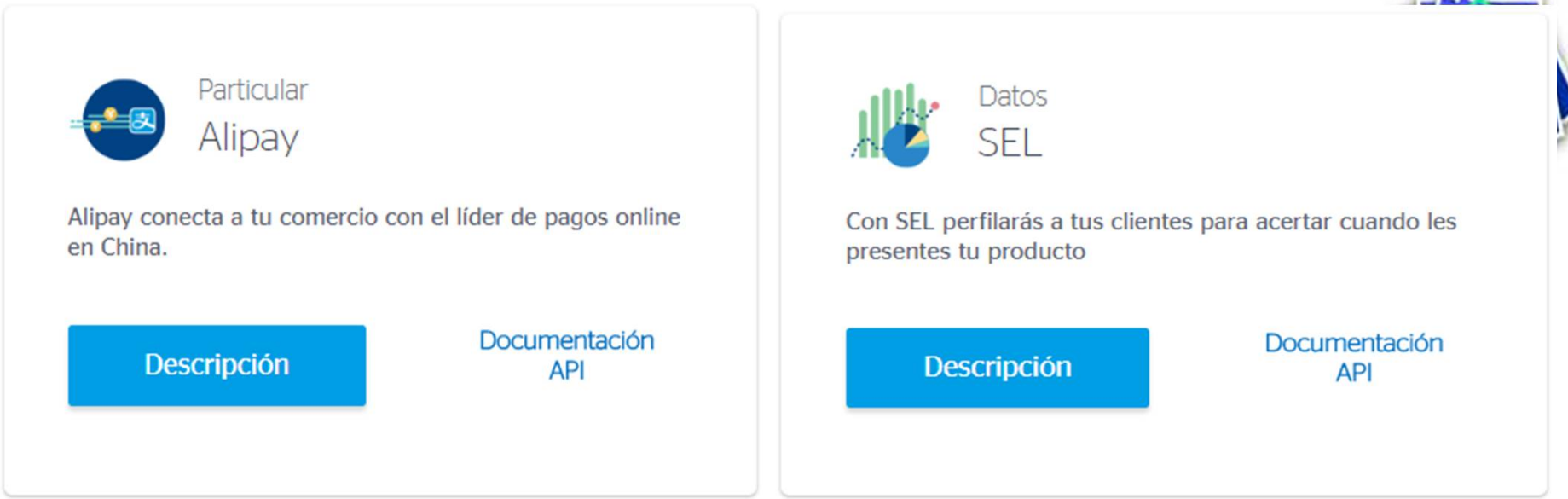
Loans permite que las aplicaciones de los terceros **gestionen los préstamos de un usuario de BBVA** incluyendo los siguientes extremos:

- Confirmar la pre-concesión de un préstamo y las condiciones.
- Posibilidad de ofrecer el préstamos pre-concedidos al cliente.
- Ofrece todos los datos relevantes sobre el préstamo, por ejemplo: límites, importes, plazos y comisiones.

Notifications permite al proveedor elegir, de entre los "eventos" disponibles, aquellos de los que desea recibir notificaciones, de este modo, **el proveedor recibe notificaciones cada vez que el usuarios realiza la operativa correspondiente**.

¡Agregadores!

GARRIGUES



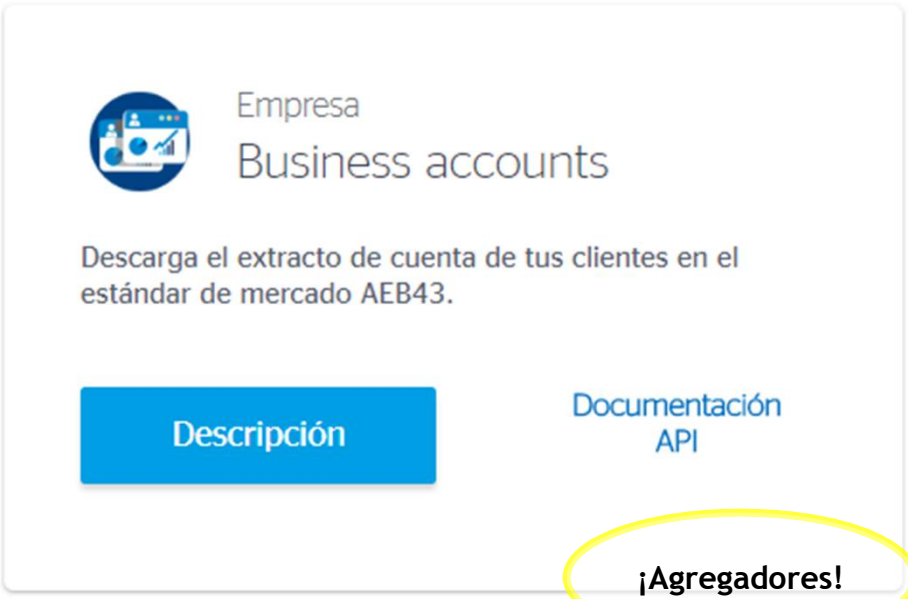
Alipay API permite **interactuar con la solución de pago ALIPAY a través de un TPV-PC de BBVA para tramitar y cobrar las compras que hagan los Usuarios** Finales (usuarios a su vez de ALIPAY) en su aplicación (del proveedor).

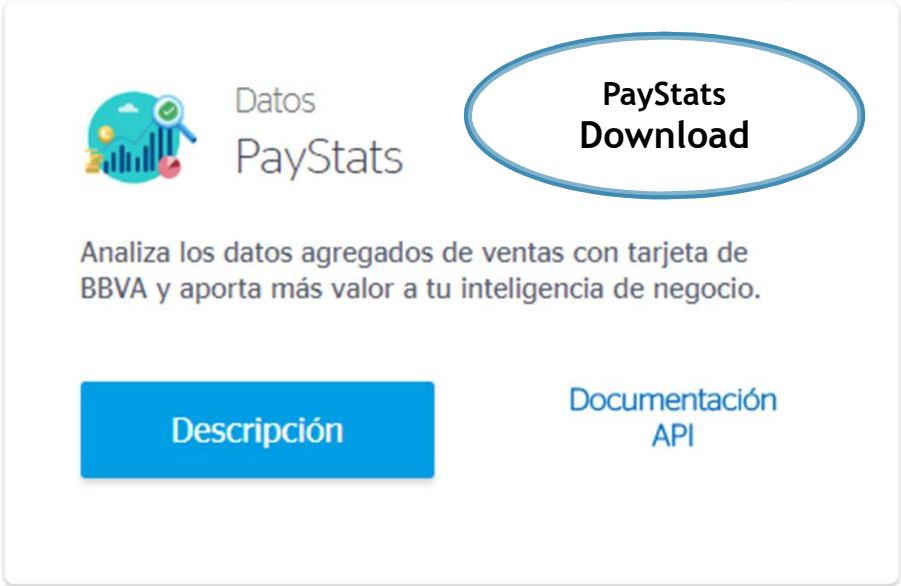
BigTech

SEL ("Socio-Economic & Lifestyle"), **permite a aplicaciones de terceros proveedores acceder a información cualificada financiera y sobre consumo sobre las familias**:

- Información estimada del entorno SEL de los usuarios.
- Su capacidad de ahorro.
- Su límite de riesgo de préstamo.
- El número de líneas móviles contratadas.
- La renta aproximada de la unidad familiar.

GARRIGUES





PayStats Download

¡Agregadores!

Business Accounts permite que las aplicaciones de terceros **accedan a las la información de las cuentas de sus empresas clientes, si que la empresa tenga que salir de ella**:

- Descarga automática de los extractos.
- Conciliación de cuentas más automatizada.
- Cálculos de la posición global, previsiones de caja y tesorería más rápidas.

Permite a los que la utilicen **obtener datos** disociados y **anonimizados irreversiblemente**, tras haber sido sometidos a técnicas de agregación, **de transacciones con tarjetas emitidas por BBVA y/o realizadas en TPVs de BBVA**, en España desde el 1 de enero de 2014 y que son actualizados semanalmente.

Información estadística elaborada sobre la base de una parte de esas transacciones correspondientes a los datos de pago que son procesados por BBVA.

GARRIGUES

APIs abiertas y screen scraping
Banco Santander: *Digilosofía*

App Santander Money Plan

› Gestiona y controla tus cuentas desde el móvil ‹

Digilosofía.

La filosofía digital del Santander.

Por eso puedes recibir en tu móvil el dinero que ganas con la Cuenta 1|2|3. Y gestionar tu cuenta, pagar, domiciliar y devolver recibos, enviar dinero de móvil a móvil, encender y apagar tus tarjetas y mucho más.

Por eso hemos sido el primer banco en permitirte pagar con cualquier móvil, y por eso el Santander es líder en pago con móvil. ¿Tienes un smartphone iOS o Android con tecnología NFC? Haz la prueba.

GARRIGUES

APIs abiertas y screen scraping
Ventajas e inconvenientes de la nueva regulación

Ventajas

- ✔ Apertura de nuevos modelos de negocio basados, fundamentalmente, en el intercambio de datos.
- ✔ Posibilidad de constituirse ellos mismos como "terceros" y actuar como iniciadores y agregadores frente a otros bancos.
- ✔ Aprovechar el desarrollo tecnológico
- ✔ Los terceros estarán sometidos a ciertos requisitos regulatorios también (autorización, capital…).

Inconvenientes

- ✖ Obligación de compartir datos de clientes –a cuya protección están obligados– de forma gratuita.

Coste regulatorio

- ✖ Obligación de realizar una notable inversión en desarrollo tecnológico: APIs, asistencia a los terceros, etc.
- ✖ Terceros con capacidad para sacar rendimiento a los datos obtenidos a través de la prestación de estos servicios.
- ✖ La norma permite a terceros acceder a datos de los bancos, pero no al revés.

GARRIGUES

IV. AUTENTICACIÓN REFORZADA DE CLIENTES

Autenticación reforzada de clientes

Autenticación reforzada: concepto

Autenticación reforzada de cliente

1

Autenticación basada en la utilización de dos o más **elementos**.

- **Conocimiento**: Algo que solo conoce el usuario: fecha de nacimiento, número pin …
- **Posesión**: Algo que solo posee el usuario: token, tablet, dispositivo móvil, tarjeta…
- **Inherencia**: Algo que es el usuario: huella digital, iris, sensores biométricos…

2

Los elementos son **independientes**.

La vulneración de uno de los elementos no debe comprometer la fiabilidad de los demás.

3

Diseñada para proteger la confidencialidad de los datos de autenticación.

GARRIGUES

Autenticación reforzada de clientes
Principales requisitos

Trigger de la obligación

1

Acceso por el usuario a su **cuenta de pago en línea.**

2

Inicio por el usuario de una **operación de pago electrónico.**

3

Realización, a través de un **canal remoto**, de cualquier acción que pueda entrañar riesgo o fraude en el pago.

Canal remoto: canal que permite el pago sin que pagador y pagado estén en el mismo sitio

E.g., pago on line

Código de autenticación

La aplicación de la autenticación en los tres casos anteriores:

Resultado

Generación de un **código de autenticación**

De un solo uso

GARRIGUES

Autenticación reforzada de clientes
Exenciones a la autenticación reforzada

Exenciones

Información de cuentas

- Consulta del saldo de una cuenta.
- Consulta de movimientos de los últimos 90 días.
- Que el usuario tenga acceso **exclusivo** a una de las dos.

No están exentas

- Acceso en línea al saldo por primera vez
- + 90 días desde el último acceso en línea

Pagos contactless en el punto de venta

- Importe máx. **50€**.
- Importe acumulado operaciones previas contactless, desde la última AR, máx. **150€**.
- Operaciones contactless consecutivas, desde la última AR, máx. 5.

Pagos de escasa cuantía

- Pagos de escasa cuantía en operaciones **remotas**.
- Importe máx. **30€**.
- Importe acumulado operaciones remotas previas, desde la última AR, máx. **100€**.
- Operaciones remotas consecutivas, desde la última AR, máx. 5.

Autenticación reforzada de clientes
Exenciones a la autenticación reforzada

Otras exenciones

Terminales no atendidas para tarifas de transporte o pagos de aparcamiento

Cuando el ordenante inicie una operación de pago electrónico en una terminal de pago no atendida con el fin de abonar una tarifa de transporte o un pago de aparcamiento

Beneficiarios de confianza

Cuando el ordenante inicie una operación de pago y el beneficiario esté incluido en una lista de beneficiarios de confianza previamente creada por el ordenante.

Operaciones frecuentes

Para la iniciación de todas las operaciones de pago subsiguientes incluidas en la serie de operaciones de pago frecuentes con el mismo importe y el mismo beneficiario.

Transferencias entre cuentas mantenidas por la misma persona física o jurídica

Cuando el ordenante inicie una transferencia en circunstancias en las que el ordenante y el beneficiario sean la misma persona física o jurídica y ambas cuentas de pago sean mantenidas en el mismo banco.

PBC/FT

Prevención del blanqueo de capitales y FinTech

Pilar fundamental objeto de protección por la normativa del sector financiero: PSD2, Sandbox, etc.

1 **On boarding en línea**

Proceso de identificación no presencial que permite a los usuarios darse de alta como nuevos clientes de manera cien por cien remota, a través de canales online.

2 **Regulación española**

La identificación de los nuevos clientes en un entorno no presencial (como es el online), requiere que concurra alguna de las 4 circunstancias

1. Copia **del documento de identidad**, siempre que dicha copia esté **expedida por un fedatario público**.
2. El **primer ingreso** proceda de una **cuenta a nombre del mismo cliente abierta en una entidad de crédito.**
3. Identidad del cliente acreditada según la normativa de firma electrónica.
4. Identidad del cliente quede acreditada mediante el **empleo de otros procedimientos seguros de identificación.**

3 **Regulación española**

Procedimientos seguros de identificación **aprobados por el SEPBLAC**

- Videoconferencia
- Videoidentificación

GARRIGUES

Sandbox español

Anteproyecto de Ley: 12 de julio de 2018.

Supervisores

- Evaluación previa
- Protocolo de pruebas
- Designación de monitor
- Seguimiento del proyecto y la pruebas
- Control del examen de resultados
- Cauce específico de colaboración y consultas escritas

Ventanilla Única

Solicitudes: Ministerio Economía y Empresa

▼

Reparto a las autoridades supervisoras por materia

▼

Evaluación previa y celebración del protocolo de pruebas

▼

Pruebas

▼

Salida y pasarela de acceso a la actividad

Regulación aplicable

Ley Sandbox

+

Protocolo

=

Obtención de autorización para la actividad regulada

GARRIGUES

GARRIGUES

www.garrigues.com