WhitePaper

¿Cómo afronta Flanks la seguridad?

Con Sergi Lao

Flanks

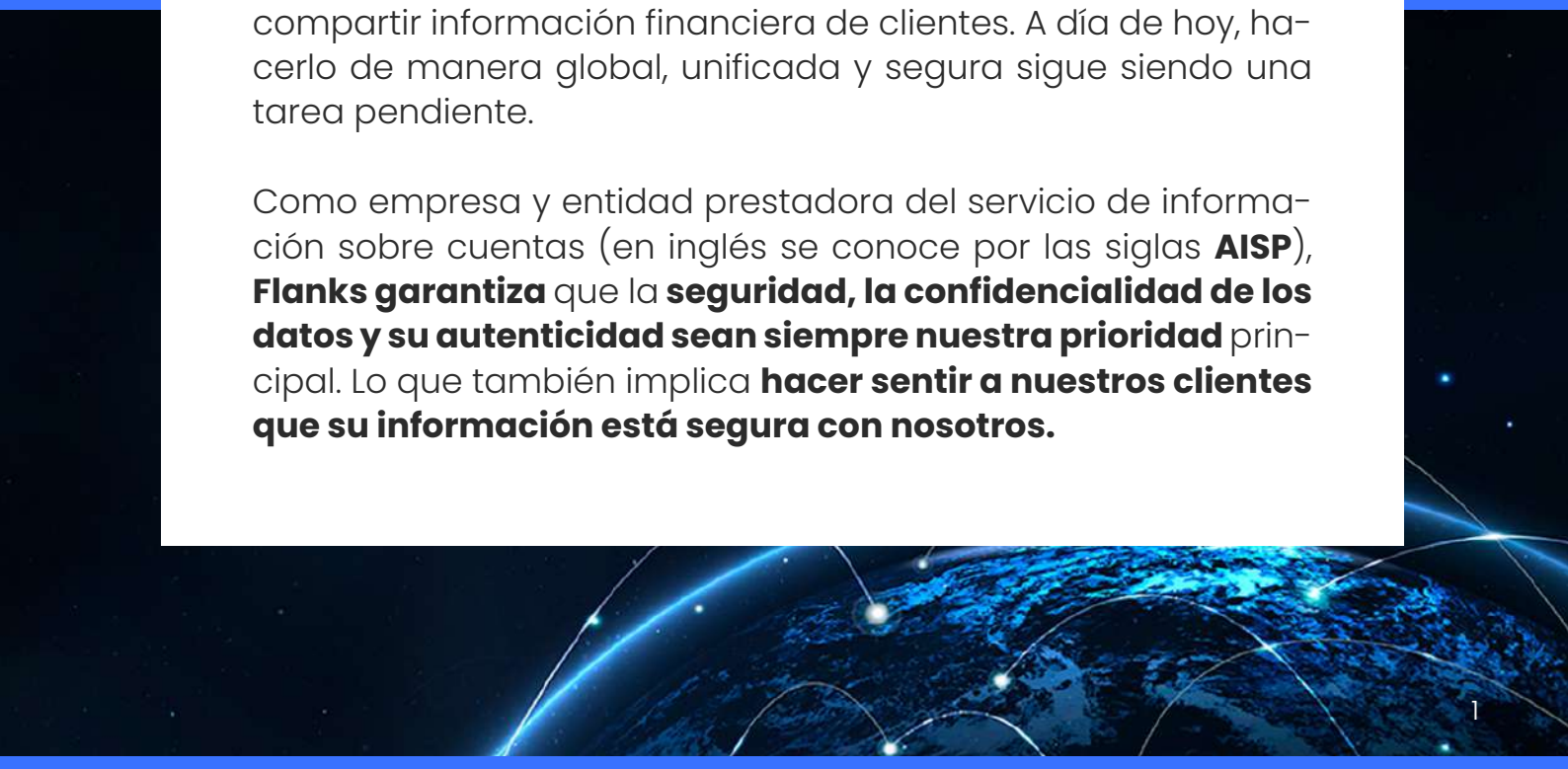
flanks.io | hello@flanks.io

El contexto del Open Banking

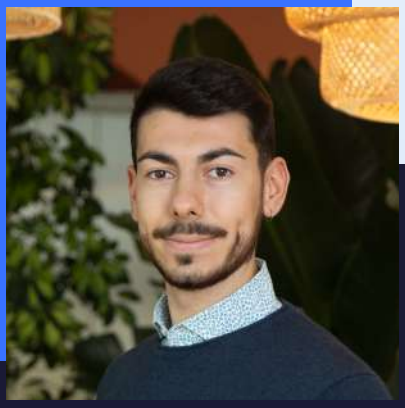
Desde el crecimiento de las iniciativas de Open Banking por todo el mundo a partir de 2018, **los clientes han ido solicitando** cada vez más **una versión consolidada de sus datos financieros en una misma aplicación.**

A pesar de que Europa cuenta con la **regulación PSD2** que afecta a cuentas corrientes, **sigue habiendo una gran necesidad de consolidar otros productos, como las cuentas de inversión.** En cuanto a Latinoamérica y Oriente Medio, la regulación aún está por llegar.

> Aunque el Open Banking la para gestión del patrimonio es una iniciativa reciente pero en crecimiento, sigue habiendo la necesidad de establecer un estándar operativo global para compartir información financiera de clientes. A día de hoy, hacerlo de manera global, unificada y segura sigue siendo una tarea pendiente.
>
> Como empresa y entidad prestadora del servicio de información sobre cuentas (en inglés se conoce por las siglas **AISP**), **Flanks garantiza** que la **seguridad, la confidencialidad de los datos y su autenticidad sean siempre nuestra prioridad** principal. Lo que también implica **hacer sentir a nuestros clientes que su información está segura con nosotros.**



En Flanks la seguridad, la confidencialidad de los datos y su autenticidad son siempre nuestra prioridad principal.



Por esta razón, entrevistamos al experto en seguridad y ciberseguridad de Flanks: **Sergi LAO, CTO y CISO de la empresa.**

Esperamos que este documento le ayude a aclarar cualquier duda o pregunta que tenga en referencia a los estándares de seguridad de Flanks, los procesos que hay detrás de nuestra recopilación de datos entre otras muchas cosas.

1. ¿Por qué es importante la seguridad hoy en día?

Sergi Lao: En la actualidad, la ciberseguridad es clave en todas las industrias, especialmente en las que tratan con datos sensibles como la sanitaria y la financiera. Asimismo, la seguridad es algo que también debe convivir con la experiencia del usuario, algo que es todo un reto.

Garantizar la privacidad, la confidencialidad y la integridad de los datos (conocido como CIA) debería ser uno de los objetivos principales de empresas dentro de los sectores previamente mencionados. No debemos olvidar que el sector financiero está altamente regulado con la intención de garantizar un nivel destacado de seguridad, calidad y transparencia de servicios.

2. ¿Qué hace Flanks en cuanto a seguridad?

Sergi Lao: Flanks protege los datos a todos los niveles del modelo OSI (Open Systems Interconnection: El estándar de referencia para los protocolos de red). Apoyamos la seguridad física de nuestra infraestructura con las certificaciones de calidad y seguridad de Google Cloud Platform. Desde la capa de transporte hacia arriba, se siguen medidas de seguridad, como el cifrado de las comunicaciones externas e internas. Dichos métodos de extracción de datos (el RSA y AES-256) no son personalizados, pero forman parte de unos estándares de mercado seguros y bien probados.

Cabe destacar que Flanks es una empresa regulada como entidad prestadora del servicio de información sobre cuentas, lo que significa que el Banco de España valida nuestros procedimientos. De la misma manera, pasamos por auditorías anuales con empresas externas como Deloitte.

3. ¿Qué es una entidad prestadora del servicio de información sobre cuentas (AISP en inglés)?

Sergi Lao: Una entidad prestadora del servicio de información sobre cuentas es una empresa autorizada para recuperar datos de cuentas proporcionados por bancos y otras instituciones financieras. Es un tipo de actor clave en el entorno comercial de Open Banking actual, y un servicio básico que implica un riguroso proceso de alta.

Ser una entidad de este tipo permite que una empresa financiera como Flanks recopile datos de múltiples cuentas bancarias. Un AISP también tiene la labor de explicar al usuario final a qué datos se accede, durante cuánto tiempo y quién tendrá acceso a ellos. Este proceso de consentimiento digital da forma a la base del procesamiento de datos para AISPs bajo el GDPR. Además, ser un AISP significa que se siguen estándares y metodologías de seguridad aplicables a cuentas corrientes y a otros productos financieros. Asegurando, de esta manera, que todos los procesos sean auditados, seguros y monitoreados.

4. ¿Dónde se almacenan los datos?

Sergi Lao: La solución de Flanks se encarga de conectar datos financieros a cualquier sistema, ofreciendo la más amplia flexibilidad para el almacenamiento de información. Ofrecemos la posibilidad de guardarla de maneras, nodos y regiones diferentes. Podemos también limitar o extender el rango de los datos guardados para garantizar su máxima privacidad.

Flanks se despliega en dos modelos de almacenamiento de datos: On-premise o como Software as a Service (en la nube). En ambos modelos, los datos y las credenciales se obtienen con el consentimiento del cliente.

En la primera opción, los datos y las credenciales extraídas se alojan en el entorno IT del cliente. Su equipo de IT se encargará de la seguridad de ambos, así como de la estabilidad de la solución. El equipo de Flanks estará a su disposición para cualquier tipo de duda. Si opta por la segunda opción, sus datos y credenciales se almacenarán en Europa, más concretamente en los Países Bajos. Flanks se encargará del hosting, de mantener y gestionar la seguridad de estas. También gestionarán la información y las credenciales, que se mantendrán encriptadas y separadas de las claves de encriptación en sí.

5. ¿Cómo se traduce todo esto en nuestro día a día como clientes?

Sergi Lao: Como empresa regulada, Flanks lleva a cabo una serie de chequeos de consentimiento con cada inversor, cada asesor y sus respectivos accesos de e-banking. Del mismo modo, toda la información sobre inversiones pasadas y presentes se encripta de inicio a fin.

Respecto a la confidencialidad de datos, dentro del marco del GDPR Flanks es un procesador de datos: **no analiza ni comparte información con terceros sin una autorización previa.** La empresa cumple con el reglamento GDPR y actúa en nombre del usuario de las credenciales, quien da su consentimiento previo para recuperar y compartir los datos extraídos por Flanks con nuestro cliente. Las credenciales van directamente a Flanks y el cliente obtiene un identificador por estas. Finalmente, el usuario puede solicitar en todo momento que estas se eliminen de Flanks si así se desea.

6. ¿Cómo se enfrenta Flanks a las credenciales bancarias y su inicio de sesión con doble autenticación?

Sergi Lao: Para Flanks, la autenticación reforzada de clientes (SCA) o Autenticación de doble factor (2FA) es una capa de seguridad añadida para los usuarios que acceden a sus sistemas. Esta replica el comportamiento de un banco durante el proceso de inicio de sesión de cada entidad: Si el banco manda un código SMS como método, Flanks lo recibirá y tendrá visibilidad sobre el proceso de inicio de sesión. Somos conscientes que la SCA puede afectar a la experiencia del usuario. Por eso, trabajamos para tener flujos personalizados y así obtener la autorización de nuestros clientes de manera optimizada.

Aparte del código a través de SMS, hay varias maneras más de autenticarse: Por llamada, con una aplicación de autenticación a través de códigos temporales, por reconocimiento facial o de huella dactilar, con claves de seguridad, a través de código QR... Flanks admite cualquier tipo de método manteniendo el proceso de seguridad de cada entidad custodia.

7. ¿Cómo se recupera la información?

Flanks usa un sistema propio de extracción de datos para asegurar que cada acceso está encriptado de punto a punto. Su sistema no solamente cumple con los estándares de seguridad principales, sino que también replica la seguridad que proporciona la institución financiera a la que se accede (sea a través de doble factor biométrico, SMS, token... etc). La información siempre se extrae a través de APIs públicas y privadas proporcionando un nivel óptimo de seguridad, dado que no hacen falta herramientas de terceros para acceder.

8. ¿Cómo se encripta la información?

Sergi Lao: Flanks almacena los accesos con un mecanismo de doble encriptación a través del servicio de KMS de Google. Solo se comparten las credenciales bajo el consentimiento del usuario, que acepta que Flanks transfiera los datos extraídos al cliente final (su asesor financiero o una aplicación de visualización de inversiones). Cada operación que Flanks gestione es de solo lectura por defecto, y los tokens de las autenticaciones reforzadas de clientes no se almacenan en ningún sitio.

9. ¿Cómo se asegura un acceso de solo lectura a la interfaz?

Por motivos de regulación, las entidades bancarias requieren de un autenticación reforzada de cliente para realizar cualquier operación que tenga un impacto directo e irreversible en su situación financiera. Por ejemplo una transferencia, una compra de acciones o un cambio en un fondo de inversión. Por lo tanto, el acceso que se le otorga a Flanks no es suficiente para realizar cambios irreversibles en la empresa. Del mismo modo, Flanks es una compañía regulada que pasa auditorías regulares para reforzar la confianza que los usuarios tienen en nosotros.

10. ¿Si un cliente da sus datos de autenticación a un tercero, no está incumpliendo los términos y condiciones de la entidad custodia?

Sergi Lao: No sería el caso, ya que el GDPR es un estándar superior que cualquier política interna. Esto significa que, a pesar de que una entidad custodia tenga políticas o términos y condiciones en contra del GDPR, el usuario tiene el derecho de poder compartir información con una entidad tercera. Flanks tiene a su disposición diferentes informes de opinión legal vinculantes que validan el uso de la herramienta. No dude contactarnos si surge alguna duda o pregunta al respecto.

11. ¿Cómo puedo empezar a beneficiarme de Flanks?

Sergi Lao: Puede contactarnos a través de la página de contacto de nuestra página web. Allí podrás programar una llamada con nuestro departamento de ventas en cuatro idiomas diferentes: español, inglés, francés y portugués. El equipo estará encantado de ayudarle a resolver cualquier pregunta que tenga sobre su transformación digital.

Información de contacto

Nuestros asesores están siempre aquí para responder cualquier pregunta que puedas llegar a tener.

flanks.io/contact

hello@flanks.io

Más rápido, seguro y más fiable.

Flanks