COMISIÓN PARA EL MERCADO FINANCIERO

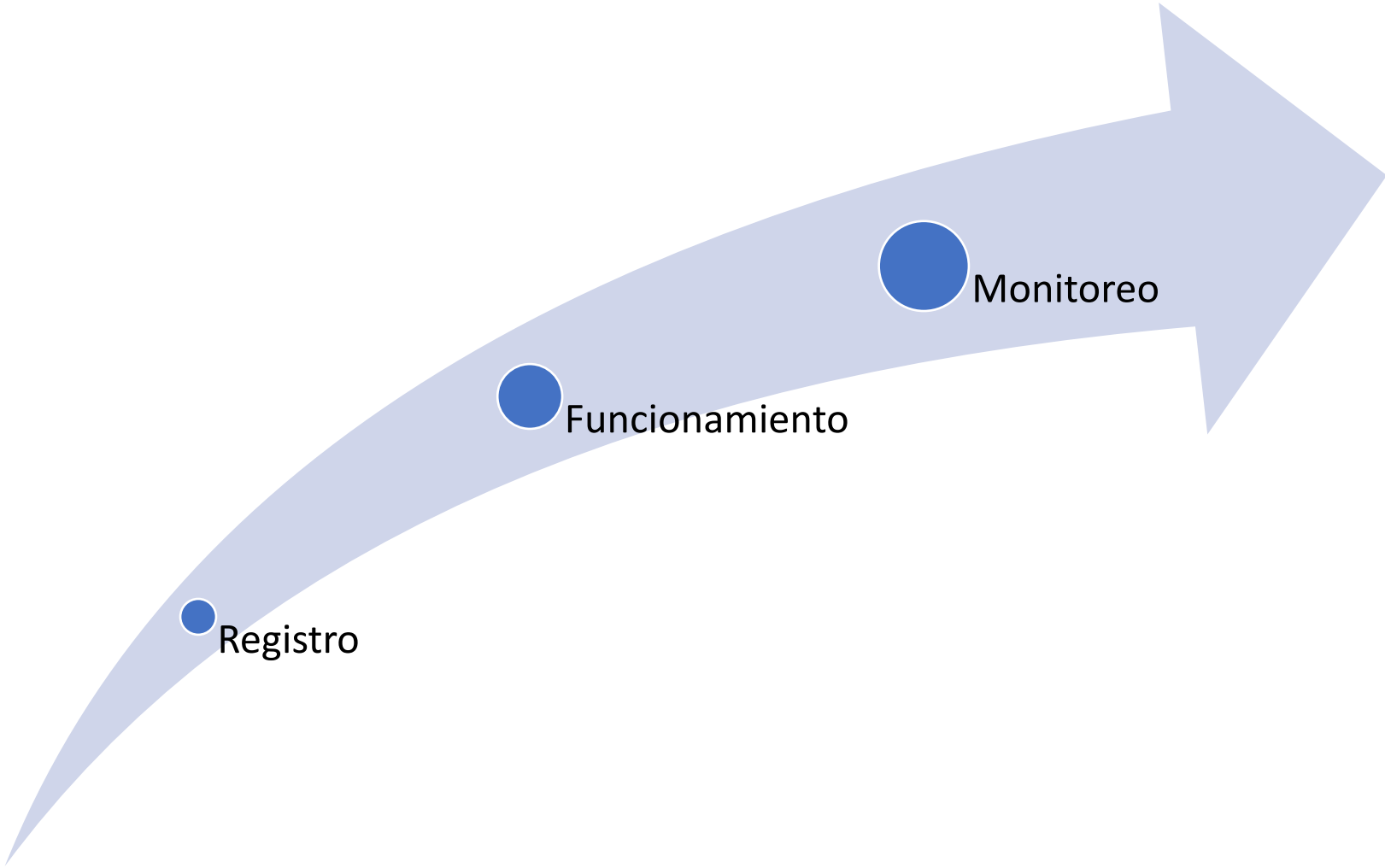
FINTEC
Sistema de Finanzas Abiertas

Mesa Consultiva: Modelo del SFA

Marzo 2024

Modelo

Abordaremos el estado del modelo del SFA según tres bloques temáticos:



Registro/nómina

Presentación de requisitos **obligatorios** de participación

IPI

Presentación de requisitos participación

PSBI

Licenciamiento

(2) CMF confirma recepción de los certificados correspondientes que a su vez provienen de instituciones reconocidas para emitir dichos certificados. Además de los formularios de consentimiento. Junto con políticas de gestión de riesgos en SFA (aspecto modular).

- A. Conformidad de Certificación
- B. Formulario de Consentimiento
- C. Política de gestión de riesgos en SFA

(3) Debe tener lo anterior aprobado presentar resultados de pruebas de funcionamiento

- D. Pruebas de Funcionamiento
- E. Pruebas de calidad de información

(4) La entidad envía el resultado de las pruebas de funcionamiento a la CMF que autorizaría finalmente el paso a etapa de producción.

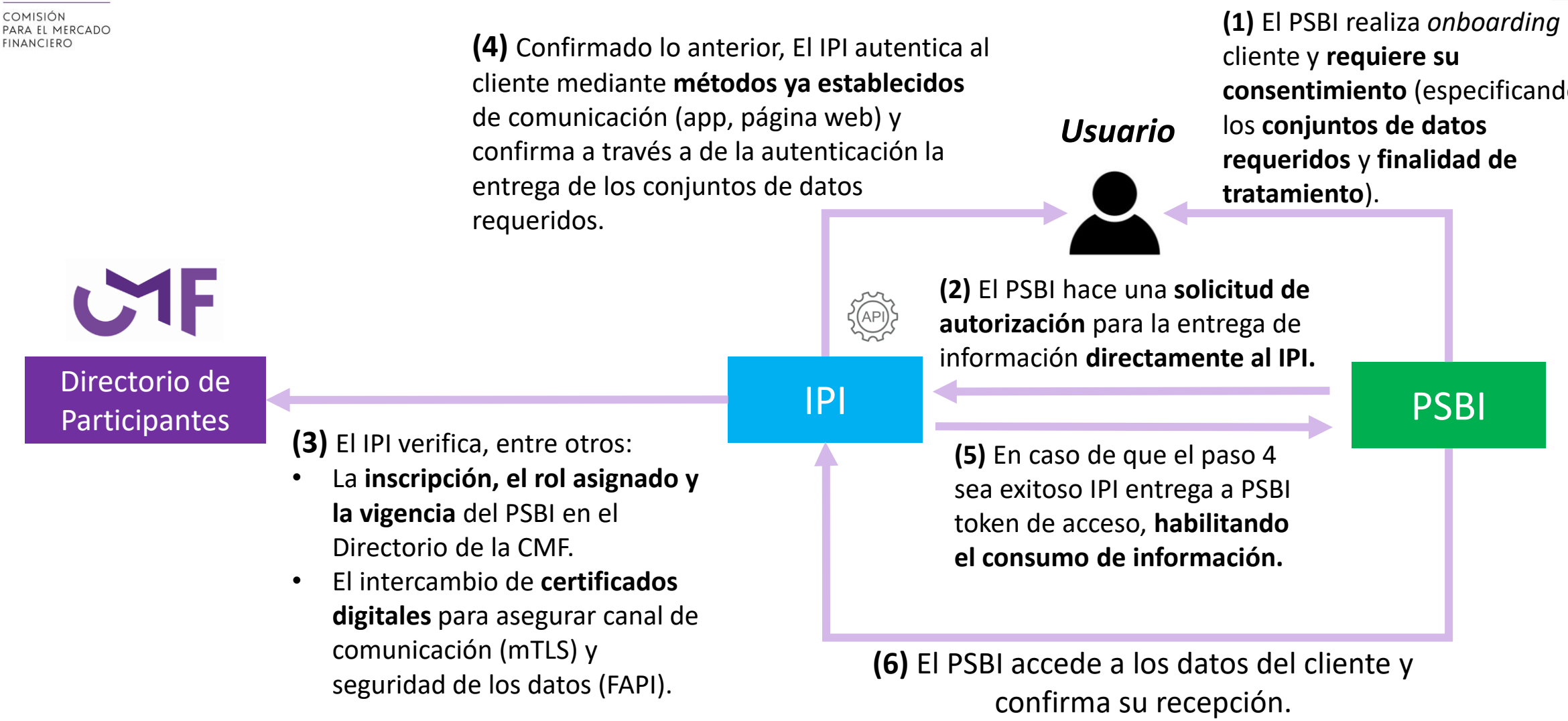
F. Autorización de participación

Zoom: Licenciamiento de Nóminas y Registros

Zoom: Elementos de Participación en SFA

Zoom: Estándares de seguridad de la información

Funcionamiento



Nota: En general aplica este diagrama al caso de IPC/PBIP, exceptuando algunos detalles. Para efectos de simplificación se omiten las interacciones propias del registro e interacción OAuth-OIDC

Zoom: Estándares de las APIS

El Directorio de la CMF

- Contiene **información de los participantes habilitados** para operar en el SFA, en aspectos tales como:
  1. Datos de identificación
  2. Ubicaciones de recursos de APIs (*endpoints*)
  3. Información sobre sus Certificados Digitales (Ej. Ubicación de descarga y *fingerprint* de clave pública)

- El Directorio operará bajo una configuración de alta disponibilidad y se distribuirá a través de un archivo descargable en formato estructurado.

- Instituciones **tendrán obligación de consulta periódica del Directorio y de mantener actualizada su información.**

- Acceso a Directorio es exclusivo de los participantes y estará basado autenticación mTLS

Los Certificados Digitales

- Los Certificados Digitales (CD) permiten a las instituciones realizar una serie de funciones en el SFA.
  - Identificarse
  - Autenticarse (entre ellas y con el Directorio)
  - Firmar y cifrar mensajes

- Los CD utilizan una infraestructura de claves públicas (PKI) para su funcionamiento, y son emitidos por una autoridad certificadora.

- Como autoridad certificadora para el SFA operarán los Prestadores de Servicios de Certificación (PSC) autorizados por el Ministerio de Economía para la emisión de **firma electrónica avanzada** (FEA), las que se emiten a personas naturales. Este certificado se generará bajo las condiciones establecidas por el SFA.

- Dentro de la información del certificado se incorporará por la PSC datos que los hagan aptos para el SFA, tales como:
  - Persona jurídica asociada (IPI/IPC o PSBI/PSIP)
  - Poderes y representante
  - Datos de permisos, roles y código de autorización CMF.

Monitoreo del sistema

A. Funcionamiento	B. Calidad de la información	C. Desarrollo de mercado y adopción
• Funcionamiento técnico del sistema (métricas de Uptime y rendimiento de la NCG). • Ocurrencia de incidentes operativos y de ciberseguridad. • Suspensiones temporales de participantes. • Gestión de consultas entre participantes	• Solicitar reportes de calidad de información a los participantes. • Reportería (archivos de información).	• Análisis de la evolución del sistema y casos de uso implementados. • Generación de métricas de adopción y uso. • Revisión y perfeccionamiento de variables. • Educación financiera.

Zoom: Estándares de reporte de incidentes de ciberseguridad

Temas para desarrollar en el Foro

Funcionamiento

- Especificaciones de las API
  → Ej.: Diccionarios técnicos y manuales de implementación
- Definición de campos para los Certificados Digitales.
  → Especificar los nuevos campos, asociados al SFA, que deben rellenarse. Ej.: Rol partipante, número de registro.
- Definiciones de perfil de seguridad de FAPI.
  → Debido a la existencia de diversos perfiles de seguridad dentro del estándar, asociados a variadas tecnologías de autenticación y registro, se deberán determinar cuáles serán aplicables en cada etapa.
- Definición de elementos técnicos del directorio y mensajería.
  → Forma de comunicación, mecanismo de descarga, condiciones de consulta y pruebas.
  → Mecanismos de mensajería entre participantes, indicando actualizaciones de información.

Registro y nóminas

- Definición de pruebas funcionales.
  → Características de las pruebas funcionales: tipo de ejercicio, criterios de éxito.
  → Características de las APIs de prueba de las IPI.

Pasos a seguir

1. Preparación normativa para consulta pública

2. Planificación de trabajo del Foro para los 18 meses, considerando los nuevos elementos del modelo y cronograma de entregables, incluyendo su comunicación al público.

3. Planificación de entregables normativos posteriores a dictación NCG de julio (ej. Diseño de archivos normativos).

COMISIÓN PARA EL MERCADO FINANCIERO

FINTEC
Sistema de Finanzas Abiertas

Mesa Consultiva: Modelo del SFA

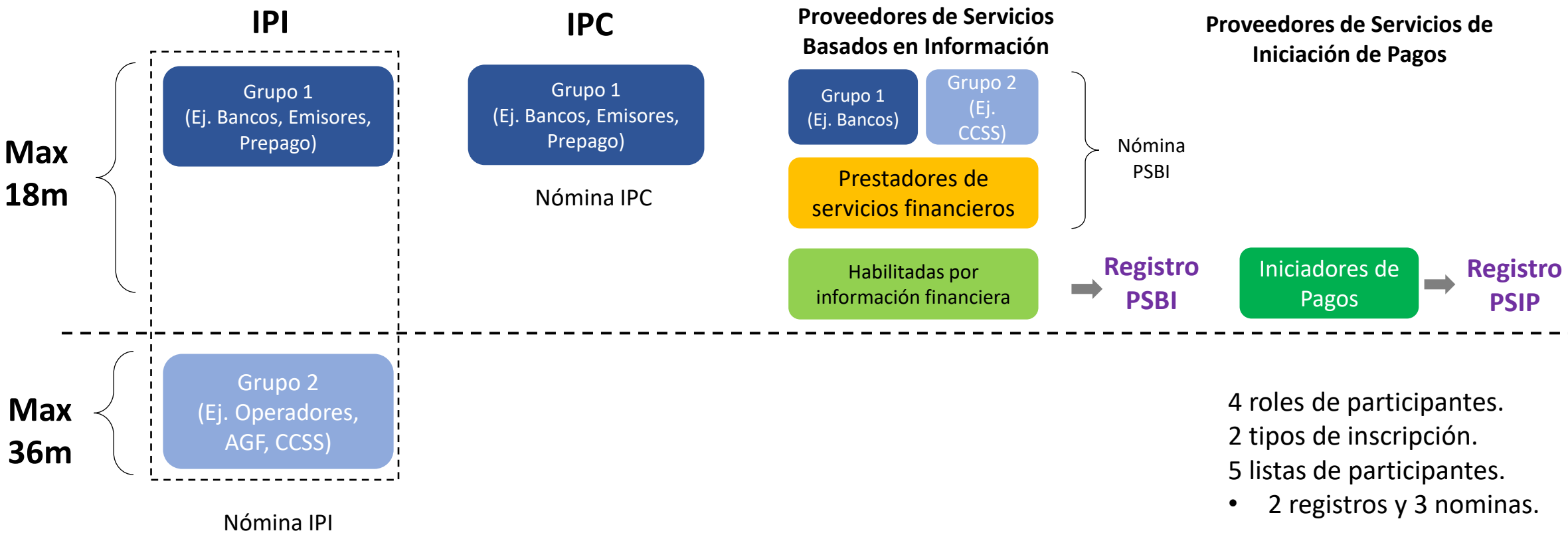
Marzo 2024

Licenciamiento de Nóminas y Registros

VOLVER

Nómina y registro:

- Tendremos una **nómina de participantes IPI y una participantes IPC**. Deberán cumplir con pruebas funcionales y todos los requisitos de seguridad aplicables.
- Para los PSBI tipo Habilitados por Información Financiera (entrantes) y los Iniciadores de pagos tendremos un **proceso registral** propiamente tal.
- Para las IPI y Prestadores de Servicios Financieros que voluntariamente quieran participar como PSBI tendremos una **nómina adicional, sin necesidad de registro**, pero sujeto al cumplimiento de aspectos técnicos requeridos.



4 roles de participantes.
2 tipos de inscripción.
5 listas de participantes.

- 2 registros y 3 nominas.

Elementos de Participación en SFA

VOLVER

A. **Evidencias de certificaciones (externas):**
   - **Pruebas de Perfiles de Seguridad:** Resultados de conformidad de estándar FAPI, según los perfiles de la institución, empleando la suite de conformidad de OpenID Foundation.

B. **Formulario de Consentimiento:** Verificación de que el formulario cumpla con los estándares asociados.

C. **Políticas de gestión de riesgo en relación a participación SFA**: Las instituciones deberán entregar el acápite, *addendum* o política (según el caso) donde se aborde la gestión de riesgos en el SFA, según los lineamientos contenidos en la NCG generada por la CMF, que en todo momento podría tener revisiones por parte del área de supervisión.

D. **Pruebas de funcionamiento**: Se realizan luego de la revisión satisfactoria de la etapa anterior. Se generan pruebas por parte de la IPI donde se evalúa si los PSBI se pueden conectar satisfactoriamente a las APIs.

E. **Pruebas de calidad de la información**

F. **Autorizaciones:** Una vez entregada satisfactoriamente las pruebas de funcionamiento el área de supervisión entregara la autorización para pasar a etapa de producción.

Estándares de seguridad de la información

VOLVER

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.

Estándares de las APIS

VOLVER

Medios de intercambio: APIs*

Disponibilidad y rendimiento

- Se propone que las API estén disponibles con un **tiempo de actividad mínimo del 99,5%** (medido por unidad de tiempo global a definir por la Comisión) y puedan **procesar transacciones en un máximo entre 0,8 a 1,5 segundos (considerando TTLB, tiempo de transmisión de último byte)**.
- Además, el proveedor de la API deberá tener medidas adecuadas para monitorear, rastrear e informar sobre la disponibilidad y el rendimiento de sus API.

Mecanismos alternativos ante indisponibilidad

- Las IPI deberán adoptar **mecanismos alternativos de comunicación** ante indisponibilidad de interfaces principales.

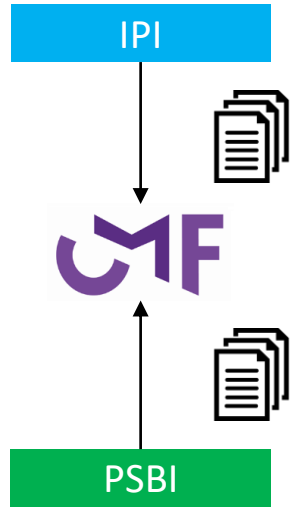
**Especificaciones de APIs: Mensajería (intercambio de información)*: JSON; *Especificación y diseño*: OpenAPI (v3).; *Arquitectura*: REST (RESTful); *Perfiles de seguridad*: FAPI 2.0 (modelo de atacante); *Protocolo de transporte*: mTLS 1.3; *Token de comunicación:* JWT; *Comunicación y diccionario*: ISO 20022.

Estándares de reporte de incidentes de ciberseguridad

VOLVER

Tanto IPI y PSBI deberán reportar eventuales incidentes de ciberseguridad

Aplica a:



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*).

Art 20 Ley 21.000;
Ley de Fraudes