COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Sesión 24
Foro del Sistema de Finanzas Abiertas (FSFA)

Comisión para el Mercado Financiero
Febrero 2025

Agenda

01 Presentación EdS: Entregable Etapa 3

02 Presentaciones miembros GC: posiciones sobre entregable Etapa 3

Agenda

01 Presentación EdS: Entregable Etapa 3

02 Presentaciones miembros GC: posiciones sobre entregable Etapa 3

Entrega Etapa 3
Sistema Finanzas Abiertas

Grupo Consultivo 20 de febrero

Se distribuyó entregable Etapa 3 al GC

	Etapa 0 **(Fase 1)**	Flujo de solicitud de información de términos y condiciones y canales (completado)
	Etapa 1:	Flujo de consulta de información de Persona Natural* (incluye mecanismo alternativo)
	Etapa 2:	Monitoreo + Plan de Prueba (Onboarding) + Gestión posterior al consentimiento (revocación, consultas, etc.) + Portal Web
	Etapa 3:	**Flujo de consulta de información de Persona Jurídica***
	Etapa 4:	Iniciación de pagos

(Fase 2)

* Información para Bancos, Emisores de tarjetas de pago y otros proveedores de cuenta

Se distribuyó tercer documento, correspondiente a Etapa 3

- Documento consideró: **los entregables de las Etapas anteriores (0, 1 y 2)**, la NCG, antecedentes del Directorio presentados por la CMF (2 reuniones), **los Workshops (Etapas 1, 2 y 3)**, **reuniones de los GT** sostenidas entre el 2 y 9 de enero, **retroalimentación entregable de las Etapas anteriores**, visión informada del Equipo de Soporte, y resultados de posiciones de los participantes de los GT a consultas del Equipo de Soporte (EdS).

- El objetivo fue generar un documento consistente, basado en las visiones planteadas por los partícipes de los GT, para su discusión en el Grupo Consultivo.

- En el documento se fue cuidadoso de consignar las opiniones de los distintos gremios dentro del mismo cuerpo del entregable, con el fin de facilitar la lectura.

- Se agregó un anexo correspondiente a los payloads de los endpoints de información. Por otro lado, el resto de los anexos dan trazabilidad al relato del cuerpo, y permiten trazabilidad tanto de las posiciones como de las conversaciones sostenidas en el proceso.

Estructura del documento

01

Capítulos transversales con las abreviaciones, estándares y definiciones, introducción, **contribuciones proceso de discusión Etapa 3**, y la conclusion (enfocado al proceso metodológico).

02

El cuerpo con la Infraestructura, aspectos técnicos de las APIs, requerimientos de seguridad, comunicación y gestión de incidentes de Seguridad, **y experiancia de usuario (PN y PJ).**

03

El documento contiene todas las temáticas que el Equipo de Soporte propuso para que los GT entregaran su posición, junto con la retroalimentación que cada gremio y Banco Estado entregó respecto a sus posiciones (en anexos).

04

Finalmente, los anexos contienen las posiciones respecto a cosultas que hizo el EdS, las minutas de todas las reuniones de los GT, las presentaciones de cada participante, y **los payloads de los endpoints de información.**

Contribuciones proceso de discusión Etapa 3

Autoridades Certificadoras

Se avanzó en desarrollar propuestas en ausencia de una CA raíz, como resultado de las conversaciones con grupo trabajo de la ACTI.

Comentarios CMF Entregable 2

Se recibieron comentarios de parte de la CMF posterior a los ciclos de reuniones, por lo que no se pudieron conversar en los GT. Se dejaron recuadros con respuestas del EdS.

Gestión del consentimiento

La mayor parte de la discusión de los GT giró en torno a dos modelos de consentimiento (API o RAR + Grant Management). La propuesta se decantó por el modelo que más se alinea con el estándar FAPI 2.0.

Infraestructura e Intercambio de Información

Autoridades Certificadoras

Hubo consenso respecto a operar con una estructura de 2 capas (tier) de certificados SSL, integrado por Autoridades Certificadoras Intermedias y Autoridades Certificadoras Raíz. Esta estructura permite balancear seguridad, escalabilidad y flexibilidad.

Certificación APIs, disponibilidad, TPM y TPS

Se refinaron y profundizaron las propuestas de la etapa 2.

Gestión del consentimiento

Se decantó por la utilización de RAR + Grant Management, debido al RFC RAR (RFC 9396), que permite tener un marco de trabajo ya definido, alineado con FAPI 2.0.

Payloads de endpoints de información

El EdS recolectó el trabajo de los gremios y Banco Estado respecto a los payloads de los endpoints y generó un anexo con esta información.

Requerimientos de Seguridad

Perfil Financiero de Seguridad FAPI 2.0

En esta etapa principalmente se profundizaron en aspectos del perfil FAPI 2.0 a utilizar en el SFA en Chile.

Consideraciones implementación FAPI 2.0

Sección que resume algunos de los acuerdos que se han tomado en la implementación del perfil FAPI 2.0 en Chile.

Ejemplo Flujo FAPI 2.0

Explicación de los flujos de consentimiento y su lineamiento con el perfil FAPI 2.0.

Requerimientos de Seguridad y Experiencia de usuario

Perfil Financiero de Seguridad FAPI 2.0

Se profundizaron en aspectos del perfil FAPI 2.0 a utilizar en el SFA en Chile, en base a las respuestas al cuestionario FAPI 2.0.

Grants OAuth 2.0 y listas blancas

Se acordaron los grants adicionales (no obligatorios) a utilizar. Por otro lado, se acordó no utilizar listas blancas de IP para el Directorio.

Gestión de Reclamos

Se incorporan elementos de gradualidad en la propuesta, como también algunas buenas prácticas y sugerencias (como ticketera centralizada).

Consentimiento Persona Jurídica

Siendo este uno de los puntos de mayor complejidad y divergencia, se propone un flujo de usuario tomando varios elementos y sugerencias de distintos gremios, siguiendo un principio de simplificación del flujo.

Temas arrastre y consultas a CMF

Temas arrastre:

- Mecanismos alternativos:
    - Conclusión de la discusión en Grupo Consultivo
    - Consulta a CMF: a qué nivel es la uniformidad que señala la NCG 514 respecto del mecanismo alternativo

Consultas CMF Abiertas:

- Consistencia entre NCG 514 y poderes de las mallas societarias de las empresas
- Interpretación normativa para ver cómo abordar la experiencia usuaria para la selección de múltiples productos.
- Borde del sistema de finanzas abiertas y finanzas embebidas.

Comenzó el trabajo de la Etapa 4

- El día 16 de enero los distintos participantes del SFA dieron el kickoff a la Etapa 4, iniciación de pagos.
- Para este ciclo, se ha optado por tener dos reuniones en donde se unen todos los GT para que cada gremio y Banco Estado propongan flujos de iniciación de pagos, partiendo de los acuerdos de las etapas anteriores (por ejemplo, todos los aspectos acrodados del perfil FAPI 2.0).
- Por otro lado, el EdS comenzó la discusión los casos de uso más simples:
  - PN y PJ de bajo valor, 1 a 1 para pagos con todo tipo de tarjeta y TEF.
  - Se revisarán modificaciones que se deban introducir a esos flujos, pero para pagos batch y el caso de múltiples aprobadores.
- Si bien el alcance de esta etapa se acotó a los casos de uso más simples, debido a la variedad de casos de uso que tiene la iniciación de pagos, es probable que queden elementos que no se revisen con la profundidad necesaria, quedando pendientes para la siguiente fase (junto con los casos de uso más complejos).

Entrega Etapa 3
Sistema Finanzas Abiertas

Grupo Consultivo 20 de febrero

Agenda

01 Presentación EdS: Entregable Etapa 3

02 Presentaciones miembros GC: posiciones sobre entregable Etapa 3

Cooperativas de Ahorro y Crédito Asociación Gremial - COOPERA A.G.

Entregable
Etapa 3

Posición Coopera

Entregable – Etapa 3

Autoridades Certificadoras

Marcha blanca

Mecanismo alternativo

Entregable – Etapa 3

Autoridades Certificadoras

Consultas importantes:

- ¿Considerando los requerimientos que deben cumplir las CA, cual es la visión de la CMF?
- ¿Si las CA no acceden, está pensada una solución alternativa? (por ejemplo, buscar fuera de la lista del MINECOM, fuera de Chile o adaptar la NCG)

Contexto:
La NCG 514 establece la importancia de las autoridades certificadoras (CA) en la implementación de los certificados digitales que servirán para validar a las instituciones en el SFA.

Durante noviembre y diciembre se realizaron sesiones de los grupos técnicos con las CA. En estas sesiones las CA manifestaron no estar dispuestas a adecuar sus servicios para los flujos del SFA

Posición Coopera:
En base a lo anterior, manifestamos nuestra preocupación sobre la postura de parte de las CA de no modificar sus servicios para adaptarse las necesidades del SFA

Entregable – Etapa 3

Contexto:
El entregable de la etapa 3 se enuncian 4 puntos respecto de la marcha blanca:

- Aspectos de seguridad no sacrificables
- Flexibilidad en requisitos no funcionales
- Medición de TPS y TPM
- Períodos de marcha blanca (3 meses en prueba y 12 meses en observación).

No se detalla ninguno de estos puntos

Posición Coopera:
Sobre la disponibilidad y rendimiento ante alguna degradación de servicio no debiese generar sanciones durante el periodo de marcha blanca.

Marcha blanca

Consultas importantes:

- ❑ ¿Desde cuándo se miden los periodos de prueba y observación?
- ❑ ¿Cuáles son los requisitos no funcionales?
- ❑ ¿Cuáles serán los criterios de éxito de estas marchas blancas y cuáles serán las acciones si no se cumplen? (¿se avanza a la siguiente etapa?¿existirán sanciones?)

Entregable – Etapa 3

Mecanismo alternativo

Consultas importantes:

- ¿Se definirán métricas de disponibilidad y rendimiento especificas al MA?

Contexto:
Se presentan las estrategias de activación del mecanismo alternativo (MA):

- Activación desde la IPI ante la degradación de un servicio
- Siempre activo

Posición Coopera:
Consideramos la opción de un mecanismo de activación ante la degradación del servicio (activo – pasivo).
Adicional a lo anterior, seguimos manifestando nuestra postura de postergar la implementación del MA hasta que podamos medir el funcionamiento del sistema y se defina la real necesidad de implementarlo. Más aún, cuando el mecanismo principal ya es altamente exigente.
Una forma de medir la necesidad de implementarlo es utilizar la marcha blanca para estos fines.

Entregable
Etapa 3

Posición Coopera

Banco del Estado de Chile (BancoEstado)

Entregable Etapa 3:
Flujos de Solicitud de Información de Datos Públicos de PJ

Visión BancoEstado

Implementación SFA

20 de Febrero de 2025

Infraestructura

❑ Múltiples Registros PSBI e IPI

- ➢ La **propuesta** contiene **varios elementos positivos**
  - Permitir **múltiples registros** bajo una institución del SFA
  - Existencia de un **SSA diferente para cada cliente** registrado en la IPI/IPC
- ➢ Creemos que hay **elementos que se deben precisar** de mejor manera
  - **SSA firmado por el Directorio no es suficiente** a nivel de **seguridad,** dado que sólo se valida la relación de cada marca inscrita con el PSBI en forma bilateral vía DCR
- ➢ **Sugerimos** que se establezca un **mTLS** tradicional como **elemento de seguridad adicional**
  - En línea con **experiencia** de **Brasil y UK** en este sentido.

APIs

❑ Generación y Gestión del Consentimiento

- ➢ **No adherimos** a la **propuesta** de **utilizar RAR + Grant Management** para la gestión del consentimiento
  - Estándar posee **elementos** que se encuentran aún **en etapa de desarrollo**
  - Aún **no utilizado en otras jurisdicciones ➔ riesgo de implementación**
- ➢ **Recomendamos** la utilización de **API de Consentimiento**
  - Alternativa ya probada en **Brasil y UK ➔ disminuye riesgo de implementación**
  - Existencia de **soluciones de mercado**

APIs

❑ Marcha Blanca

- ➢ La **propuesta** posee **varios elementos positivos**
  - Inclusión de varios **elementos de seguridad**
  - Consideración de **marcha blanca pre-productiva** (período de pruebas) **y productiva** (período de observación)
- ➢ **Recomendamos** un **ajuste** en los **períodos de marcha blanca** propuestos
  - **3 meses** para **período de pruebas** se considera **insuficiente**
    - Plazos debieran estar en línea con fechas para la puesta en producción de los diferentes componentes de los Grupos 1 y 2
    - Avance por fases
  - **12 meses** para **período de observación** se considera **insuficiente** de acuerdo a experiencia de **Brasil y UK**
    - Período debiera durar hasta Julio de 2029 (entrada en producción de Grupo 2)
    - Aclarar métricas (TPS, TPM, uptime, etc.) que serán referenciales

UX

❑ Flujo Consentimiento PJ

- Si bien la **propuesta** tiene **varios elementos positivos**, creemos que **algunos** de ellos **deben ser mejorados**.
  - **Creemos** que la **PSBI no debe rescatar información de PJ a partir de PN** en el redireccionamiento, en vista que esta información ya la posee y la mantiene actualizada la IPI, además de poseer las atribuciones para la validación de consentimientos.
  - **No debiera existir** una definición ex ante de **URL de entrada distintas para PN y PJ**. Esto es una decisión de cada IPI.
  - **No es necesario el uso de login_hint de OpenID Connect Core** para la identificación de la persona que autoriza el consentimiento, en vista que esto es algo que ya se encuentra recogido en soluciones como la API de Consentimiento.

❑ Fortalecimiento medios de prueba jurídicos

- **De acuerdo** con **FAPI 2.0 Message Signing** como medida obligatoria para ayudar a garantizar el no repudio mediante el uso de firmas digitales en las transacciones
- Sin embargo, **no estamos de acuerdo** con la **firma diaria de logs** con estampa de tiempo como medida obligatoria adicional.
  - Esta solución reviste una serie de **complejidades técnicas** para su implementación

Gracias

BancoEstado
desde 1855

Asociación de Aseguradores de Chile, Asociación Gremial - Asociación de Aseguradores de Chile A.G. (AACH)

ASOCIACION DE ASEGURADORES DE CHILE A.G.

Revisión etapa 3

20 de Febrero 2025

Agenda

ASOCIACION DE ASEGURADORES DE CHILE A.G.

Overview etapa 3

Comentarios generales

Principales temas pendientes

Comentarios generales etapa 3

1 GT Infraestructura

Reportes de indesponibilidad

- Se plantea un Cross check como **reporte mensual para las PSBI**, con datos diarios por IPI, es decir, cantidad de llamadas totales y exitosas y momentos de indisponibilidad
- Como AACH **nos preocupa** la propuesta, dado que el reporte de **cross check** realizado por las PSBI podría ser no **representativo** de la disponibilidad de las APIs expuestas desde las IPI, lo que pudiese **distorsiona**r los indicadores de indisponibilidad.

2 GT APIs

RAR + Grant Management

- La AACH adhiere a utiliza RAR + Grant Management, siempre y cuando sea para **etapas evolutivas del SFA**
- Dado que en las primeras etapas no se contemplan casos de uso que requieran RAR, se busca facilitar la adopción del SFA con la **menor fricción posible para todos los participantes**
- Además, RAR + Grant Management aún se **encuentra en proceso de estandarización**, y su implementación recién comienza a considerarse en geografías de referencia como el Reino Unido y Brasil
- Para reducir la incertidumbre en el desarrollo, **se mantiene la postura de utilizar APIs de consentimiento en la fase inicial,** priorizando la estabilidad y la facilidad de implementación.

3 GT Seguridad

Mecanismos de comunicación

- Se han logrado avances significativos en la **definición de los mecanismos de comunicación**.
- Sin embargo, la definición del **mecanismo alternativo sigue pendiente.**

4 GT UX

Tiempos de Resolución de Conflictos

- Proponemos que los **tiempos de respuesta y resolución** debiesen ser **ajustados** considerando la **criticidad del dato compartido**. Por ejemplo, una falla en la iniciación de pagos requiere una respuesta más rápida que la indisponibilidad de una API de términos y condiciones.

Principales temas pendientes

Utilización de scopes o RAR + Grant Management:

- Es clave definir que **mecanismo se utilizara**, dado que esto dependerá las definiciones de las APIs de consentimiento y APIs de negocio en caso de no utilizar RAR + Grant Management y aterrizar los esfuerzos de desarrollo que puede estar asociado uno del otro.
- Se propone estandarizar el uso de ***scopes*** como mecanismo principal. Dicha propuesta surge ante la incertidumbre y complejidades asociadas a la implementación del modelo RAR + Grant Management, considerando que:
    - **RAR + Grant Management** aún se encuentra en proceso de definición como estándar, lo que implica posibles ajustes y cambios futuros.
    - Países referentes en Open Finance, como **Brasil** y **Reino Unido (UK)**, no han implementado aún este modelo.
- Asimismo, el uso de *scopes* se presenta como una solución funcional y testeada en otros países, que permitirá bajar los esfuerzos de implementación e incertidumbre, siempre con el objetivo de disminuir fricción a la adopción del SFA.

Firmado del SSA autofirmado o directorio

- Queda pendiente la definición sobre como se firmará el SSA durante el registro en el DCR, auto firmado versus firma por el directorio

Mecanismo Alternativo:

- Se mantiene pendiente la definición de un **mecanismo alternativo**. Se sugiere enfocarse en **garantizar la disponibilidad y continuidad de la API**, siguiendo experiencias exitosas como las implementadas en **Brasil** y el **Reino Unido**

ASOCIACION DE ASEGURADORES DE CHILE A.G.

Revisión etapa 3

20 de Febrero 2025

Overview etapa 3

GT Infraestructura

- En el Entregable 3 se profundizó en la discusión para evaluar la creación de una **CA raíz para el SFA**, acordando un **esquema provisional** para certificados SSL ante la ausencia de una CA raíz
- Se introdujo la discusión sobre permitir **múltiples registros** de marcas bajo una misma IPI
- Se abre la conversación sobre el uso del SSA firmado por el **Directorio versus auto-firmado** por los PSBI en la inscripción mediante el DCR
- Se agregaron propuestas para definir los **límites de TPS/TPM** y el método de cálculo de disponibilidad (uptime), aspectos que estaban pendientes en el Entregable 2

GT APIs

- Se discutieron dos modelos de consentimiento para personas jurídicas: uso de **API de consentimiento o RAR +** Grant Management. No se llegó a consenso, pero se identificó la necesidad de alinear con FAPI
- Se especificaron los contenidos de los **planes de pruebas** (unitarias, integración, end-to-end) y se planteó un cronograma preliminar para la marcha blanca
- Se plantean que las **mantenciones programadas** sean comunicadas al regulador y las entidades puedan consultarlas. Estas mantenciones deberán ser **adhoc a la realidad de cada entidad**

GT Seguridad

- La AACH plantea una propuesta para los **mecanismos de comunicación**, definiendo los siguientes acuerdos:
- Se establece el **mTLS** como el mecanismo principal de comunicación entre servidores (autorización,recursos y DCR)
- Se acuerda, en consenso con los gremios, **no implementar DPoP en las fases iniciales** del SFA, debido a que los casos de uso abordados en estas etapas no justifican su aplicación
- No obstante, se deja abierta la posibilidad de integrar **DPoP** en futuras evoluciones del SFA, considerando su potencial utilidad para escenarios más complejos que puedan surgir en etapas avanzadas del sistema

GT UX

- Se plantea que el uso de **logs** no garantizan por completo su validez legal para certificar la trazabilidad transaccional, pero sí contribuyen a fortalecer su uso como evidencia complementándolo con:
  - Adopción de FAPI 2.0 Message Signing
  - Firma Diaria de Logs con Timestamps
- Se avanza en definiciones sobre la **gestión de incidencias**
- Se plantea adherir a la propuesta de la CMF sobre el uso de un **representante legal** para las personas jurídicas en la toma de consentimiento, a excepción de casos de usos que sean más complejos o que lo requieran (Iniciación de pagos)

Asociación Gremial de Cajas de Compensación de Asignación Familiar - Cajas de Chile A.G.

Cajas de Chile

Jueves 20 de Febrero

Presentación Cierre Etapa 3

Foro Consultivo

Caja 18 · La Araucana más cerca · Los Héroes · Caja Los Andes

INFORMACIÓN RESERVADA Y CONFIDENCIAL

Toda información a la que se tenga acceso o se reciba en el contexto de la implementación del Sistema de Finanzas Abiertas está sujeta a la obligación de confidencialidad contenida en la Declaración de Confidencialidad del Foro de SFA firmada por todos los participantes. En consecuencia, dicha información no debe divulgarse, reproducirse ni utilizarse para fines distintos al proceso de implementación antes mencionado, salvo autorización expresa de la Secretaría Técnica o del titular de la información.

Temario

1. Mirada Temas de posición GT UX
2. Temas de posición GT Infraestructura
3. Temas de posición GT APIs
4. Temas de posición GT Seguridad

Tema de Posición GT UX

Flujo de consentimiento PJ

- **No adherimos y cambiamos la posición**

La idea general está bien, pero se debe mejorar los siguientes detalles:

- Cuando el segundo factor pueda entregar información adicional, es mejor que se muestre al final, de modo que incluya la información de tipos de datos, plazo y finalidad. Cuando el segundo factor sean sólo un código, como ocurre con las coordenadas de tarjetas, nos parece bien que se pida al hacer login.

Gestión de reclamos

El EdS plantea procedimientos para la gestión de reclamos de un usuario final y entre participantes.

- **Adherimos.**

Fortalecimiento de medios de prueba

El EdS plantea procedimientos para el fortalecimiento de medios de prueba.

- **Adherimos.**

Tema de Posición GT Infraestructura

Certificados

- **Adherimos.**

Múltiples registros

- **No adherimos y tenemos una posición nueva:**

La propuesta del EdS obliga al PSBI a pasar por el Directorio para obtener un SSA antes de cada DCR en cada IPI. Esto complica las cosas porque:

- El Servidor de Autorización validará la posesión de la clave privada del PSBI en forma indirecta: Asume que si puede obtener un SSA, entonces está en posesión de la clave privada.
- Para evitar la repetición de SSA se debe incluir un identificador de la IPI en el SSA. Esto se puede hacer, pero muestra que hay escenarios de ataque que se introducen con el modelo y se abre la puerta a cometer errores en un escenario desconocido y no evaluado.
- No se indican los criterios que usará la CMF para otorgar o negar los SSA y por lo tanto, no se puede evaluar si el modelo puede ser más seguro y más simple.

Nuestra propuesta es usar TLS con certificado en ambas puntas según lo indicado en TLS 1.3, sección 4.3.2: Request Certificate, para que sólo los PSBI autorizados puedan iniciar un DCR en los servidores de autorización. Así no se asigna carga al Directorio, se cierra el Sistema y es liviano de implementar.

Si se quiere definir algún criterio para limitar la cantidad de aplicaciones cliente que los PSBI podrán inscribir en un período de tiempo, lo más simple es definir la regla sin agregar carga funcional al Directorio.

Disponibilidad

- **Adherimos**

Tema de Posición GT API’s

Gestión del consentimiento

- **Adherimos.**

Marca blanca

- **Adherimos.**

Plan de pruebas

- **Adherimos.**

Mantenciones programadas

- **Adherimos.**

Tema de Posición GT Seguridad

Seguridad para el Directorio

- **No adherimos y tenemos una nueva posición**

Para consultar datos de descubrimiento como Participantes, certificados o finalidades, lo más parecido entre los estándares usados en FAPI 2.0 es OpenID Connect Discovery (OIDD). Es un estándar muy simple, que hace una petición GET y recibe una respuesta JSON, con una comunicación protegida usando TLS. No exige que TLS utilice certificado en ambas puntas, pero tampoco lo prohíbe y nuestra recomendación es seguir ese modelo para las consultas al Directorio. Es decir, TLS con certificado en ambas puntas y una petición GET diseñada de modo que se vea parecida a OIDD.

Nota: TLS con certificado en ambas puntas corresponde formalmente a RFC 8446 punto 4.3.2 (TLS 1.3 Certificate Request). Lamentablemente, es normal referirse a esto usando la expresión “mutual TLS” o abreviarlo como mTLS. A pesar de que mutual TLS es un término comúnmente usado para esto, puede inducir a confusión porque hay 2 estándares que llevan en el nombre las palabras “mutual” y “TLS”, (RFC 8120 y 8708), pero ninguno de los 2 corresponde a lo que se quiere al decir TLS 1.3 con certificado en ambas puntas o formalmente TLS 1.3 Certificate Request.

mTLS vs DPoP

- **No adherimos y cambiamos nuestra posición**

En general estamos de acuerdo, pero creemos incorrecto exigir mTLS de RFC 8705 a todas las comunicaciones entre el PSBI y la API. Lo correcto es partir de TLS 1.3 with Client Request (de RFC 8446). La diferencia con mTLS es que este último agrega un client_id en todas las peticiones y esto no tiene sentido para muchos casos, por ejemplo al usar OIDD lo normal es usar TLS con certificado en el servidor y si se desea seguridad adicional, que es nuestra recomendación, se puede exigir también un certificado al lado cliente, pero agregar un client_id a todas las peticiones muchas veces estará fuera de contexto y cuando sea exigido, como ocurre con los flujos del consentimiento, habrá una referencia a un estándar que así lo imponga.

Cajas de Chile

COMISIÓN
PARA EL MERCADO
FINANCIERO

Asociación Gremial de Empresas de Innovación Financiera de Chile A.G. (FinteChile)

Resultados Temario Etapa 3

FinteChile

Febrero 2025

www.fintechile.org

FinteChile

Índice

- **Posiciones Presentadas** Página **1...6**
- GT Infraestructura Página **3**
- GT Medios Página **4**
- GT Seguridad Página **5**
- GT UX Página **6**

GT Infraestructura

Posiciones que difieren del entregable

Posición	Argumento
2	Es más simple y a la vez más seguro que el **SSA** sea firmado por los **PSBIs** y el directorio se limite únicamente a almacenar los certificados que usa el **PSBI** para firmar (de manera que las **IPIs** puedan validar la firma). Si el **SSA** es firmado por directorio, ya no funciona para autenticar el PSBI en el flujo de **DCR**, dado que el PSBI ya no controla la llave privada con la que se firmó el SSA.

FinteChile

Votación de Posiciones

1 **Certificados:**
Adhiero

2 **Múltiples registros:**
No adherimos y tenemos una posición nueva

3 **Disponibilidad:**
Adhiero

GT Medios

Posiciones que difieren del entregable

Posición	Argumento
4	Durante las sesiones con los gremios de esta etapa, se levantó que las mantenciones programadas no coinciden con las mantenciones que la **CMF** permite para las **TEFs**. También se discutió sobre distinguir entre mantenciones exclusivas de las **APIs** versus mantenciones de los sistemas de **TEF**. Consideramos que este punto necesita de mayor claridad y ser discutido en etapas futuras nuevamente.

FinteChile

Votación de Posiciones

1. **Gestión del consentimiento:**
   Adherimos
2. **Marcha Blanca**
   Adherimos
3. **Plan de pruebas APIs:**
   Adherimos
4. **Mantenciones programadas:**
   No adherimos y mantenemos nuestra posición presentada en los GTs

GT Seguridad

Posiciones que difieren del entregable

- No tenemos posiciones que difieran de lo presentado en el entregable de esta etapa.

Votación de Posiciones

1. **FAPI 2.0 para Directorio:**
   Adherimos

2. **mTLS/private key/DPoP:**
   Adherimos

GT UX

Posiciones que difieren del entregable

Posición	Argumento
1	Para este punto si bien, estamos de acuerdo con la posición presentada nos parece importante hacer las siguientes observaciones: • Es necesario precisar que ***todas las fotos de GUI del flujo de consentimiento para persona jurídica, en el PSBI son referenciales y no normativas***, ya que el PSBI puede implementar GUIs con más libertad • En la IPI se está colocando el 2FA en el login, lo cual sólo es bueno cuando el 2FA no puede entregar información de contexto como: el alcance, plazo o finalidad de la autorización que se está solicitando. Además, no es coherente con el viaje del usuario que se buscará lograr con CIBA. **Nuestra propuesta es que en los casos en que el 2FA no pueda entrar información de contexto sobre el consentimiento, entonces se use al entrar como se muestra en la propuesta del EdS. En los otros casos, creemos mejor usar el 2FA una sola vez y usando la información de contexto.**

FinteChile

Votación de Posiciones

1 **Flujo de consentimiento PJ:**
No adherimos y tenemos una nueva posición

2 **Ajuste gestión de reclamos:**
Adherimos

3 **Fortalecimiento medios de prueba jurídicos:**
Adherimos

Asociación de Bancos e Instituciones Financieras de Chile A.G (ABIF)

Grupo Consultivo SFA

Entrega Etapa 3

20 de enero de 2025

banca
asociación de bancos

Agenda

1. Calendario Anexo N°3
2. Entregable Etapa 3
   i. API
   ii. Experiencia de Usuario
   iii. Infraestructura
   iv. Seguridad
3. Definiciones faltantes para la adecuada implementación del SFA

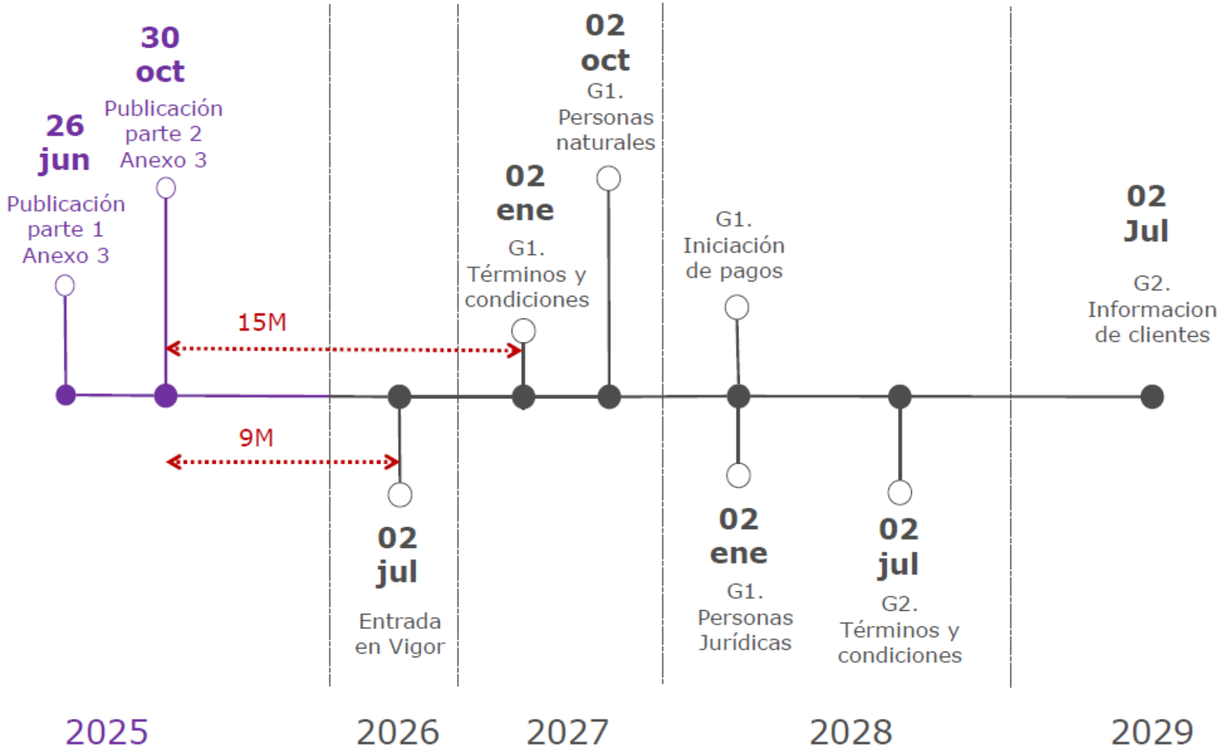
Agenda

1. **Calendario Anexo N°3**
2. Entregable Etapa 3
   i. API
   ii. Experiencia de Usuario
   iii. Infraestructura
   iv. Seguridad
3. Definiciones faltantes para la adecuada implementación del SFA

Información recibida el 17 de febrero 2025
Revisión de Grupo Consultivo de 20 de febrero 2025

banca
asociación de bancos

CALENDARIO DE IMPLEMENTACIÓN



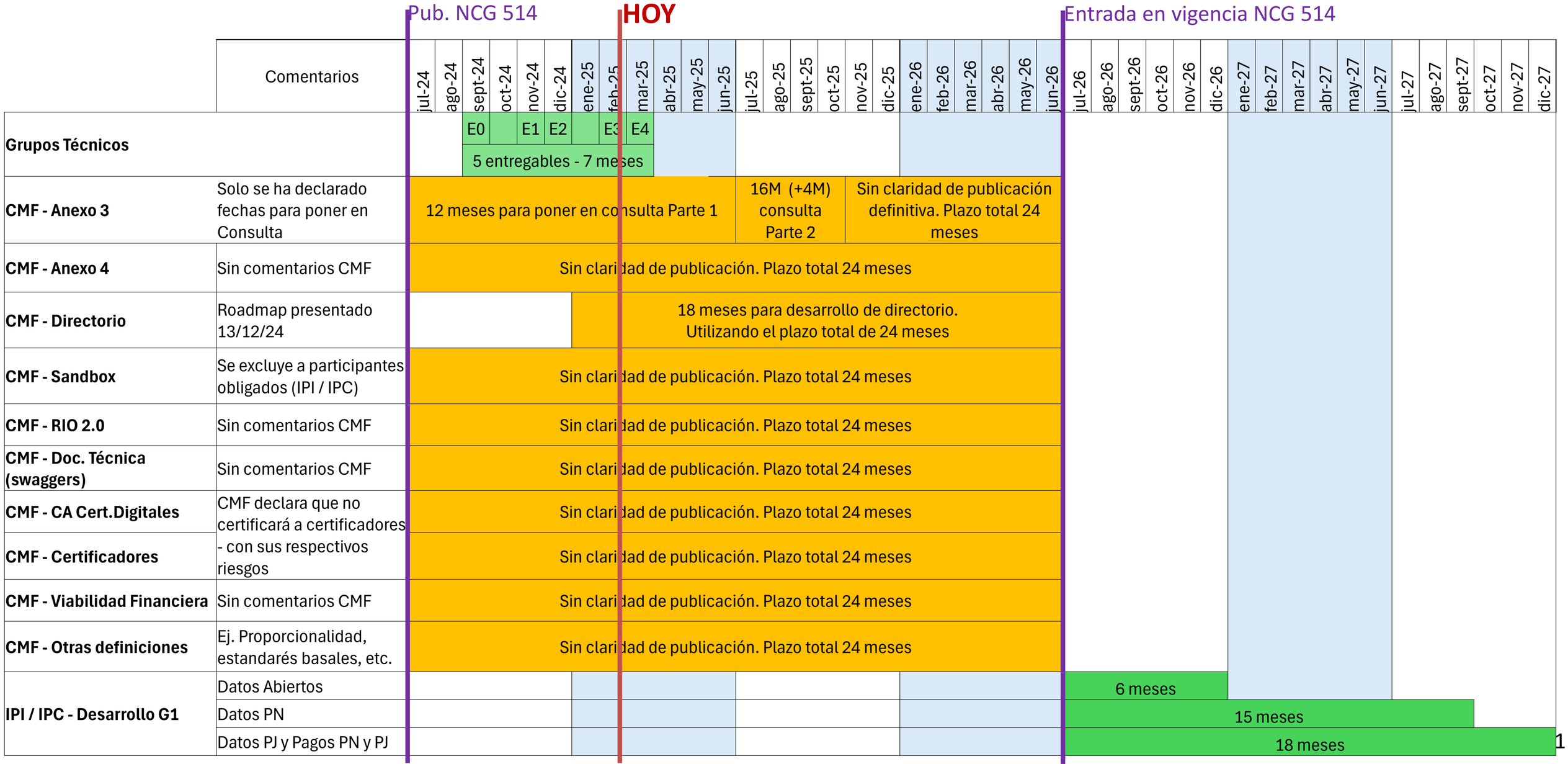
La publicación de la segunda parte y final de temas del Anexo N°3 se haría **9 meses** antes de la **entrada en vigor de la norma del SFA** y **15 meses** antes del **primer hito de implementación** sobre información de términos y condiciones generales.

Análisis General de Plazos

- **Grupos Técnicos**
  - → **7 MESES** para entregar TODO el input técnico
- **IPI / IPC**
  - → **18 MESES** para que desarrollar TODO el SFA (grupo 1)
- **CMF**
  - → **16 MESES** para poner en consulta el Anexo 3
  - → **24 MESES** ¿para cerrar esa consulta?
  - → **24 MESES** para desarrollar Directorio (6 para partir + 18 de desarrollo)
  - → **24 MESES** para desarrollar Sandbox incompleto (excluyendo participantes obligados IPI / IPC)
  - → **Sin fechas para:** RIO 2.0, documentación técnica (swaggers), definiciones de finalidad y proporcionalidad, selección de producto, viabilidad financiera de pagos, etc.
  - → **Se resta de su rol supervisor,** al no certificar a los certificadores (certificaciones obligadas en la NCG 514), dejando responsabilidad a IPI/IPC/PSBI/PSIP

- No parece correcto que los GT's entreguen **TODO el input técnico en 7 meses** y la **CMF demore MÁS DEL DOBLE** del tiempo en pasarlo a texto en el Anexo 3
- No parece correcto que los IPI/IPC tengan que **desarrollar TODO el SFA en 18 Meses** y la CMF demore **24 Meses en desarrollar el Directorio y un Sandbox incompleto** (aparte de otros elementos sin visibilidad)
- No parece correcto que los **participantes se tengan que hacer responsables por un rol que es de la CMF**

Análisis General de Plazos



Solicitud para la adecuada implementación del SFA

En base a lo anterior se solicita a la CMF:

1. **Norma en Consulta** a más tardar en Abril 2025 para Datos y Mayo 2025 para Pagos

2. Publicación de **Norma Definitiva**, con Anexo 3 y 4 en Junio 2025

3. En **Junio 2025** contar con:
    1. **Directorio** en versión 1 productiva
    2. **Sandbox** en versión 1 para IPI / IPC (sujetos obligados)
    3. **CA** – Certificados Digitales
    4. ***Swaggers*** en versión 1
    5. **Certificadores aprobados** por la CMF

4. En Marzo 2025 contar con **Definiciones Base** para que participantes puedan comenzar con el trabajo (laminas a continuación)

Definiciones Base – Experiencia de Usuario (1/2)

a. Datos:

i. Consentimiento:

1. ¿Finalidades van a estar definidas?
2. ¿Va a existir correlación *exante* proporcionalidad entre tipo de datos a solicitar y finalidad?
3. ¿Va a existir correlación con el plazo?

ii. Flujo

1. Confirmar que cliente pueda seleccionar detalle de cuentas a compartir en IPI
2. PJ: Confirmar empresa debe definir en IPI los apoderados habilitados y que pueda haber información de no divulgación

b. Pagos:

i. Confirmar flujo redirect (postergando flujos desatachados)

ii. Confirmar alcance Etapa 1 (hasta enero 2028) solo enfocarnos en pagos inmediatos, uno a uno, en pesos, basados en TEF, para PN y PJ.

iii. Confirmar que cliente seleccionará cuenta de origen de fondos en IPC

Definiciones Base – Experiencia de Usuario (2/2)

c. Transversal:

i. Confirmar postergación de Finanzas Embebidas

ii. Tratamiento casos especiales:

1. Confirmar exclusión de casos como menores de edad, fallecimiento, etc.
2. Dejar a criterio de IPI manejo de cuentas PEP, cuentas tutelares, bipersonales, etc.

iii. Confirmar estándares de consultas y reclamos para la marcha blanca

iv. Confirmar que pauta WCAG será opcional

Definiciones Base – Seguridad

a. Autenticación FAPI:

i. Confirmar mTLS (se excluye DPoP)

ii. Confirmar mTLS (se excluye *private key* JWT)

iii. Definiciones de comunicaciones con el directorio (ej. mTLS RFC 8705 para información sensible y mTLS tradicional para comunicación de mensajería)

b. Otras definiciones:

i. Tipos de Grants

ii. Definición de Security Profile de FAPI 2.0 (ej. TLS 1.3)

iii. Confirmar criptografía y estructura de Logs

iv. Certificado de seguridad, confirmar *Self Assessment* por OIDF

Definiciones Base – Infraestructura

a. Dimensionar infraestructura:

a. TPS y TPM iniciales

b. Confirmar cualquier otro requisito no funcional útil para dimensionar infraestructura

b. Diseño de Marcas DCR:

i. Confirmar múltiples marcas IPI/IPC y PSBI/PSIP

ii. Confirmar SSA firmado por directorio + mTLS tradicional

c. Establecer condiciones de Certificados Digitales:

i. Estructura Certificadoras – Lineamientos de seguridad (¿CA raíz única?)

ii. Definir flujo de validación de firmas

iii. Rol del Directorio en el CSR

d. Otros:

i. Condiciones que debe cumplir empresas certificadoras

ii. ¿Va a ser necesario mecanismo alternativo obligatorio en una etapa inicial? Si la respuesta es sí, ¿Qué tipo y alcance tendrá?

Definiciones Base – Medio de Intercambio de Información (API´s)

a. Gestión del consentimiento:

a. ¿API de Consentimiento o RAR + G.Management?

b. Lineamientos generales API's:

a. Documentación técnica: Definir estructura de endpoints y payloads (Versión 0.0 de swaggers – son componentes que se actualizan constantemente, pero si aporte contar con un punto de partida) – incluir los del Directorio.

b. Establecer lineamientos de Paginación y Ordenamiento Endpoints

c. Establecer relación de finalidad con permisos y grupos de datos, a nivel de endpoints y grupos de permisos.

c. Otros:

a. ¿Qué se está pensando en prueba de calidad de datos?

b. ¿Se revisara la opción de tener un Sandbox para los participantes obligados IPI / IPC?

Definiciones Base – Otros

a. Sostenibilidad Financiera de Iniciación de pagos:

i. Indicar alternativas para que el proceso de pago sea viable

b. Plazos de implementación de:

i. Directorio

ii. Sandbox

iii. RIO 2.0

iv. Portal Desarrolladores, etc.

c. Versiones Anexo 4

Agenda

1. Calendario Anexo N°3
2. **Entregable Etapa 3**
   i. **API**
   ii. Experiencia de Usuario
   iii. Infraestructura
   iv. Seguridad
3. Definiciones faltantes para la adecuada implementación del SFA

Marcha Blanca pre y post producción – Propuesta Equipo de Soporte

banca
asociación de bancos

Marcha blanca

En términos de marcha blanca, se definen los siguientes lineamientos:

- Debe incluir aspectos de seguridad, los cuales no son sacrificables en marcha blanca.
- Es deseable que tenga flexibilidad en términos de requisitos no funcionales.
- Se deben medir TPS y TPM, para poder diagnosticar el uso del sistema.
- Existirán dos marchas blancas:
  - Marcha blanca de preproducción: Período de pruebas (3 meses)
  - Marcha blanca de producción: Período de observación (12 meses)

Comentarios ABIF:

- Marcha blanca preproducción
  - Escenarios a validar incompletos, sin correlación entre componentes y plazo
  - Plazo de 3 meses insuficiente – se debe contar con elementos como: doc. técnica de desarrollo (swaggers), Directorio, RIO 2.0, Sandbox, entre otros
- Marcha blanca postproducción:
  - Periodo de aprendizaje – experiencia internacional muestra que requisitos (ej. uptime) son no vinculantes por más de dos años
  - Se debe especificar todos los elementos sujetos a revisión de este periodo

Actor	Responsabilidad	Pruebas
PSBI	▪ Consultar al Directorio ▪ Descubrir IPIs Directorio ▪ Consultar correctamente los endpoints de TyCs y Canales de Atención ▪ DCR – Registro como cliente de una IPI ▪ Flujo de autorización de un usuario real (obtener Access token) ▪ Consultar endpoints de información de persona natural con Access token. ▪ Consultar endpoints de información para persona jurídica con Access token	▪ Autenticación y consulta del Directorio ▪ Consulta de endpoint de TyC ▪ Consulta de endpoint de Canales de atención ▪ Registro como cliente en una IPI ▪ Autorización con usuario real (obtención de Access token) ▪ Consultar endpoints de información de persona natural con Access token. ▪ Consultar endpoints de información para persona jurídica con Access token.
IPI	▪ Metadata de OpenID (.well-known) ▪ Endpoints de TyCs y Canales de Atención ▪ DCR – Registrar nuevos PSBIs como clientes ▪ Flujo de entrega de Access token (authorization server) ▪ Validación de Access token ▪ Exponer endpoints de información de persona natural (resource servers) ▪ Exponer endpoints de información de persona natural (resource servers)	▪ Endpoints de metadata (urls, contenido, y formato) ▪ Endpoints de TyCs (urls, contenido, y formato) ▪ Endpoints de Canales de Atención(urls, contenido, y formato) ▪ Registro de un PSBI como nuevo cliente ▪ Flujo de entrega de Access token a PSBI en nombre de un usuario real ▪ Validación de Access token emitido para consultar información ▪ Validar todos los endpoints de consumo de datos (urls, autenticación, contenido y formato) ▪ Validar todos los endpoints de consumo de datos (urls, autenticación, contenido y formato).
Directorio	▪ Endpoints de descubrimiento de IPIs ▪ Endpoints de validación de participantes (PSBIs) ▪ Autenticación en Directorio	▪ Consultar endpoints de descubrimiento ▪ Validar vigencia de un participante del SFA ▪ Autenticarse correctamente en el Directorio
Sandbox	▪ Exponer metadata de IPI de prueba ▪ Exponer datos de TyC de IPI dummy ▪ Exponer datos de canales de atención de IPI dummy ▪ Exponer endpoints de información de persona natural para IPI dummy ▪ Endpoints dummy con información de persona jurídica	▪ Endpoints de metadata (urls, contenido, y formato) ▪ Endpoints de TyCs (urls, contenido, y formato) ▪ Endpoints de Canales de Atención(urls, contenido, y formato) ▪ Validar todos los endpoints de consumo de datos (urls, autenticación, contenido y formato) ▪ Poder consultar datos de persona jurídica en el Directorio

Tabla 20: Marcha blanca

Marcha Blanca pre y post producción – Propuesta ABIF

banca
asociación de bancos

	jul-25	ago-25	sept-25	oct-25	nov-25	dic-25	ene-26	feb-26	mar-26	abr-26	may-26	jun-26	jul-26	ago-26	sept-26	oct-26	nov-26	dic-26	ene-27	feb-27	mar-27	abr-27	may-27	jun-27	jul-27	ago-27	sept-27	oct-27	nov-27	dic-27	ene-28	feb-28	mar-28	abr-28	may-28	jun-28	jul-28	ago-28	sept-28	oct-28	nov-28	dic-28	ene-29	feb-29	mar-29	abr-29	may-29	jun-29
Plazos SFA	**Entrada en vigencia**												**Banco y emisores de tarjetas (G1) - 18M**																																			
													T&C + C.atención - **PN y PJ - 6M**																																			
													Datos de clientes - **Personas Naturales - 15M**																																			
													Datos de clientes - **Personas Juridicas - 18M**																																			
													Iniciación Pagos - **Personas Naturales y Juridicas - 18M**																																			
													Grupo 2 - 36M																																			
													T&C + C.atención - **P.Nat y P.Jur - 24M**																																			
													Datos de clientes - **Personas Naturales y Juridicas - 36M**																																			
Marcha blanca preproducción (periodo de pruebas)	**Fase 1:** Probar endpoints del Directorio y Sandbox + vigencia de participantes + autenticarse en el Directorio + pruebas de mensajería + RIO 2.0 + *swaggers*													**Fase 2:** Probar endpoints de datos abiertos de los participantes + DCR (registro del PSBI en IPI)											**Fase 3:** endpoints de flujo de datos de PN + renovación de tokens, pruebas en IPI de validación reglas de campo, respuestas, payloads, etc.																																			
																										Fase 4: Endpoints generales de flujo de datos de PJ y flujo de pagos (PN y PJ)																																			
Marcha blanca productiva (periodo de observación)																											Datos PN	Definir claramente las mediciones y estándares que serán referenciales: TPS, TPM, uptime, % calidad de datos, % solicitudes exitosas en disponibilidad, proceso reclamos clientes e instituciones, tiempo de respuesta, mecanismo alternativo, umbrales de consulta, todas las otras métricas y herramientas que comiencen referenciales para ajustarlas posteriormente.																																			
																											Datos PJ Pagos PN/PJ																																			

Gestión del consentimiento – API de consentimiento vs RAR + Grant Management

banca
asociación de bancos

Propuesta del Equipo de Soporte → RAR + Grant management

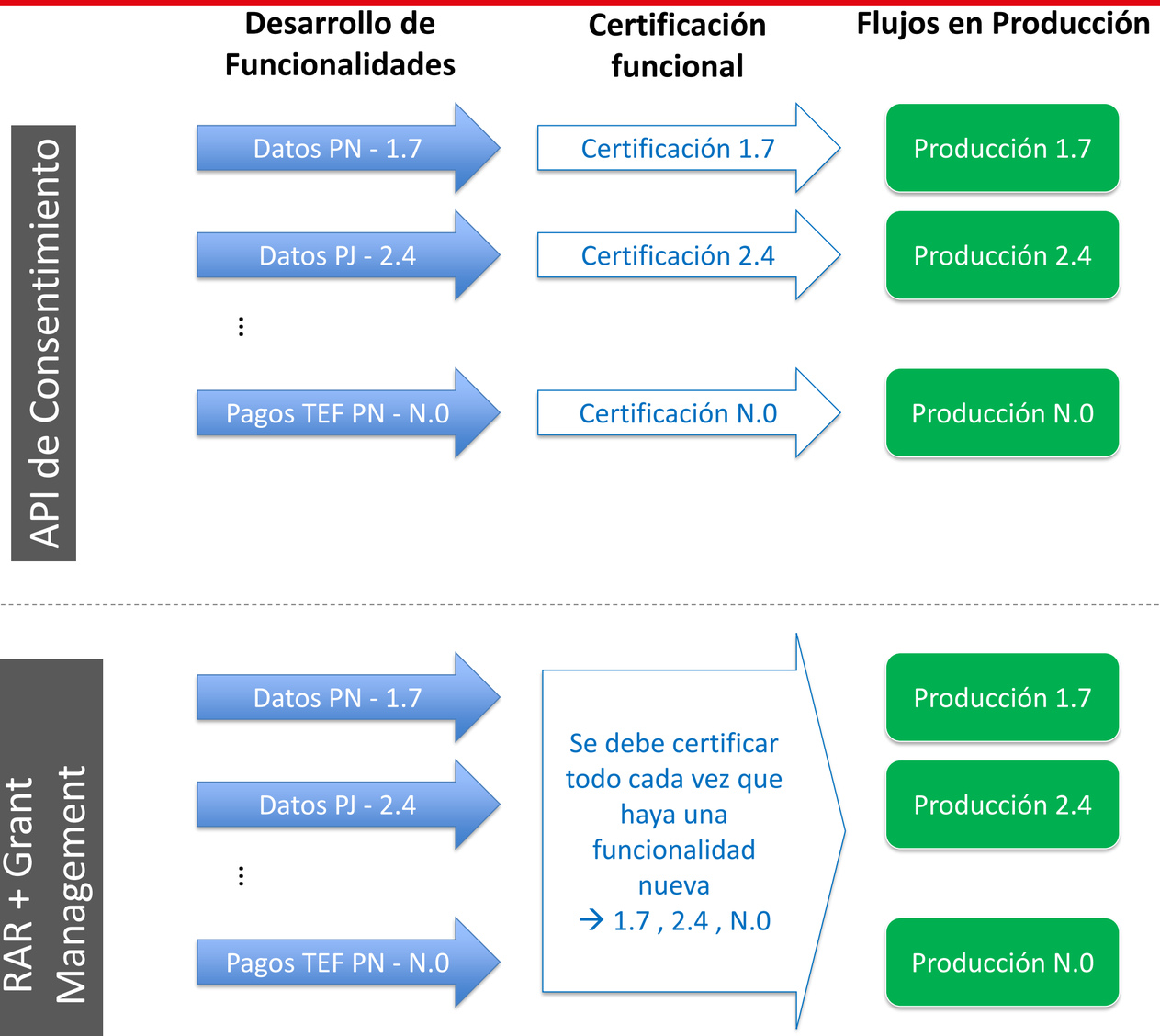
API de Consentimiento		RAR + Grant Management
API de consentimiento posee autenticación vía *Access token client credentials* y mTLS	**Nivel de Seguridad**	*Endpoint* PAR posee autenticación vía mTLS o private_key_JWT
Necesario desarrollar API de Consentimiento, crear un consentimiento vacío y relacionar el *consent_id* con los *refresh tokens* y *Access tokens.*	**Desarrollo y flujo técnico**	Flujo inicia en *endpoint* PAR, requiere *endpoints* para *grant management*. *Endpoint* PAR se vuelve más complejo dadas las nuevas validaciones implementadas
Se debe certificar solo las funcionalidades nuevas o actualizadas	**Certificación funcional**	**Riesgos de generación de bugs en funcionalidades previas**, ya que se ajustan piezas funcionales existentes cada vez que se actualiza o crea una nueva funcionalidad (generando recertificaciones)
Modelo utilizado en las principales geografías	**Experiencia comparada**	En una reunión con el OIDF, comentaron que aún no hay implementaciones significativas que utilicen RAR + Grant Management

Detalle

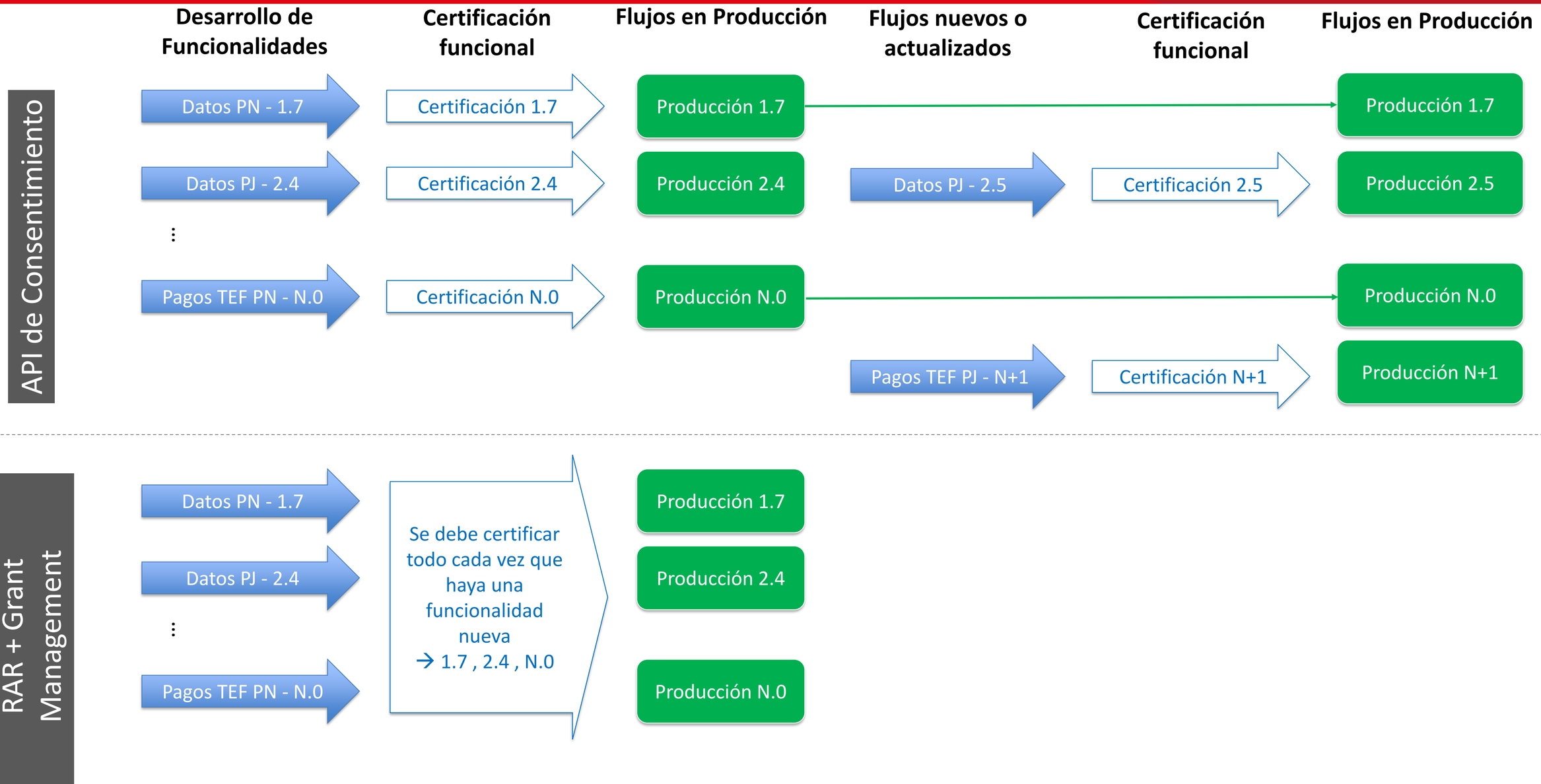
Notas: más ventajoso | menos ventajoso | equivalentes

ABIF: <u>Proponemos utilizar API de consentimiento</u>, porque es un modelo que no requiere certificar todos los componentes cada vez que se haga una actualización. Además de estar muy probado en las principales geografías

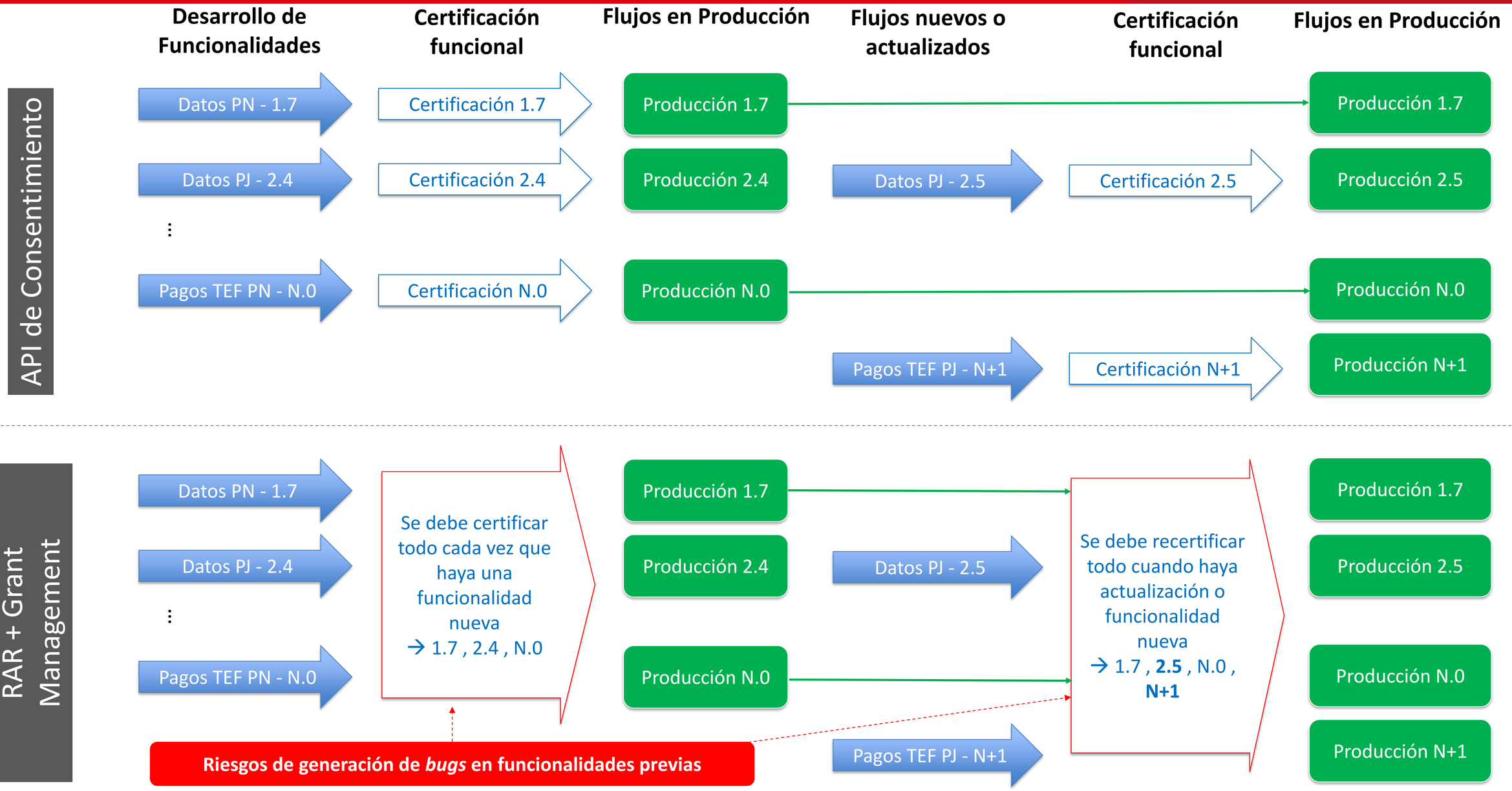
Gestión del consentimiento – Certificación funcional



Gestión del consentimiento – Certificación funcional



Gestión del consentimiento – Certificación funcional



Diagramas de Flujo – Modificación de grant sin necesitar autorización del usuario

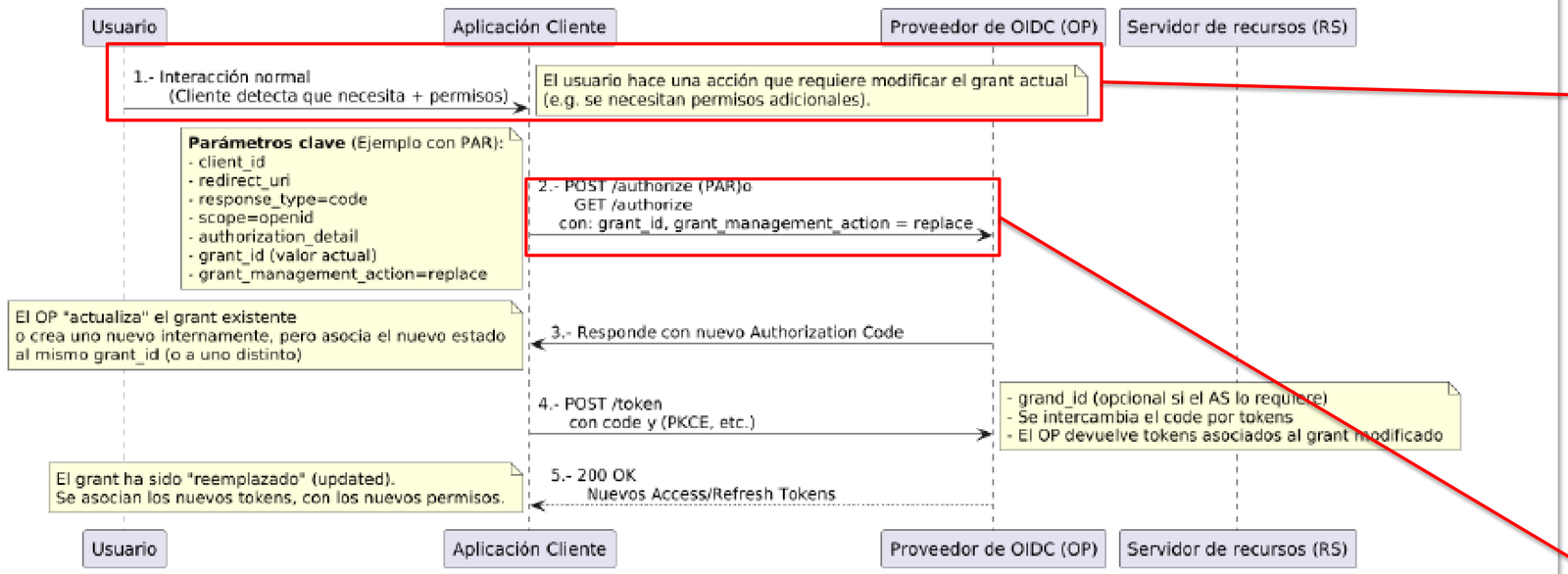


Figura 14: Modificación de grant sin necesitar autorización del usuario.

Comentarios ABIF:

Se debe permitir exclusivamente una actualización de un consentimiento si este cambio es de finalidad sin afectar a datos o plazos. **Necesitar permisos adicionales requiere intervención del usuario financiero.**

El uso del ***endpoint* PAR requiere la autorización del usuario financiero.** Para poder actualizar el consentimiento se requiere un **método PATCH** hacia el *endpoint* consents/{consentId}

Prueba de Calidad de Datos – Mencionado en Entregable Etapa 2 y Etapa 3

Propuesta UAI:
Granularidad por dimensiones DAMA

Dimensión	Descripción	Métrica
Exactitud (accuracy)	Que tan exactos son los datos en relación a otras instancias	% registros con errores % de error de los datos
Completitud (completeness)	Que tan completos son los registros en relación a otras instancias	% registros completos
Integridad (integrity)	Que tan correctas son las relaciones entre distintos datos y en el tiempo	% registros integros
Actualización (timelines)	Que tan actualizados están las APIs relativas a otras fuentes	% registros actualizados
Validez (validity)	Cumplimiento de los formatos acordados	% registros con formatos correctos
Duplicación (uniqueness)	Ausencia de registros duplicados	% registros no duplicados

Tabla 19: Matriz DAMA

Propuesta ABIF y Banco Estado:

Consistente con tener informes al inicio del SFA que sean **simples de implementar y a la vez ricos para la toma de decisiones**. Sin perjuicio que **post marcha blanca productiva** se puedan implementar mediciones más sofisticadas como DAMA

Informe de Calidad de Información (Ejemplo)

Tamaño de la muestra: **579 consentimientos únicos**

Numero de endpoints: 2

Total de llamadas: 1158

Prueba de Comparabilidad

API XYZ	Adecuado	Inadecuado	adecuado %
Total	**940**	**218**	*81%*
Endpoint 1	**162**	**48**	*77%*
Dato x	44	26	*63%*
Dato y	58	12	*83%*
Dato z	60	10	*86%*
Endpoint n	**42**	**6**	*87%*
Dato a	16	0	*100%*
Dato b	14	2	*87%*
Dato c	12	4	*75%*

Propuesta Inicial (Marcha Blanca)

Excelente: > 85%
Bueno: entre 70% y 85%
Regular: entre 60% y 70%
Aceptable: entre 50% y 60%
Insatisfactorio: < 50%

Agenda

1. Calendario Anexo N°3
2. **Entregable Etapa 3**
   i. API
   ii. Experiencia de Usuario
   iii. Infraestructura
   iv. Seguridad
3. Definiciones faltantes para la adecuada implementación del SFA

Flujo de Consentimiento P. Jurídicas – Imágenes de documento UAI: Entorno PSBI – PJ

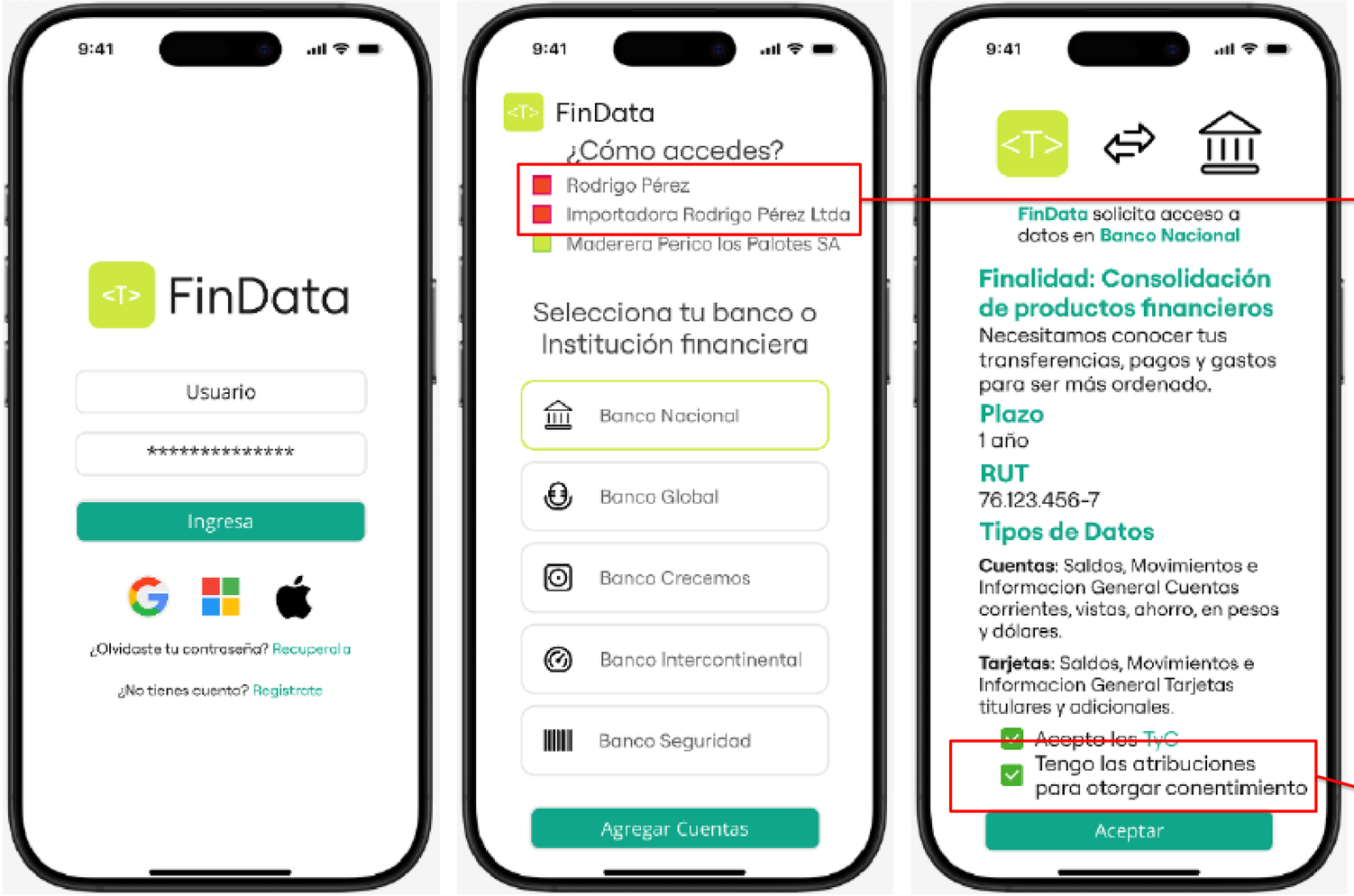


Figura 20: Mock Entorno PSBI Persona Jurídica

Checkbox cuadrados indican que un usuario podría seleccionar más de uno. Lo que no sería correcto para el flujo establecido

En el texto se indica que este *checkbox* es disuasivo. Sin embargo, no parece correcto agregar textos que no tendrá ningún efecto, ya que de todas formas la validación se realizará cuando el usuario vaya al IPI

Flujo de Consentimiento P. Jurídicas – Imágenes de documento UAI: Entorno IPI – PJ

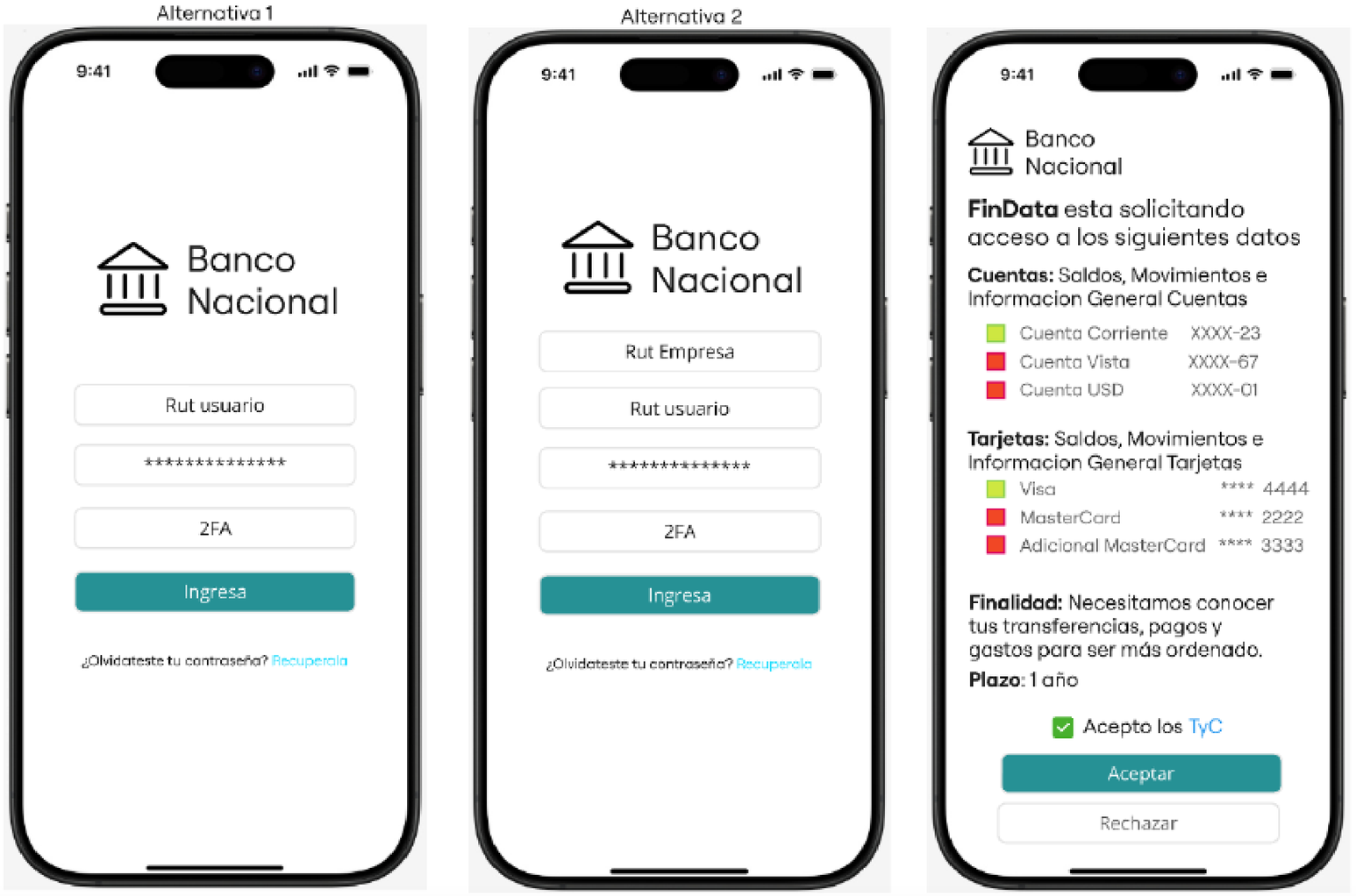


Figura 21: Mock Entorno IPI Persona Jurídica

Puntos positivos de propuesta:

- Maquetas referenciales, cada PSBI e IPI podrán modificarlas según su criterio, siguiendo los lineamientos de las secciones complementarias.
- Alternativa 1 y/o 2 va a depender de la forma de autenticar de cada IPI.

Flujo de Consentimiento P. Jurídicas – IPI son las responsables de verificar los poderes de las PJ

Puntos positivos de propuesta:

Sección Experiencia de Usuario – Consentimiento PJ (punto 7 – pág.110):

Cada IPI deberá tener sus verificaciones internas para los siguientes casos:

i. la verificación de que la PN efectivamente tenga las atribuciones para actuar como representante legal o apoderado de la PJ,

ii. empresas que declaren que no quieren operar en el SFA; y

iii. empresas que quieran definir cierta información como información sujeta a no divulgación.

Es responsabilidad de cada empresa informar a la IPI sobre estas situaciones.

Sección Experiencia de Usuario – Tablero de Control (pág.119):

Como un requerimiento específico para el caso de Personas Jurídicas, todos los representantes o apoderados con las atribuciones correspondientes, y en concordancia con la NCG N.º 514, deben tener acceso a revisar y gestionar los consentimientos otorgados para esa Persona Jurídica.

Gestión de Reclamos

Cliente → Institución

Institución → Institución

Ppta. Etapa 3 Marcha Blanca

Canales

Mantener plataformas actuales

SLA

10 días incidente interno (corridos si afecta viaje) + 5 días hab. coordinación entre instituciones

Canales

Correo entre instituciones con ID único SFA

SLA

10 días incidente interno (corridos si afecta viaje) + 5 días hab. coordinación entre instituciones

Nueva Propuesta

Marcha Blanca tiene la lógica expuesta en otras materias de contar con un proceso inicial simple.

Cliente final: automáticamente se regirá por los canales y SLA actuales de cada institución → NO es necesario normar.

Institución: Correo sin ID y SLA fijo de 15 días, pudiendo extenderse por razones de fuerza mayor.

Ppta. Etapa 3 Post Marcha Blanca

Mantener plataformas actuales

10 días incidente interno (corridos si afecta viaje) + Matriz SLA's coordinación entre instituciones (4hrs a 7 días)

Correo entre instituciones con ID único SFA

10 días incidente interno (corridos si afecta viaje) + Matriz SLA's coordinación entre instituciones (4hrs a 7 días)

Nueva Propuesta

La marcha blanca es el periodo de aprendizaje, para normar de mejor manera.

Dado esto, los estándares se podrán ajustar una vez finalizada la marcha blanca productiva

Casos especiales

Propuesta Positiva:

Sin Acceso al SFA

- Menores de 18 años
- Casos de fallecimiento

Casos Excepcionales

- PEP: IPI es responsable de tomar los resguardos
- Cuentas bipersonales y Sucesiones: Reglas quedan a cargo de la IPI
- Personas sujetas a limitaciones: Dependerá del permiso del representante
  (Especificar que es responsabilidad de la IPI validar los permisos)
- Apoderados: Propuesta que en la IPI se pueda seleccionar en nombre de quién va actuar

Finalidad y Proporcionalidad – Mencionado en Entregable Etapa 2 y Etapa 3, sin definición

Ley Fintech - N°21.521 (Art. 23):

Los **Proveedores de Servicios basados en Información** y los **Proveedores de Servicio de Iniciación de pago**, en su caso, deberán adoptar mecanismos de autentificación del Cliente y **obtener su consentimiento previo y explícito**…

…**consentimiento del cliente** deberá manifestarse en forma libre, informada, expresa y **específica en cuanto al tipo de información financiera, la finalidad y el periodo máximo de validez**…

Ley Datos Personales - N°21.719 (modifica N°19.628, Art. 3°):

c) **Principio de proporcionalidad.** Los **datos personales** que se traten **deben limitarse estrictamente a aquéllos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento**…

Consentimientos expresos, con finalidad específica y proporcionalidad en datos según finalidad

Establecer Proporcionalidad *ex ante*

Reglas claras potencian la adopción del SFA, la innovación y los nuevos servicios, ya que dan certezas a las Personas, Reguladores y Participantes

Establecer Proporcionalidad *ex post*

Incertidumbre produce desconfianza en el SFA (ej. Australia), disminuyendo la adopción por parte de las Personas y la innovación por parte de los Participantes. Afectando la materialización de los potenciales beneficios

Detalle

Selección de Productos – Mencionado en Entregable Etapa 2 y Etapa 3, sin definición

Selección de Productos
Definición pendiente CMF sobre entorno de selección de productos

- Definición pendiente CMF
- Definición habilitante para establecer flujos

Figura 21: Mock Entorno IPI

UAI consultó a CMF acerca de si esa selección de **detalle de producto era posible de acuerdo a su interpretación de la Ley**.

En caso de no serlo, la experiencia de cliente para autorizar compartir datos **se vería mermada,** lo que **afectaría la adopción del SFA.**

Cabe mencionar que en **Brasil, UK y Australia si se permite esa selección de detalle de producto**, como se expone en el mock

Agenda

1. Calendario Anexo N°3
2. **Entregable Etapa 3**
   i. API
   ii. Experiencia de Usuario
   iii. Infraestructura
   iv. Seguridad
3. Definiciones faltantes para la adecuada implementación del SFA

Certificados

Autoridades Certificadoras

- Esquema de 2 tiers: CAs intermedios y CAs raíz
- Sin CA raíz única del SFA.
- Estándares y complementos de acuerdo con el cambio de definición de CA

Comentarios Rol CMF:

- Existencia de CA's raíz y CA's intermedias para la validación de certificados, supone un rol relevante de CMF al asegurar que estas CAs están dentro de los estándares exigidos por el ecosistema.
- No contar con una CA raíz única (o listado acotado), conlleva que la CMF deberá garantizar la uniformidad de los estándares de certificados para aceptarlos como validos en el SFA.

→ Es necesario que la CMF revise su posición de no tomar este rol supervisor, ya que conllevaría riesgos operacionales y de seguridad para el funcionamiento del SFA

Comentarios Directorio:

- Cumplir rol de exponer claves y certificados siguiendo el RFC 7517 – JSON web key.
- Garantizar que los certificados sean emitidos siguiendo los estándares establecidos para el SFA.
- Validar de forma periódica (al menos diariamente) el estado de certificados (en caso de que se encuentren revocados o caducados).
- Capacidad de bloquear los certificados o certificadoras por motivos de seguridad del ecosistema.

Múltiples registros

Diseño Marcas DCR

Múltiples marcas IPI/IPC y PSBI/PSIP

Autenticación DCR

- Autenticación vía SSA
  (propuesta ABIF vía mTLS)
- Opción SSA firmado por directorio
- Un *client* por SSA

Elementos positivos:

- Permitir múltiples registros (SSA para PSBI/PSIP o AS para IPI/IPC) bajo una institución del SFA (cmf_id);
- Que exista un Software Statement Asertion (SSA) diferente para cada cliente registrado en la IPI/IPC.

Comentarios Autenticación vía SSA:

- SSA firmado por el Directorio **no es suficiente a nivel de seguridad**, ya que solo se valida la relación de la marca inscrita con el participante.
- Para que Autorization Server valide que participante está correctamente inscrito en el Directorio, es necesario establecer un mTLS tradicional (en capa de transporte, o TLS en las “dos puntas), como **método de seguridad complementario para este proceso**
- Mecanismo de seguridad utilizado en Brasil y UK

Monitoreo disponibilidad

Monitoreo Disponibilidad

- Monitoreo de cada institución
- Reporte con estructura simple
- Falta determinar códigos de respuesta considerados y actuación en mal uso

Elementos positivos:

- Separación conceptual de monitoreo y reporte
- Dejar a criterio de cada institución el tipo de monitoreo a realizar, así como la unidad de medida que reportarán normativamente (milisegundo, segundo, minuto, etc). Esto resulta de suma importancia, debido a las diversas realidades e implementaciones con que cuenta cada IPI / IPC

Comentarios Reportes:

- **Contexto:** Códigos de respuesta HTTP 429 y 529, son los relacionados con bloqueos por TPS y TPM. Códigos 4xx son respuestas asociadas a solicitudes mal ejecutadas por la PSBI.
- **“Reporte mensual IPI” y “Cross check PSBI”:** En la propuesta, las llamadas exitosas excluyen las 4xx, 429 y 529. Sin embargo, se deben incluir ya son códigos de respuesta responsabilidad del PSBI. Al excluirlas se afectará el % de disponibilidad de la IPI.
- **“Momentos de indisponibilidad”:** En la propuesta, se excluyen todos los códigos de respuesta 5xx. Sin embargo, el código 529 que se utiliza como límite de infraestructura y no debe ser detectado como indisponible del IPI/IPC.
- **Adicionar monitoreos y reporte de disponibilidad a PSBI y Directorio:** Al ser un sistema interoperable, para velar por la experiencia del cliente y el ecosistema completo, es necesario contar con elementos consistentes de disponibilidad para todos componentes del SFA.

Mal uso de infraestructura

Sin mención en Entregable 3

Comentarios ABIF

En caso de situaciones donde algunos PSBI hagan mal uso del SFA. Ejemplo: múltiples llamados de códigos 4xx, generando una carga innecesaria en el sistema.

→ **IPI / IPC debe proteger su infraestructura con los TPS y TPM**; y en el extremo podría denegar la conexión a ese participante.

→ **Consecuencia: se afectaría a las Personas, la Reputación del SFA** y a las PSBI que si estén haciendo buen uso del SFA

En necesario agregar en el Anexo 3 el Marco de Actuación para este tipo de situaciones, incluyendo la denegación a estos participantes

Agenda

1. Calendario Anexo N°3
2. **Entregable Etapa 3**
   i. API
   ii. Experiencia de Usuario
   iii. Infraestructura
   iv. Seguridad
3. Definiciones faltantes para la adecuada implementación del SFA

Fortalecimiento Medios de Pruebas Jurídicos

Equipo de soporte propone dos medidas obligatorias:

- FAPI 2.0 Message Signing ayuda a garantizar el no repudio mediante el uso de firmas digitales en las transacciones. Esto asegura que las transacciones no puedan ser negadas por las partes involucradas.
- Firma diaria de los logs con estampas de tiempo.

Comentarios ABIF

Si bien se adhiere a la propuesta del EdS, es una **condición necesaria que la CMF establezca en la NCG 514**, que las definiciones y/o estándares que se determinen en el Anexo N°3, son **elementos suficientes para establecer los respaldos, con validez jurídica**, de que se efectuaron los flujos de consentimiento, de intercambio de información o iniciación de pagos entre los participantes del SFA

Firma diaria de los logs tiene **complejidades técnicas las cuales no tienen sentido implementar, si es que no se confirma el punto anterior.**

Agenda

1. Calendario Anexo N°3
2. Entregable Etapa 3
   i. API
   ii. Experiencia de Usuario
   iii. Infraestructura
   iv. Seguridad
3. **Definiciones faltantes para la adecuada implementación del SFA**

Definiciones faltantes para la adecuada implementación del SFA

- **Implementación –** *ST-CMF el plazo de 18 meses para el desarrollo completo del SFA es altamente exigente. Es fundamental contar con estos plazos para planificar.*

  1. Directorio: En *roadmap* de Reunión 13/12/24, se establece “Pruebas Integrales con Instituciones” en Q1/26. Se indicó posibilidad de adelantar a Q1/25 → **ST-CMF favor confirmar**
  2. Sandbox, RIO 2.0, Portal de Desarrolladores, etc. → **ST-CMF favor establecer plazos y especificaciones aún faltantes**
  3. Anexo 3 → **Es importante tener definiciones basales a marzo 2025**
  4. Anexo 4: Umbrales y soluciones técnicas para cumplir con lo definido en la norma → **ST-CMF favor dar visibilidad de la versión 1 de este documento**

- **Seguridad de los datos –** *Mitigar el riesgo de mal uso de la información es clave, sin confianza en este punto, se límita el alcance del SFA*

  1. Finalidad, relación finalidad/datos proporcionales y especifica → **ST-CMF ¿Cuándo se tendrán definiciones?**
  2. Selección de productos: Consulta realizada a la CMF → **ST-CMF ¿Cuándo se tendrá respuesta?**

Definiciones faltantes para la adecuada implementación del SFA

- **Sostenibilidad financiera –** *Costos elevados puede limitar el alcance y materialización de los potenciales beneficios del SFA (competencia e inclusión financiera), remuneración de infraestructura de pagos está pendiente*

  1. Gradualidad en la implementación: Enfocarse en casos de usos más relevantes y contar con requisitos tecnológicos no vinculantes en una primera instancia → **ST-CMF ¿Existirá alguna definición?**
  2. Viabilidad financiera iniciación de pagos → **ST-CMF ¿Existirá alguna definición para hacer viable la iniciación de pagos?**

- **Rol CMF** – *Institución con un importante rol en la implementación del SFA*

  1. Servicios centralizados: Se exige en la NCG 514 contar con diversas certificaciones, pero CMF indica que ellos no supervisarán a los certificadores, lo que implica riesgos operacionales y de seguridad → **ST-CMF ¿Mantendrán esa definición?**
  2. Sandbox: Sistema interoperable, pero se excluye entorno de pruebas de los participantes obligados (IPI / IPC) → **ST-CMF ¿Mantendrán esta definición?**

Grupo Consultivo SFA

Entrega Etapa 3

20 de enero de 2025

banca
asociación de bancos

COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Sesión 24
Foro del Sistema de Finanzas Abiertas (FSFA)

Comisión para el Mercado Financiero
Febrero 2025