COMISIÓN PARA EL MERCADO FINANCIERO

FINTEC
Sistema de Finanzas Abiertas

Mesa Consultiva 2: Estándares técnicos del SFA

Ciberseguridad y Autenticación

Diciembre 2023

Agenda

1. Principios generales establecidos en la Ley
2. Propuesta de estándares para discutir en la mesa
3. Propuesta de modelo de provisión de servicios
4. Preguntas para la mesa

Anexo: Modelos y flujos para compartir información

1. Principios generales establecidos en la Ley

Principios generales según la Ley

A. Consentimiento y autenticación del cliente (art 23)

- Los **PSBI** y los PSIP, en su caso, deberán adoptar mecanismos de **autentificación** del Cliente y obtener su **consentimiento** previo y explícito para realizar consultas de información o iniciar pagos en su nombre a través del Sistema de Finanzas Abiertas, según corresponda, a través de medios o canales electrónicos o digitales expeditos y seguros.
- Las **IPI** e IPC, en su caso, deberán **adoptar mecanismos** para la **autenticación de los Clientes** que hubieren dado su consentimiento a los PSBI o los PSIP, según sea el caso.
- Los mecanismos de autenticación y confirmación de Clientes antes referidos deberán ajustarse a los **estándares mínimos** que defina la Comisión por norma de carácter general. Estos métodos podrán considerar reglas diferenciadas, incluyendo mecanismos de autenticación reforzada, considerando entre otros el riesgo, el tipo de datos o de servicios involucrados.
- Los mecanismos de autenticación de Clientes para estos efectos deberán **ser compatibles** con los métodos ya disponibles en las IPI e IPC para el acceso a sus canales electrónicos.

B. Identificación del proveedor de servicios basados en información o de iniciación de pagos (art 23)

- Las **IPI** deberán implementar mecanismos para la **autenticación de los PSBI** y **PSIP**, a fin de verificar que se encuentren inscritas en los Registros (Directorio) que lleva la Comisión, conforme a los estándares que ésta defina por NCG.

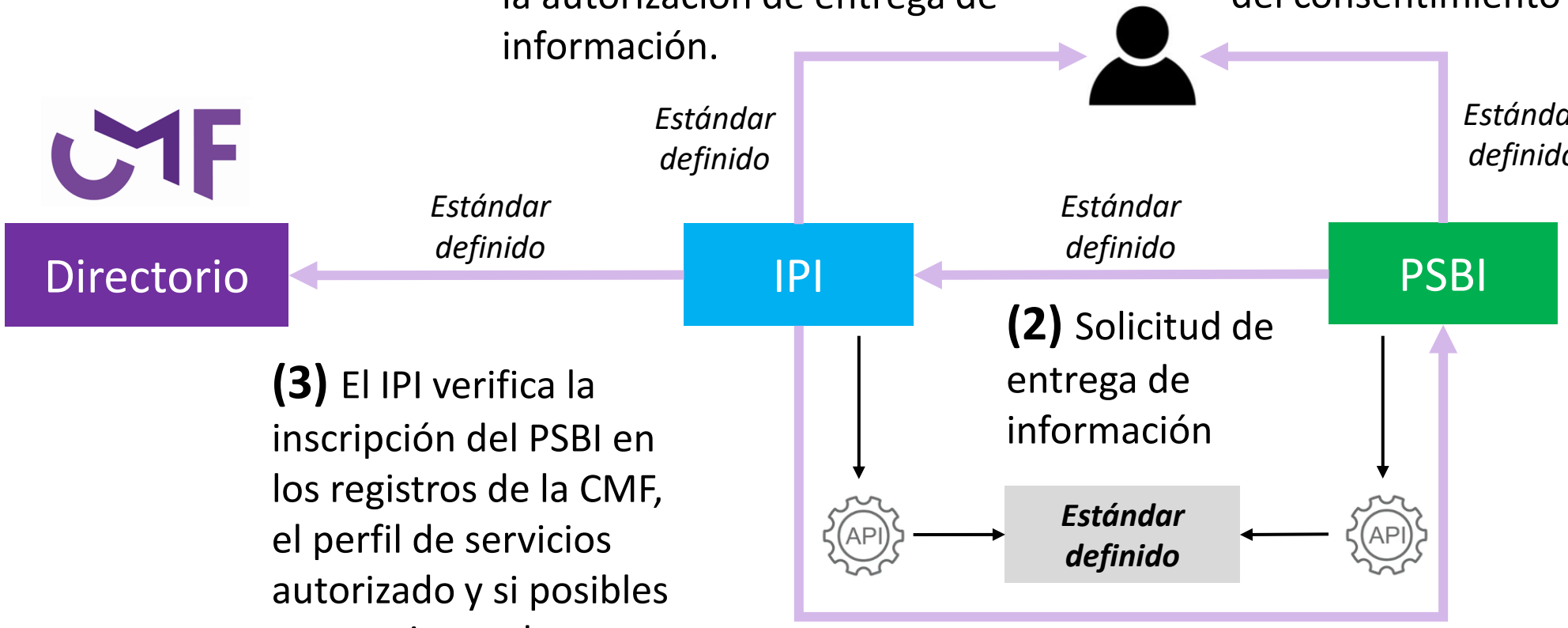
C. Intercambio de información (art 21)

- La entrega y el intercambio de información deberá efectuarse por medio **de una o más interfaces**, de acceso remoto y automatizado que deberán mantener disponible los participantes del Sistema de Finanzas Abiertas.
- Deben regularse (por parte de la CMF) aspectos de **estándares mínimos** de funcionamiento
- Debe existir un **mecanismo alternativo** ante inhabilidad de la interfaz

Proceso general establecido en la Ley

(4) El IPI autentica al cliente verifica la autorización de entrega de información.

(1) Autenticación y obtención del consentimiento del cliente



(2) Solicitud de entrega de información

(3) El IPI verifica la inscripción del PSBI en los registros de la CMF, el perfil de servicios autorizado y si posibles suspensiones de funcionamiento.

(5) En caso de validar exitosamente los pasos anteriores se entrega la información del cliente

2. Propuesta de estándares

Referencias utilizadas

Documentos técnicos

- Documentos del BIS
  - BIS (2018) Implications of fintech developments for banks and bank supervisors
  - BIS (2019) Report on open banking and application programming interfaces
  - BIS (2020) Enabling open finance through APIs
  - BIS (2022) API standards for data-sharing (account aggregator)
- Documento de propuestas del BM
  - BM (2022) Technical Note on Open Banking - Comparative Study on Regulatory Approaches

Experiencia internacional

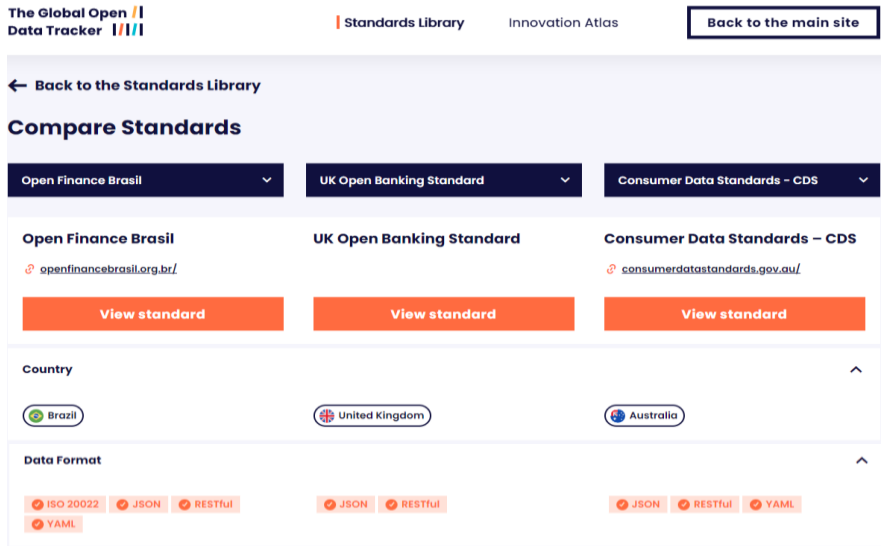
- UK, Brasil, Colombia, Otros casos...

Acuerdos de la industria

Reuniones bilaterales

- Mercado Pago Brasil, Chicago, otras.

Cuestionario interno IPIS



Solicitud de estándares

Estándar	Fuente legal
A. Estándares mínimos que deberán cumplir los medios de **autenticación** y **confirmación** de Clientes y en cuanto su inscripción en Registro CMF.	**Art 23.- Requisitos de consentimiento y autenticación**
B. Estándares de **verificación de inscripción** de la institución proveedora de información sobre la institución prestadora de servicios.	
D. Estándares de **seguridad de la información**	**Art 22.- Estándares de seguridad de información**
E. Estándares de **reporte de incidentes** de ciberseguridad	
C. Estándares mínimos de **medios de entrega** e **intercambio** de información	**Art 21.- Medios de entrega e intercambio de información**
F. Estándares al interrumpir el **acceso de información** y la realización de **nuevas órdenes** de pago.	**Art 24.- Responsabilidad de instituciones participantes en el SFA**
G. Estándares de **interoperabilidad**.	**Art 26.- Resguardos para garantizar interoperabilidad y trato no discriminatorio entre instituciones participantes**

TABLA

Estándares propuestos

A. Estándares mínimos que deberán cumplir los medios de autenticación y confirmación de Clientes.

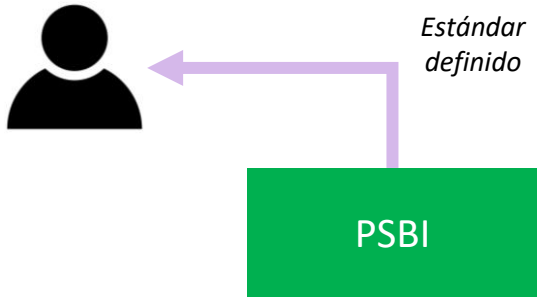
Autenticación del PSBI al cliente financiero

- Deberá estar en línea con la NCG de **consentimiento**.
- Corresponderá utilizar, en lo que corresponda, el estándar OAuth 2.0 para estos efectos.

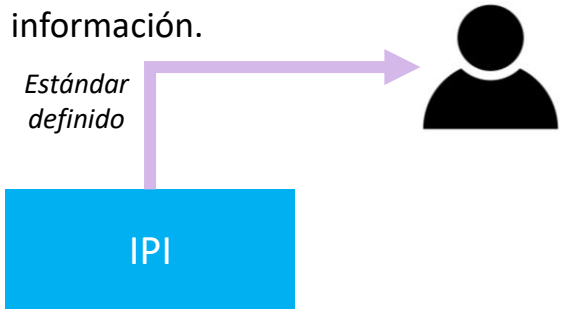
Autenticación del IPI al cliente financiero

- Se requerirá una **Autenticación Reforzada** del Cliente -SCA- para aquellos servicios del Sistema de Finanzas Abiertas que consideren información de depósitos y captaciones del cliente.
- Esta autenticación deberá considerar el uso de **dos o más elementos** categorizados como **conocimiento** (algo que sólo el usuario sabe), **posesión** (algo que sólo el usuario posee) e **inherencia** (algo que el usuario es) que son independientes, en el sentido de que el incumplimiento de uno de ellos no comprometer la confiabilidad de los demás, y está diseñado de tal manera que proteja la confidencialidad de los datos de autenticación.
- Los IPI deberán, una vez autenticado al PSBI, **confirmar con el cliente la prestación del servicio requerido**. Esta confirmación solo puede hacerse mediante **mecanismos compatibles** métodos ya disponibles que tengan las IPI para el acceso a sus canales electrónicos por parte de sus clientes.
- Este mecanismo deberá contar con al menos **dos factores de autenticación**.

(1) Autenticación y obtención del consentimiento del cliente



(4) El IPI autentica al cliente verifica la autorización de entrega de información.

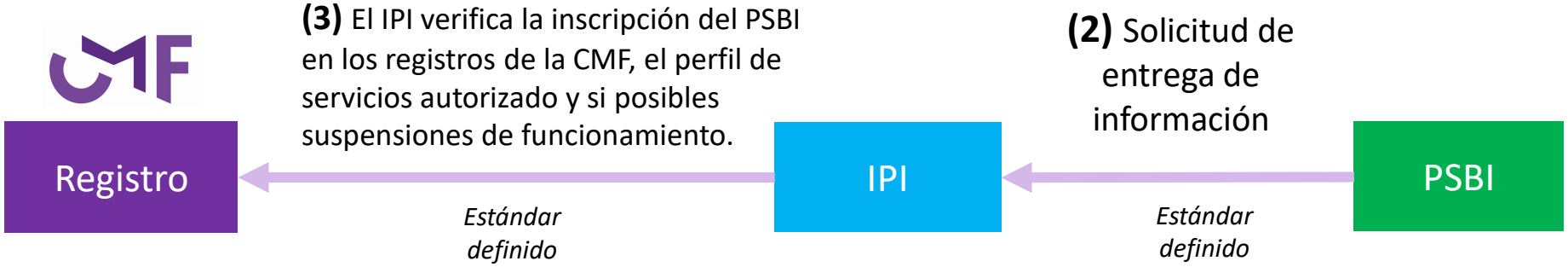


TABLA

Estándares propuestos

B. Estándares de verificación de inscripción de la institución proveedora de información sobre la institución prestadora de servicios

- Los **PSBI** deben entregar un **certificado digital** a las IPI al momento de iniciar una solicitud de información autorizada por un cliente donde se autentique su identidad.
- Este **certificado digital** deberá ser emitido por una la entidad acreditadora definida para tal efecto (ej. Firma Digital@Ministerio de Economía).
- Adicionalmente, el **IPI**/IPC deberán comparar y confirmar los permisos/roles indicados por el certificado versus los **perfiles autorizados en el directorio que llevara la Comisión para estos efectos**.
- Esta confirmación con el Directorio deberá ser realizada **de acuerdo con lo que establezca la normativa**, en función de la **solicitud que acompaña al certificado**.
- Deberá confirmarse periódicamente la vigencia del servicio de cada **PSBI**/PSIP



TABLA

Aplica a:

PSBI

IPI

Estándares propuestos

D. Estándares de seguridad de la información

Las entidades supervisadas deben **contar con políticas**, procedimientos y recursos técnicos y humanos para monitorear que las solicitudes de datos presentadas a través de API se realicen en condiciones de seguridad. Para el efecto, las entidades deberán contar con una norma de **gestión de riesgos** que contenga como ejemplo los siguientes elementos, en línea con el **modelo supervisor**:

i. Mantener los sistemas relacionados con los ecosistemas de finanzas abiertas y las API en una **red interna independiente** de los demás sistemas de información.

ii. **Monitorear** la información que circula a través de las API, para lo cual deben verificar y garantizar que las especificaciones de los campos de las solicitudes de datos de la API y sus respuestas se ajusten a las definiciones establecidas entre las entidades vigiladas y los terceros receptores de datos.

iii. Deben existir **resguardos y respaldos adecuados de la información** de acuerdo con la Ley General de Bancos y otras normativas aplicables. Abstenerse de exponer públicamente los repositorios de información y recursos a los que tienen acceso las APIs.

iv. **Mantener logs, por el término de 5 años**, por cada solicitud de datos realizada a través de las API, las cuales deben contener la información necesaria para determinar, como mínimo: el origen desde el cual se realizó la solicitud, el momento en que se realizó el consumo, el usuario que lo ejecutó, la información que circula por la API y el estado del proceso. En todo caso, según el nivel de sensibilidad o criticidad de la información esta se deberá enmascarar.

v. Que la información sea correctamente **eliminada una vez venzan los plazos máximos de información histórica permitidas en la Ley (cinco años).**

Se solicitará a las IPI y IPC ***sites*** **de contingencia** que permitan dar funcionamiento al sistema en caso de fallar las APIs debido a incidentes operacionales. Esto es independiente a la existencia de mecanismos alternativos fijados por norma ante inhabilidad de funcionamiento.

TABLA

Estándares propuestos

E. Estándares de reporte de incidentes de ciberseguridad

Tanto IPI y PSBI deberán reportar eventuales incidentes de ciberseguridad

Los incidentes de ciberseguridad deberán ser enviada a través de la **plataforma dispuesta especialmente** para estos efectos por esta Comisión, en cualquier horario, tanto en días hábiles como no hábiles, en el plazo máximo de 30 minutos luego de su ocurrencia.

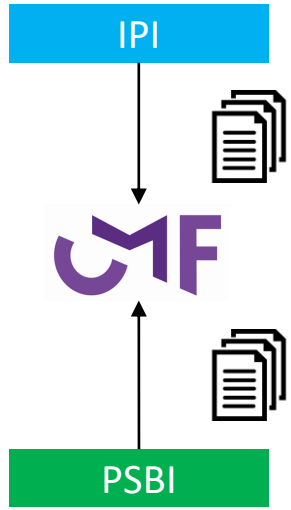
Para estos efectos, la entidad deberá **definir un funcionario encargado**, quien realizará los reportes y enviará la información según lo indicado en este numeral, y su designación y/o reemplazo deberá ser comunicado mediante carta a la CMF. Esta persona o quien la reemplace deberán tener un **nivel ejecutivo** y ser designados por la compañía tanto para este efecto, como para responder eventuales consultas por parte de este Servicio.
La información deberá ser reportada de acuerdo al siguiente **esquema**:

a. Al momento de inicio del incidente (*Número único identificador del incidente asignado por la CMF, Nombre de la entidad informante, Descripción del incidente, Fecha y hora de inicio del incidente, Causas posibles o identificadas, entre otras definidas en el documento de lineamientos*).

El no contar con toda la información de los campos mencionados previamente no debe ser impedimento para el envío de la comunicación dentro del plazo definido en este numeral. En los casos que este Servicio lo estime necesario, se podrá requerir a las compañías un plan de recuperación.

b. Al momento de cierre del incidente (*Número único identificador del incidente, Nombre de la entidad informante, Descripción del incidente, Causas identificadas, Fecha y hora de inicio del incidente, , entre otras definidas en el documento de lineamientos*).

Aplica a:



Art 20 Ley 21.000;
Ley de Fraudes

3. Propuesta de modelo de provisión de servicios

Propuesta de provisión externa de servicios

- La propuesta de estándares considera un **modelo descentralizado** para todos los procesos.

- Este modelo tendrá **estándares para cada etapa del ciclo de autenticación, verificación y compartición de información en el SFA.**

- No obstante, vemos factible para que los servicios previamente mencionados sean **tercerizados o externalizados**, siempre de **manera voluntaria**.

- Siempre el **responsable final es la entidad registrada**, cualquier externalización seria considerando los principios de la RAN 20-7 (adaptados).

Servicios necesarios en el SFA

(1) Directorio → 

- Listado de participantes con sus vigencias y roles respectivos > **Lugar oficial**.
- Información de accesos(Lectura, ejecución)

---

(2) Autenticación de los clientes y verificación del PSBI y certificaciones → **Externalización de servicios**

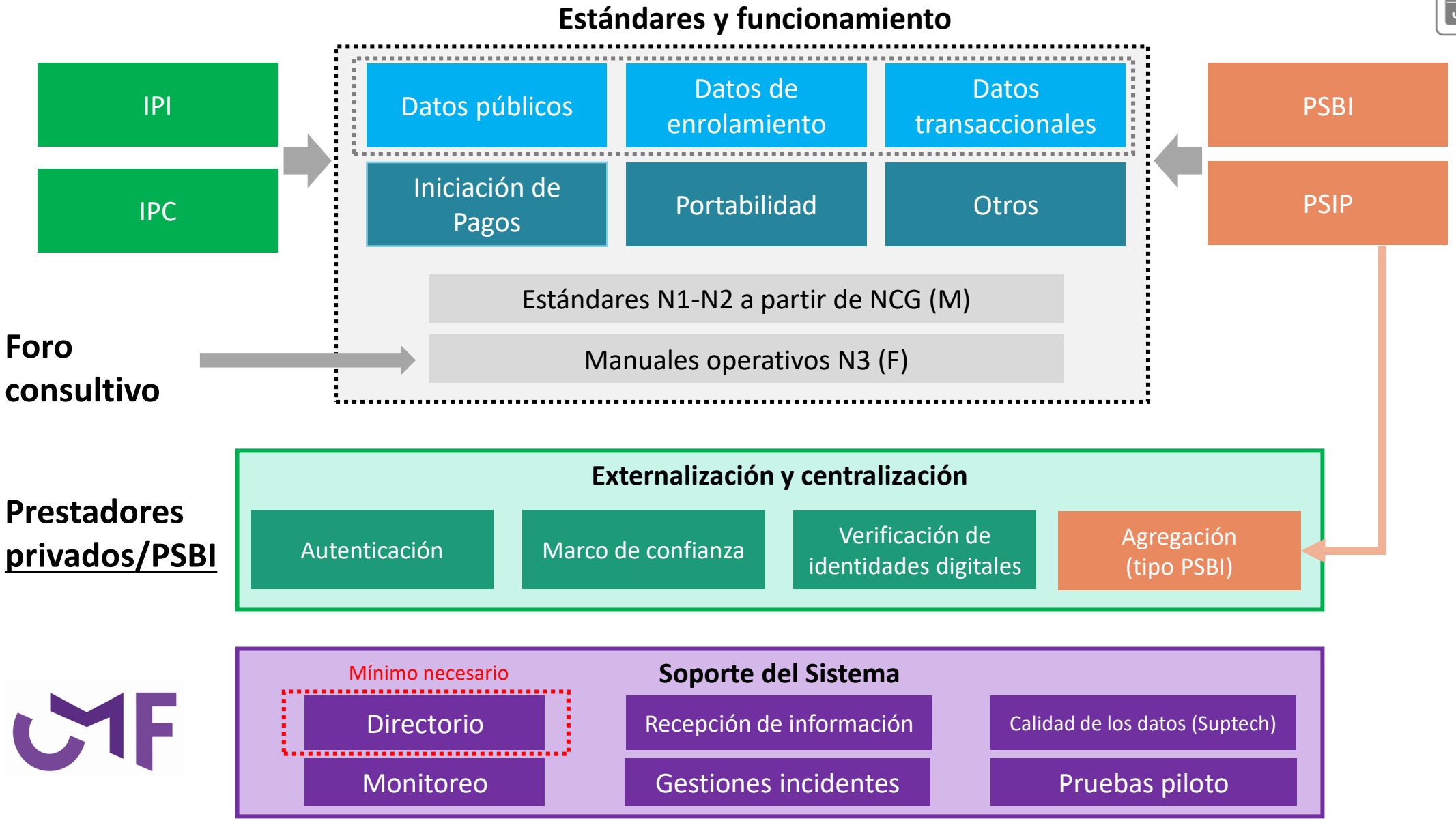
- El mercado puede proveer soluciones externas centralizadas o no que tengan el enfoque de un **Trust Framework o Certificación**.
- La entidad regulada es la responsable final para todos los efectos.
- Estas soluciones privadas son voluntarias, siempre el sistema tiene un formato descentralizado base donde operar.
- **Este podría ser el primer tema a tratar por parte del Foro Consultivo**

---

(3) Agregación de datos → **PSBI tipo Agregador**

- PSBI que tiene permisos para acceder a las APIS de los IPI
- No mantiene la información, solo la entrega
- Solo entrega información a los PSBI.
- Ganancias de la centralización de nodos de información (n de participantes elevado)

Modelo global del SFA



4. Preguntas para la mesa

Preguntas a discutir en las sesiones

Estándar	Preguntas
A. Estándares mínimos que deberán cumplir los medios de autenticación y confirmación de clientes y en cuanto su inscripción en registro CMF (art 23)	• ¿Qué otros estándares adicionales a los mencionados en este documento podrían aplicarse?
B. Estándares de verificación de inscripción de la institución proveedora de información sobre la institución prestadora de servicios (art 23)	• ¿Como debería efectuarse el certificado digital de las entidades? ¿De forma centralizada, descentralizada?
D. Estándares de seguridad de la información (art 22)	• ¿Qué nivel de diferenciación en las exigencias debería existir en función al tipo de participante y tipo de dato asociado?
E. Estándares de reporte de incidentes de ciberseguridad (art 22)	• ¿Podría existir algún otro mecanismo de centralización de estos eventos?
C. Estándares de medios de entrega e intercambio de información (art 21)	• Comentarios generales sobre la propuesta • ¿Qué mecanismos alternativos podrían considerarse en la norma, distintos de Webscrapping seguro, ante situaciones de indisponibilidad de servicios? • ¿Cuáles deberían ser los alcances normativos de un posible “agregador de datos”? • ¿Cómo debería resguardarse la externalización de servicios?
F. Estándares de interrumpir el acceso de información y la realización de nuevas órdenes de pago (art 24)	• ¿Qué otros eventos deberían constituir una interrupción de servicio?
G. Estándares de interoperabilidad (art 26)	• ¿Cómo debería resguardarse adicionalmente la interoperabilidad?

COMISIÓN PARA EL MERCADO FINANCIERO

FINTEC
Sistema de Finanzas Abiertas

Mesa Consultiva 2: Estándares técnicos del SFA

Ciberseguridad y Autenticación

Diciembre 2023