Flanks

flanks.io

Whitepaper

¿Cómo garantiza Flanks la seguridad?

con Sergi Lao

Chief Information Security Officer y Cofundador

El contexto de Open Banking

Desde 2018, han surgido iniciativas de Open Banking en todo el mundo, y los clientes buscan tener una **visión consolidada de su patrimonio** en un solo lugar.

Aunque en Europa la regulación PSD2 se limita a cuentas corrientes, **la necesidad de consolidar cuentas de inversión es alta**. En América Latina y Oriente Medio, la regulación aún está por desarrollarse.

> “El Open Banking en la gestión patrimonial es una iniciativa reciente pero en crecimiento. Sin embargo, todavía es necesario establecer un estándar operativo global para compartir los datos financieros de nuestros clientes. Hasta hoy, no existe una forma global, unificada y segura de compartir esta información.”

Como empresa AISP (Account Information Service Provider), en Flanks siempre priorizamos **la confidencialidad, integridad y disponibilidad de los datos.** Esto implica garantizar que nuestros clientes se sientan seguros de que su información está protegida.

Flanks garantiza que la confidencialidad, integridad y disponibilidad sean siempre nuestras principales prioridades.

Por este motivo, entrevistamos a Sergi Lao, Chief Information Security Officer y Co-Fundador de Flanks, nuestro mayor experto en ciberseguridad.

Este whitepaper tiene como objetivo aclarar cualquier duda sobre los **estándares de seguridad de Flanks, los procesos de agregación de datos** y otros aspectos relacionados.

Sergi Lao
CISO y Cofundador

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

Actualmente, la ciberseguridad es clave en todos los sectores, pero es especialmente crítica en aquellos que manejan datos sensibles, como la salud y las finanzas.

La seguridad debe convivir con la experiencia de usuario, lo que representa un reto considerable. Garantizar la privacidad, la confidencialidad y la integridad de los datos debe ser uno de los principales objetivos en estas industrias. Los servicios financieros están altamente regulados para asegurar estándares de seguridad, calidad y transparencia.

2 ¿Qué hace Flanks en términos de seguridad?

En Flanks aplicamos medidas de protección en todas las etapas del ciclo de vida del dato: en reposo, en tránsito y en uso. Nos apoyamos en la seguridad física y en las certificaciones de calidad y seguridad de Google Cloud Platform. Aplicamos estándares de cifrado en todas nuestras comunicaciones internas y externas.

Los métodos de cifrado que utilizamos, RSA y AES-256 no son personalizados, sino que son **estándares del mercado probados y seguros.**

Flanks cuenta con la certificación **SOC3 y SOC2 Tipo II**, lo que demuestra nuestro compromiso con un control riguroso en el tratamiento y seguridad de los datos.

Además, estamos regulados como empresa AISP, lo que implica que el **Banco de España valida nuestros procesos y procedimientos.** También somos auditados anualmente por firmas externas como EY.

3 ¿Qué es un Proveedor de servicios de información de cuentas (AISP)?

Un AISP es una empresa autorizada para obtener datos de cuentas proporcionados por bancos y otras instituciones financieras. Es un actor clave en el ecosistema actual de Open Banking, y requiere un riguroso proceso de autorización.

La licencia AISP del Banco de España nos otorga la autorización oficial para acceder y procesar datos financieros de forma segura, demostrando nuestra **fiabilidad y credibilidad** en el sector financiero.

Ser un AISP permite a empresas como Flanks compilar datos de múltiples cuentas bancarias. Además, informa al usuario final qué datos se recopilan, por cuánto tiempo y quién tendrá acceso. Este consentimiento digital es la base del tratamiento de datos bajo el **RGPD.**

Asimismo, cumplir con el estándar de AISP nos permite aplicar estas metodologías de seguridad a cuentas corrientes y a otros productos financieros, garantizando que todo esté **auditado, seguro y monitorizado.**

4 ¿Dónde se almacenan los datos?

Flanks se centra en conectar datos financieros con cualquier sistema. Ofrecemos **gran flexibilidad** para almacenar la información, con posibilidad de usar diferentes modelos y regiones. También podemos limitar o ampliar el alcance de los datos guardados para garantizar su máxima privacidad, siguiendo el principio de minimización del RGPD.

Nuestra solución opera en dos modelos de almacenamiento: **On-premise (en las instalaciones del cliente), Software como Servicio (SaaS, en la nube).** En ambos casos, el acceso a datos y credenciales se hace con consentimiento explícito del cliente.

En la primera opción, los datos extraídos y las credenciales se alojan en el entorno de TI del cliente. Su equipo de TI se encargará de la seguridad y del correcto funcionamiento de la solución, mientras que el equipo de Flanks estará disponible para cualquier duda.
Si elige la segunda opción, sus datos y credenciales se almacenarán en Europa, específicamente en los Países Bajos. Flanks se encargará del alojamiento, mantenimiento y de garantizar su seguridad. Flanks también gestionará y protegerá tus credenciales, y tanto los datos como las credenciales serán cifrados y separados de las claves de cifrado.

5 ¿Cómo se traduce todo esto en la experiencia del cliente día a día?

Como empresa regulada, Flanks realiza verificaciones de consentimiento para cada inversor, asesor y sus accesos de e-banking. Toda la información sobre sus inversiones pasadas y presentes está cifrada de extremo a extremo.

En cuanto a la confidencialidad de los datos, dentro del ámbito del RGPD, Flanks es un procesador de datos. Esto significa que Flanks no comparte los datos con terceros no autorizados y opera en nombre del propietario de las credenciales, quien otorga su consentimiento para recuperar y compartir los datos extraídos por Flanks con nuestro cliente.

Las credenciales se transmiten directamente a Flanks bajo los más altos y reconocidos estándares de seguridad. El cliente recibe un identificador asociado, y puede **eliminar sus credenciales en cualquier momento.**

6 ¿Cómo accede Flanks a los datos patrimoniales de los clientes?

Ofrecemos múltiples vías para acceder a los datos financieros, según las preferencias del cliente y las capacidades de sus entidades financieras.

Para las instituciones que permiten el acceso estructurado a los datos, utilizamos el Poder Notarial (PoA), un método seguro y escalable que habilita la recuperación automatizada de datos:

Credenciales Flanks con Poder Notarial (Power of Attorney - PoA): la entidad financiera crea un acceso online de solo lectura para Flanks. Esto nos permite agregar datos financieros de manera independiente, sin la necesidad de credenciales proporcionadas por el cliente, mientras se garantiza una obtención de datos segura y fluida.

Data feeds (también requiere PoA): se establece un intercambio directo y estructurado de datos entre Flanks y la institución financiera. En lugar de depender del acceso basado en inicio de sesión, la institución proporciona de manera segura archivos de datos financieros en un formato estandarizado. Este enfoque mejora la precisión de la automatización y minimiza la interacción del cliente. Aunque la disponibilidad de los Flujos de Datos depende de las capacidades de cada institución, representan la forma más **eficiente y escalable** de agregar datos financieros.

7 ¿Hay algún método con PoA mejor que los demás?

Todos los métodos son seguros, pero los **Data Feeds** son los más eficientes y escalables. Automatizan la extracción, refuerzan la seguridad y ofrecen una experiencia de usuario más fluida y sin fricciones. Adicionalmente, las entidades financieras suelen preferirlo por facilitar la gestión de datos y hacer más eficiente la agregación patrimonial.

En conclusión, aunque todos los métodos siguen siendo alternativas sólidas, los Data Feed proporcionan el mejor equilibrio entre seguridad, conveniencia y eficiencia operativa.

8 ¿Qué pasa si el cliente prefiere un método alternativo al Poder Notarial (PoA)?

El cliente puede decidir usar sus propias credenciales. En estos casos, se aplica la **Autenticación Reforzada del Cliente (SCA** en inglés, conocida como **2FA**) para poder acceder de forma segura a la institución financiera. A diferencia del PoA, este método puede requerir autenticaciones periódicas por parte del cliente.

Flanks solo activa el SCA o 2FA cuando el usuario está presente, evitando riesgos como aprobar notificaciones desconocidas. Soportamos múltiples métodos: SMS, llamadas, apps de autenticación, biometría, llaves de seguridad y códigos QR, siempre siguiendo las políticas de seguridad de cada entidad custodiante.

9 ¿Cómo protege Flanks las credenciales si las proporciona el cliente?

Usamos un **mecanismo de doble cifrado** con Google Cloud KMS. Solo almacenamos las credenciales con el consentimiento del usuario. Todas las operaciones con credenciales son **monitorizadas, registradas y son solo lectura por defecto**. Los códigos SCA/2FA **no se almacenan.**

10 ¿Cómo garantizan que el acceso sea solo de lectura?

Por regulación, para realizar operaciones que impacten de manera directa e irreversible la situación financiera del cliente, como una transferencia bancaria, compra de acciones o cambio de un fondo de inversión, se requiere SCA. El acceso de Flanks **no permite este tipo de cambios irreversibles** dentro de las cuentas. Adicionalmente, Flanks está regulada y auditada para reforzar la confianza de nuestros usuarios. Mantenemos un registro detallado de qué datos se extraen y cuándo.

11 ¿No estaría violando el cliente los T&C del banco al compartir sus credenciales?

No. El RGPD tiene prioridad sobre las políticas internas. Esto significa que aunque un banco tenga cláusulas en contra, el usuario **tiene derecho legal a compartir sus datos con una entidad tercera.**

Flanks cumple con **PSD2 y RGPD,** y cuenta con informes legales vinculantes que respaldan el uso de la herramienta a su disposición. Además, Flanks simula el comportamiento de un navegador web y limita el uso de ancho de banda para no afectar la web del banco.

12 ¿Cómo puedo empezar a utilizar la solución de Flanks?

Puedes contactarnos desde la página de contacto en nuestro sitio web. Allí puedes agendar una llamada con nuestro equipo en español, inglés, francés o portugués.

Estaremos encantados de ayudarte en tu proceso de transformación digital.

Contáctanos

Nuestros expertos en gestión patrimonial están listos para ayudarte. Si tienes preguntas o necesitas más información, no dudes en escribirnos.

Flanks

Wealth, easily managed

¡Hablemos!

Flanks.io